BIZCOMMUNITY

SA's Cybercrimes Act - will it change how you use the internet?

By Matthew Campbell

14 Dec 2021

With the arrival of the festive season comes new legislation, and a new weapon in the fight against cybercriminals. On 1 December, several elements of South Africa's new Cybercrimes Act came into effect, six months after president Cyril Ramaphosa first signed the bill into law.

Matthew Campbell | image supplied

The act is a major step forward in regulating online spaces. It gives law enforcement the teeth to go after criminals and helps victims of digital misconduct protect themselves and seek justice, which is good news as cybercrime is on the rise. According to the *2021 Norton Cyber Safety Insights Report*, 477 million people globally have been the victim of cybercrime in their lifetime, with 328.5 million taking place in the 12 months prior to May 2021 alone. South Africa has the third-highest number of cybercrime victims worldwide, and it's estimated that it costs us R2.2bn a year.

What does this new act mean for South African consumers and businesses online? Here's what you need to know about it, and how it may affect how you and others use the Internet.

What the Cybercrimes Act covers

Some elements of the Cybercrimes Act refer to state regulatory processes, but what's most relevant to ordinary Internet users is what it covers in terms of illegal digital and online activity. The act breaks this down into two categories: cybercrimes and malicious communications.

As defined by the act, cybercrimes include the unlawful access of computer systems and interception of data, unlawful acts in respect of software and hardware tools, and interference with data or computer programs. This also includes interference with computer data storage mediums or systems, but this section of the act has not yet come into effect.

Other cybercrimes include cyber fraud, forgery and uttering (the term used when something has been forged), extortion, aggravated offences, and theft of incorporeal property.

Acts of malicious communications include sending data messages that incite damage to property or violence, messages that threaten someone, and sharing messages with intimate images.

The act also lists the kind of orders that you can seek in order to protect yourself from the effect of malicious communications. These include orders to protect someone while criminal proceedings are being finalised, for service providers like social media companies to supply information to courts, and to finalise criminal proceedings.

For those of us who don't speak legalese?

For many, cybercrime takes the form of someone stealing or using your information for nefarious purposes. This can include identity theft, where scammers pose as you to access things such as your bank and mobile accounts. This is what the Cybercrimes Act covers, along with stealing and sharing passwords or access codes that are used on computers and other digital devices.

Also included in the act is a cyber forgery (when someone forges your digital signature), extortion (where your information is held by someone else for ransom), and the theft of incorporeal property (such as company shares or cryptocurrency). So, this should mean better protection for victims of cybercrime.

In the case of malicious communications, the act applies broadly and could cover something as simple as a WhatsApp message. This can include any message sent on a social media platform that incites or threatens someone with violence or damage to property, as well as messages that contain an intimate image that's shared without consent.

Notably, the Act came into effect just before experts identified social media as having played a role in the civil unrest South Africa experienced in July 2021.

Whether it's a post on your Facebook profile or a Telegram message, it's up to you to make sure that what you're sharing is appropriate and does not hurt anyone. If you're convicted of malicious communications related crimes, you can face fines or prison sentences of up to three years.

What the future holds

More work needs to be done as the rest of the act has yet to come into effect. As the government finalises more of the regulations – such as the obligations of service providers and building capacity for law enforcement to detect and prevent cybercrime – we should always be on the lookout and take precautions when posting and sharing content online and on social media platforms.

ABOUT MATTHEW CAMPBELL

Head of SME and FTTH at Seacom

- The death of third-party cookies: What businesses and marketers need to know - 10 Feb 2022
- SA's Cybercrimes Act - will it change how you use the internet? - 14 Dec 2021
- 5 steps to help SMEs succeed in digital transformation - 22 Jan 2021
- How FTTH powers economic growth, education and sustainability - 19 Jun 2020

View my profile and articles...