THE CYBERCRIMES BILL: RECENT AMENDMENTS

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Sadia Rizvi | October 10, 2020

Recently, the parliamentary committee on security and justice, adopted the Cybercrimes Bill ("**the Bill**") along with several other pieces of legislation. The Bill establishes and defines procedures in which cyber-related crimes can be investigated and creates various new offences for crimes committed on the internet. One of the most important aspects the Bill addresses is that it criminalises the distribution of harmful data messages and provides interim relief for an applicant. Cybercrime can be defined as a criminal activity that involves a computer and the internet.

With more South Africans working from home during the COVID-19 pandemic, the need for the Bill to be passed into law has become increasingly important. We have recently seen an increase the volume of cyber-attacks since the beginning of the COVID-19 pandemic. Thus, companies and businesses working remotely need to ensure secure working practices by keeping their organisation protected from attackers exploiting the work-from-home situation.

The pandemic has forced us to find new ways of working in order to meet consumer demands. Criminals have concomitantly adapted their tactics to exploit the situation that employers find themselves in. Many businesses operating without security protections such as firewalls and VPNs are even more susceptible to cyberattacks, and this can cause exponential damage to the company and its reputation. South Africans need to be more cognisant of hackers using malware and ransomware to breach the security of their organisation and gain access to confidential information.

The delay in the passing of the Bill can largely be attributed to the fact that many academics viewed it as a potential threat to internet freedom as some of the provisions grant far-reaching powers to State Security structures. After many months of comments and reworking, the drafters of the Bill stripped out many sections which gave, arguably excessive, power to State Security structures and offered key improvements which addressed many of the concerns relating to the rights of privacy and freedom of expression.

The Bill, in its most recent form, criminalises the distribution of harmful data messages, provides for

interim protection orders, and regulates the powers to investigate cybercrimes and imposes obligations on them. When in operation, the Bill makes it an offence to unlawfully and intentionally access data, a computer program, a computer data storage medium and a computer system as well as to unlawfully intercept data and be in possession of such data. The Bill also deals with the unlawful interference with data or a computer program, as well as cyberfraud, forgery, uttering and extortion among various other offences. The Bill also creates a new offence, where it would be unlawful for anyone to come into possession of a password or access code without prior authorisation. One of the most notable features of the new Bill is that it criminalises revenge pornography and offers protection to victims of revenge pornography. A person convicted of committing such an act can face up to three years of imprisonment and/or a fine.

Once in operation, the police minister must, after public consultations, provide for standard operating procedures to be followed by the South African Police Services (SAPS) in the investigation of an offence or suspected offence. The Bill also creates an obligation on an electronic communications service provider or financial institution that is aware of or becomes aware that its computer system is involved in the commission of certain offences must without undue delay, not later than 72 hours after having become aware of the offence, report the offences to the SAPS and preserve any information which may be of assistance to the law enforcement agencies in investigating the offence. In the event of non-compliance with the provisions of the Cybercrimes Bill, the penalties that may be imposed consists of a fine, imprisonment, or both. The Bill does not specify the amount of a fine imposed, but an offender could spend between one and fifteen years in prison, depending on the offence committed.

The major issue facing the parliamentary committee is that the Cybercrimes Bill, in its current form, allows authorities to search ordinary citizens' computers without a warrant. The Bill, if passed in law, will be the first in South Africa to be non-binary legislation, and it will also repeal certain sections of the Electronic Communications and Transactions Act that deal with cybercrime. There are also further concerns amongst academics, in the SAPS' ability to implement the sections of the Bill for which they are responsible. It is known that despite South Africa having some of the most progressive criminal law legislation in the world, the implementation of it is deeply lacking.

Although the Bill has all the right intentions, it still remains to be seen whether it is enough to deter cyber criminals and prompt organisations to address cybersecurity challenges.