IN PLAIN ENGLISH: THE CYBERCRIMES ACT IN A NUTSHELL

Category: Commercial Law,Media and OTT,Privacy Law, Infosec, and POPIA,Technology Law
written by Kelly Lekaise | January 28, 2022

On 1 December 2021, certain parts of the Cybercrimes Act, 19 of 2020 came into full effect. The Cybercrimes Act seeks to address the rise of crimes that are now committed online due to the use of the internet and various emerging technologies. With the move from physical offices to virtual offices as a result of COVID-19, there has been an increase in dependence on computers for work and school. This created a breeding ground for cybercrimes as more and more people communicate virtually. This piece of legislation has a far-reaching target, from big corporate businessmen to a grade 7 learner in a village experiencing bullying on a social network. This article will simplify the Cybercrimes Act with a focus on the sections dealing with cybercrimes which commenced on 1 December 2021.

Chapter 2 of the Cybercrimes Act

This chapter introduces the crimes of hacking, unlawful interception of data, cyber fraud, forgery and uttering, ransomware, and malicious communication.

Unlawful access((Section 2 of the Cybercrimes Act.))

The crime of unlawful access, or “hacking” as it is most commonly called, refers to when a person unlawfully and intentionally accesses computers, smart phones, and entire network systems. Hacking is usually carried out by some form of software or hardware tool. An example of hacking might be when a person, without the permission of their spouse, link their device to their spouse’s WhatsApp so as to view and read incoming messages.

Unlawful interception of data((Section 3 of the Cybercrimes Act.))

This section prohibits a person from unlawfully intercepting or preventing any data communications

from reaching its intended recipient. This includes acquiring, viewing or copying data that is not of a public nature through the use of software or hardware tools. An example of this is where one uses a software or hardware tool to intercept any emails that were meant to reach another, to now reach the offender.

Cyber fraud((Section 8 of the Cybercrimes Act.))

The common law definition of fraud is where a person unlawfully and intentionally makes misrepresentations which causes another to suffer actual harm or could potentially suffer harm. Cyber fraud, however, requires that the fraud must be carried out using a computer to delete, alter, or damage any computer data in order to obtain a certain advantage. An example of this can be where someone changes your banking details to his own in order to get your money. Another real-life example of this is a law firm, based in Pretoria, received an email from the client's email address, supplying them with "new bank details" to make several payments of money that was held for the client by the firm into the new banking account. The law firm later found out that a cybercriminal had hacked the client's emails, changed the client's banking details and got paid instead of the client. The court held that had the firm verified the clients banking details, the fraud would not have happened.

Cyber forgery and uttering((Section 9 of the Cybercrimes Act.))

Cyber forgery is where one party creates false information with the intention to fraud another person while cyber uttering is presenting false information or a false computer program with the intention of causing actual or potential harm to another. An example of this is when someone alters or creates an Identity Document in a digital form and passes it as authentic in order to obtain some advantage.

Cyber extortion((Section 10 of the Cybercrimes Act.))

Cyber extortion, more often referred to as "ransomware", is when a person uses software to prevent the user from accessing his or her computer systems until a ransom has been paid. An example of this is the 2019 ransomware attack on the City of Johannesburg.

Malicious communication((Section 13 of the Cybercrimes Act.))

This refers to instances where someone distributes or shares data messages (this can be on social media platforms) with the intention to incite damage to the property of another or actual violence to another. In June 2021, civil unrest unfolded after the arrest of the former president Jacob Zuma causing illegal protesting and burning and destruction of property. The Minister of State Security, Minister Ayanda Dlodlo stated that an investigation was underway into certain people who were inciting the protests on social media. Such people included prominent politicians who posted Twitter messages calling on people to "let it burn". If the Cybercrimes Act had been in full operation, these messages which incited violence could have been criminalised. In addition to this, malicious communication also includes cyber bulling, cyber stalking, or revenge pornography.

Penalties

A person will also be found guilty of the above crimes if he or she attempted, conspired with other people to commit the above crimes, and assisted with the above-mentioned cybercrimes. An offender can face a sentence that ranges from 1 to 15 years imprisonment and/or a fine. Where a person commits cyber fraud, cyber forgery and cyber uttering, the Act provides that the court will have a discretion to impose a sentence it considers to be appropriate under section 276 of the Criminal Procedure Act 51 of 1977.

Conclusion

As can be seen from the above crimes, the Cybercrimes Act covers a broad range of cybercrimes. Although it creates specific crimes, it is also quite broad and that might lead to impracticalities. In terms of this act, you could face jail time for linking your WhatsApp messages to that of a cheating spouse to monitor his or her messages if he or she does not know about it. On the other hand, victims of revenge porn and cyberbullying can finally get assistance from the state.

Contact us for more good, clear, precise advice.