DISSECTING THE CYBERCRIMES ACT – THE CRIME OF HACKING (PART 1)

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Melody Musoni | January 1, 2021



INTRODUCTION

If we put aside the misery around Covid-19 for a moment, we can notice that a lot of exciting developments have taken place and are still taking place in South Africa's legislative landscape. We are 5 months away from POPIA[1] coming into full effect. By 1 July of this year, both private and public companies, organisations and institutions will have to follow the requirements of POPIA when processing personal data. That is not all. The long-awaited Cybercrimes Act[2] is expected to be signed into law by the President any day this month. This has been after a long-winded process which dates back to the inception of the first bill in 2015. The Department of Home Affairs has also published a draft policy on digital identity.[3] The policy will promote e-government initiatives as it allows for interoperability of different government departments' identity management systems. The policy also emphasises on lawful processing of personal information as well as efforts to curb cybercrimes like identity theft. This contribution will be part of a series of commentary on the offences under the Cybercrimes Act. It discusses the offence of hacking or unauthorised access. Part 2 of the contribution will look at the offence of hacking as an unlawful interception of data.

WHAT IS HACKING?

When the term hacking was originally introduced, it referred to the technique that was used by IT personnel who were always on the lookout to find computer shortcuts that made computing tasks quicker.[4] Hacking is defined as gaining unauthorised access to a computer system, program or data.[5] Hackers sometimes crack into government or business networks for profit, for sport or for bragging rights.[6] Earlier in 2020, millions of Nedbank customers' data was compromised when a cybercriminal infiltrated Nedbank's service provider's system.[7] POPIA provides punitive and remedial sanctions to responsible parties in cases of unlawful processing of personal data. POPIA is targeted at public and private bodies who determine the purpose of processing of personal information. It could not be relied on when individuals in their personal capacity unlawfully access and process personal information of others. The hacking provisions under the Cybercrimes Act are quite extensive and broad. They cover different scenarios where there is unlawful access and processing of any data, including personal data. The Act defines a person as either a natural person or juristic person. This means that the law applies to instances where juristic persons unlawfully access data of either natural persons or of other juristic persons. The Act also applies to cases where individuals are unlawfully accessing data of other individuals or of juristic persons.

Hacking is a major concern for businesses. Most hackers either possess or use hacking tools to unlawfully access into computer systems and networks without authorisation. Botnets are an example of tools used by hackers. Botnets are pieces of software that run automatically to commandeer massive numbers of computers to allow cybercriminals to conduct large scale malicious activity including spreading spam, stealing log-in credentials and personal information or distributing malware to others.[8] When cybercriminals use botnets, they widen their attack base, and the proceeds are likely higher than when employing traditional hacking techniques.

WHAT DOES THE CYBERCRIMES ACT SAY ABOUT HACKING?

Section 2 (1) of the Cybercrimes Act provides that any person who unlawfully and intentionally accesses a computer system or computer data storage medium is guilty of an offence. Access to data, computer program and computer storage medium is broadly defined under the Cybercrimes Act. When entities engage in corporate espionage and hack into their competitor's computers, they are committing a crime under the Act. Website defacement is another example of unlawful access where a person accesses a website, modifies or deletes its contents or manipulate its software programs. Unlawful access could also mean downloading a file to a USB drive, a computer or onto OneDrive or Google Drive or emailing the file to someone else.[9]

It is also an offence for a person to unlawfully and intentionally acquire, possess, provide to another person or use a password, an access code or similar data or device for purposes of contravening the provisions of the Cybercrimes Act.[10] Password, access code or similar data or device includes any of the following –

- a secret code or pin;
- an image;
- a security token;
- an access card;
- any device;
- biometric data; or

- a word or a string of characters or numbers

used for financial transactions or user authentication in order to access or use data, a computer program, a computer data storage medium or a computer system.[11]

Making available software, hardware or computer access codes with the intent that it be used for the purpose of committing illegal access of data constitutes a cybercrime. This would mean that software developers of malware like trojan horses or hacking software should be careful as they can be held liable. The same also applies to their distributors, importers and other parties.[12] Our courts have successfully prosecuted hackers in the past by relying on the ECT Act.[13] In *S v Myeni*[14], the criminals wrongfully and unlawfully used a software called Winspy to overcome security measures designed to protect computer names and passwords of accounting personnel at Koukamma Municipality. The court found the accused guilty of the crime of hacking in terms of section 86 (1) and 86 (4) of the ECT Act. The cybercrime provisions of the ECT Act will be replaced by the Cybercrimes Act as it provides more robust provisions addressing cybercrime.

When one considers the provisions of the Cybercrimes Act, one can note that the law applies in scenarios that people would generally not consider as criminal conduct. When a person hacks into their neighbour's Wi-Fi and use the Wi-Fi without permission, that is a crime. This would also include using someone else's log-in credentials without permission to access certain services like Netflix. Common examples include snooping on another person's communications and going through their social media 'DMs'[15] or emails. Our courts have in the past acknowledged that hacking into someone's social media accounts like Facebook communications amount to criminal conduct. ***[16]***

WHAT ARE THE PENALTIES?

Any person who unlawfully and intentionally accesses data, computer program or computer storage of another person, is guilty of an offence. The penalties for such an offence are either a fine or going to prison for as long as 5 years.[17] In some instances, the magistrate may impose a sentence of both imprisonment and fine.

CONCLUSION

The Cybercrimes Act is a welcome development in our law. Not only does it criminalise different types of cybercrimes, but it is also a powerful tool for data protection. The Act criminalises the unlawful and intentional access of data, computer storage medium and computer systems. Businesses which unlawfully process personal data can now be penalised in terms of both POPIA and the Cybercrimes Act. Unlike POPIA which only works between a responsible party and data subject relationship, the Cybercrimes Act can be used in different contexts. Businesses can rely on the Act and report other businesses which may be unlawfully accessing their confidential information or manipulating their computer systems. The Act also protects individuals from having their data unlawfully accessed by other individuals or by juristic persons.

[1] The Protection of Personal Information Act, 4 of 2013.

[2] Cybercrimes Act, 19 of 2020.

[3] Draft Official Identity Management Policy Government Gazette 44048 published on 31 December 2020.

[4] The first and original computer hackers emerged in 1960 at the Massachusetts Institute of

Technology (MIT). John Baiden ‘Cybercrimes’ 1 at 4.

[5] Ibid.

[6] Ibid.

[7] https://www.zdnet.com/article/nedbank-says-1-7-million-customers-impacted-by-breach-at-third-party-provider/

[8] John Baiden opcit note 4.

[9] Section 2 (2) (b) Cybercrimes Act.

[10] Section 7 (1) Cybercrimes Act.

[11] Section 7(3) Cybercrimes Act.

[12] Paul Przemyslaw Polanski Chapter 10 The internationalization of internet law at 204.

[13] The Electronic Communications and Transactions Act 25 of 2002.

[14] *S v Myeni* 2019 (1) SACR 360 (ECG).

[15] Direct Messages. https://www.lifewire.com/slide-into-dms-meaning-3485730#:~:text=DMs%20means%20direct%20messages.,as%20a%20DM%20for%20short.

[16] *Harvey v Niland & Others* 2016 (2) SA 436 (ECG).

[17] Section 19 of the Cybercrimes Act.