WERKSMANS
ATTORNEYS

REGULATORY

Cybercrimes Act: South Africa Finally Joins The Big Boy Table

1 June 2021 *4 min read*

President Cyril Ramaphosa has just signed the Cybercrimes Bill, which seeks to bring South Africa's cybersecurity laws in line with the rest of the world, into law. This Bill which is now an Act of Parliament creates offences for and criminalises, amongst others, the disclosure of data messages which are harmful. Examples of such data messages include:

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

Not every crime is a cybercrime – The dichotomy of cyber-enabled crimes and cybercrimes.

Other offences include **cyber fraud**, forgery, extortion and theft of incorporeal property. The unlawful and intentional access of a computer system or computer data storage medium is also considered an offence along with the unlawful interception of, or interference with data.

This creates a broad ambit for the application of the Cybercrimes Act which defines "data" as electronic representations of information in any form. It is interesting to note that the Act does not define "cybercrime" but rather creates a number of offences such as those canvassed above.

There is no doubt that the Cybercrimes Act will be of particular importance to electronic communications service providers and financial institutes as it imposes obligations upon them to assist in the investigation of cybercrimes, for example by furnishing a court with certain particulars which may involve the handing over of data or even hardware on application. There is also a reporting duty on electronic communications service providers and financial institutions to report, without undue delay and where feasible, cyber offences within 72 hours of becoming aware of them. A failure to do so may lead to the imposition of a fine not exceeding R50 000.

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 fifteen years or to both a fine and such imprisonment as may be ordered in terms of the offence.

It is further interesting to note the impact this Act will have on businesses, especially considering its overlap with the Protection of Personal Information Act 4 of 2013 (POPIA), amongst other regulatory codes and pieces of legislation. POPIA, which deals with personal information, aims to give effect to the right to privacy by protecting persons against the unlawful processing of personal information. One of the conditions for lawful processing in terms of POPIA is security safeguards which prescribes that the integrity and confidentiality of personal information must be secured by a person in control of that information. This is prescribed by POPIA in order to prevent loss, damage or unauthorised access to or destruction of personal information. POPIA also creates a reporting duty on persons responsible for processing personal information whereby they must report any unlawful access to personal information (data breach) to the Information Regulator within a reasonable period of time.

In light of the above, companies should be cognisant of their practices especially in dealing with data or information. The value of data as an asset, the oil of the new economy, cannot be understated. To quote the CEO of Apple, Tim Cook:

> *We shouldn't ask our customers to make a trade-off between privacy and security. We need to offer them the best of both. Ultimately, protecting someone else's data protects all of us.*

Read more on the major cyber security risks to your business here.

by Ahmore Burger-Smidt, Director and Head of Data Privacy Practice and member of Competition Law Practice; and Nyiko Mathebula, Candidate Attorney.

Ahmore Burger-Smidt

Head of Regulatory

View Profile