WERKSMANS
ATTORNEYS

REGULATORY

Your Actions in Cyberspace can Land You in Prison!

1 December 2021 *3 min read*

Cybercrimes Act, 19 of 2020

By proclamation in the *Gazette*, President Cyril Ramaphosa has fixed 1 December 2021 as the date on which certain sections of the Cybercrimes Act, 19 of 2020 ("**Cybercrimes Act**"/"**the Act**") come into operation. This means that the Act is now enforceable.

The following cybercrimes, amongst others, will as of 1 December 2021 be punishable by fine or imprisonment:

- unlawfully accessing a computer system or computer data storage medium; which allows the person to intercept data or interfere with data or the computer system;
- unlawfully intercepting data, for example acquiring, viewing, capturing or copying any data that is non public so as to make it available to a person other than the lawful owner or holder of the data;
- unlawfully interfering with a computer program, data program, or computer system, for example through deleting, altering, or damaging the computer program or system;
- committing cyber fraud such as unlawfully gaining access to a victim's personal identity, bank accounts, and other information to steal information or money;
- cyber forgery, for example where digital signatures are unlawfully replicated;
- cyber extortion, for example where a person uses another person's sensitive information and threatens to share it publicly unless a demand is met such as paying a ransom; and
- theft of incorporeal property such as shares in a company.

On 1 June 2021 we published an article discussing the criminalisation of certain offences which are described as malicious communications in the Cybercrimes Act, in particular –

- those which incite violence or damage to property (see our other article on this topic specifically);
- those which threaten persons with violence or damage to property; and
- those which contain an intimate image.

By definition, the above acts can be carried out by way of social media communication such as WhatsApp or any other social media platform. This is because WhatsApp or other social media communications fall within the definition of "data" and "data message" as set out in the Act.

What does this mean then?

South African citizens are now afforded the legislative means to protect themselves against a new form of criminal activity which previously escaped prosecution. Also, South Africa now joins the rest of the world in having enacted similar legislation to deal with online based offences.

Without a doubt, the Fourth Industrial Revolution cannot be pursued without a robust Cybercrimes Act in place.

Consequently, we now have an operational Cybercrimes Act to help us deal with increasingly sophisticated and novel forms of crimes committed via online means. What remains to be seen is how our law enforcement and court system will deal with and give effect to this powerful piece of legislation.

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



Ahmore Burger-Smidt

Head of Regulatory

View Profile