The Cyberchrimes Act, Act 19 of 2020.

By Johanette Rheeder

Part of the COVID whirl and the "new-normal" is the rapid increase in digital and cyber activity, which also resulted in an increase in cyberbullying, cyberstalking and the hacking of Governments, companies, and individuals alike. With the grace period of compliance to the Personal Information Act of 2013, ending on 30 June 2021, President Cyril Ramaphosa has now approved and signed the Cybercrimes Act, Act 19 of 2020 into law on 26 May 2021.

THE PURPOSE OF THE ACT?

The purpose of the Act is to regulate the interception of information, data, hardware and software, to which the recipient is *not entitled to*, especially when the aim is to incite, inflict or cause another person or entity harm. It brings South Africa's cyber security legislation more in line with the rest of the world.

Most people and business use digital and cyber space on a daily basis and the *unlawful and intentional access* of a computer system or storage medium is now an offence in terms of the Act. The Act also creates offences for various cyber-crimes and disclosure of data messages which are harmful, through the provisions such as Sections 14 to 16 of the Act. Cyberbullying and the sharing of images of an intimate nature with someone other than the person who sent it, is declared to be an offence.

Data is specifically and widely defined in the Act as "electronic representations of information in any form". This definition creates a broad ambit covered by the Act.

In summary, the Act broadly aims at preventing cybercrimes such as cyber fraud, cyber forgery and altering, and extortion of people as well as the theft of incorporeal property.

WHO WILL BE AFFECTED?

Although the Act has a practical impact on the Government, natural and juristic persons when they process information via any digital or cyber medium (such as a computer or smartphone and internet users) the biggest impact will be on the Information Technology (**'IT'**) sector. Companies such as Electronic Communications Service Providers, Financial Institutions, Providers and/or vendors of IT software or hardware tools, will have to consider developing and implementing *policies and procedures* to ensure compliance with the provisions of the Act, as the Act requires the reporting, without delay, any cyber offence, within 72 hours of becoming aware of the offence. The failure to do so, may carry a fine not exceeding R 50 000.00. Conviction of an offence in terms of the Act includes fines and/or imprisonment for a period up to 15 years or both a fine and imprisonment.

Examples of data messages prohibited and covered by the Act are:

1. Messages on social media which incite violence or damage, for instance to incite damage to property of another;
2. The threat of violence against another or the threat of damage to property of another; and
3. Messages that contain images of another which are of intimate nature; and which are sent without the consent of the person.

PROTECTION OF PERSONAL INFORMATION ACT OF 2013 (POPIA)

The Act will clearly dovetail with POPIA, especially condition 7 which deals with the security safeguards that a responsible party must put in place, when the responsible party processes the personal information of a data subject. Processing under POPIA also must comply to the requirements of *lawfulness and reasonableness.* Therefore, apart from the organisational and technical measures that a responsible party must implement when processing personal information, processing which are falling foul of the Act, will also not pass the lawfulness test of POPIA.

Contact for training and further information at

Johanette@smartPrivacy.co.za; johanette@jrattorneys.co.za

Or visit us at www.jrattorneys.co.za