The extent of the Cybercrimes Act 19 of 2020 in addressing and combatting cybercrime

R Pyper

orcid.org 0000-0001-5374-2268

Dissertation accepted in fulfilment of the requirements for the degree *Master of Laws in Criminal and Procedure Law* at the North-West University

Supervisor: Prof W Erlank

Graduation: July 2024

ACKNOWLEDGEMENTS

I would like to extend my gratitude to the NWU Potchefstroom Campus and Faculty of Law for making this dissertation a possibility. My heartfelt appreciation goes out to both my parents, Johan and Magriet for their consistent and steadfast support. I could not have done it without you. And lasty, special thanks to my brilliant supervisor. Thank you for all your unwavering guidance and academic insight throughout the process of writing this dissertation. I would like to dedicate this dissertation to my Lord and Saviour, Jesus Christ. (Job 22:28 – "You will decide on a matter, and it will be established for you, and light will shine on your ways.").

ABSTRACT

Considering the immense impact and effect of the 4th Industrial Revolution on modern technology, is it no surprise to remark that new and advanced challenges are faced daily by various countries, information and communication technologies, and internet service providers. These challenges have established an international movement between various countries and their governments regarding cybercrime and cyber-attacks. Although cybercrime is still considered a new crime, the crime appears to be evolving at a rapid pace and countries seem to neglect the procedure of adopting or developing cybercrime frameworks to appropriately address and combat the crime. South Africa is the first African country to develop and implement the *Cybercrimes Act* 19 of 2020. The development and implementation procedures of the *Cybercrimes Act* was considered quite complex and extensive especially regarding the impact and effect of the previous pieces of cybercrime legislation in South Africa. A comprehensive overview of the position of cybercrime in South Africa will be discussed.

Keywords: Cybercrime; Cyber-attacks; Cybersecurity; Cyberspace; Online environment; *Cybercrimes Act* 19 of 2020

LIST OF ABBREVIATIONS

4IR	Fourth Industrial Revolution
AC:AJCV	Acta Criminologica: African Journal of Criminology & Victimology
AJIC	African Journal of Information and Communication
Amendment Bill	Electronic Communications and Transactions Amendment Bill, 2012
AU Convention	African Union Convention on Cyber Security and Personal Data Protection
Budapest Convention	Council of Europe, Convention on Cybercrime, 23 November 2001
CC	Constitutional Court
CILSA	Comparative and International Law Journal of Southern Africa
Commonwealth Law Bulletin	The Journal of Commonwealth Law
Constitution	Constitutional of the Republic of South Africa, 1996
CPA	Criminal Procedure Act 51 of 1977
CPEA	Civil Proceedings Evidence Act 25 of 1965
CRIMSA	Criminological Society of Africa
CSIR	Council for Scientific and Industrial Research
CSIRT	National Computer Security Incident Response Team
Cybercrimes Act	Cybercrimes Act 19 of 2020

Cybercrimes Bill	Cybercrimes and Cybersecurity Bill [B – 2015]
DA	Democratic Alliance
DCPI/Hawks	Directorate for Priority Crime Investigation
DDoS	Distributed denial-of-service
DFL	Digital Forensic Laboratory
ECTA	Electronic Communications and Transactions Act 25 of 2002
ECSPs	Electronic Communications Service Providers
ECU	Electronic Crime Unit
Email	Electronic mail
FIC	Financial Intelligence Centre
FPA	Films and Publications Act 65 of 1996
FPAA	Films and Publications Amendment Act 11 of 2019
FPB	Film and Publications Board
GB	Gigabyte
GDPR	European Union's General Data Protection Regulation
GG	Government Gazette
GN	Government Notice
ICTs	Information and Communication Technologies
ID	Identification

IJETTCS	International Journal of Emerging Trends & Technology in Computer Science
IJCS	International Journal of Communication Systems
IJLPA	International Journal of Law and Public Administration
IJPAM	International Journal of Pure and Applied Mathematics
InSITE 2004: Informing Science + IT Education	Informing Science Institute
Interpol	International Criminal Police Organisation
IOSR	International Organisation of Scientific Research
ISPs	Internet service providers
ISSN	International Standard Serial Number
JAPSS	Journal of Academic Perspective on Social Studies
JCPS	Justice, Crime Prevention and Security Cluster
JOC	Journal of Organic Chemistry
Juta's Business Law	Sabinet African Journals
LSSA	Law Society of South Africa
MOU	Memorandum of understanding
NASA	National Aeronautics and Space Administration
NCB	National Central Bureau
NCC	National Communications Centre

NCPF	National Cybersecurity Policy Framework
NPA	National Prosecuting Authority
OIC	Office for Interception Centres
PER/PELJ	Potchefstroom Elektroniese Regsjoernaal/ Potchefstroom Electronic Law Journal
Police Act	Police Service Act 68 of 1995
POPIA	Protection of Personal Information Act 4 of 2013
PSLR	Pretoria Student Law Review
Regulator	Information Regulator
Republic	Republic of South Africa
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002
RICA Amendment Bill	Regulation of Interception of Communications and Provision of Communication-Related Information Amendment Bill [B 9B 2006]
SABRIC	South African Banks Risk Information Centre
SACJ	South African Computer Journal
SACSAA	South African Cyber Security Academic Alliance
SAHRC	South African Human Rights Commission
SAJIM	South African Journal of Information Management
SALRC	South African Law Commission

SAPS	South African Police Service
SCA	Supreme Court of Appeal
SIM-card	Subscriber Identity Module-card
SIU	Special Investigating Unit
SMEs	Small and medium-sized enterprises
SSA	State Security Agency
TB	Terabyte
The Bill	Protection of Personal Information Bill [B9]
The Regulations	Films and Publications Amendment Regulations, 2022
UGC	User Generated Content
UK	United Kingdom
WHO	World Health Organisation
Wi-Fi	Wireless Fidelity
YILC	Yearbook of the International Law Commission
ZAR	South African Rand

TABLE OF CONTENTS

Chapter 1 Introduction to Cybercrime in South Africa

1 Problem statement

Cybercrime first became evident in the early 1970's when back then,[1] cybercrime was referred to as "hacking" performed by computer criminals called "phreakers" acting, performing, and engaging in the online environment with the primary objective to commit a cybercrime,[2] for example, online extortion.[3] Since the 1970's,[4] cybercrime continued to increase significantly until the present day, where cybercrime is effortlessly committed because of the lack of a safe and secure online environment.[5] Another reason to consider the increase in cybercrime is that computer criminals (also called cyber-criminals or cyber-attackers) choose to remain completely anonymous while performing or committing a cybercrime by the use of advanced protection software.[6]

Taking into consideration the nature of modern society, in which people constantly communicate, connect and interact by sharing information, files, or data on information and communication technologies (ICTs),[7] cybercrime and online crimes[8] quickly became a troublesome international challenge to various countries and their national cybercrime legislation over the last few years.[9] Due to the increased rate of cybercrime,[10] the nature and objective of national ICTs evolved significantly since the social, economic, and political aspects of a country appear to depend, directly and indirectly on national ICTs and the cyberspace along with its advanced cyber-dimensions.[11]

Regarding the progression of ICTs and the evolutionary as well as the extensive nature of cybercrime, it is no surprise to remark that the number of cybercrimes also increased

1 Von Solms 2022 https://theconversation.com/five-things-south-africa-must-do-to-combat-cybercrime-186089.
2 GOOSEVPN 2015 https://goosevpn.com/blog/origin-cybercrime.
3 According to Buxton 2022 https://www.minclaw.com/how-avoid-being-extorted-online/, "Online extortion, also commonly referred to as cyber extortion, can take many forms on the internet, but often the threat is the release of private or explicit photos unless a sum of money is paid.".
4 Alkaabi *Combatting Computer Crime: An International Perspective* 3.
5 Alkaabi *Combatting Computer Crime: An International Perspective* 3.
6 Alkaabi *Combatting Computer Crime: An International Perspective* 3.
7 Alkaabi *Combatting Computer Crime: An International Perspective* 1.
8 For purposes of this study cybercrime and online crimes are considered interchangeable.
9 Alkaabi *Combatting Computer Crime: An International Perspective* 1.
10 Grobler, Zaaiman and Van Vuuren 2013 *CSIR* 34.
11 According to Mbanaso and Dandaura 2015 at *IOSR*, "The term "cyberspace" is yet to have a globally accepted definition though it is sometimes tantamount to the notion of Internet or the view of a digital virtual realm.".

significantly due to the adverse impact of the Covid-19 pandemic.[12] Since the start of the Covid-19 pandemic, various countries declared and implemented a national lockdown;[13] countries, national- and international organisations, as well as educational institutions were forced to implement and operate from cloud-based communication[14] and working platforms, such as Microsoft Teams.[15] The international impact and effect of enforcing a "remote working"-protocol led to an overly engaged online environment progressing and expanding the international cyberspace and creating numerous opportunities for cyber-attackers to interact with cybercrime.[16]

This ultimately led to an advanced proliferation of cybercrime and cyber-attacks,[17] including phishing attacks, email harassment, DDoS (distributed denial-of-services) attacks and malware attacks.[18] After considering the impact of the Covid-19 pandemic on the cyberspace, numerous countries either started or continued to actively invest more time, money and national legislation to cybercrime and cybersecurity.[19] Numerous countries started attempting to combat cybercrime from constantly occurring by adopting, promulgating, and implementing national cybercrime legislation.[20] Regardless,[21] it appeared that even if a country's national cybercrime legislation were effectively implemented,[22] cybercrime remained a challenge, especially considering the continuous development of sophisticated ICTs and the cyberspace.[23]

---

12 Pietrangelo 2019 https://www.healthline.com/health/negative-effects-of-technology#positive-effects.
13 Pietrangelo 2019 https://www.healthline.com/health/negative-effects-of-technology#positive-effects.
14 According to Cheng 2021 at https://www.ringcentral.com/us/en/blog/what-is-cloud-communications, "Cloud communications are internet-based voice and data communications tools for businesses to manage applications, storage, and switching- all hosted by a third party on the cloud.".
15 Pietrangelo 2019 https://www.healthline.com/health/negative-effects-of-technology#positive-effects.
16 According to Olofinbiyi and Singh 2020 at *IJCS* 221, "Recently, as coronavirus evolved on the global spectrum, there seems to be an exponential upsurge in the activities of cyber criminals, as most of them have relentlessly been taking undue advantage of the emerging pandemic, using the available cyberspace to exploit people and organizations of their resources.".
17 According to Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack, "Cyber Attacks exploit vulnerabilities in computer systems and networks of computer data, or trick users to gain illegal access, with the intent to either steal, destroy or manipulate data and systems.".
18 Bandakkanavar 2020 https://krazytech.com/technical-papers/cyber-crime.
19 Alkaabi *Combatting Computer Crime: An International Perspective* 2.
20 Alkaabi *Combatting Computer Crime: An International Perspective* 2.
21 Alkaabi *Combatting Computer Crime: An International Perspective* 2.
22 Alkaabi *Combatting Computer Crime: An International Perspective* 2.
23 Alkaabi *Combatting Computer Crime: An International Perspective* 2.

Regarding the position of cybercrime in South Africa, according to Cassim,[24] cybercrime appears to be progressing rapidly as access to the internet[25] is constantly demanded, considering the use of modern ICTs.[26] Cassim[27] also mentions that according to various research reports focused on the position of cybercrime in South Africa, the rate of cybercrime increased significantly over the past 30-years because South Africa has been too focused on managing and addressing imperative issues, such as political instability and traditional crimes, for example homicide.[28] Cassim also briefly mentions,[29] it appears that South Africa lacks the adequate and advanced cyber-infrastructure to appropriately respond to cybercrime, therefore South Africa will continue to face the challenges and increased rate of cybercrime.[30]

South Africa experienced various challenges regarding the adoption, development, and implementation of national cybercrime legislation; however,[31] the recently implemented *Cybercrimes Act* 19 of 2020 (hereafter the "*Cybercrimes Act*") is considered the foundation of a committed South Africa in appropriately responding to and combatting cybercrime as well as promoting national cybersecurity measures.[32] Since the implementation of the *Cybercrimes Act*, South Africa's national cybercrime legislation presumably proved itself as internationally advanced compared to the international standard of other countries' national cybercrime legislation.[33]

South Africa's Justice and Correctional Services Minister, Mr Ronald Lamola,[34] commented on the implementation of the new ground-breaking *Cybercrimes Act* and proclaimed that it was of absolute importance for the *Cybercrimes Act* to align with international cybercrime legislation and practices to ensure its impact and effectiveness in addressing and

---

24 Cassim 2011 *CILSA* 126.

25 According to the Merriam-Webster Dictionary 2023 at https://www.merriam-webster.com/dictionary/Internet, the internet can be defined as, "an electronic communications network that connects computer networks and organisational computer facilities around the world.".

26 Cassim 2011 *CILSA* 126.

27 Cassim 2011 *CILSA* 127.

28 Cassim 2011 *CILSA* 127.

29 Cassim 2011 *CILSA* 127.

30 Cassim 2011 *CILSA* 127.

31 Williams, Fourie and Siyaya 2021 https://www.golegal.co.za/newly-enacted-cybercrimes-act/.

32 Williams, Fourie and Siyaya 2021 https://www.golegal.co.za/newly-enacted-cybercrimes-act/.

33 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.

34 South African Government News Agency 2021 https://www.sanews.gov.za/south-africa/lamola-welcomes-ramping-cybercrimes-act.

combatting cybercrime.[35] Lamola[36] added in supporting the implementation of the *Cybercrimes Act*,[37]

> "the methods of committing cybercrimes change rapidly and our laws need to keep pace with the more intrusive and complex investigative measures which are needed to investigate cybercrime."[38]

The implementation of the *Cybercrimes Act* is considered fundamental, especially regarding the release of a research report conducted by international cybersecurity company, Surfshark,[39] stating that the rate of cybercrime increased rapidly in 2021 due to the adverse impact and effect of the Covid-19 pandemic in 2020.[40] Surfshark's research report also presented an international hierarchy of various countries with the most recorded cybercrime and cyber-attacks in 2021 and secured South Africa as country number six on the list.[41] The report also included and listed other countries such as the Netherlands, France and Germany.[42]

Taking into consideration the prosperous political and economic position of the listed countries and the various reasons for the substantial number of cybercrime cases, it is quite evident that significant factors which cyber-attackers tend to consider when committing or performing a cybercrime is the political position, financial infrastructure and economic resources of the targeted country.[43] Cyber-attackers tend to target countries with powerful developed and advanced infrastructure and resources, for example South Africa, to ensure that the cybercrime delivers the most beneficial outcome for the cyber-attacker.[44]

---

35 South African Government News Agency 2021 https://www.sanews.gov.za/south-africa/lamola-welcomes-ramping-cybercrimes-act.

36 South African Government News Agency 2021 https://www.sanews.gov.za/south-africa/lamola-welcomes-ramping-cybercrimes-act.

37 South African Government News Agency 2021 https://www.sanews.gov.za/south-africa/lamola-welcomes-ramping-cybercrimes-act.

38 South African Government News Agency 2021 https://www.sanews.gov.za/south-africa/lamola-welcomes-ramping-cybercrimes-act.

39 Ernest 2022 https://www.timeslive.co.za/news/south-africa/2022-05-04-sa-ranked-6th-country-most-affected-by-cybercrime-research-finds/.

40 Ernest 2022 https://www.timeslive.co.za/news/south-africa/2022-05-04-sa-ranked-6th-country-most-affected-by-cybercrime-research-finds/.

41 Ernest 2022 https://www.timeslive.co.za/news/south-africa/2022-05-04-sa-ranked-6th-country-most-affected-by-cybercrime-research-finds/.

42 Ernest 2022 https://www.timeslive.co.za/news/south-africa/2022-05-04-sa-ranked-6th-country-most-affected-by-cybercrime-research-finds/.

43 Allen 2021 https://issafrica.org/iss-today/critical-infrastructure-attacks-why-south-africa-should-worry.

44 Allen 2021 https://issafrica.org/iss-today/critical-infrastructure-attacks-why-south-africa-should-worry.

However, the alternative of cyber-attackers attacking prosperous countries is that cyber-attackers also tend to target countries with a lack of appropriate or adequate cybersecurity measures, resulting in an easy and effortless target.[45] Therefore, the urgency for international cooperation between different countries appears once again, as the most constructive and appropriate measure of developing and implementing online security against cybercrime.[46] This will also encourage numerous countries to pay attention to the promulgation and implementation of national cybercrime legislation.[47]

1.1 Background

In 2004,[48] an internationally binding protocol, the Council of Europe, *Convention on Cybercrime*, 23 November 2001 (hereafter the "Budapest Convention") was ratified[49] by 67 international states.[50] South Africa was the only African country to sign the Budapest Convention,[51] but has not (yet) ratified or adopted it into any South African legislation.[52] Although the Budapest Convention fails to provide a definition of "cybercrime" or "online crime"[53] in article 1,[54] it consists of 48 articles with the objective of educating countries about cybercrime and the impact it has on the social, economic and political infrastructure of a country.[55] The Budapest Convention focuses on appropriately addressing cybercrime and providing the legal procedures for investigating and prosecuting cybercrime in various countries.[56]

The Budapest Convention also focuses on implementing online security, explaining the infringement of privacy rights, and discusses the implications of the distortion of data or information in the cyberspace.[57] The Budapest Convention also acts as an international

---

45 Bischoff 2022 https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/.
46 Schultz *Cybercrime: An Analysis of Current legislation in South Africa* 42.
47 Schultz *Cybercrime: An Analysis of Current legislation in South Africa* 42.
48 Council of Europe, *Convention on Cybercrime*, 23 November 2001 (hereafter the "Budapest Convention") 2-3.
49 According to Brierly 1952 in *YILC* 53, "Ratification is an act by which a State, in a written instrument, confirms a treaty as binding on that State.".
50 Council of Europe 2022 https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.
51 Cassim 2012 *PER/PELJ* 402.
52 Council of Europe 2022 https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.
53 See para 3 above.
54 The Budapest Convention 1-3.
55 The Budapest Convention 1-3.
56 The Budapest Convention 1-3.
57 The Budapest Convention 1-3.

guideline to various countries regarding the implementation of cybercrime legislation.[58] The Budapest Convention assists in delegating the various powers of national authorities and encourage international associations to cooperate in preventing the expansion of cybercrime in the cyberspace.[59] The Budapest Convention is regarded as a fundamental cybercrime framework for countries worldwide when they promulgate or adopt cybercrime legislation or frameworks.[60]

Regardless of the various attempts in defining cybercrime, it appears that no precise definition for these interchangeable concepts, "cybercrime" or "online crime" are formally known or published.[61] However, according to research,[62] cybercrime can be briefly defined as an illegal online activity or action, punishable by a country's national law and jurisdiction, performed by an online-criminal using a specific smart device,[63] for example a computer, with the general motive of personal gain, for example, to steal confidential information.[64]

A more comprehensive definition of cybercrime is that cybercrime can be introduced in the cyberspace as any illegal online activity or action where the motive of this specific online activity consists of gaining unauthorised access to a specific smart device, for example a computer or software systems.[65] Cybercrime focuses on intercepting or stealing data from information networks and attempts to retrieve classified information, while the cyber-criminal uses another smart device, for example, a software system or a data-information network.[66]

In the writer's opinion regarding the definition of cybercrime:[67] Cybercrime does not exclusively occur in the online environment or in the cyberspace, but can also occur in the physical world, for example through fraud.[68] Cybercrime is an electronic illegal activity

58 The Budapest Convention 1-3.
59 Daskal and Kennedy-Mayo 2020 https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/?cn-reloaded=1.
60 Mabeka and Cassim 2023 *Obiter* 30.
61 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 7.
62 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 7.
63 According to Ellis 2022 at https://www.makeuseof.com/smart-device-meaning/, "A smart device can be defined as an electronic device connected to the internet, an application, a local network or a wireless connection for example Wi-Fi, used for high technology communication.".
64 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 7.
65 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 8.
66 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 8.
67 Writer's definition of cybercrime.
68 Writer's definition of cybercrime.

executed (on-/ or offline) by an individual or smart device using either technology (for example software programmes) or technological instruments (for example a computer) to attack, infringe or damage the physical or intellectual property of another individual, organisation or country with various motives such as personal gain or revenge.[69]

According to Casey,[70] there are three key elements of cybercrime which can be used as distinct factors to define cybercrime.[71] These elements are:[72] (a) The target of the crime is a smart device for example a computer, (b) the instrument used to commit the crime is a smart device, for example a computer, and (c) the smart device used had to play an essential role in committing the cybercrime.[73] Cassim[74] continues to add and discuss two additional components which must also be considered when defining cybercrime.[75] These two components refer to the position in which cybercrimes are generally performed and carried out by the use of either a computer or smart device, where the smart device is either used as an object or a subject to commit the cybercrime.[76]

When a smart device is used as an object to commit a cybercrime,[77] the smart device is the only instrument that performs and carries out the cybercrime, for example intercepting online communication.[78] When a smart device is being used as a subject to commit a cybercrime, the cyber-attacker (the performing object) uses the smart device (subject) as an instrument to perform a traditional crime, for example, fraud.[79] It is important to distinguish when the smart device is the object committing the crime and when the smart device is being used as a subject or instrument to commit a crime.[80] Considering the distinct factors discussed above, it is imperative to understand that cybercrime can also be divided into several categories, including, an individual cybercrime, a government cybercrime, property cybercrime and others.[81]

---

69 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 8; Writer's definition of cybercrime.
70 Casey *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 14.
71 Casey *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 14.
72 Casey *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 14.
73 Casey *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 14.
74 Cassim 2009 *PER/PELJ* 59.
75 Cassim 2009 *PER/PELJ* 59.
76 Cassim 2009 *PER/PELJ* 59.
77 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 7.
78 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 7.
79 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 7.
80 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 7.
81 Upadhyay 2020 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

When a cyber-criminal commits an individual cybercrime, the target of the crime is always an individual or a specific smart device.[82] The objective of this type of cybercrime is usually to gain access or release confidential information about another individual.[83] Examples of this type of cybercrime include online stalking or harassment.[84] The second category, government cybercrime, also known as cyber-terrorism,[85] is considered to be a serious form of misconduct in countries.[86] Cyber-terrorism usually indicates the unauthorised infiltration of government-based websites to obtain or release confidential information, for example, nuclear launch codes.[87]

Property cybercrime generally refers to cybercrime committed with the objective of obtaining personal information from an individual, for example banking details or an ID number.[88] An example of property cybercrime is the unauthorised access and control of another individual's computer or smart device.[89] Lastly, the most common category of cybercrime includes malware attacks and software piracies.[90] Malware attacks are a combination of the concepts, "malicious"[91] and "software program"[92] and refers to a computer programme designed to infiltrate, compromise, or damage another smart device, network or server (without the knowledge or consent of a user) with the objective of gaining confidential information.[93] An example of a malware attack is a virus.[94] The last category of cybercrime to be discussed is advanced software piracies.

---

82 Dashora 2011 *JAPSS* 240-257.

83 Upadhyay 2020 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

84 Upadhyay 2020 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

85 According to Dashora 2011 in *JAPSS* 240-257, Cyber-terrorism is defined as an intentional execution of unlawful or disruptive online threats as well as online spying activities, with the focus on social, economic, and political objectives of a certain country and their government.

86 Upadhyay 2020 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

87 Upadhyay 2020 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

88 Upadhyay 2020 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

89 Upadhyay 2020 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

90 Upadhyay 2020 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

91 According to the Merriam-Webster dictionary 2022 at https://www.merriam-webster.com/dictionary/malicious, "Definition of malicious: having or showing a desire to cause harm to someone.".

92 According to Britannica 2022 at https://www.britannica.com/technology/software, "Software comprises the entire set of programs, procedures, and routines associated with the operation of a computer system.".

93 Arce 2018 *JOC* 1.

94 Arce 2018 *JOC* 1.

Advanced software piracies are the illegal distribution, download, and use of unlicensed software programmes to a computer or a smart device.[95] Cyber-attackers tend to release their very own generated unlicensed software programme in the online environment, victims then often download these programmes with a virus attached, infiltrating their smart device and damaging their files.[96] The list of the different types of cybercrime is not limited to the above-discussed, but is in fact extensive and evolving (Chapter 2).[97] Numerous different types of cybercrime are discovered daily, which raise the concerns of countries regarding advanced cyber-challenges.[98] The impact and effect of these cyber-challenges involve the lack of cyber-awareness, numerous cyber-attacks and being exposed, resulting in the extensive evolution of the international cyberspace.[99]

1.2 Motivation

According to research conducted by Hakmeh, Naylor and Wallace,[100] the most common reason for the international magnitude of cybercrime is that cyber-attackers tend to focus, target and disrupt different countries, different governments, and different legal justice systems.[101] It has been reported that the majority of cybercrime cases aim to attack and threaten a country's national infrastructure such as their healthcare sectors or transportation networks.[102] Attacking and threatening a country's national infrastructure has the ability to cause a major disruption in a country's economy, therefore not only does cybercrime, being a borderless crime, affect a country's national infrastructure or economy but it can also progress and adversely affect the position of the general global economy.[103]

Therefore, it is important to acknowledge that the primary reason for the general increase in cybercrime in various countries is due to the significant fact that countries do not entirely comprehend or understand the extensive and complex nature of cybercrime and

95 Norwich University Online 2020 https://online.norwich.edu/academic-programs/recources/types-of-cyber-crime.
96 Norwich University Online 2020 https://online.norwich.edu/academic-programs/recources/types-of-cyber-crime.
97 Kleijssen and Perri 2016 https://rm.coe.int/cybercrime-evidence-and-territoriality-issues-and-options/168077fa98.
98 Kleijssen and Perri 2016 https://rm.coe.int/cybercrime-evidence-and-territoriality-issues-and-options/168077fa98.
99 Poonia 2014 *IJETTCS* 119.
100 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.
101 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.
102 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.
103 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.

the threat it holds.[104] Regardless of this reason, forcing a country and its government to suddenly implement rigid cybercrime legislation and cybersecurity measures can be considered quite challenging and complex because of the political and economic position of the country.[105] Nevertheless, it appears that countries seem to have recognise the need for the development and implementation of cybercrime legislation to properly address and respond to cybercrime in a lawful manner.[106]

To ensure that the development and implementation of cybercrime legislation is considered adequate and effective, countries need to first, fully understand what they must secure, determine where the country's national infrastructure appears to be the most vulnerable, and consider where these cybercrime-incidents and cyber-threats emerge from.[107] Second, countries must thoroughly educate, train, and prepare themselves to be able to properly respond to cybercrime.[108] This is done by focusing on the social, political and economic resources of a country and the impact which cybercrime has on a country and only then, develop and implement national legislation which addresses and combats cybercrime, while also focusing on protecting the rights of citizens to prevent any infringement repercussions.[109] Focusing on these two factors will assist countries in the development and implementation of cybercrime legislation.

It is of the utmost importance for a country and its government to understand that cybercrime cannot only be addressed and combatted through national pieces of legislation or the country's common law.[110] As mentioned, cybercrime is considered a borderless crime which makes it possible for a cyber-attacker to commit a cybercrime from anywhere in the world.[111] Various cyber-reports claim that international cooperation between countries will partially establish an international cyber-regulation with the primary objective to combat and respond to cybercrime.[112] However, in focusing on the position of cybercrime in South Africa, a distinct conclusion can be drawn from the standard of South

104 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.
105 Grobler, Zaaiman and Van Vuuren 2013 *CSIR* 33.
106 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.
107 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.
108 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.
109 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.
110 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.
111 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.
112 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.

Africa's previous cybercrime legislation compared to the current standard of South Africa's cybercrime legislation.

It is quite evident that South Africa is committed to addressing and combatting cybercrime.[113] Regardless,[114] taking into consideration the sophisticated and advanced nature of cybercrime, cybercrime is currently regarded as more complex than ever, due to the fact that these crimes are no longer limited to a specific set of elements or do not fall within the exact borders of a country's jurisdiction or national legal justice system.[115] Therefore, this borderless crime poses a major threat since these crimes are mostly committed by an individual or a software programme that prefers to remain anonymous and is protected by advanced software programmes when committing a cybercrime.[116] As mentioned, the evolutionary nature of cybercrime directly contributes to the accelerated rate of cybercrime in countries around the world.[117]

Countries consider it demanding and onerous to keep their national legislation up to date regarding cybercrime which can, if neglected or delayed, lead to a substantial number of cybercrime cases.[118] However, it is important to recognise that over the past few years, countries such as South Africa have been actively attempting to combat cybercrime through numerous pieces of cybercrime legislation, such as the *Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002 (hereafter the "*RICA*"),[119] the *Electronic Communications and Transactions Act* 25 of 2002 (hereafter the "*ECTA*"), the *Protection of Personal Information Act* 4 of 2013 (hereafter the "*POPIA*") and the recently amended *Films and Publications Amendment Act* 11 of 2019 (hereafter the "*FPAA*").[120]

Although the above-mentioned national legislation was successfully implemented by the South African government in addressing only a few cybercrime characteristics and issues,

---

113 Campbell 2021 https://businesstech.co.za/news/cloud-hosting/546856/how-south-africas-cybercrimes-act-will-change-how-you-use-the-internet/.

114 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 18.

115 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 18.

116 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 18.

117 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 6.

118 Alkaabi *Combatting Computer Crime: An International Perspective* 3.

119 In *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* CCT 278/19; *Minister of Police v AmaBhungane Centre for Investigative Journalism NPC* CCT 279/19, the Constitutional Court of South Africa found and handed down the judgement that certain provisions of the *RICA* are declared unconstitutional and is in the process of being amended.

120 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 6.

the increased rate of cybercrime remained a troublesome challenge.[121] Since then, the rate of cybercrime in South Africa has only escalated, especially when one considers the impact and effect the Covid-19 pandemic had and still has on South African ICTs.[122] During the Covid-19 pandemic, the South African legislature finally agreed upon promulgating a specific piece of cybercrime legislation, the *Cybercrimes Act* 19 of 2020 (hereafter the "*Cybercrimes Act*"), as the primary cybercrime legislation to address and combat cybercrime inside the borders of South Africa.[123]

The promulgation and implementation of the *Cybercrimes Act* came at exactly the right moment, taking into consideration the magnitude of cybercrime occurring in South Africa.[124] For South Africa, the main objective of the *Cybercrimes Act* represents a transparent online security measure where cybercrime investigation and prosecution procedures can be executed without any unnecessary hindrances such as objections to privacy or electronic evidence delays.[125] According to Chapter 2 and Chapter 4 of the *Cybercrimes Act*,[126] cybercrime investigations and prosecution procedures no longer have to rely on or be conducted through various articles of different national pieces of legislation such as the *RICA*, the *ECTA*, the *POPIA* or the *FPAA,* and national authorities (for example, the South African Police Service (SAPS)) no longer have to conduct guideless or restrictive investigation procedures.[127]

In general, when a country's government recognises the need for developing and implementing specific new legislation, it is quite important for the government to also accept, manage and evaluate the effect and impact the new national legislation has and will have on the country, its citizens and the country's legal justice system.[128] This includes addressing and evaluating the legal checks and balances, legal tensions and the possibilities of the infringement of rights regarding the new piece of legislation.[129] Therefore, these concerns present the objective and motivation for this study.

---

121 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 6.
122 Olofinbiyi and Singh 2020 *IJCS* 221.
123 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.
124 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.
125 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.
126 Chapter 2, Chapter 4 of the *Cybercrimes Act*.
127 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.
128 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.
129 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.

This study will primarily address two objectives: (a) Discuss the evolution and extensive nature of cybercrime in South Africa and the extent of combatting cybercrime using the recently implemented *Cybercrimes Act* 19 of 2020 (hereafter the "*Cybercrimes Act*") and; (b) Discuss and compare the potential effect and impact of the *Cybercrimes Act* along with considering the previous cybercrime legislation such as the *RICA*, the *ECTA*, the *POPIA,* the *FPAA*, the National Cybersecurity Policy Framework (NCPF) and the Budapest Convention (as well as the African Union Convention on Cyber Security and Personal Data Protection (hereafter the "AU Convention")). This study will consist of five chapters, being literary, historical, and comparative in nature.

Chapter 2, Cybercrime in a South African context; a comprehensive historic literature review on cybercrime and the evolution thereof will be discussed. This chapter will focus on identifying and defining the nature of cybercrime, the origin of cybercrime in South Africa, list the different types of cybercrime, and refer to the position of past and present cybercrime cases and challenges in South Africa. Chapter 3, Previous Cybercrime Legislation in South Africa; this chapter will discuss South Africa's previous national cybercrime legislation prior to the promulgation and implementation of the *Cybercrimes Act*. Numerous pieces of national legislation such as the *RICA*, the *ECTA*, the *POPIA* and the *FPAA* will be referred to and discussed regarding the cyber-components that they address.

Chapter 4, the *Cybercrimes Act* 19 of 2020 will be critically discussed and partially compared to previous cybercrime legislation. This chapter will also discuss the different types of cybercrime found in the *Cybercrimes Act* and address the reporting, investigation, and prosecution procedures. The shortcomings of the *Cybercrimes Act* will also be discussed, considering that the *Cybercrimes Act* is South Africa's first official piece of national cybercrime legislation.

Chapter 5, the Conclusion and Recommendations will present an entire overview of the study and briefly mention the main objectives and essence of each chapter again. This chapter will also present recommendations regarding South Africa's cybercrime legislation, especially regarding the *Cybercrimes Act*. This chapter will also conclude the entire aim and objective of the study, discuss various comments on the *Cybercrimes Act* and present suggestions as to how the *Cybercrimes Act* can be amended or altered, to ensure and

deliver more ground-breaking results regarding the rate and impact of cybercrime in South Africa.

1.3 Research question

The research question and primary focus of this study is: To what extent does the recently implemented *Cybercrimes Act* effectively address and deal with the extensive and complex nature of cybercrime, to combat cybercrime in South Africa? This discussion will also include the following sub-question: Does the *Cybercrimes Act* have any shortcomings regarding privacy matters or concerns, the procedures of reporting, investigating and prosecuting cybercrime, and provide adequate guidance for the delegation of powers regarding national authorities concerning cybercrime?

2 Research aim and objectives

The primary research aim of this study is to critically analyse and discuss the legal impact and effect of the *Cybercrimes Act* in appropriately addressing and combatting cybercrime in South Africa against the background of existing cybercrime legislation. Although the *Cybercrimes Act* is still considered new national cybercrime legislation, it is important for the South African government and legislature to monitor, determine and evaluate the impact and effect the *Cybercrimes Act* has on South Africa and its legal justice systems. Therefore, the focus of this study will be on the evolution of cybercrime in South Africa, the position of past and present cybercrime challenges and discuss the promulgation, implementation, shortcomings and recommendations of the *Cybercrimes Act* and lastly, whether the *Cybercrimes Act* appropriately amended previous existing cybercrime legislation.

This study will also consider, discuss, and partially compare previous national cybercrime legislation and frameworks such as the *RICA*, the *ECTA* (along with the *CPA*), the *POPIA* and the *FPAA* with the *Cybercrimes Act*. The National Cybersecurity Policy Framework (NCPF) and the Budapest Convention (as well as the AU Convention) will also be discussed and partially compared with the *Cybercrimes Act*. The *Cybercrimes Act*, being the focus of this study will also be critically discussed. Lastly, the discussion of shortcomings and recommendations on the *Cybercrimes Act* will be presented as well as suggestions for the amendment of the *Cybercrimes Act*. Although this study has various objectives, the main

objective is to introduce and evaluate the recently implemented *Cybercrimes Act* in South Africa, taking into account previous cybercrime legislation.

The extensive history of cybercrime in South Africa and the past and present position and challenges will also be discussed, the relevant case law regarding cybercrime, and a partial comparison will be conducted regarding the history of previous cybercrime legislation such as the *RICA*, the *ECTA* (along with the *CPA*), the *POPIA* and the *FPAA* with the recently implemented *Cybercrimes Act*. The *Cybercrimes Act* and what it entails will also be critically discussed and evaluated along with considering the position and influence of the *Constitution of the Republic of South Africa*, 1996 (hereafter the "*Constitution*").[130] Lastly, a few suggestions to amend the *Cybercrimes Act* will also be presented.

3 Premises, assumptions, and hypotheses

The premise of this study is based on the critical discussion, analysis, and evaluation of the objective and legal effect of the *Cybercrimes Act* in properly responding to cybercrime in South Africa. The increased rate of cybercrime and cyber-attacks over the past few years captured the concern and attention of the South African government. In response to these cybercrime and cyber-attacks, the South African government and legislature agreed upon promulgating and implementing the *Cybercrimes Act* to fulfil their duty and responsibility to secure and protect the citizens of South Africa against cybercrime in the cyberspace. The promising effect and impact of the *Cybercrimes Act* on South Africa already appears substantial and to have proven itself to a certain extent, ensuring to deliver promising results.

However, can the *Cybercrimes Act* be regarded as adequate in being the only piece of national cybercrime legislation in South Africa? This question remains a definite concern regarding the impact and effect of the *Cybercrimes Act* on South Africa, as it appears that the *Cybercrimes Act* cannot be regarded as adequate when one considers the continuous occurrence of cybercrime in South Africa. The assumption of this study is that according to section 9(1) and section 14(d) of the *Constitution*, every South African citizen has the right to equal protection and benefit of the law as well as the fundamental right to privacy.[131] This directly places the government and legislature in the line of duty to protect and

130 *Constitution of the Republic of South Africa*, 1996 (hereafter the "*Constitution*").
131 Section 9, section 14 of the *Constitution*.

ensure a safe and secure online environment.[132] Whether it be in a social context or online, the government has the duty to protect.

South African cybercrime and cyber-attacks continue to rapidly progress as the popularity of the crime escalates, resulting in a defenceless cyberspace and numerous cyber-victims.[133] South Africa responded to the increase of cybercrime in the country by promulgating and implementing national cybercrime legislation focused on combatting cybercrime, the ground-breaking *Cybercrimes Act*.[134] Since the implementation of the *Cybercrimes Act*, South Africa's national authorities have been hoping that the number of cybercrime cases and cyber-attacks in South Africa would diminish, ultimately then leading to promising prospects.[135] South Africa's national authorities are excited to use and enjoy the internet and cyberspace without having to look over their shoulder and to fear of becoming a potential cyber-victim.[136]

However, although the *Cybercrimes Act* was specifically developed to respond to and combat cybercrime, the rate of cybercrime and cyber-attacks still appear to be increasing as the process of implementing the *Cybercrimes Act* is ongoing.[137] This leads to the question: Can the *Cybercrimes Act* be considered adequate in properly addressing and combatting cybercrime in South Africa? The hypothesis of this study is, although the recently implemented *Cybercrimes Act* of South Africa appears quite promising and the legal impact thereof, quite positive, the *Cybercrimes Act* cannot be regarded as adequate or effective enough on its own, in addressing and combatting cybercrime to the greatest extent of the crime.

During this study it will be made clear that although South Africa responded in an appropriate manner in combatting cybercrime, considering the previous national cybercrime legislation, relevant case law and international conventions, the *Cybercrimes*

---

132 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com

133 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com

134 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com

135 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com; Mcanyana and Brindley 2020 https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa.

136 Mcanyana and Brindley 2020 https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa.

137 Mcanyana and Brindley 2020 https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa.

Act cannot on its own, provide the necessary protection for South Africa and its citizens in the manner it wishes and aims to. The *Cybercrimes Act* must be supported through additional legislation to ensure a safe and secure cyberspace.

4 Research methodology

During the execution of this study various research methods will be used. The primary research method to be used, will consist of a broad literature review which will represent two main categories, primary resources, and secondary resources. The primary resources will consist of various pieces of national legislation and frameworks, case law and other regulatory policies or conventions. The secondary resources of this study will consist of textbooks, an online cybercrime seminar, various journal articles, electronic documents, and theses as well as other dissertations and internet resources.

The secondary research method used during this study will be conducted by using the historical method, specifically looking into the evolutionary and progressive aspect of cybercrime, considering both the past and present positions, and challenges of cybercrime in South Africa. An historic overview of the evolution and development of cybercrime will be presented and primarily focus on being informative in nature as well as aiming to discuss the development procedures that led to the implementation of the *Cybercrimes Act*. The historic overview of cybercrime in South Africa will also discuss past and present challenges regarding cybercrime and cybercrime legislation, specifically focusing on previous pieces of national legislation such as the *RICA*, the *ECTA*, the *POPIA* and the *FPAA*.

Considering the historical method, the external legal history will be discussed during the execution of this study, focusing on the various resources which directly and indirectly contributed to the development and implementation of the *Cybercrimes Act*. The external legal history resources refer to the constitutional, political, and economic factors that had an influence and effect on the development of South Africa's legal justice systems. In general, the scope of this study will primarily focus on the South African history and evolution regarding cybercrime, the previous national legislation addressing cybercrime, discuss the recently implemented *Cybercrimes Act* along with the *Constitution*, and suggest amendments and recommendations.

The third research method, the comparative method, will also be used during the execution of this study. The comparative method will include a critical discussion and comparison between the various pieces of South African national legislation regarding cybercrime, such as the recently implemented *Cybercrimes Act*, the *RICA*, the *ECTA*, the *POPIA* and the *FPAA*. The international Budapest Convention and AU Convention will also be discussed and compared to the *Cybercrimes Act*, along with considering the NCPF. The primary objective for the comparison of the various pieces of cybercrime legislation of South Africa is to determine, examine and evaluate the general standard and objective of the *Cybercrimes Act* compared to previous pieces of national cybercrime legislation in South Africa.

The comparison will conclude with whether the *Cybercrimes Act* appropriately addresses and combats cybercrime in South Africa. It will also present whether the *Cybercrimes Act* has properly amended South Africa's previous national cybercrime legislation. Therefore, the scope of this study focuses on the past and present position of cybercrime in South Africa and the extent of the *Cybercrimes Act* in addressing and combatting cybercrime. Regarding the limitations of the study, this study will not present an international comparison between South Africa's cybercrime legislation or another country's cybercrime legislation; however, there are two conventions that will be discussed and partially compared to. Also, no specific statistics will be presented regarding cybercrime and no specific distinction will be drawn between South Africa or any country regarding the matter of cybercrime.

5 Framework

Chapter 1 Introduction to Cybercrime in South Africa

Chapter 1 of this study will introduce the problem statement, the background of the problem statement and the research question of this study. The chapter will also discuss the research aim and objectives as well as the premise, assumptions, and hypotheses of this study.

Chapter 2 Cybercrime in South Africa: Past and Present

This chapter will focus on the position of cybercrime in South Africa. This chapter will also focus on the previous position of cybercrime in South Africa, the challenges of cybercrime and the different types of cybercrime.

Chapter 3 Previous Cybercrime Legislation in South Africa

This chapter will discuss the history and evolution of cybercrime legislation in South Africa. This discussion will include the *Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002, the *Electronic Communications and Transactions Act* 25 of 2002, the *Criminal Procedure Act* 51 of 1977, the *Protection of Personal Information Act* 4 of 2013, and the *Films and Publications Amendment Act* 11 of 2019.

Chapter 4 The *Cybercrimes Act* 19 of 2020

Chapter 4 will address and discuss the history and evolution of cybercrime in South Africa that led to the promulgation and implementation of the Cybercrimes Act 19 of 2020 (hereafter the "*Cybercrimes Act*"). This chapter will also address the position and relationship of the Cybercrimes Act 19 of 2020 with the Constitution of the Republic of South Africa, 1996.

Chapter 5 Conclusion and Recommendations

This chapter is the conclusion and recommendations. Legislative and practical recommendations will be presented.

Major subject

Cyber Law

Ancillary subjects

Public Law; Criminal Law; Civil Law

Chapter 2 Cybercrime in South Africa: Past and Present

2 Understanding Cybercrime

2.1 The Evolution of Cybercrime

Ever since South Africa was classified as the country with the sixth highest cybercrime density in 2022,[138] it is no surprise that the evolutionary nature of the cyberspace is considered to be anything but a new phenomenon to South Africa and its government.[139] Cybercrime has been evident in South Africa since the early 1990's,[140] recently exceeding the thirty-year parameter,[141] and still continues to emerge as one of the most extensive and sophisticated crime threats present in South African ICTs.[142] For South Africa, its individuals, organisations, and the government it is considered essential to be connected to the world, either via national or international network platforms or ICTs.[143]

According to Dr. Jenna Clark,[144] senior behavioural researcher,[145] these types of ICTs and technology-mediated interactions are considered high in demand regardless of the complications and challenges they produce.[146] The effect of the progressive development of ICTs and the online environment are still considered beneficial for countries and their governments to develop certain fields of national infrastructure such as medicine, sciences, and engineering.[147] Therefore, considering that communication technologies and the online environment continue to develop and evolve, South Africa becomes more reliant

---

138 According to Von Solms, Director of Cyber Security at the University of Johannesburg, 2022 at https://theconversation.com/five-things-south-africa-must-do-to-combat-cybercrime-186089, "Cybercrime density is defined as the percentage of cyber victims per one million internet users.".

139 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 17.

140 Von Solms 2022 https://theconversation.com/five-things-south-africa-must-do-to-combat-cybercrime-186089.

141 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 4.

142 According to Giles 2022 at https://www.michalsons.com/blog/what-is-ict/2525, "ICT is an acronym for "information communications technology.".

143 Clark 2019 https://greatergood.berkeley.edu/article/item/what_makes_technology_good_or_bad_for_us.

144 Linkedin 2023 https://www.linkedin.com/in/jenna-clark-b0221a132.

145 Linkedin 2023 https://www.linkedin.com/in/jenna-clark-b0221a132.

146 Clark 2019 https://greatergood.berkeley.edu/article/item/what_makes_technology_good_or_bad_for_us.

147 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 5.

on the online environment, resulting in individuals, organisations and the government being exposed and operating defenceless in the cyberspace against cybercrime.[148]

As mentioned above, cybercrime can be defined as any illegal online activity performed by a cyber-criminal with the collaboration of a smart device, for example a computer, to cause harm to another internet user or their computer in the online environment.[149] Cybercrime continues to be part of the progressive element of ICTs as it continues to rapidly increase on a scale that the South African legislature and their justice systems struggle to balance.[150] According to Hart,[151] society appears extremely vulnerable and exposed in the world and its ICTs, and, therefore, a rule of law in a country is a requirement to ensure that citizens remain safe and protected in the online environment.[152]

Applying Hart's statement directly to the extensive concept of the cyberspace, a country's government has the duty and responsibility to ensure that internet users are protected from cybercrime and cyber-attacks in the online environment and that when cybercrimes or cyber-attacks occur, they can be appropriately addressed through the country's legal justice system.[153] There are, however, numerous reasons for the success rate of cybercrime as mentioned above; the list of reasons varies from, unauthorised access to smart devices or a computer's operating system, the use of decoding software to "crack" the numerical nature of a computer system and the negligent conduct or lack of cybersecurity from a natural person (normal human beings)[154] or a juristic person (specific natural persons or- associations, for example organisations)[155] in the cyberspace.[156]

---

148 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 4.

149 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 8.

150 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 5.

151 Hart *The Concept of Law* 81.

152 Hart *The Concept of Law* 81.

153 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

154 Ramages *Capacities and Rights of the Legal Subject* 3.

155 Ramages *Capacities and Rights of the Legal Subject* 3.

156 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

When one analyses any type of cybercrime, it is important to identify and understand the operating position as well as the outcome orientation of the cyber-attacker.[157] Several different categories of cyber-attackers have been identified, based on the objective and outcome of the cybercrime.[158] The first category of cyber-attackers are individuals between the ages of 7 – 18 years.[159] This specific type of cyber-attackers are often referred to as "Script kiddies".[160] Script kiddies are inexperienced and immature cyber-hackers, often just as dangerous as experienced cyber-hackers with the objective of exploring the online environment.[161]

The objective of this specific group of individuals is generally to focus on exploiting the vulnerabilities of the online environment and accidentally gaining access to protected or unprotected information.[162] Another objective to consider is that children often find themselves trying to prove that they are exceptional amongst other children in society; this typically refers to online boastfulness.[163] The last and most preferential objective to consider is that the child has been bullied or harassed by another person and, therefore, the child seeks revenge.[164]

The next category of cyber-attackers is called organised hackers.[165] This type of cyber-attacker is considered to be objectively organised and committed to fulfil a specific task or reach a specific target or goal in the online environment.[166] Organised hackers generally focus on targeting a country's government and its national infrastructure for example, political reasons or fundamentalism;[167] these types of cyber-attacks are also closely

---

157 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

158 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

159 Lutkevich 2021 https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie.

160 Lutkevich 2021 https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie.

161 Lutkevich 2021 https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie.

162 Lutkevich 2021 https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie.

163 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

164 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

165 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

166 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

167 According to the Merriam-Webster Dictionary 2023 at https://www.merriam-webster.com/dictionary/fundamentalism#:~:text=%3A%20a%20movement%20or%20attitude%20stressing,Islamic%20fundamentalism, the definition of fundamentalism is, "a movement or attitude stressing strict and literal adherence to a set of basic principles".

related to cyber-terrorism, which will be discussed later.[168] Various organisations and governments have reported experiencing this specific type of organised cyber-attack before, for example NASA.[169]

The third category of cyber-attackers are professional hackers.[170] This group of cyber-attackers is fixated on financial gain and accessing confidential information.[171] These cyber-attackers tend to hack into an organisation's or government's website to steal funds or confidential information by detecting loopholes in the website's security system.[172]

The last category of cyber-attackers are discontented employees.[173] This category of cyber-attackers focuses on hacking into their employer's or organisation's information systems or websites, usually due to dissatisfaction or revenge.[174]

Since the impact of the Covid-19 pandemic, the World Economic Forum Global Risk Report noted an increase of 12% in cybersecurity breaches during the pandemic and in 2021, when the online environment became a broadband highway.[175] Although, focusing on the sophisticated nature of cybercrime, even though cybercrime evidently varies from a traditional crime in several ways,[176] it is important to understand that these crimes still consist of similar elements, for example, both of these crimes involve an act or omission (failure to act) which constitutes a recorded offence and is punishable by the law of the country where the crime was geographically committed.[177]

According to research,[178] the nature and elements that distinguish cybercrime from traditional crimes are quite comprehensive; these elements include, the type of cyber-

168 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
169 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
170 Shea and Lutkevich 2021 https://www.techtarget.com/searchsecurity/definition/cracker.
171 Shea and Lutkevich 2021 https://www.techtarget.com/searchsecurity/definition/cracker.
172 Shea and Lutkevich 2021 https://www.techtarget.com/searchsecurity/definition/cracker.
173 Cutler 2022 https://terrycutler.com/the-malicious-hacking-employee/.
174 Cutler 2022 https://terrycutler.com/the-malicious-hacking-employee/.
175 BusinessTech 2022 https://businesstech.co.za/news/technology/639277/the-world-faces-a-cybercrime-catastrophe-including-south-africa/.
176 Pinto 2022 https://www.eatmy.news/2022/11/how-cyber-crimes-differ-from.html.
177 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
178 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

medium involved in the crime,[179] the evidence of the crime,[180] the scale of the crime,[181] the reach of the crime[182] and the speed of the crime.[183] The first element,[184] the type of cyber-medium[185] involved in the crime, refers to asking the following two questions: Is any digital smart device involved in committing the crime, and was the smart device used as an object or a subject to the crime?[186] This separates the cyber-medium involved in cybercrime from traditional crimes and identifies the type of crime that was committed.[187]

The second element,[188] the evidence of the crime, refers to the indication that a crime was committed. For example,[189] traditional criminals often leave a trace of evidence when a crime was committed; this evidence includes, DNA evidence through hair, semen, or fingerprints, or evidence either through verbal confessions or physical actions.[190] Cyber-attackers solely depend on remaining completely anonymous when committing a cybercrime as the crime often leaves little to no concrete evidence of the cyber-attacker, apart from the results of the cyber-attack or an electronic trail, like the digital footprint.[191]

The third element, the scale of the crime,[192] refers to the amount of cyber-attacks and cyber-victims that are recorded in a specific timeframe.[193] The exact scale of recorded

---

179 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

180 Prakash and Rajan 2018 *IJPAM* 1454.

181 PGI 2018 https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/.

182 PGI 2018 https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/.

183 PGI 2018 https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/.

184 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

185 The type of cyber-device used to commit the crime.

186 See Chapter 1.1 for distinction; Maat *Cyber Crime: A Comparative Law Analysis* 18.

187 Maat *Cyber Crime: A Comparative Law Analysis* 20.

188 Prakash and Rajan 2018 *IJPAM* 1454.

189 Pinto 2022 https://www.eatmy.news/2022/11/how-cyber-crimes-differ-from.html.

190 Pinto 2022 https://www.eatmy.news/2022/11/how-cyber-crimes-differ-from.html.

191 Prakash and Rajan 2018 *IJPAM* 1454; According to Reyes 2023 at https://blog.reputationx.com/digital-footprint, "A digital footprint is the trail of data that you intentionally or unintentionally leave behind while using the internet. This includes social media posts, passwords, online purchases, IP addresses, and more.".

192 Mukherjee 2023 https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/#:~:text=Cybercrimes%20include%20phishing%2C%20hacking%2C%20spoofing,%2C%20i.e.%2C%20mainly%20offline%20crimes.

193 Mukherjee 2023 https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/#:~:text=Cybercrimes%20include%20phishing%2C%20hacking%2C%20spoofing,%2C%20i.e.%2C%20mainly%20offline%20crimes.

cybercrime and cyber-attacks are often unclear in comparison to traditional crimes.[194] The explanation for this statement can be illustrated by the following example:[195] If a criminal wishes to attack a traditional bank it would be possible for them to successfully reach one to three banks per week before it is required of them to withdraw into "safety"; however,[196] in the case of cybercrime, a cyber-attacker can target multiple banks and bank sites at once and still remain "safe" and "undiscoverable" by operating anonymously.[197]

The fourth element, the reach of the crime,[198] refers to the fact that cyber-attacks can be committed from any place, anywhere in the world; whereas traditional crimes have a specific geographical location in where they are committed.[199] This element directly refers to the borderless characteristic of cybercrime and for being able to anonymously commit a cybercrime within a country's jurisdiction, considering that the cybercrime might or might not be addressed by that specific country's criminal justice system.[200] For example, a cyber-attack can be initially conducted and launched from America, but be committed in South Africa, or the target of the cyber-attack can be South Africa.[201]

Another approach in comprehending the extensive reach of the crime:[202] Cyber-attackers have the skill, ability, and the advanced software programmes to extract a greater number of digital files or data from anywhere in the cyberspace (this refers to any country,

---

194 Mukherjee 2023 https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/#:~:text=Cybercrimes%20include%20phishing%2C%20hacking%2C%20spoofing,%2C%20i.e.%2C%20mainly%20offline%20crimes.

195 PGI 2018 https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/.

196 PGI 2018 https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/.

197 PGI 2018 https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/.

198 Mukherjee 2023 https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/#:~:text=Cybercrimes%20include%20phishing%2C%20hacking%2C%20spoofing,%2C%20i.e.%2C%20mainly%20offline%20crimes.

199 Mukherjee 2023 https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/#:~:text=Cybercrimes%20include%20phishing%2C%20hacking%2C%20spoofing,%2C%20i.e.%2C%20mainly%20offline%20crimes.

200 PGI 2018 https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/.

201 PGI 2018 https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/.

202 PGI 2018 https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/.

website, etc.), than extort the same number of files or data from the physical world (being a in specific geographical location).[203] An example of this type of extortion can be illustrated by understanding that cyber-attackers have the ability to extract 2 GB (gigabyte) of digital files, for example, e-books from the internet, which amounts to an estimated 8 000 paperback books in the physical world.[204] Thus, one can understand the reach of cybercrime.

The fifth element, the speed of the crime refers to the timeframe in which the crime was committed.[205] This timeframe includes the administration and preparation of the cybercrime and starts at the first engagement of the criminal activity and ends when the crime is committed.[206] For example,[207] a cybercrime can be conducted at a maximum speed because a skilful cyber-attacker has the ability to instantaneously launch a software code which targets multiple websites in less than a minute, whereas traditional crimes take a few minutes or even a few hours to be diligently conducted without the criminal getting caught or being arrested.[208]

Another element to consider when distinguishing cybercrime from traditional crimes would be the consequences of the crime.[209] The consequences of cybercrime tend to linger longer after the committed crime than the consequences of a traditional crime.[210] For example, if a cyber-attacker posts explicit images of an individual online, those images can

---

203 PGI 2018 https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/.

204 PGI 2018 https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/.

205 Mukherjee 2023 https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/#:~:text=Cybercrimes%20include%20phishing%2C%20hacking%2C%20spoofing,%2C%20i.e.%2C%20mainly%20offline%20crimes.

206 Mukherjee 2023 https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/#:~:text=Cybercrimes%20include%20phishing%2C%20hacking%2C%20spoofing,%2C%20i.e.%2C%20mainly%20offline%20crimes.

207 Mukherjee 2023 https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/#:~:text=Cybercrimes%20include%20phishing%2C%20hacking%2C%20spoofing,%2C%20i.e.%2C%20mainly%20offline%20crimes.

208 Mukherjee 2023 https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/#:~:text=Cybercrimes%20include%20phishing%2C%20hacking%2C%20spoofing,%2C%20i.e.%2C%20mainly%20offline%20crimes.

209 Leukfeldt and Malsch 2019 https://nscr.nl/en/gevolgen-cybercrime-zeer-ingrijpend-voor-slachtoffers/.

210 Mukherjee 2023 https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/#:~:text=Cybercrimes%20include%20phishing%2C%20hacking%2C%20spoofing,%2C%20i.e.%2C%20mainly%20offline%20crimes.

be disseminated in the online environment at an accelerated rate.[211] Although the dissemination of these explicit images can take place indefinitely, these images can, regardless of the period of time, be successfully removed from the online environment by a qualified computer forensic investigator;[212] however, there is always the possibility that the cyber-attacker might post these images again.[213] Therefore, cyber-victims tend to fear the lingering consequences of a cyber-offence.[214]

The last element to consider is the national capacity of a country's cyber-infrastructure to properly report, address, investigate and prosecute cybercrime.[215] Many cyber-experts believe that national authorities such as the police forces neglect to prepare, educate and train themselves for the impact and effect cybercrime has on natural and juristic persons.[216] Cyber-experts continue to discuss the situation regarding the fact that the national police force fail to implement or receive the adequate training necessary for the cyber-field as the national police often consider cybercrime too broad and complex to be addressed and investigated by any general police force.[217]

Regarding traditional crime infrastructure,[218] there appear to be numerous pieces of adequate legislation and frameworks available in various countries along with their qualified national authorities being able and willing to successfully convict criminals of any traditional crime.[219] Although cybercrime and traditional crimes are distinguishable as discussed, what South Africa and the rest of the world find worrisome is the fact that more traditional crimes are being committed through the active use of smart devices in the online environment.[220] Therefore, an international critical question arises: Where is the

---

211 Leukfeldt and Malsch 2019 https://nscr.nl/en/gevolgen-cybercrime-zeer-ingrijpend-voor-slachtoffers/.

212 According to Lutkevich 2021 at https://www.techtarget.com/searchsecurity/definition/computer-forensics, "Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.".

213 Leukfeldt and Malsch 2019 https://nscr.nl/en/gevolgen-cybercrime-zeer-ingrijpend-voor-slachtoffers/.

214 Leukfeldt and Malsch 2019 https://nscr.nl/en/gevolgen-cybercrime-zeer-ingrijpend-voor-slachtoffers/.

215 Leukfeldt and Malsch 2019 https://nscr.nl/en/gevolgen-cybercrime-zeer-ingrijpend-voor-slachtoffers/.

216 Leukfeldt and Malsch 2019 https://nscr.nl/en/gevolgen-cybercrime-zeer-ingrijpend-voor-slachtoffers/.

217 Leukfeldt and Malsch 2019 https://nscr.nl/en/gevolgen-cybercrime-zeer-ingrijpend-voor-slachtoffers/.

218 Prakash 2018 *IJPAM* 1456.

219 Leukfeldt and Malsch 2019 https://nscr.nl/en/gevolgen-cybercrime-zeer-ingrijpend-voor-slachtoffers/.

220 Mukherjee 2023 https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/#:~:text=Cybercrimes%20include%20phishing%2C%20hacking%2C%20spoofing,%2C%20i.e.%2C%20mainly%20offline%20crimes.

legal distinction drawn between committing a cybercrime or committing a traditional crime (assisted by the use of smart devices) in the online environment?[221]

Cybercrime has become the pinnacle point of an international concern for numerous countries.[222] For countries the best possible reaction and response is to strategically develop and implement cybersecurity measures and cyber-policies in order to combat cybercrime.[223] However,[224] countries such as South Africa still appear to be in the early stages of developing and implementing cybercrime legislation as they are yet to be informed and educated by various seminars, conventions and legislation in order to understand the sophisticated nature of cybercrime.[225] South Africa has been on top of the list regarding cybercrime and started to confront this pressing matter through cooperation between the government, the private and public sector, and various organisations.[226] South Africa also considered the policies of the NCPF and the Budapest Convention.[227]

South Africa has also established numerous cybercrime emergency response teams and enhanced the cyber-infrastructure of ICTs by adjusting its safety perimeter in an attempt to address and combat cybercrime and its consequences.[228] According to Steve Morgan,[229] the Editor-in-Chief at Cybercrime Magazine,[230] an international organisation operating under Cybersecurity Ventures,[231] the global impact and cost of cybercrime will reach a considerable number between a billion and a trillion dollars by the end of 2025; Cybercrime Magazine continued by stating,[232]

> "This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from

---

221 Mukherjee 2023 https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/#:~:text=Cybercrimes%20include%20phishing%2C%20hacking%2C%20spoofing,%2C%20i.e.%2C%20mainly%20offline%20crimes.

222 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 29.

223 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 29.

224 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 29.

225 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 29.

226 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 29.

227 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 29.

228 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 29.

229 Morgan 2022 https://cybersecurityventures.com/our-company/.

230 Morgan 2022 https://cybersecurityventures.com/our-company/.

231 Cybersecurity Ventures is an international researcher and publisher focused on the global cyber economy.

232 Von Solms 2022 https://theconversation.com/five-things-south-africa-must-do-to-combat-cybercrime-186089.

natural disasters in a year and will be more profitable than the global trade of all major illegal drugs combined."[233]

Considering that South Africa has made remarkable strides towards developing and addressing cybercrime,[234] South Africa still appears to be facing various challenges regarding the development and implementation of cybercrime legislation.[235] These challenges include,[236] the detection and identification of cybercrime, the reporting of cybercrime, cyber-investigation procedures, prosecution procedures and the most effective manner in combatting cybercrime.[237] The first challenge is the detection and identification of cybercrime.[238] Numerous individuals, organisations and governments regularly encounter cybercrime and the threat it holds.[239] National authorities and police forces often struggle to immediately respond to cybercrime due to the slow detection and report rate of cybercrime in South Africa.[240]

Firstly, these national authorities and police forces need to understand cybercrime and the manner in which cybercrime is committed in order to detect, identify and report cybercrime.[241] Secondly, cyber-experts explain that the establishment of a cooperative cybersecurity strategy from the country's public and private sector, the SAPS, and the government authorities will be the foundation of South Africa responding to the detection and reporting of cybercrime.[242] Cyber-experts continue by informing and urging individuals, organisations and the government to not abstain from using antivirus software programmes as well as other types of security software, for example firewalls, as these types of applications and software programmes are internationally applied to detect and combat cybercrime on smart devices.[243]

The second challenge: The cyber-investigation procedures refer to the procedure after a cybercrime has been committed and the victim has reported it to their national or local

233 Morgan 2022 https://cybersecurityventures.com/our-company/; Von Solms 2022 https://theconversation.com/five-things-south-africa-must-do-to-combat-cybercrime-186089.
234 Sutherland 2017 *AJIC* 88.
235 Sutherland 2017 *AJIC* 84.
236 Dlamini and Mbambo 2019 *ISSN* 6.
237 Dlamini and Mbambo 2019 *ISSN* 6.
238 Dlamini and Mbambo 2019 *ISSN* 6.
239 Dlamini and Mbambo 2019 *ISSN* 6.
240 Dlamini and Mbambo 2019 *ISSN* 6.
241 Dlamini and Mbambo 2019 *ISSN* 6.
242 Sutherland 2017 *AJIC* 84.
243 Sutherland 2017 *AJIC* 84; Dlamini and Mbambo 2019 *ISSN* 6.

authorities.[244] This procedure involves the victim, the targeted smart device, the cyber-attacker's digital footprint and the evidence of the cybercrime.[245] Cyber-victims are often reluctant or too uneducated to report a cybercrime immediately after it occurs, leaving a space of progressive delay in the investigation procedure which makes it more difficult to address the cybercrime.[246] Another element to consider regarding delaying the investigation procedure is the targeted smart device, such as the computer involved;[247] this computer can fail to operate effectively or be destroyed by a virus and compromise evidence needed in the cyber-investigation.[248]

The third challenge is effectively combatting cybercrime.[249] The forms of cyber-attacks and cybersecurity threats are increasing, which ultimately means that individuals, organisations, and the government must improve and adapt their cybersecurity defences regularly to assist in effectively combatting cybercrime.[250] To effectively detect and combat cybercrime, individuals, organisations and the government must consider implementing the following methods:[251] Advanced security technology software, undertaking ICT risk-assessments, implementing digital preservation software, secure firewalls and antivirus programmes, implementing intrusion and detection software, applying ID content, running cyber-intelligence and cyber-surveillance and finally, implementing monitoring network systems.[252]

With the implementation of the above-mentioned methods, the national legislature of South Africa will be greatly assisted in combatting, promulgating and developing adequate cybercrime legislation.[253] Hence,[254]

> "Cyber forensic investigators can detect an intrusion irrespective of the level or criminal intent of the cyber-attack, they can also make use of an existing live connection from a suspect's device to counter attacks by deflecting, disrupting or infecting the attacking device(s) irrespective of the criminal's location."[255]

---

244 Sutherland 2017 *AJIC* 84; Dlamini and Mbambo 2019 *ISSN* 6.
245 Dlamini and Mbambo 2019 *ISSN* 6.
246 Sutherland 2017 *AJIC* 85.
247 Sutherland 2017 *AJIC* 85.
248 Sutherland 2017 *AJIC* 85.
249 Dlamini and Mbambo 2019 *ISSN* 6.
250 Sutherland 2017 *AJIC* 84.
251 Dlamini and Mbambo 2019 *ISSN* 7.
252 Dlamini and Mbambo 2019 *ISSN* 7.
253 Dlamini and Mbambo 2019 *ISSN* 7.
254 Dlamini and Mbambo 2019 *ISSN* 7.
255 Dlamini and Mbambo 2019 *ISSN* 7.

However, the challenge of implementing these methods to combat cybercrime are considered costly; natural and juristic persons often lack the sufficient financial resources for it to be implemented and be successful.[256] Additionally, most natural and juristic persons are convinced that they do not appear profitable enough to fall victim as a beneficial target for cyber-attackers, thus making the mistake of not implementing any cybersecurity technology software or monitoring network systems.[257] According to Van Niekerk[258] and Sutherland,[259] unless the South African government declares it mandatory or law for natural and juristic persons to report cybercrime immediately after it occurs, the difficulty of conducting in-depth assessments of the compositions of these cyber-activities will be considered inaccurate.[260]

Sutherland[261] continue by adding that the national awareness of cybercrime and cybersecurity would receive the attention they deserve when individuals, organisations or the government can be held legally liable for refusing to report a cybercrime or cyber-incident.[262] Cybercrime is often left unreported by numerous individuals and organisations considering the uncertain position and restricted cyber-capacity of national authorities, for example, the SAPS, regarding the evolutionary cyberspace, its consequences and its prosecution procedures.[263]

2.2 The Different Types of Cybercrime

From the first officially recorded computer virus called "The Morris Worm",[264] created in the 1980's, cybercrime and cyber-attacks only became more sophisticated and complex in the cyberspace.[265] Today, cybercrime and cyber-attacks are considered extremely advanced crimes unravelling in abundance due to the reliant factor of the ever expanding online environment.[266] Considering the borderless nature of cybercrime and cyber-attacks,

256 Dlamini and Mbambo 2019 *ISSN* 7.
257 Dlamini and Mbambo 2019 *ISSN* 7.
258 Van Niekerk 2017 *AJIC* 128.
259 Sutherland 2017 *AJIC* 85.
260 Van Niekerk 2017 *AJIC* 128.
261 Sutherland 2017 *AJIC* 85.
262 Sutherland 2017 *AJIC* 85.
263 Sutherland 2017 *AJIC* 85.
264 According to the Federal Bureau of Investigation 2018 at https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218, the Morris Worm was a malicious computer program with the objective of infiltrating computer operating systems, which caused delays and other hindrances with operating systems.
265 Smiley 2019 https://blog.thinkreliability.com/case-study-the-morris-worm-brings-down-the-internet.
266 Townsend 2022 https://www.securityweek.com/cyber-insights-2022-improving-criminal-sophistication/.

the nature of the online environment makes it almost impossible for national law enforcement and cybersecurity organisations or cyber-resources to track down and pinpoint the exact moment, nature and characteristics of the committed cybercrime and the cyber-criminal behind it.[267]

In order to properly identify, detect and discuss the most common types of cybercrime in the online environment, a taxonomy is the best recommended method to present the extensive list.[268] A taxonomy can be defined as a simplified technique or method to reduce the complexity of a specific knowledge domain along with its distinct elements or factors,[269] in this context, cybercrime and cyber-attacks are the main knowledge domain.[270] Cybercrime can be broadly classified into the following three main categories:[271] Cybercrime against individuals, cybercrime against society, and cybercrime against organisations.[272] Examples of the three main categories will follow.

The first main category,[273] cybercrime against individuals, can be divided into two sub-categories, i.e. the individual, or the property of the individual.[274] Cybercrime against the individual refers to the individual as the target; this often includes email harassment, dissemination of personal information or data, unauthorised computer access, defamation and incident exposure.[275] Cybercrime against the property of the individual often includes fraud, computer vandalism, unauthorised access to the computer or the computer's operating system, intellectual property crimes, and the transmission of viruses and worms.[276] The second main category,[277] cybercrime against society directly affects individuals or society as a whole; this includes government terrorism, pornography, forgery, trafficking, illegal online sales, and financial thefts.[278]

---

267 Townsend 2022 https://www.securityweek.com/cyber-insights-2022-improving-criminal-sophistication/.
268 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 30.
269 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 30.
270 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 30.
271 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
272 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
273 Coolidge 2021 https://coolidgelawfirmaz.com/what-are-the-major-types-of-cybercrime/.
274 Coolidge 2021 https://coolidgelawfirmaz.com/what-are-the-major-types-of-cybercrime/.
275 Coolidge 2021 https://coolidgelawfirmaz.com/what-are-the-major-types-of-cybercrime/.
276 Coolidge 2021 https://coolidgelawfirmaz.com/what-are-the-major-types-of-cybercrime/.
277 Coolidge 2021 https://coolidgelawfirmaz.com/what-are-the-major-types-of-cybercrime/.
278 Coolidge 2021 https://coolidgelawfirmaz.com/what-are-the-major-types-of-cybercrime/.

The third main category,[279] cybercrime against organisations, often includes unauthorised access and control over an organisation's website or their computer operating systems, the distribution of pirated system-software in the organisation's network system and lastly, the unlawful possession of confidential information or data.[280] The most severe type of cybercrime in the third category is cyber-terrorism; this is a cybercrime committed against a country's government, a government organisation or a government department.[281] This type of cybercrime is considered as the utmost form of misconduct,[282] and is a global concern for numerous countries and governments.[283]

The devastating consequences of this specific type of cybercrime has the world in quite an uproar as to what the future in cyber-terrorism might hold.[284] Cyberterrorism can be defined as an unlawful intentional series of disruptive activities, or the possible threat thereof, in the cyberspace or online environment to alter or intimidate the religious, social, political and ideological ideas and objectives of a country.[285] The cyber-attacker, referred to as the cyber-terrorist, is often an individual who inflicts publicised violence, causes an abrupt disruption of government services, or strives to cause damage to any property with the main objective of inducing fear in society, disrupting the harmony between different groups of citizens, coercing the country's established government or endangering the integrity of the country.[286]

Nevertheless, this discussion does not present a complete list of the different types of cybercrime and cyber-attacks, but is merely a brief overview of the most commonly recorded cybercrimes: Currently, the latest cybercrime in South Africa appears to be committed through emails and electronic messaging.[287] This includes phishing attacks, email bombing, email harassment and email spoofing.[288] Phishing attacks are quite similar

279 Ellerbeck 2022 https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business/.
280 Ellerbeck 2022 https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business/.
281 Ellerbeck 2022 https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business/.
282 Sheldon and Hanna 2022 https://www.techtarget.com/searchsecurity/definition/cyberterrorism.
283 Sheldon and Hanna 2022 https://www.techtarget.com/searchsecurity/definition/cyberterrorism.
284 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
285 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
286 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
287 Domains 2022 https://companies.mybroadband.co.za/domains/2022/11/01/cybercrime-in-south-africa-what-every-sme-needs-to-know/.
288 Domains 2022 https://companies.mybroadband.co.za/domains/2022/11/01/cybercrime-in-south-africa-what-every-sme-needs-to-know/.

to social engineering[289] and operate mainly via malicious emails, links or websites with the objective of completely deceiving a victim into sharing confidential information or persuading the victim into clicking on the malicious email, link or website posted or distributed by the cyber-attacker.[290]

The cyber-attacker then gains unauthorised access through the victim's computer system, in searching data, files, or confidential information such as login credentials in order to threaten or blackmail the victim.[291] Email bombing can be defined as the criminal activity of sending a large number of email spam to an individual or organisation's computer which can result in their mail server-system malfunctioning or completely crashing.[292]

The next two types of cybercrime are email harassment and cyber-stalking.[293] Email harassment and cyber-stalking are not considered new cyber-concepts as both of the criminal activities involve harassment and stalking that can take place in any form, on-/ or offline.[294] This typically refers to harassment via emails or electronic messaging which often results in blackmailing or threatening a victim.[295] Cyber-stalking involves trailing and monitoring an individual's online movements (or digital footprint) which ultimately leads to harassment and blackmailing.[296]

Email spoofing is directly linked to misrepresentation and identity fraud.[297] This cybercrime fabricates its attack based on a disguised or misrepresented origin which appears legitimate but carries a virus or worm ready to infiltrate a smart device or network

---

289 According to Jansen van Rensburg in *The human element in information security: An analysis of social engineering attacks in the greater Tswane area of Gauteng, South Africa*, "Within the scope of information security, social engineering entails a type of attack against the human element during which the perpetrator induces the victim to release information or perform unauthorised actions.".

290 Domains 2022 https://companies.mybroadband.co.za/domains/2022/11/01/cybercrime-in-south-africa-what-every-sme-needs-to-know/.

291 Jigsaw Academy 2022 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

292 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

293 Domains 2022 https://companies.mybroadband.co.za/domains/2022/11/01/cybercrime-in-south-africa-what-every-sme-needs-to-know/.

294 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

295 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

296 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

297 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

system.[298] Email spoofing and a phishing attack appear to be quite similar, however, the distinction drawn between the two is based on the target of the cybercrime and the manner in which it is conducted.[299] Other common types of cybercrime found in South African ICTs are ransomware attacks and hacking.[300]

Ransomware attacks are quite similar to phishing attacks and occur when a cyber-attacker gains unauthorised access via a phishing email or by exploiting a security breach or vulnerability on a smart device's system.[301] When the cyber-attacker gains access to the information, data, or files from the victim's smart device, they demand a financial ransom from the victim in order for the victim to gain access to their own files or data once again.[302]

The next common type of cybercrime is DDoS (distributed denial-of-service) attacks.[303] DDoS attacks tend to flood a smart device or a network system with multiple requests in order to slow down the operating system of the smart device or the network system and make it inaccessible to its users.[304] DDoS are often weaponized by cyber-attackers to infiltrate confidential documents, financial accounts, and financial statements of various organisations and firms.[305]

A Trojan attack, also known as a "Trojan Horse", is an unauthorised software programme representing itself as an authorised software programme in order to gain access and control over a smart device's operating system.[306] It also damages data and files on the smart device.[307] This type of cybercrime typically gains access through emails.[308]

---

298 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

299 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis; Domains 2022 https://companies.mybroadband.co.za/domains/2022/11/01/cybercrime-in-south-africa-what-every-sme-needs-to-know/.

300 Docrat 2022 https://isite.co.za/ransomware-attacks-south-africa/; Domains 2022 https://companies.mybroadband.co.za/domains/2022/11/01/cybercrime-in-south-africa-what-every-sme-needs-to-know/.

301 Docrat 2022 https://isite.co.za/ransomware-attacks-south-africa/.

302 Docrat 2022 https://isite.co.za/ransomware-attacks-south-africa/

303 Jigsaw Academy 2022 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

304 Jigsaw Academy 2022 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

305 Jigsaw Academy 2022 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

306 Jigsaw Academy 2022 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

307 Jigsaw Academy 2022 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

308 Jigsaw Academy 2022 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.

The next type of cybercrime is virus and worm-attacks.[309] Virus and worm-attacks are considered the most common type of cybercrime internationally.[310] Virus attacks are software programmes that attach and secure themselves to files, data, or network platforms in order to erase or alter files, data, or a network platform.[311] Worm-attacks however, do not attach or secure themselves to documents or files, but rather copy these documents or files to the smart device to reduce storage space on the smart device's available memory.[312]

Salami attacks are linked to financial crimes;[313] what makes this type of cybercrime appealing is that it occurs in a manner where the financial alteration is so small that it would be extremely difficult to notice on a daily scale;[314] for example, if a cyber-attacker hacks into a bank's networking system or account administration platform, they can deduct 50 cents from every bank account administered at the bank and transfer the funds into their personal bank account.[315]

Web-jacking is derived from the concept of "Hi-jacking" and occurs when a cyber-attacker gains access and control over an online website.[316] The cyber-attacker is then able to alter any information on the website, for example a contact number or banking details.[317]

Another very common type of cybercrime is intellectual property cybercrime.[318] Intellectual property cybercrime refers to natural and juristic persons being deprived of their property rights by a cyber-attacker.[319] A few common forms of intellectual property cybercrime are copyright infringement, software piracies and trademark violations.[320]

---

309 Jigsaw Academy 2022 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.
310 Latto 2020 https://www.avast.com/c-worm-vs-virus.
311 Latto 2020 https://www.avast.com/c-worm-vs-virus.
312 Latto 2020 https://www.avast.com/c-worm-vs-virus.
313 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
314 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
315 Jigsaw Academy 2022 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.
316 Jigsaw Academy 2022 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.
317 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
318 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
319 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
320 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.

The last common type of cybercrime is identity theft or fraud.[321] Identity theft or fraud takes place when a cyber-attacker steals a victim's online identity; this typically includes their name, surname, ID number or anything related to the victim to commit fraud or buy unauthorised products in the victim's name.[322]

The list of the different types of cybercrime continues to develop and evolve daily.[323] However, it appears that many countries and their governments are devoting themselves to ensure that national authorities are being educated and trained to be able to address and combat cybercrime in the most effective manner.[324]

2.3 Previous Position of Cybercrime in South Africa

2.3.1 The history of cybercrime in South Africa

According to national research conducted by Van Niekerk,[325] South Africa faced an inaccurate total number of fifty-four reported cyber-attacks from April 1994 until December 2016, excluding, of course, the number of unreported cyber-attacks due to the fact that South Africa did not have the appropriate cyber-reporting and assisting resources at the time.[326] Van Niekerk's national research revealed that most of these attacks were in the form of data exposure and financial theft.[327] Referring to another research report along with considering Van Niekerk's report,[328] an unbelievably low number of seventy-four reported cyber-attacks have been recorded in South Africa since January 2010 until December 2020, again, excluding the number of unreported cyber-attacks.[329]

In the writer's opinion, the above-mentioned reported cyber-statistics are considered inaccurate and impossible regarding the evolution and the rapid rate of cybercrime. However, it is important to acknowledge that not all cyber-incidents were reported, therefore leaving South African cyber-experts with inaccurate reports and statistics.[330] Nevertheless, the research reports' selective choice of cyber-attacks and cyber-incidents

321 Jigsaw Academy 2022 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/.
322 Borges 2019 https://securitytrails.com/blog/types-of-cyber-crime.
323 Borges 2019 https://securitytrails.com/blog/types-of-cyber-crime.
324 Borges 2019 https://securitytrails.com/blog/types-of-cyber-crime.
325 Van Niekerk 2017 *AJIC* 115.
326 Van Niekerk 2017 *AJIC* 115.
327 Van Niekerk 2017 *AJIC* 126.
328 Pieterse 2021 *AJIC* 4.
329 Pieterse 2021 *AJIC* 4.
330 Pieterse *Electronic Crime Unit* 7.

were based on South African individuals, organisations, and the government as well as the impact of these cyber-attacks, and the objective and manner in which they occurred.[331] These cyber-attacks were distinctly categorised in the following categories:[332] An incident type, the South African sector affected, the perpetrator type and the motivation for the cyber-attack.[333]

The research report concluded with an extensive list and brief discussion of the seventy-four high-profile reported cyber-attacks and presented a list of recommendations for South Africa in properly responding to cybercrime.[334] Cybercrime and cyber-attacks have been adversely affecting South Africa's national economy, public administration, and ICTs.[335] In 2016 an estimated number of 28 580 290 South Africans were recorded as actively partaking in the online environment and ICTs which was an estimated 52% of South Africa's national population.[336] South Africa has been the country with the most recorded cyber-attacks on the African continent and still continues to uphold the title.[337]

In 2021, the South African Banking Risk Information Centre (SABRIC) confirmed that the total number of recorded cybercrime losses in online banking increased by a remarkable 45%.[338] After that, South Africa was reviewed and established as the country with the third-highest number of cyber-victims along with presenting the grand total loss of ZAR 2 billion from cyber-attacks.[339] According to an international cybersecurity company, Surfshark,[340] the rate of cyber-victims in South Africa increased drastically over the last decade, from twelve victims per one million internet users in 2016 to fourteen victims in 2019 and fifty-one victims in 2020 during the Covid-19 pandemic.[341] The impact and effect

331 Pieterse 2021 *AJIC* 4.
332 Pieterse 2021 *AJIC* 4.
333 Pieterse 2021 *AJIC* 4.
334 Pieterse 2021 *AJIC* 17.
335 Pieterse *Electronic Crime Unit* 7.
336 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 5.
337 Sutherland 2017 *AJIC* 85.
338 BusinessTech 2022 https://businesstech.co.za/news/technology/639277/the-world-faces-a-cybercrime-catastrophe-including-south-africa/.
339 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 4.
340 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com.
341 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com.

the Covid-19 pandemic had on South Africa's infrastructure and national economy was considered catastrophic.[342]

The government along with President Cyril Ramaphosa declared a national state of disaster in South Africa and implemented various restrictions to flatten the infection-curve of the contagious Covid-19 disease.[343] These restrictions included a national lockdown demanding all social, economic, educational and organisational activities to be terminated, effective immediately along with restricting the travelling of South African citizens between different countries, cities and provinces.[344] Individuals, organisations and educational institutions instantly converted all operations to online platforms creating a social, work and educational infrastructure to continue with business.[345] Cyber-attackers took complete advantage of this opportunity and targeted multiple organisations, services, and agencies.[346]

The primary target of cyber-attackers in South Africa during the Covid-19 pandemic was financial institutions and services, for example, the South African banks.[347] Cyber-attackers were determined and focused on conducting illegal financial activities such as money laundering.[348] During the pandemic, numerous South African banks responded and implemented national educational platforms available for all clientele; these platforms presented safe online banking instructions, updated banking security protocols, descriptive reports regarding different cyber-attacks, the identification of false emails and warned clientele against phishing attacks.[349] The South African banks also referred distressed clientele to SABRIC to assist them in banking safely on-/ and offline.[350]

Another primary target was South Africa's healthcare service systems.[351] The majority of South Africa's healthcare service systems completely rely on- and operate from ICT platforms and e-healthcare services available 24/7 for their clientele and healthcare

342 Chigada and Madzinga 2021 *SAJIM* 1.
343 Chigada and Madzinga 2021 *SAJIM* 1.
344 Minnaar and Herbig 2022 *AC:AJCV* 155.
345 Minnaar and Herbig 2022 *AC:AJCV* 156.
346 Minnaar and Herbig 2022 *AC:AJCV* 156.
347 Chigada and Madzinga 2021 *SAJIM* 4.
348 Chigada and Madzinga 2021 *SAJIM* 4.
349 Chigada and Madzinga 2021 *SAJIM* 4.
350 Chigada and Madzinga 2021 *SAJIM* 4.
351 Minnaar and Herbig 2022 *AC:AJCV* 163.

personnel.[352] The Covid-19 pandemic exploited these ICT platforms and system services by overloading the resource centre's operating website, which resulted in leaving healthcare systems exposed and vulnerable against any type of cyber-attack.[353] The World Health Organisation (WHO) was also exposed to multiple malware, ransomware and phishing attacks during the pandemic and had to address and critically manage the release of personal information of four hundred and fifty patients after a WHO server was hacked into.[354]

The reason that healthcare service systems were and still continue to be high in demand by cyber-attackers is due to the records of personal information (names, numbers, etc.) and the opportunity to commit identity theft, fraud or credit card scams.[355] The defeat of healthcare services lies in the fact that, healthcare services are considered quite determined in settling the ransom of a cyber-attack due to the fact that healthcare sectors are adamant in recovering and protecting their healthcare systems and infrastructure.[356]

The last main target was the South African government and its operational aspects.[357] As mentioned, during the pandemic South Africa's government implemented a national lockdown and Parliament was forced to continue meetings and conferences via online communication platforms.[358]

These online platforms included Microsoft Teams, Zoom and Skype.[359] The online meetings and conferences conducted by Parliament were constantly under attack by cyber-attackers and exploited fears, propaganda, vulnerabilities and shared malicious information or comments regarding the South African government.[360] Parliament later implemented another online communication platform[361] to conduct business in a safe and secure manner.[362] Zoom, however, was later banned as an online communication platform

352 Minnaar and Herbig 2022 *AC:AJCV* 163.
353 Minnaar and Herbig 2022 *AC:AJCV* 163.
354 Chigada and Madzinga 2021 *SAJIM* 4.
355 Minnaar and Herbig 2022 *AC:AJCV* 160.
356 Minnaar and Herbig 2022 *AC:AJCV* 168.
357 Chigada and Madzinga 2021 *SAJIM* 5.
358 Minnaar and Herbig 2022 *AC:AJCV* 163.
359 Chigada and Madzinga 2021 *SAJIM* 5.
360 Chigada and Madzinga 2021 *SAJIM* 5.
361 The platform was not specified; Chigada and Madzinga 2021 *SAJIM* 5.
362 Chigada and Madzinga 2021 *SAJIM* 5.

by the United States and Taiwan in 2020.[363] In 2020, Accenture[364] released a cyber-threat landscape report discussing the general position of cybercrime statistics in South Africa.[365]

The report confirmed that South Africa experienced an acceleration of cyber-incidents in 2019, especially regarding internet service providers (ISPs), mobile banking applications, national electricity providers and ecommerce platforms.[366] The report discussed eight fundamental cyber-attacks which included amongst others, a South African pre-paid electricity provider, Garmin South Africa, South Africa's largest ISPs and several banks.[367] Accenture continued by discussing a list of reasons why South Africa appears on top of the list regarding cyber-attacks.[368] The list is not exclusive, but presents a general overview of the most remarkable reasons; It appears that South African organisations have a lower cyber-defence barrier,[369] various South African organisations lack in investing in appropriate cybersecurity[370] and there appears to be a lack of adequate national cybercrime legislation and law enforcement.[371]

The list continued by discussing the lack of cybercrime awareness and education resulting in inexperienced and vulnerable internet users[372] and mentioned the advanced risk exposure of organisations to multiple applications and software programmes.[373] Accenture concluded their report by mentioning and discussing a number of South Africa's fundamental cyber-attacks and provided recommendations on how South Africa is to appropriately combat cybercrime.[374] As mentioned above, over the past decade, South Africa has been battling with the threat of cybercrime and experienced numerous high-

363 Chigada and Madzinga 2021 *SAJIM* 5.
364 Accenture is an international multi-service technology company.
365 Mcanyana, Brindley and Seedat 2020 *Insight into the Cyberthreat Landscape in South Africa* 1.
366 Mcanyana, Brindley and Seedat 2020 *Insight into the Cyberthreat Landscape in South Africa* 3.
367 Mcanyana, Brindley and Seedat 2020 *Insight into the Cyberthreat Landscape in South Africa* 5.
368 Mcanyana and Brindley 2020 https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa.
369 Mcanyana and Brindley 2020 https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa.
370 Mcanyana and Brindley 2020 https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa.
371 Mcanyana and Brindley 2020 https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa.
372 Mcanyana and Brindley 2020 https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa.
373 Mcanyana and Brindley 2020 https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa.
374 Mcanyana, Brindley and Seedat 2020 *Insight into the Cyberthreat Landscape in South Africa* 10.

profile cyber-attacks.[375] These high-profile attacks started occurring in 2021 against South African capital organisations and had an adverse effect on the country's national economy, infrastructure and exporting services.[376]

An example of these capital organisations included Transnet, one of South Africa's biggest logistics companies, and the Department of Justice and Constitutional Development.[377] Nevertheless, it appears that cyber-attackers are progressively shifting their focus from targeting enterprise systems and network systems to targeting end-users,[378] this refers to personnel and employees (behind the computer) of a capital organisation or a national authority service who have access to and operate within the organisation's corporate files and networking systems.[379] South Africa's Department of Justice estimated that the cost of damage caused by these types of cyber-attacks on capital organisations or national authorities rounds up to ZAR 1 billion per year.[380]

Early in May 2022, TransUnion, a South African credit management company, was targeted by cyber-attackers located in Brazil.[381] The cyber-attackers stole 4 TB (terabyte) of data and 50 million personal credit records of South African citizens, and demanded ZAR 225 million as a ransom from TransUnion for retrieving the data;[382] President Cyril Ramaphosa was among the 50 million victims of this substantial cyber-attack.[383] The reported remarks regarding this cyber-attack stated that the cyber-attackers gained unauthorised access via end-users, and cyber-experts stated that the success of this

---

375 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com.

376 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com.

377 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com.

378 According to Rouse 2013 at https://www.techopedia.com/definition/610/end-user, an end-user refers to an individual or person that uses a smart device or computer, another way of explaining an end-user is referring to an individual as a consumer.

379 Von Solms 2022 https://theconversation.com/five-things-south-africa-must-do-to-combat-cybercrime-186089.

380 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 4.

381 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com.

382 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com.

383 Von Solms 2022 https://theconversation.com/five-things-south-africa-must-do-to-combat-cybercrime-186089.

cyber-attack was based on the lack of cyber-awareness and cybersecurity as well as uneducated personnel.[384]

In the case *Fourie v Van Der Spuy and De Jongh Inc.* 2019 JDR 1801 (GP) (hereafter the "*Fourie* case") acting Judge Klein discussed and commented on the promulgation and implementation of the *Cybercrimes Act* 19 of 2020 (hereafter the "*Cybercrimes Act*") and how the *Cybercrimes Act* is considered a "beacon of hope" for South Africa and its citizens regarding the position of cybercrime in the cyberspace.[385] The *Fourie* case primarily addressed and dealt with the false notion of intercepted online communication between an unknown third-party acting as Fourie (hereafter the "*Applicant*"), a client of Van Der Spuy and De Jongh Inc. law firm (hereafter the "*Respondent*"), and the online transfer of the *Applicant's* trust funds from the *Applicant's* bank account into another fraudulent bank account by the *Respondent* under the false online instruction from the unknown third-party purporting to be the *Applicant*.[386]

During the trial, the Supreme Court of Appeal (SCA) ruled that the *Respondent* failed to properly verify the correct online banking details and transfer instructions from the *Applicant* as it was found that the *Applicant's* email was hacked into by a cyber-attacker.[387] The *Applicant* suffered a major financial loss due to the false instructions, and the SCA found the *Respondent* negligent and ordered them to pay the loss suffered by the *Applicant* with interest.[388] The SCA continued by discussing the necessary skill, knowledge and diligence a practicing attorney must exercise when working with large sums of money regarding online transactions and transfers.[389]

Considering the potential prospect of the *Cybercrimes Act* in South African legislation as remarked in the *Fourie* case, it has to be acknowledged that South Africa has implemented various strategic cyber-interventions over the past few years through the Justice, Crime Prevention and Security Cluster (JCPS).[390] The JCPS Cluster is also in the process of

---

384 Von Solms 2022 https://theconversation.com/five-things-south-africa-must-do-to-combat-cybercrime-186089.

385 Bhangattjee, Govuza and Sebanz *Technology, Media & Telecommunications Alert* 3.

386 Bhangattjee, Govuza and Sebanz *Technology, Media & Telecommunications Alert* 2.

387 Bhangattjee, Govuza and Sebanz *Technology, Media & Telecommunications Alert* 2.

388 Bhangattjee, Govuza and Sebanz *Technology, Media & Telecommunications Alert* 2.

389 Bhangattjee, Govuza and Sebanz *Technology, Media & Telecommunications Alert* 3.

390 *National Cybersecurity Policy Framework For South Africa* 10; The JCPS is a South African security cluster made up by the Justice and Correctional Services and Defence, the Department of Home Affairs, Military Veterans and the Department of Police.

implementing cyber-interventions and cyber-resources to support South Africa in the fight against cybercrime.[391] The South African government encouraged the JCPS Cluster to sign the JCPS Delivery Agreement on 24 October 2010,[392] where this Delivery Agreement held that it is considered a requirement to develop and implement cybersecurity policies and regulations in South Africa and broaden the capacity for combatting and investigating cybercrime.[393]

Therefore, the National Cybersecurity Policy Framework (NCPF)[394] was implemented in 2015 by the Minister of State Security and the South African Cabinet.[395] The implementation of the NCPF acknowledged the lack of international and national cooperation within South African borders, and discussed the inadequate existing legal cybercrime measures and legislation available in South Africa.[396] The NCPF also remarked that cybersecurity challenges and the addressing thereof have a personal, national, and international nature.[397] One of the purposes of the NCPF is to create a reliable, safe and secure cyberspace in South Africa that supports the infrastructure of protecting information and network systems, whilst considering individuals' shared values, expectations and the comprehension of cybersecurity in national security imperatives.[398]

The key objectives of the NCPF are to establish and support cybercrime frameworks and policies, facilitate cooperation between individuals, organisations, and the government, promote international cyber-prevention cooperation, develop and promote South Africa's cybersecurity capacity, and promote the appropriate standards for cybersecurity in South Africa.[399] The National Cybersecurity Hub was implemented along with the NCPF in 2015 to create cybersecurity awareness as well as facilitate and ensure secure information technology platforms for individuals and organisations as well as the government.[400] According to South Africa's national government Computer Security Incident Response Team (CSIRT), part of South Africa's State Security Agency (SSA), the Cybersecurity Hub

391 *National Cybersecurity Policy Framework For South Africa* 10.
392 Justice, Crime Prevention and Security Cluster (JCPS) Delivery Agreement, 24 October 2010.
393 *National Cybersecurity Policy Framework For South Africa* 10.
394 GN 609 in GG 39475 of 4 December 2015.
395 Pieterse *Electronic Crime Unit* 9.
396 Sutherland 2017 *AJIC* 91.
397 *National Cybersecurity Policy Framework For South Africa* 10.
398 *National Cybersecurity Policy Framework For South Africa* 14.
399 *National Cybersecurity Policy Framework For South Africa* 15.
400 Du Toit, Hadebe and Mphatheni 2018 *CRIMSA* 120.

also provides for a contact-based platform for all cyber-related matters and the reporting thereof.[401]

Examples of the type of members of the CSIRTs in South Africa are the First National Bank group and the Standard Bank group.[402] As for the objective of the Cybersecurity Hub, it has been declared that the,[403]

> "Cybersecurity Hub enhances interactions, consultations and promotes a coordinated approach regarding engagements with the private sector and civil society."[404]

South Africa's Directorate for Priority Crime Investigation (DPCI), also known as the "Hawks",[405] have identified cybercrime as a high-priority crime within South Africa's criminal justice system, and therefore, established the Electronic Crime Unit (ECU) and the Digital Forensic Laboratory (DFL) within the scope of the Directorate's Commercial Crime unit.[406] The main objective of the ECU is to prevent, combat and investigate any cyber-related matter occurring on an online financial platform.[407] The main objective of the DFL is to examine and analyse the technological instruments in relation to any organised crimes, on-/ or offline.[408] The mandate of the DCPI also includes to prevent, combat, and investigate national offences conducted in South Africa according to section 17A of the South African *Police Service Act* 68 of 1995 (hereafter the "*Police Act*").[409]

South Africa, however, has gone to extraordinary lengths in adopting, developing, and implementing national law statutes and frameworks regarding cybercrime.[410] For the purposes of this study, the following common law statutes will be discussed: The *Electronic Communications and Transactions Act* (hereafter the "*ECTA*")[411] is a statute promulgated and implemented in 2002 to address and facilitate all electronic communications, transactions and government ecommerce sites in South Africa.[412] The *ECTA* repealed the *Computer Evidence Act* 57 of 1983,[413] and addresses the establishment

401 Du Toit, Hadebe and Mphatheni 2018 *CRIMSA* 120.
402 Sutherland 2017 *AJIC* 90.
403 Du Toit, Hadebe and Mphatheni 2018 *CRIMSA* 120.
404 Du Toit, Hadebe and Mphatheni 2018 *CRIMSA* 120.
405 Pieterse *Electronic Crime Unit* 6.
406 Pieterse *Electronic Crime Unit* 6.
407 Pieterse *Electronic Crime Unit* 8.
408 Pieterse *Electronic Crime Unit* 8.
409 Pieterse *Electronic Crime Unit* 7.
410 Du Toit, Hadebe and Mphatheni 2018 *CRIMSA* 119.
411 *Electronic Communications and Transactions Act* 25 of 2002.
412 Heselman and Warren "Cyber Crime Influencing Business in South Africa" 256.
413 Heselman and Warren "Cyber Crime Influencing Business in South Africa" 256.

of a cyber-inspectorate, discusses numerous cyber-related crimes, such as unauthorised access and the interception of data and facilitates the procedures of online transactions.[414]

The *Regulation of Interception of Communications and Provision of Communication-Related Information Act* (hereafter the "*RICA*")[415] was also promulgated and implemented in 2002[416] and addressed the right to privacy, data retention, unlawful surveillance practices and the interception of any form of communication.[417] Along with the implementation of the *RICA*, numerous cyber-resources and committees, such as the Office for Interception Centres (OIC) and the National Communications Centre (NCC) were created.[418] *The Criminal Procedure Act* 51 of 1977 (hereafter the "*CPA*") will be partially discussed along with the *RICA*.

The first attempt of the *Protection of Personal Information Bill* [B9] (hereafter the "*Bill*") was promulgated and implemented in 2009, the *Bill* was later replaced by the *Protection of Personal Information Act* 4 of 2013 (hereafter the "*POPIA*")[419] implemented in 2013, but has yet to come into full effect since the announcement from the South African Cabinet of amending the 2013 *POPIA* in 2021.[420] The amendment will be discussed further on. The effect and impact of the *POPIA* was considered quite remarkable since the awareness of cybercrime and cybersecurity increased as well as the reporting of cybercrime in South Africa.[421]

The *Films and Publications Act* (hereafter the "*FPA*")[422] was first promulgated and implemented in 1996, with the main objective of addressing and facilitating the regulation of online commercial distribution, the rights and position of online distributors and the required procedure to properly distribute online content in South Africa.[423] However, the *FPA* was later amended and republished as the *Films and Publications Amendment Act* 11

414 Heselman and Warren "Cyber Crime Influencing Business in South Africa" 256.
415 *Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002.
416 Van Niekerk 2017 *AJIC* 115.
417 Sutherland 2017 *AJIC* 92.
418 Sutherland 2017 *AJIC* 97.
419 *Protection of Personal Information Act* 4 of 2013.
420 Van Niekerk 2017 *AJIC* 115.
421 Van Niekerk 2017 *AJIC* 127.
422 *Films and Publications Act* 65 of 1996.
423 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.

of 2019 (hereafter the "*FPAA*")[424] which was signed into national legislation by the Cabinet and the president and was published in the *Government Gazette* on 3 October 2019.[425] Considering the extensive administration process of the promulgated *Cybercrimes Act*, individuals, organisations, and the government are focused on combatting cybercrime in a lawful manner.[426]

The legislative process of the *Cybercrimes Act* started in 2015.[427] During the past five years the South African legislative branch of government endured continual objections, reviews and amendments which were at last accepted and signed by the president, and the *Cybercrimes Act* was formally introduced and implemented in December 2021.[428] According to Von Solms,[429] during the last few years the capacity of cybercrime exceeded illegal drug and firearm trafficking by alarming numbers.[430] Nonetheless, it appears that the ability to properly address and combat cybercrime in South Africa seems to lie not too far in the future given the recently implemented *Cybercrimes Act*.[431] However, the prevalence of various cyber-attacks can be expected to continue in the future.[432]

2.3 Present Position of Cybercrime in South Africa

As previously mentioned, cybercrime continues to have an adverse impact and effect on South Africa and the country's national infrastructure due to the evolutionary nature of the crime.[433] As the online environment becomes more established and heavily populated, the number of cybercrime cases and cyber-incidents rose and the challenge to properly combat and address it becomes more challenging.[434] Internationally, cybercrime is distinctly characterised as, (a) anonymous and, (b) borderless regarding countries' national and international frameworks and jurisdictions; this however, directly contributes

---

424 *Films and Publications Amendment Act* 11 of 2019.
425 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.
426 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com.
427 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com.
428 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com.
429 Professor Basie von Solms, Director of the Centre for Cyber Security at the University of Johannesburg.
430 BusinessTech 2022 https://businesstech.co.za/news/technology/639277/the-world-faces-a-cybercrime-catastrophe-including-south-africa/.
431 Sutherland 2017 *AJIC* 85.
432 Pieterse 2021 *AJIC* 17.
433 Dlamini and Mbambo 2019 *ISSN* 1.
434 Dlamini and Mbambo 2019 *ISSN* 1.

towards the challenge of identifying, detecting, investigating, and combatting cybercrime.[435]

According to Surfshark's report, Data Breach Impact Statistics,[436] 2% of national internet users tend to become a victim or target of cybercrime in South Africa through their online experience.[437] The research report also revealed that a number of ninety-seven South African citizens are deceived daily into sharing personal information online or tend to click on a malicious link, email or website while cyber-attackers tend to rely on this "human error" in order to gain access to their primary target.[438] In general, cyber-attackers tend to depend on this "human error" made by a cyber-victim regarding cybercrime.[439] This "human error" delivered the result of a shocking 82% chance of it being the reason for a cyber-breach.[440]

Cybercrime does not only affect South African citizens but it also adversely affects small and medium-sized enterprises or organisations (SMEs) through phishing attacks, ransomware attacks and DDoS attacks (distributed denial-of-service).[441] The reason for this is that organisations appear to have a limited financial security budget and the capacity to develop and implement safe ICTs as well as introduce courses regarding ICT skills, thus requiring support from the national government concerning cyber-resources.[442] The International Criminal Police Organisation (Interpol) has announced that, keeping in mind the challenges of SMEs and national websites, the South African government must be prepared to identify, address, and combat the upsurge in cyber-attacks on general career-exploring websites and job-hiring platforms.[443]

The Interpol working alongside the National Central Bureau (NCB) which is located in Pretoria, Gauteng issued this warning stating that they noticed many false reports and articles concerning Interpol regarding individuals exploring online career options

435 Dlamini and Mbambo 2019 *ISSN* 1.
436 Surfshark 2021 https://surfshark.com/research/data-breach-impact/statistics.
437 Surfshark 2021 https://surfshark.com/research/data-breach-impact/statistics.
438 Surfshark 2021 https://surfshark.com/research/data-breach-impact/statistics.
439 Surfshark 2021 https://surfshark.com/research/data-breach-impact/statistics.
440 Domains 2022 https://companies.mybroadband.co.za/domains/2022/11/01/cybercrime-in-south-africa-what-every-sme-needs-to-know/.
441 Domains 2022 https://companies.mybroadband.co.za/domains/2022/11/01/cybercrime-in-south-africa-what-every-sme-needs-to-know/.
442 Sutherland 2017 *AJIC* 99.
443 ITWeb 2023 https://www.itweb.co.za/content/8OKdWqDXg92qbznQ.

specifically connected to jobs advertised and available at the South African Interpol.[444] The Interpol added that these false reports and articles about jobs available at the Interpol inaccurately presented inflated salary figures and that the Interpol is an organisation undergoing lawful prescribed financial and recruitment procedures when hiring.[445] The Interpol continued by stating that any further investigation regarding the matter will be conducted by South Africa's leading agency in transitional police investigations, the SAPS.[446]

Considering career-exploring websites, BusinessTech,[447] a business news website in South Africa stated that cybercrime in the South African real estate industry is also causing quite the predicament.[448] Considering the nature of the real estate industry dealing with large sums of money, online transactions and transfers, cyber-attackers seem to have fixated their focus on exploiting the vulnerabilities of the real estate industry.[449] The real estate industry became an easy target for these fraudulent activities in the process of buying, selling and renting property.[450] According to Jackie Smith, the head of Buyers Trust,[451] the most common type of cybercrime the real estate industry has to face is when cyber-criminals often advertise a property online available to rent or buy, but the moment the lessee or buyer pays the first deposit or the amount owed, the cyber-criminal disappears along with the money.[452]

Another common type of cybercrime found in the real estate industry is phishing attacks.[453] With this cyber-attack, criminals access personal information about the lessor or lessee, for example, their banking details or credit card details, and hack into the transactions and transfers between the "company" and the client.[454] Smith continued to explain the importance of an "in-person" deposit and why the company, Buyers Trust,

444 ITWeb 2023 https://www.itweb.co.za/content/8OKdWqDXg92qbznQ.
445 ITWeb 2023 https://www.itweb.co.za/content/8OKdWqDXg92qbznQ.
446 ITWeb 2023 https://www.itweb.co.za/content/8OKdWqDXg92qbznQ.
447 BusinessTech 2022 https://businesstech.co.za/news/property/637305/south-africas-real-estate-industry-is-worried-about-this-type-of-crime/.
448 BusinessTech 2022 https://businesstech.co.za/news/property/637305/south-africas-real-estate-industry-is-worried-about-this-type-of-crime/.
449 BusinessTech 2022 https://businesstech.co.za/news/property/637305/south-africas-real-estate-industry-is-worried-about-this-type-of-crime/.
450 Dikgole 2022 https://www.moneyweb.co.za/news/south-africa/cyber-security-threats-to-real-estate/.
451 Dikgole 2022 https://www.moneyweb.co.za/news/south-africa/cyber-security-threats-to-real-estate/.
452 Dikgole 2022 https://www.moneyweb.co.za/news/south-africa/cyber-security-threats-to-real-estate/.
453 Dikgole 2022 https://www.moneyweb.co.za/news/south-africa/cyber-security-threats-to-real-estate/.
454 BusinessTech 2022 https://businesstech.co.za/news/property/637305/south-africas-real-estate-industry-is-worried-about-this-type-of-crime/.

recommends keeping the "human element" in the equation when large financial transactions are involved.[455] Numerous real estate agencies in South Africa face the threat of cybercrime in their daily transactions and transfers, therefore, Smith urges the real estate industry to take advanced cybersecurity measures and encourage in-person deposits for the safety of the company and the client.[456]

According to David Mahlobo,[457] the Minister of State Security in South Africa, cybersecurity is considered one of the top five strategic objectives the government and Department of State Security must enforce.[458] Mahlobo continued by stating that the department is also tasked with the improvement of the criminal justice system and the reduction of corruption.[459] Mahlobo further discussed cybersecurity with the objective to assist the process of cybercrime legislation; this list included,[460] the development of advanced security software, the use of hardware and monitoring computer systems, the implementation of a holistic approach regarding cybercrime, the responsibility of evaluating legislation, the spread of cybercrime and cybersecurity awareness and to educate internet users in the cyberspace and corporate espionage.[461]

Mahlobo continued by stating the rest of the department's objectives and priorities, being,[462] the enhancement of South Africa's cybersecurity capacity and infrastructure, the review and finalisation of national cybercrime legislation and regulations, the promotion of national and international cooperation on cyber-awareness, implementing partnerships with the African Union, the South African Development Community and SABRIC, and the establishment of a cyber-related centre, regarding the pressing issue of cybercrime and cybersecurity.[463]

The Council for Scientific and Industrial Research (CSIR) and the Special Investigating Unit (SIU) confirmed and signed their active partnership by a memorandum of understanding (MOU) in 2022 to assist in addressing and combatting cybercrime by the use of advanced

455 BusinessTech 2022 https://businesstech.co.za/news/property/637305/south-africas-real-estate-industry-is-worried-about-this-type-of-crime/.
456 BusinessTech 2022 https://businesstech.co.za/news/property/637305/south-africas-real-estate-industry-is-worried-about-this-type-of-crime/.
457 Mahlobo 2015 https://www.politicsweb.co.za/politics/on-cybersecurity-in-south-africa--david-mahlobo.
458 Mahlobo 2015 https://www.politicsweb.co.za/politics/on-cybersecurity-in-south-africa--david-mahlobo.
459 Mahlobo 2015 https://www.politicsweb.co.za/politics/on-cybersecurity-in-south-africa--david-mahlobo.
460 Mahlobo 2015 https://www.politicsweb.co.za/politics/on-cybersecurity-in-south-africa--david-mahlobo.
461 Mahlobo 2015 https://www.politicsweb.co.za/politics/on-cybersecurity-in-south-africa--david-mahlobo.
462 Mahlobo 2015 https://www.politicsweb.co.za/politics/on-cybersecurity-in-south-africa--david-mahlobo.
463 Mahlobo 2015 https://www.politicsweb.co.za/politics/on-cybersecurity-in-south-africa--david-mahlobo.

technology security services.[464] The CSIR and SIU confirmed in their partnership agreement that their main objective for collaborating is to actively invest in assisting South Africa in addressing and combatting cybercrime.[465] The agreement also stated that the use of these advanced technology services is to prohibit maladministration and online corruption in the online environment and that the partnership will encourage data analysis, digital forensics and investigation services and enhance cyber-infrastructure support.[466] Dlamini[467] commented on the agreement and said,[468]

> "The fight against corruption and cybercrime is a major issue in South Africa. Through this partnership, the CSIR will utilise its research competency to assist the SIU with technological solutions to tackle cybercrime. Our experts in data science, information security, as well as cybersecurity, blockchain and artificial intelligence, are ready to assist." [469]

As mentioned, the Budapest Convention[470] played a remarkable role in South Africa's journey regarding the development of cybercrime legislation and policies.[471] It is important to understand that although South Africa implemented the *Cybercrimes Act*, the Budapest Convention is still considered an international and relevant cyber-guideline to various countries, including South Africa.[472] The Budapest Convention continues to have an international influence in the online environment and cyberspace.[473] The treaty's main objective was to establish international cooperation between various countries regarding cybercrime.[474] South Africa signed and partially complied with the objectives of the treaty by starting to develop and address online criminal activities that amount to cybercrime.[475]

---

464 defenceWeb 2022 https://www.defenceweb.co.za/cyber-defence/siu-csir-collaborate-to-fight-cybercrime/.
465 defenceWeb 2022 https://www.defenceweb.co.za/cyber-defence/siu-csir-collaborate-to-fight-cybercrime/.
466 defenceWeb 2022 https://www.defenceweb.co.za/cyber-defence/siu-csir-collaborate-to-fight-cybercrime/.
467 Dr Thulani Dlamini is the Chief Executive Officer of the CSIR.
468 defenceWeb 2022 https://www.defenceweb.co.za/cyber-defence/siu-csir-collaborate-to-fight-cybercrime/.
469 defenceWeb 2022 https://www.defenceweb.co.za/cyber-defence/siu-csir-collaborate-to-fight-cybercrime/.
470 Council of Europe 2001 Convention on Cybercrime (ETS No. 185).
471 Dlamini and Mbambo 2019 *ISSN* 4.
472 Dlamini and Mbambo 2019 *ISSN* 4.
473 Dlamini and Mbambo 2019 *ISSN* 4.
474 Dlamini and Mbambo 2019 *ISSN* 4.
475 Dlamini and Mbambo 2019 *ISSN* 4.

South Africa also promulgated and implemented the *ECTA*[476] which fundamentally addressed and dealt with the specific requirements and elements of cybercrime found in the treaty.[477] However, the treaty was later criticised and reviewed for obligating the participating parties to enforce the treaty's specific requirements and elements and, due to the fact that law enforcement mechanisms differentiated in the various participating countries.[478] South Africa also signed but did not ratify the African Union Convention on Cyber Security and Personal Data Protection (AU Convention)[479] as only a few countries ratified it; therefore it was never enforced.[480]

Considering the implementation of the NCPF,[481] after the Budapest Convention, South Africa recognised that cybercrime and cybersecurity research and training has been severely neglected by natural and juristic persons.[482] Therefore the South African Cyber Security Academic Alliance (SACSAA) was created along with its acting branches, the University of South Africa, the Nelson Mandela University, and the University of Johannesburg.[483] The SACSAA is focused on acting as a centre for exclusive development research in cybersecurity and spreading cybersecurity awareness in South Africa.[484] Over the last years South Africa has been confronted by numerous challenges regarding cybercrime and the process of adopting and developing cybercrime legislation and regulations.[485]

However, the challenges South Africa has faced over the years are not considered unique, as numerous countries seem to have struggled when facing the exact same cyber-challenges.[486] It appears that the national legislature of South Africa has been struggling with the evolutionary upkeep of the development and implementation of cybercrime policies considering the rate and nature of cybercrime.[487] However, it is imperative to note that South Africa has been careful to implement various international conventions and policies regarding cybercrime due to the possibility of adversely affecting South Africans

476 *Electronic Communications and Transactions Act* 25 of 2002.
477 Dlamini and Mbambo 2019 *ISSN* 4.
478 Dlamini and Mbambo 2019 *ISSN* 4.
479 African Union Convention on Cyber Security and Personal Data Protection EX.CL/846.
480 Sutherland 2017 *AJIC* 92.
481 *National Cybersecurity Policy Framework for South Africa*.
482 Sutherland 2017 *AJIC* 100.
483 Sutherland 2017 *AJIC* 100.
484 Sutherland 2017 *AJIC* 100.
485 Dlamini and Mbambo 2019 *ISSN* 5.
486 Dlamini and Mbambo 2019 *ISSN* 5.
487 Dlamini and Mbambo 2019 *ISSN* 5.

constitutional rights.[488] And, according to Dlamini and Mbambo[489], it appears that several South African government departments fail to operate and participate in preventing and combatting cybercrime through the development and implementation of their own cyber-policies or security regulations.[490]

South Africa also battles with outdated policies and uneducated individuals, organisations and the government regarding cybercrime;[491] however, it appears that the public and private sectors of South Africa decided to start cooperating with the policing of cybercrime by spreading cyber-awareness in the country.[492] Therefore, it is quite evident that South African cybercrime legislation is definitely in the process of being promulgated, amended and implemented to properly recognise, understand and address the cyberspace and cybercrime considering the paramount importance of the recently passed *Cybercrimes Act*.[493]

488 Dlamini and Mbambo 2019 *ISSN* 5.
489 Dlamini and Mbambo 2019 *ISSN* 5.
490 Dlamini and Mbambo 2019 *ISSN* 5.
491 Dlamini and Mbambo 2019 *ISSN* 5.
492 Dlamini and Mbambo 2019 *ISSN* 5.
493 Du Toit, Hadebe and Mphatheni 2018 *CRIMSA* 119.

Chapter 3 Previous Cybercrime Legislation in South Africa

3 The History of Cybercrime Legislation

3.1. Introduction

It is important to acknowledge and understand that South Africa has established numerous attempts in combatting and addressing cybercrime in the past.[494] As mentioned, these attempts included the establishment of various clusters,[495] several departments,[496] pieces of legislation, and policies[497] as well as agencies and centres,[498] all with the common interest and objective of addressing and combatting cybercrime.[499] Regardless, the South African cyberspace still continued to produce several challenges.[500] These challenges included the increased number of daily internet users and the evolution of sophisticated technology and progressive ICTs.[501]

The evolution of South African cybercrime legislation and frameworks date to the signing of the Budapest- and AU Conventions, the implementation of the NCPF, the *Constitution of the Republic of South Africa*, 1996 (hereafter the "*Constitution*") and various pieces of national law statutes.[502] South Africa's journey regarding cybercrime legislation and policies started with the Council of Europe's Convention on Cybercrime (23 November 2001), also known as the Budapest Convention.[503] The Budapest Convention was the first relevant international legal instrument passed in 2001, addressing the cyberspace as well as cybercrime, but only came into force in 2004.[504] As mentioned above, South Africa signed the Budapest Convention, but did not ratify it.[505]

The Budapest Convention mainly addresses the criminalisation of cybercrime involving smart devices, such as a computer, either used as a subject or an object to a crime.[506]

---

494 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 29.
495 For example, the Justice, Crime Prevention and Security Cluster Cybersecurity Response Committee.
496 For example, the Justice and Constitutional Development.
497 For example, the Regulation of Interception of Communications and Provision of Communication-related Information Act and the National Cybersecurity Policy Framework.
498 For example, the State Security Agency and the South African Police Service.
499 Sutherland 2017 *AJIC* 88.
500 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 29.
501 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 29.
502 Sutherland 2017 *AJIC* 88.
503 Sutherland 2019 https://www.itweb.co.za/content/lwrKxv3JLOJqmg1o.
504 Sutherland 2019 https://www.itweb.co.za/content/lwrKxv3JLOJqmg1o.
505 Sutherland 2019 https://www.itweb.co.za/content/lwrKxv3JLOJqmg1o.
506 Sutherland 2019 https://www.itweb.co.za/content/lwrKxv3JLOJqmg1o.

The Budapest Convention aims to provide criminal procedure legislation in assisting the detection and investigation of cybercrime.[507] The Budapest Convention also assists in the collection, evaluation and preservation of electronic evidence regarding cybercrime, and it encourages international cooperation between various countries and governments in effectively combatting cybercrime.[508] The Budapest Convention also discussed a list of various cyber-offences, including illegal access and data interferences.[509]

Considering the fact that South Africa only signed the Budapest Convention, it is not required of South Africa to implement the Budapest Convention's regulations just yet; however, South Africa did react to it by implementing the *Electronic Communications and Transactions Act* 25 of 2002 (hereafter the "*ECTA*").[510] The next convention South Africa considered was the African Union Convention on Cyber Security and Personal Data Protection (AU Convention).[511] The AU Convention was originally drafted in 2011, but was only adopted a few years later in 2014.[512] Although South Africa signed the AU Convention, it did not ratify it.[513] The AU Convention primarily defines the objective of having a legal cybercrime framework regarding the standard proceedings of information and telecommunication technologies.[514]

It also encourage the implementation of legal procedural measures regarding cybercrime and the investigation thereof.[515] The AU Convention also establishes and delegates the authority of forensic investigators and sets out the prosecution procedures.[516] And finally, the AU Convention redefines the objectives of existing national cybercrime legislation, it encourages the mobilization of all national public and private sectors for the promotion of cybercrime and cybersecurity, and also establishes strict regulatory cybercrime and

---

507 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 55.

508 Seger 2016 https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/#:~:text=The%20Budapest%20Convention%20is%20a,more%20effective%20and%20subject%20to.

509 Sutherland 2019 https://www.itweb.co.za/content/lwrKxv3JLOJqmg1o.

510 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 56.

511 African Union Convention on Cyber Security and Personal Data Protection EX.CL/846.

512 NATO Cooperative Cyber Defence Centre of Excellence 2020 https://ccdcoe.org/organisations/au/.

513 Sutherland 2017 *AJIC* 92.

514 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 54.

515 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 54.

516 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 54.

cybersecurity frameworks along with the advanced protection of personal data considering the fundamental rights of citizens in different countries.[517] In brief, the AU Convention specifically focused on the three main areas of electronic transfers and transactions, personal data protection and cybersecurity.[518]

The next South African cybercrime framework, as thoroughly discussed in Chapter 2, is the NCPF.[519] The main objectives of the NCPF are to address, regulate and support cybercrime and cybersecurity irregularities in South Africa, encourage and facilitate national and international cooperation between different countries, and to develop and promote appropriate cybersecurity frameworks as well as update substantive and procedural laws regarding cybercrime in different countries.[520] Although the NCPF was reviewed and criticized for being too broad and vague without mentioning specific implementation strategies, the NCPF was considered as a fundamental blueprint for the development of South African cybercrime legislation, considering South Africa's limited cyber-capacity to properly address and respond to cybercrime.[521]

As for the effect and impact of the *Constitution* on the common law, the development and implementation of the common law is often quite restricted to a certain extent considering the supremacy of the *Constitution* in which the Bill of Rights (chapter 2) is contained.[522] The *Constitution* strives to uphold and protect these fundamental rights of South African citizens.[523] However, considering the law of general application, the fundamental rights of South African citizens can be limited if the common law is found distinctly reasonable and justifiable in democratic society.[524] At times, some of these rights envisaged in Chapter 2 restrict the very objective of the common law; these rights include the right to privacy (section 14) and the right of access to information (section 32).[525]

Section 14 of the *Constitution* states,[526]

---

517 African Union Convention on Cyber Security and Personal Data Protection 1-2.
518 African Union Convention on Cyber Security and Personal Data Protection 1-2.
519 *National Cybersecurity Policy Framework For South Africa*.
520 *National Cybersecurity Policy Framework For South Africa* 15.
521 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 37.
522 Sutherland 2017 *AJIC* 94.
523 Sutherland 2017 *AJIC* 94.
524 For example, section 36 of the *Constitution*; Molwanta *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 34.
525 Sutherland 2017 *AJIC* 94.
526 Section 14 of the *Constitution of the Republic of South Africa*, 1996 (hereafter the "*Constitution*").

Everyone has the right to privacy, which includes the right not to have –

(a) their person or home searched;
(b) their property searched;
(c) their possessions seized; or
(d) the privacy of their communications infringed.[527]

Whereas section 32 of the *Constitution* states,[528]

(1) Everyone has the right of access to –
    (a) any information held by the state; and
    (b) any information that is held by another person and that is required for the exercise or protection of any rights.
(2) National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.[529]

Although section 14 mentions the word "communications" as is, it is considered quite challenging to apply this section to a specific national law statute as the matter of the cyberspace still needs to be thoroughly introduced and discussed in the South African legislature.[530] However, for section 32 (access to information) of the *Constitution*, the *Promotion of Access to Information Act* 2 of 2000 was passed to assist in regulating section 32 accordingly.[531] Nevertheless, the relation between the *Constitution* and the *Cybercrimes Act* 19 of 2020 (hereafter the "*Cybercrimes Act*") will be discussed in chapter 4. The following discussion will primarily focus on the position of five previous South African cybercrime statutes.

However, an important principle to consider regarding the South African law of general application is the subsidiarity principle.[532] The subsidiarity principle is based on and gives legal effect to the South African courts in deciding which type of South African piece of legislation must be applied to the specific case presented before the court to ensure the most lawful outcome.[533] This type of legislation includes either a constitutional provision, parliamentary legislation or a common law provision.[534] The subsidiarity principle provides

527 Section 14 of the Constitution.
528 Section 32 of the *Constitution*.
529 Section 32 of the Constitution.
530 Van der Merwe *et al Information and Communications Technology Law* 26.
531 Van der Merwe *et al Information and Communications Technology Law* 27.
532 Nkanyane *Subsidiarity in the Context of Administrative Law* 4-10.
533 Nkanyane *Subsidiarity in the Context of Administrative Law* 4-10.
534 Nkanyane *Subsidiarity in the Context of Administrative Law* 4-10.

a legal framework available to courts to assist in the identification of the type of legislation that will appropriately govern the litigation procedure regarding the infringed right.[535]

The subsidiarity principle also entails that when enacted legislation gives effect to specific constitutional rights, the matter regarding the constitutional right must be adjudicated with specific reference to the enacted legislation rather than considering the provisions of the *Constitution* or the common law.[536] Considering the fundamental significance of section 14 and section 32 envisaged in the *Constitution*, it is important to acknowledge that these sections have to be considered in relation to the restrictive element regarding common law practices.[537]

3.2 Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

The *Regulation of Interception of Communications and Provision of Communication Related Information Act* 70 of 2002 (hereafter the "*RICA*") is considered one of the key cybercrime statutes which South Africa implemented after the NCPF was introduced.[538] The *RICA* was assented to on 30 December 2002[539] and was signed into law and implemented on 30 September 2005.[540] The *RICA* repealed the former *Interception and Monitoring Prohibition Act* 127 of 1992.[541] The primary objective of the *RICA* is found in the name: To address, prohibit and regulate the unlawful interception or monitoring of direct or indirect communication[542] and communication-related information.[543] The *RICA* also addresses the procedure of surveillance regarding direct or indirect communication systems and the collection of information through electronic communications or ICTs.[544]

---

535 Nkanyane *Subsidiarity in the Context of Administrative Law* 4-10.
536 Nkanyane *Subsidiarity in the Context of Administrative Law* 4-10.
537 Sutherland 2017 *AJIC* 94.
538 Bote *The South African National Cyber Security Policy Framework: A critical analysis* 36.
539 Maat *Cyber Crime: A Comparative Law Analysis* 10.
540 Maat *Cyber Crime: A Comparative Law Analysis* 10.
541 Maat *Cyber Crime: A Comparative Law Analysis* 10.
542 According to Molwanta at *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 35 and Ntsaluba at *Cybersecurity Policy and Legislation in South Africa* 65, direct communication entails real conversations taking place in the presence of two or more individuals; Indirect communication entails communicating through the internet, short message service (SMS), emails or phone calls.
543 The *RICA* preamble.
544 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 49.

The *RICA* is considered necessary for the protection of South African ICTs and citizens in the cyberspace.[545] The *RICA* consists of 10 chapters.[546] Chapter 1 of the *RICA* presents the introductory provisions; this includes a list of the various keywords used in the *RICA* and presents their definitions.[547] The interpretation and application of the *RICA* is also discussed.[548] Keywords to acknowledge in understanding the interpretation of the *RICA* are "interception", "monitoring", "data retention" and "decryption".[549] According to the *RICA*, "intercept" can be defined as,[550]

> 'intercept' means the aural or other acquisition of the contents of any communication through the use of any means, including the interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communications, and includes the-
> (a) monitoring of any such communication by means of a monitoring device;
> (b) viewing, examination or inspection of the contents of any indirect communication; and
> (c) diversion of any indirect communication from its intended destination to any other destination,[551]

Whereas "monitor" can be defined as,[552]

> 'monitor' includes to listen to or record communications by means of a monitoring device, and 'monitoring' has a corresponding meaning;[553]

According to Govender,[554] there are two types of categories in which the interception of communication operates; these categories are, targeted interception or bulk interception.[555] Targeted interception involves the ongoing electronic monitoring of a specific individual or group's digital footprint regarding electronic communications for a definite period of time.[556] Bulk interception involves an ongoing electronic monitoring of

---

545 Molwanta *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 34.
546 The *RICA* preamble.
547 Chapter 1 of the *RICA*.
548 Chapter 1 of the *RICA*.
549 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 50.
550 Section 1 of the RICA.
551 Section 1 of the *RICA*.
552 Section 1 of the RICA.
553 Section 1 of the *RICA*.
554 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 50.
555 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 50.
556 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 50.

the electronic communications of a general section of the population.[557] According to Rughoonandan,[558] a fundamental factor to consider when communication is intercepted, is the malicious intent (conduct) of the criminal.[559] Rughoonandan continues to state that if the offence lacks evidentiary support of the interception being intentional, the offence cannot be addressed by the *RICA*.[560]

Chapter 2 of the *RICA* assists national law enforcement agencies in addressing the criminalisation of intercepting any form of public or private communication and provides the lawful position of archived or real-time communication-related information.[561] Section 2 of the *RICA* states,[562]

> "Subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission."[563]

The *RICA* continues in Chapter 2 by discussing an extensive list of exceptions to the interception of communication including amongst others,[564] an authorised party acting under a lawful interception direction,[565] a party included in the communication,[566] a non-party acting with consent,[567] to carry out business-related responsibilities,[568] to prevent bodily harm,[569] in case of emergencies,[570] and authorisation through other national legal statutes.[571] The list of exceptions is considered quite broad and continues to be critically discussed in the remainder of Chapter 2.[572]

---

557 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 50.
558 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 46.
559 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 46.
560 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 46.
561 Molwanta *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 34; Chapter 2 of the *RICA*.
562 Section 2 of the *RICA*.
563 Section 2 of the *RICA*.
564 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 50.
565 Section 3 of the *RICA*; Interception direction can be defined as signed- or oral authorisation, issued according to the provisions as set out in *RICA* to intercept communication at any place or time within the borders of South Africa.
566 Section 4 of the *RICA*.
567 Section 5 of the *RICA*.
568 Section 6 of the *RICA*.
569 Section 7 of the *RICA*.
570 Section 8 of the *RICA*.
571 Section 9 of the *RICA*.
572 Chapter 2; Chapter 8 of the *RICA*.

Considering the impact and effect these types of exceptions can have regarding the interception of communication, according to Snail,[573] South Africa should not look any further than the English court case, *R v Secretary of State for the Home Department, Ex parte Ruddock* [1987] 2 All ER 518 (QB),[574] where a UK Court of Appeal discussed the implications of applying these exceptions based on the common law, as justification grounds to the allegations of unlawful interception and monitoring of communications.[575] The Court continued by suggesting that these exceptions must be used moderately in cases of interception where the nature of the interception is unclear and is to be investigated.[576]

The Court ruled that,[577] although the common law authorises these exceptions to intercept in communications (such as South Africa), the exceptions must entirely adhere to the common law and its requirements as an individual's right to privacy can be easily infringed upon.[578] Regarding the legal position and application of these exceptions, consider the following example: Section 5 of the *RICA* allows the lawful interception of any type of communication between parties if a non-party or a communication service provider (also a non-party) received verbal or written consent from one of the involved communicating parties.[579] However, considering this exception, the question arises whether privileged communication between a client and an attorney, or between a client and a doctor could also be lawfully intercepted in terms of the provisions stipulated in section 5 of the *RICA*?[580]

The answer is yes,[581] there are legal exceptions applied to certain circumstances;[582] however, specifically referring to the expectations of section 5 of the *RICA*,[583] in the case *AmaBhungane Centre for Investigative Journalism NCP v Minister of Justice and Correctional Services and Others*; *Minister of Police and Others v AmaBhungane Centre for*

573 Snail 2008 *Juta's Business Law* 64.
574 *R v Secretary of State for the Home Department, Ex parte Ruddock* [1987] 2 All ER 518 (QB).
575 Snail 2008 *Juta's Business Law* 64.
576 Snail 2008 *Juta's Business Law* 64.
577 Snail 2008 *Juta's Business Law* 64.
578 Snail 2008 *Juta's Business Law* 64.
579 Ntsaluba *Cybersecurity Policy and Legislation in South Africa* 67.
580 Ntsaluba *Cybersecurity Policy and Legislation in South Africa* 67.
581 DSC Attorneys 2021 https://www.dsclaw.co.za/articles/when-does-legal-professional-privilege-not-apply-in-south-africa/.
582 DSC Attorneys 2021 https://www.dsclaw.co.za/articles/when-does-legal-professional-privilege-not-apply-in-south-africa/.
583 Interception of communication with consent of party to communication, section 5 of the *RICA*.

Investigative Journalism NCP Case (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021)[584] the Constitutional Court declared the *RICA* entirely unconstitutional,[585] therefore the *RICA* can no longer be considered or applied (this will be discussed later in this chapter).[586]

South African courts find themselves caught between the position of authorised consent and the possible infringement of the fundamental rights to privacy, to the access of information or to a fair trial.[587] The courts have the duty and responsibility to consider the parameters, circumstances and requirements of the authorised consent or exception to establish if such "infringement" is deemed reasonable and justifiable.[588] As for the position regarding the prohibition of archived or real-time communication-related information;[589] archived communication-related information is information gathered, monitored and controlled by a telecommunication service provider for a specific period of time as indicated, usually after the expiration of ninety days, which can be used or referred to later.[590]

Real-time communication-related information is any relevant recorded information immediately made available or released to a telecommunication service provider before or during the ninety-day period.[591] Section 12 – 15 explains the position of prohibiting as well as providing communication-related information via a telecommunication service provider under direction, authorisation, or any other available procedure or application.[592] Chapter 3 of the *RICA* provides the legal procedures regarding the applications and the issuing of these applications, for various directions and entry warrants.[593] The different types of directions and entry warrant applications listed are, interception direction,[594] real-time

---

584 *AmaBhungane Centre for Investigative Journalism NCP v Minister of Justice and Correctional Services and Others*; *Minister of Police and Others v AmaBhungane Centre for Investigative Journalism NCP Case* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021) (hereafter the "*AmaBhungane Centre for Investigative Journalism*").

585 *AmaBhungane Centre for Investigative Journalism* 61.

586 *AmaBhungane Centre for Investigative Journalism* 61.

587 Ntsaluba *Cybersecurity Policy and Legislation in South Africa* 67; Section 14, section 32, section 34 of the *Constitution*.

588 Ntsaluba *Cybersecurity Policy and Legislation in South Africa* 67.

589 Section 12-15 of the *RICA*.

590 Section 1 of the *RICA*.

591 Section 1 of the *RICA*.

592 Section 12-15 of the *RICA*.

593 Chapter 3 of the *RICA*.

594 Section 16 of the *RICA*.

communication-related direction,[595] archived communication-related direction,[596] decryption direction[597] and an entry warrant.[598]

The requesting procedure of these applications, regardless of directions or entry warrants, can be submitted orally or in writing, by any law enforcement agency or the intelligence community and can only be requested based on national security or lawful interception-related grounds.[599] The issuing of these applications is authorised by a designated Judge of a High Court.[600] The *RICA* also states that these directions and entry warrants to intercept must be reviewed by the Office of Interception Centres (OIC).[601] This chapter also regulates the amendment and the extension procedure of existing directions, and addresses the position and the practice of oral applications.[602] The chapter concludes by addressing the cancellation procedures regarding these applications and discusses request reports on the progress of these applications.[603]

Chapter 4 of the *RICA* discusses the execution procedure regarding directions and entry warrants; it also provides assistance services from a decryption key holder, a postal service provider and a telecommunication service provider.[604] Chapter 5 of the *RICA* discusses the interception capability of the telecommunication service provider or operator and the way in which communication-related information must be preserved for a certain period of time.[605] Section 31 continues to discuss the position regarding compensation to telecommunication service providers, postal service providers and decryption key holders.[606] An important chapter in the *RICA* to consider regarding cybercrime is Chapter 6. Chapter 6 creates and establishes interception centres along with the OIC and regulates the assistance-fund available to ISPs.[607]

---

595 Section 17 of the *RICA*.
596 Section 19 of the *RICA*.
597 Section 21 of the *RICA*.
598 Section 22 of the *RICA*.
599 Chapter 2-3 of the *RICA*; Molwanta *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 35.
600 Molwanta *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 35.
601 Molwanta *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 35.
602 Section 20, section 23 of the *RICA*.
603 Section 24, section 25 of the *RICA*.
604 Chapter 4 of the *RICA*.
605 Chapter 5 of the *RICA*.
606 Section 31 of the *RICA*.
607 Chapter 6 of the *RICA*.

Section 33 confirms the establishment of the OIC, located in Pretoria, Gauteng.[608] The OIC operates and reports to the Minister of State Security Agency and is directed by an assigned member of the department acting as the head, with the power and responsibility to carry out administrative duties, to regulate the OIC and its acting staff, coordinate the OIC's activities and delegate the procedures of the OIC in accordance with the *RICA*.[609] As for the general objective of the OIC, the OIC has the duty to collect, report and provide records, such as data files, voice communications and interception files, for example, defects, for up to five years for the South African Intelligence services, the Financial Intelligence Centre (FIC) and the National Prosecuting Authority (NPA).[610]

Chapter 7 of the *RICA* addresses the duties and responsibility of telecommunication service providers in obtaining and keeping certain information when entering into a binding contract with any natural or juristic person.[611] This chapter also discusses the position, responsibility and duty of electronic communication service providers (ECSPs) who establishes and provides mobile cellular services to clients.[612] Section 41 addresses the duties of the client regarding electronic communication; this includes the registration of a SIM-card (Subscriber Identity Module-card) and the obligation to immediately report to national authorities when the client's phone or the client's SIM-card has been lost, stolen or damaged.[613]

Chapter 8 addresses the position of general prohibitions and exemptions.[614] It broadly discusses the prohibition on disclosing information in general considering the *RICA* and the disclosing of information by an authorised individual acting on official obligations.[615] The chapter continues by identifying and listing equipment used to intercept communication, this includes electronic, mechanical or acoustic equipment or instruments, and it also prohibits the manufacture and advertisement of the above-mentioned equipment.[616] In

608 Sutherland 2017 *AJIC* 97.
609 Section 35A of the *RICA*.
610 Sutherland 2017 *AJIC* 97.
611 Section 39 of the *RICA*.
612 Section 40 of the *RICA*.
613 Section 41 of the *RICA*.
614 Chapter 8 of the *RICA*.
615 Section 42, section 43 of the *RICA*.
616 Section 44, section 45 of the *RICA*.

section 46, the *RICA* addresses the exemptions relevant to internet service providers, telecommunication service providers and national law enforcement agencies.[617]

Chapter 9 of the *RICA* is considered a fundamental framework regarding civil or criminal proceedings, offences, and prosecution procedures in relation to the interception of communication.[618] This chapter sets out the law on the use of information obtained in civil or criminal proceedings, regulates the evidence and facts as signed by a designated judge, recognises the act of unlawful interception as a criminal offence and regulates the illegal provision of communication-related information.[619] Chapter 9 also provides and delivers penalties and prosecutions, determines the position of possession and reasonable cause regarding a cellular phone or SIM-card, lists illegal intercepting equipment, records reports of the loss, theft or destruction of a phone or a SIM-card, and annuls or revokes the license of electronic communication services.[620]

As for the final chapter, Chapter 10: It includes the schedule of numerous amendments, repeals, and commencements of the *RICA* through the years 2002 - 2006.[621] These amendments include the first draft of proposed amendments (2004), the amended draft of directives for internet service providers (2004), the amended draft of directives for additional telecommunications service providers (2004) and the *RICA* Amendment Bill (2006).[622] Alas, after years of the *RICA* regulating the position of intercepting communications in South Africa, the South African Constitutional Court (CC) delivered judgement on 4 February 2021, and declared the *RICA* unconstitutional on five separate grounds.[623]

Justice Madlanga and the Constitutional Court declared in the case *AmaBhungane Centre for Investigative Journalism*,[624] that the *RICA*, fails to provide appropriate safeguards (lawful protection) to a designated judge (as defined in section 1 of the *RICA*) in

---

617 Section 46 of the *RICA*.
618 Chapter 9 of the *RICA*.
619 Section 47-57 of the *RICA*.
620 Section 47-57 of the *RICA*.
621 Chapter 10 of the *RICA*.
622 Chapter 10 of the *RICA*.
623 Ongeso 2021 https://bowmanslaw.com/insights/mergers-and-acquisitions/south-africa-constitutional-court-upholds-declaration-of-invalidity-of-rica/.
624 *AmaBhungane Centre for Investigative Journalism NCP v Minister of Justice and Correctional Services and Others*; *Minister of Police and Others v AmaBhungane Centre for Investigative Journalism NCP Case* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021) (hereafter the "*AmaBhungane Centre for Investigative Journalism*").

authorising, hearing and determining interception direction applications independently according to the procedures set out in the *RICA,*[625] and fails to clearly notify any subject of surveillance, challenging the lawfulness of interception, that the subject is indeed under any form of surveillance, otherwise known as post-surveillance notification.[626]

The Court continued their in-depth discussion and determined that the *RICA* also fails to provide appropriate safeguards to obtained interception directions (*ex-parte* applications), fails to provide and determine lawful parameters in protecting, sharing, destroying data or information obtained (management of data or information challenge) and lastly, fails to provide appropriate safeguards to attorneys and journalists regarding the confidential nature of their business in sharing information (attorney and journalist challenge).[627] The Court also mentioned and discussed the highly invasive nature of communication interception and the violation of the fundamental right to privacy[628] from the provisions envisaged in the *RICA*.[629] Therefore, the *RICA* is no longer considered applicable in addressing cybercrime in South Africa.[630]

3.3 Electronic Communications and Transactions Act 25 of 2002

One of the fundamental pieces of cybercrime legislation originating from the impact and effect of the NCPF was the *Electronic Communications and Transactions Act* 25 of 2002 (hereafter the "*ECTA*").[631] The *ECTA* was assented to by Parliament on 31 July 2002.[632] The *ECTA* repealed the *Computer Evidence Act* 57 of 1983.[633] The *ECTA* consists of 14 chapters and 2 schedules with the objective of providing assistance and regulation regarding electronic-related communications as well as transactions in South Africa, to encourage the development of e-strategies, to provide access to electronic communications and transactions, to establish human-resource development in electronic

625 *AmaBhungane Centre for Investigative Journalism* 16-19.
626 *AmaBhungane Centre for Investigative Journalism* 16-19.
627 *AmaBhungane Centre for Investigative Journalism* 16-19.
628 Section 14 of the *Constitution*.
629 *AmaBhungane Centre for Investigative Journalism* 61.
630 Ongeso 2021 https://bowmanslaw.com/insights/mergers-and-acquisitions/south-africa-constitutional-court-upholds-declaration-of-invalidity-of-rica/.
631 Eboibi 2020 *Commonwealth Law Bulletin* 6.
632 Snail *Legal Development in Cyber Crime Law in South Africa* 16; Preamble of the *ECTA*.
633 Maat *Cyber Crime: A Comparative Law Analysis* 12.

communications and transactions, to prohibit the abuse and misuse of information systems, and to develop and implement e-government services.[634]

Chapter I provides a list of keywords and their definitions found in the *ECTA*; it also includes the objectives, the interpretation, and the application of the *ECTA*.[635] According to section 3 of the *ECTA*,[636] the interpretation section, the *ECTA* must not be interpreted to the extent of excluding other binding pieces of legislation or statutory legislation which can be lawfully applied to electronic communication or transaction-related matters where the *ECTA* falls short.[637] Chapter II entails the position regarding the national e-strategy and presents the electronic transactions policy.[638] Chapter III addresses the facilitation of electronic transactions.[639] This forms part of the fundamental objective of the *ECTA*, including, the nature and legal requirements for data messages.[640]

Chapter IV provides for national e-government services, this entails the electronic filing, evaluating and issuing of legal documents and their lawful requirements.[641] Chapter V establishes cryptography providers, addresses the registration procedure of these services, and provides the restrictions and offences regarding these services.[642] Chapter VI entails the authentication of service providers and the accreditation authority.[643] Chapter VII addresses the protection of personal or private information and general consumer protection;[644] this chapter is also considered fundamental in the nature of electronic communications and transactions.[645] Chapter VIII continues with addressing the protection of personal information and explains the scope as well as the legal principles in collecting personal or private information in terms of the *ECTA*.[646]

Chapter IX provides for the scope, identification, registration, management, and protection of critical databases and sets out the lawful rights and responsibilities of inspections

634 Preamble of the *ECTA*.
635 Chapter I of the *ECTA*.
636 Section 3 of the *ECTA*.
637 Madziwa and Snail 2021 https://www.hg.org/legal-articles/cyber-crime-in-south-africa-5351; Snail *Legal Development in Cyber Crime Law in South Africa* 16.
638 Chapter II of the *ECTA*.
639 Chapter III of the *ECTA*.
640 Chapter III of the *ECTA*.
641 Chapter IV of the *ECTA*.
642 Chapter V of the *ECTA*.
643 Chapter VI of the *ECTA*.
644 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 39.
645 Chapter VII of the *ECTA*.
646 Chapter VIII of the *ECTA*.

regarding a database.[647] Chapter X addresses domain name authority in South Africa and administration;[648] this chapter lists and discusses 6 specific elements,[649] i.e. the establishment, the governance and staffing, the primary functions, the financial position and reporting procedure, various regulations, and the option of alternative dispute resolution.[650] Chapter XI entails the authority of service providers and their position regarding the limitations on liability.[651] Although the *ECTA* fails to explicitly define the word "cybercrime",[652] Chapter XII and Chapter XIII of the *ECTA* are considered the two most important chapters regarding this discussion.[653]

Chapter XII establishes and discusses the necessity of cyber-inspectors[654] and Chapter XIII addresses cybercrime.[655] These two chapters will be critically discussed. Chapter XIV entails the *ECTA*'s general provisions, such as the jurisdiction of the courts, the repealing of acts, limitations, and additional regulations.[656] The two schedules list several South African acts in relation to section 4 (the sphere of application) in the *ECTA*.[657] Chapter XII, entitled "Cyber Inspectors" establishes the necessity of an appointed cyber-inspector.[658] Section 80[659] introduces and discusses the offences of hindering an appointed cyber-inspector from their duty and responsibility and the offence of misrepresenting or identifying as an appointed cyber-inspector.[660]

Section 81 sets out the powers of an appointed cyber-inspector,[661] this discusses the monitoring and reporting of unlawful or suspicious online activities, the investigation of compliance and non-compliance matters from cryptography service providers as well as authentication service providers, the issuing of court orders and the performing of audits concerning databases.[662] Section 82 continues with a cyber-inspector's power to lawfully

---

647 Chapter IX of the *ECTA*.
648 Chapter X of the *ECTA*.
649 Section 59-69 of the *ECTA*.
650 Section 59-69 of the *ECTA*.
651 Chapter X of the *ECTA*.
652 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 39.
653 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 39.
654 Eboibi 2020 *Commonwealth Law Bulletin* 6.
655 Chapter XIII of the *ECTA*.
656 Section 90-95 of the *ECTA*.
657 Schedule 1 and Schedule 2 of the *ECTA*.
658 Chapter XII of the *ECTA*.
659 Section 80(5) of the *ECTA*.
660 Section 80(5) of the *ECTA*.
661 Section 81(1)-(2) of the *ECTA*.
662 Section 81(1)-(2) of the *ECTA*.

inspect, search and seize relevant articles or premises.[663] In the case of a cyber-offence,[664] the cyber-inspector has the legal right to access, search or enter a premises (including a communication- or information system), to seize any article, document, file or data believed to be relevant to the cyber-offence and extract any information or data where deemed necessary.[665]

A cyber-inspector may also lawfully request registration forms and licences from any type of service providers.[666] The execution of these rights are generally referred to the *Criminal Procedure Act* 51 of 1977 as well as considering section 14 (right to privacy) of the *Constitution*.[667] Section 83 addresses the procedure of obtaining of a search warrant by a cyber-inspector.[668] This section also refers to the issuing of a search warrant in terms of the relevant provisions in the *Criminal Procedure Act*.[669] The issuing of a search warrant is conducted by any magistrate or judge upon a reasonable and lawful request.[670] Section 84 obliges the cyber-inspector to abstain from disclosing any obtained information or data to another party unless it is required in terms of the *ECTA*.[671] The cyber-inspector will be guilty of an offence if they disclose the obtained information unlawfully.[672]

Chapter XIII, entitled "Cyber Crime" as envisaged in the *ECTA*, is the first statutory provision on cybercrime in South Africa[673] and defines a relevant keyword in the *ECTA*, "access";[674]

> "access" includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.[675]

This chapter comprehensively discusses and addresses cybercrime and continues to list a few cyber-offences recognised in terms of the provisions in the *ECTA*.[676] This list includes,

---

663 Section 82 of the *ECTA*.
664 Section 82(1) of the *ECTA*.
665 Section 82(1) of the *ECTA*.
666 Section 82(1) of the *ECTA*.
667 Section 82(4) of the *ECTA*.
668 Nortjé and Myburgh at *PER/PELJ* 10.
669 Nortjé and Myburgh at *PER/PELJ* 10.
670 Nortjé and Myburgh at *PER/PELJ* 10.
671 Section 84 of the *ECTA*.
672 Section 84 of the *ECTA*.
673 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 1.
674 Section 85 of the *ECTA*.
675 Section 85 of the *ECTA*.
676 Section 86 of the *ECTA*.

the unauthorised access or the unlawful interference or interception of data,[677] for example, hacking,[678] online extortion, online fraud, or online forgery,[679] and the offence of attempting, aiding, and abetting offences (accessory to an offence)[680] and provides the appropriate prosecution procedures available for the aforementioned offences.[681] Section 86 of the *ECTA* addresses the intentional act of unauthorised access or the unlawful interference of data, communications or transactions.[682]

This chapter also recognises the relevance of the *Interception and Monitoring Prohibition Act* 27 of 1992 (repealed),[683] similar to the position of the *RICA* regarding the unlawful interception of data as an offence.[684] This section continues with discussing the offence of intentionally modifying and destroying data obtained through unauthorised interception, once again similar to the position of the *RICA*.[685] Both section 86(3) and section 86(4) deal with the introduction of a new offence, anti-cracking or anti-thwarting;[686] this refers to the designing, producing, selling or distributing of any smart device or any software programme with the primary intent of intercepting communication, stealing personal or private information, breaking down security measures (anti-security) or intercepting and retrieving confidential passwords.[687]

It also includes the distribution of illegal files or data, for example, movies or music in relation to contravening any South African copyright protection and regulations.[688] Section 86(5) recognises the extensive offence of unlawful interception by a party to prohibit or deny another party the right to enjoy legitimate online services available in the online environment, for example,[689] email bombing, spamming or DDoS attacks.[690] Respectively,[691] section 45 is also referred to when one considers offences in terms of the

677 Section 86 of the *ECTA*.
678 Giles 2009 https://www.michalsons.com/blog/cyber-crime-explained/2667.
679 Section 87 of the *ECTA*.
680 Section 88 of the *ECTA*.
681 Section 80 of the *ECTA*.
682 Section 86 of the *ECTA*.
683 Snail *Legal Development in Cyber Crime Law in South Africa* 17.
684 Section 86(1) of the *ECTA*.
685 Section 86(2) of the *ECTA*.
686 Snail *Legal Development in Cyber Crime Law in South Africa* 18.
687 Section 86(3)-(4) of the *ECTA*; Snail *Legal Development in Cyber Crime Law in South Africa* 18.
688 Madziwa and Snail 2021 https://www.hg.org/legal-articles/cyber-crime-in-south-africa-5351.
689 Snail *Legal Development in Cyber Crime Law in South Africa* 20.
690 Snail *Legal Development in Cyber Crime Law in South Africa* 20.
691 Snail *Legal Development in Cyber Crime Law in South Africa* 20.

provisions found in the *ECTA*.[692] Section 45 entails that the distribution of unsolicited (unwanted) commercial communications to a party who already informed the sender to desist the distribution thereof, will be guilty of an offence.[693]

Section 87 of the *ECTA* discusses the different types of cybercrime, for example, online extortion, online fraud, and online forgery.[694] Section 87(1) provides for an alternative type of extortion than that in terms of the South African common law,[695] as this type of cybercrime focuses on threatening or causing intentional damage or harm to another natural or juristic person in the online environment.[696] These offences will be prosecuted in terms of the *ECTA* by a monetary fine or imprisonment.[697] It is important to understand that the above-mentioned cybercrimes are not exclusively limited to the offences enlisted in the *ECTA*.[698] There are various additional cyber-related laws and pieces of legislation identifying several types of cybercrime, for example, identity theft and identity fraud envisaged in the *Personal Protection of Information Act* 4 of 2013.[699]

Regarding the general position of evidence in South African courts, section 14 (original),[700] and section 15 (evidence of data messages)[701] of the *ECTA* play a crucial role in addressing the legal position of data and data messages considered as evidence in a court of law.[702] According to section 1 of the *ECTA*,[703] "data" can be defined as any form or type of electronic information making up a sequence,[704] and,[705]

> "data message" means data generated, sent, received or stored by electronic means and includes-
> (a) voice, where the voice is used in an automated transaction; and
> (b) a stored record;[706]

---

692 Madziwa and Snail 2021 https://www.hg.org/legal-articles/cyber-crime-in-south-africa-5351.
693 Section 45 of the *ECTA*.
694 Section 86(1)-(2) of the *ECTA*.
695 Snail *Legal Development in Cyber Crime Law in South Africa* 20.
696 Pieterse *Electronic Crime Unit* 33.
697 Section 89 of the *ECTA*.
698 Madziwa and Snail 2021 https://www.hg.org/legal-articles/cyber-crime-in-south-africa-5351.
699 Madziwa and Snail 2021 https://www.hg.org/legal-articles/cyber-crime-in-south-africa-5351.
700 Section 14 of the ECTA.
701 Section 15 of the ECTA.
702 Section 15 of the *ECTA*.
703 Section 1 of the *ECTA*.
704 Section 1 of the *ECTA*.
705 Section 1 of the *ECTA*.
706 Section 1 of the *ECTA*.

Section 14 entails the legal requirements of data or information remaining in its original form if the data or information is to be considered and presented as evidence in court.[707] Section 15 entails that evidence in the form of data messages or a certified printout (by a judicial officer) must be recognised and admissible as evidence in any circumstance or case before court, thus providing the presumption of rebuttable proof.[708] Upon admission, the evidence must include the process in which the evidence was generated, evaluated, stored or communicated, the process in which the integrity of the evidence was upheld, identify the parties involved and present any relevant factor the court seems to find necessary considering the facts and circumstances of the case.[709] These matters are often additionally referred to in the *Criminal Procedure Act*.[710]

However, the remaining legal challenge regarding the admission of electronic evidence is: To what extent can additional legislation be applied to evidence obtained from foreign countries?[711] Another important section to consider is section 90. Section 90 deals with the jurisdiction of the courts.[712] This generally creates a challenge for South African courts, cyber-inspectors and cyber-prosecutors to appropriately address and prosecute a committed cyber-offence.[713] Although the *ECTA* assigns South African courts their precise jurisdiction to offences committed in and affecting South Africa,[714] there appears to be quite the debate on whether the provisions of the *ECTA* can be referred to along with relevant international legislation regarding a cyber-offence committed abroad.[715]

In response, the *ECTA* adopted the legal conditions of identifying an offender as fulfilling an active role in the preparation of a cyber-offence or that the cyber-offence was committed by a South African citizen, a permanent resident or a juristic person;[716] however,[717] these jurisdictional provisions are not without criticism and are yet to be appropriately addressed and discussed.[718] Nevertheless, a South African court will have

---

707 Section 14 of the *ECTA*; Nortjé and Myburgh at *PER/PELJ* 10.
708 Section 15(2) of the *ECTA*.
709 Section 15(3) of the *ECTA*.
710 *Criminal Procedure Act* 51 of 1977; Pieterse *Electronic Crime Unit* 37.
711 Pieterse *Electronic Crime Unit* 39.
712 Section 90 of the *ECTA*.
713 Section 90 of the *ECTA*.
714 Cassim 2012 *PER/PELJ* 398.
715 Madziwa and Snail 2021 https://www.hg.org/legal-articles/cyber-crime-in-south-africa-5351.
716 Giles 2009 https://www.michalsons.com/blog/cyber-crime-explained/2667.
717 Cassim 2009 *PER* 61.
718 Madziwa and Snail 2021 https://www.hg.org/legal-articles/cyber-crime-in-south-africa-5351.

jurisdiction regarding perpetrators who disseminate viruses abroad and if the perpetrator is of South African nationality regardless of the geographical location.[719]

However, an important question to consider asking is: How extensive and advanced must the reach of South Africa's cybercrime legislation be, if South Africa's national legislation addressing criminal and civil issues are constantly challenged in preventing traditional crimes?[720] There appears to be two solutions in providing protection regarding electronic communications and transactions,[721] the protection of information security (this includes both physical and logical protection), and the manner in controlling the conduct of third parties.[722] The implementation of the *ECTA* achieved this to a certain extent.[723] However, there appears to be much room for the improvement of the provisions found in the *ECTA* regardless of the implementation of the new *Cybercrimes Act*.[724]

National authorities did attempt to assist in the amendment of the *ECTA* by introducing the *Electronic Communications and Transactions Amendment Bill* of 2012 (hereafter the "*Amendment Bill*").[725] The *Amendment Bill* is considered fundamental in the progressive nature of addressing cybercrime matters.[726] The *Amendment Bill* introduces the accreditation of authentication services, secures global electronic commerce, prevents the abuse or misuse of information systems, protects domain names and encourages the use of e-government services.[727]

3.4 Criminal Procedure Act 51 of 1977

The *Criminal Procedure Act* 51 of 1977 (hereafter the "*CPA*") was assented to on 21 April 1977 and came into operation on 22 July 1977.[728] The *CPA* repealed the former *Criminal Procedure Amendment Act* 9 of 1968.[729] The *CPA* was promulgated and implemented to regulate and guide criminal proceedings, investigation procedures, evidence admissibility

719 Cassim 2009 *PER* 61.
720 Giles 2009 https://www.michalsons.com/blog/cyber-crime-explained/2667.
721 Giles 2009 https://www.michalsons.com/blog/cyber-crime-explained/2667.
722 Giles 2009 https://www.michalsons.com/blog/cyber-crime-explained/2667.
723 Giles 2009 https://www.michalsons.com/blog/cyber-crime-explained/2667.
724 Cassim 2016 *CILSA* 128.
725 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 40.
726 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 40.
727 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 40.
728 *Criminal Procedure Act* 51 of 1977.
729 Van der Merwe *et al Information and Communications Technology Law* 123.

and offences along with providing their appropriate prosecutions in South Africa.[730] The *CPA* is strictly referred to in criminal matters, whereas the *Civil Proceedings Evidence Act* 25 of 1965 (hereafter the "*CPEA*") is referred to in civil matters.[731] The significance of the *CPEA* will be discussed. The *CPA* comprises an extensive 33 chapters; however, for purposes of this discussion, only certain relevant sections will be discussed regarding the matter of cybercrime.[732]

Chapter 2 of the *CPA* provides for the procedure regarding the application and issuing of (written or oral) search warrants, it also provides for the contents of the application, it sets out the requirements of a search warrant, the authority of entering a premises, the procedure for seizing an article,[733] and the disposal of articles in relation to committed offences.[734] Section 20 of the *CPA* entails that the state may, according to the provisions in the *CPA*, seize an article or anything related to a committed offence, or which might be deemed necessary as evidentiary support to the committed offence, or which was intentionally used to commit the offence.[735] According to Van der Merwe,[736] an important question to ask is whether section 20 of the *CPA* can be applied to the position of smart devices, data, computers, and information systems?[737]

Van der Merwe[738] argues that section 20 of the *CPA* appears extremely broad referring to the concept of, "anything", and continues to ask, does this really mean "anything"?[739] Van der Merwe continues by stating that the intangible, for example, data, is generally found in a tangible object, for example, a computer.[740] However, the superior courts of South Africa argued that at the time when the *CPA* was implemented, intangible objects were not included, only tangible objects, causing quite the predicament; regardless, the South

730 Preamble of the *CPA* 51 of 1977.
731 Van der Merwe *et al Information and Communications Technology Law* 123.
732 Preamble of the *CPA*.
733 According to Nortjé and Myburgh at *PER/PELJ*, seizure can be defined as an individual being deprived of any type of control regarding their property or articles.
734 Chapter 2 of the *CPA*.
735 Section 20(a)-(c) of the *CPA*.
736 Van der Merwe *et al Information and Communications Technology Law* 99-100.
737 Van der Merwe *et al Information and Communications Technology Law* 100.
738 Van der Merwe *et al Information and Communications Technology Law* 100.
739 Van der Merwe *et al Information and Communications Technology Law* 100.
740 Van der Merwe *et al Information and Communications Technology Law* 100.

African legislature and judiciary started to apply these provisions of the *CPA* to intangible objects as well.[741]

Section 21 of the *CPA* provides for authorised officials, for example, a judge, magistrate, or judicial officer to issue a search warrant for the seizing of an article if the request of the search warrant is established on reasonable grounds.[742] Du Toit[743] continues to explain that the issuing of a search warrant must be under oath or affirmation.[744] As mentioned, the request for the search warrant must be issued on reasonable grounds and the fact that the "article" (section 20) is indeed in question and related to the committed offence.[745] A search warrant application can be issued through oral authorisation in the case of emergencies.[746]

It is required that the search warrant must be accompanied by a signed affidavit containing two distinctive jurisdictional facts.[747] The first fact is the reasonable suspicion that an offence was committed.[748] The second fact is that the offence was committed with, or assisted by, certain articles or objects which might indicate an involved individual, article or premises.[749] Section 23 of the *CPA* continues to discuss the search of an arrested individual or the seizure of an article.[750] The section continues to provide that if an article or object was found on the arrested individual, the article must be placed in safe custody and protected, available to law enforcement agencies.[751]

Section 24 of the *CPA* provides for the legal search of a premises if an individual or a law enforcement agency is convinced that the specific premises contain certain articles, for

---

741 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 11.

742 Section 21(1)(a)-(b) of the *CPA*.

743 Du Toit *The Search Warrant Provisions of the Cybercrimes Act and their Relationship with the Criminal Procedure Act* 767-771.

744 Du Toit *The Search Warrant Provisions of the Cybercrimes Act and their Relationship with the Criminal Procedure Act* 767-771.

745 Du Toit *The Search Warrant Provisions of the Cybercrimes Act and their Relationship with the Criminal Procedure Act* 767-771.

746 Du Toit *The Search Warrant Provisions of the Cybercrimes Act and their Relationship with the Criminal Procedure Act* 767-771.

747 Du Toit *The Search Warrant Provisions of the Cybercrimes Act and their Relationship with the Criminal Procedure Act* 767-771.

748 Du Toit *The Search Warrant Provisions of the Cybercrimes Act and their Relationship with the Criminal Procedure Act* 767-771.

749 Du Toit *The Search Warrant Provisions of the Cybercrimes Act and their Relationship with the Criminal Procedure Act* 767-771.

750 Section 23(1)(a)-(b) of the *CPA*.

751 Section 23(2) of the *CPA*.

example, stolen goods, liquor, illegal drugs or weapons, and if there were to be any articles, that the individual or the law enforcement agency, acting under the authority of the search warrant, will remove the articles from the premises and deliver them to a police official or a national law enforcement agency.[752] Chapter 2 continues with discussing the power of the police regarding the entering of a premises, the entering of a premises to obtain evidence, resisting against the search or entry, the wrongful search of an offence, the conduct of the search, and the entire nature of an article regarding the disposal thereof and its role in criminal proceedings.[753]

The next chapter to consider is Chapter 24. Chapter 24 of the *CPA* regulates the general position of evidence in criminal proceedings.[754] Section 221 of the *CPA* provides for the admissibility of business and trade records as evidence; this entails the fact that any information, statement, or record disclosed in a single document or numerous documents will be considered as admissible evidence in a court of law.[755] Section 221 defines a "document" as,[756]

> 'document' includes any device by means of which information is recorded or stored;[757]

Section 222 of the *CPA*, assists and allows the reference and application of certain relevant provisions found in the *CPEA* to criminal proceedings regarding documentary evidence.[758] These provisions are found in Part VI of the *CPEA*.[759] Part VI regulates documentary evidence (miscellaneous provisions) from section 33 – section 38.[760] However, section 38 of the *CPEA* is the most applicable and relevant section in relation to the certain provisions of the *CPA*;[761] This section provides that nothing envisaged in the sections of the *CPEA* shall prejudice the element of admissibility of any evidentiary facts which would, apart from the provisions of the *CPEA*, be admissible.[762] This section is directly referenced to the *CPA* in criminal proceedings.[763]

---

752 Section 24 of the *CPA*.
753 Section 25-36 of the *CPA*.
754 Chapter 24 of the *CPA*.
755 Section 221 of the *CPA*.
756 Section 221(5) of the *CPA*.
757 Section 221(5) of the *CPA*.
758 Section 222 of the *CPA*.
759 Part VI of the *CPEA*.
760 Part VI of the *CPEA*.
761 Van der Merwe *et al Information and Communications Technology Law* 123.
762 Section 38 of the *CPEA*.
763 Van der Merwe *et al Information and Communications Technology Law* 123.

In South Africa, the adverse effect and impact of cybercrime have always been addressed by South African law enforcement agencies through considering the provisions of the *ECTA* along with considering the provisions of the *CPA*.[764] South African authorities have relied on the *ECTA* and the *CPA* to provide for both investigation and prosecution procedures when responding to and prosecuting cybercrime.[765] These two acts are compatible in such a manner directly related to the search-and-seizure aspect of committed offences as envisaged in section 20 and section 21 of the *CPA*; therefore, it is quite clear to understand that the two acts were directed from implementation for the objective to be referred to and referenced together when addressing cybercrime.[766]

Regarding commentary on the provisions of the *CPA*, according to Nortjé and Myburgh,[767] Bouwer,[768] and Basdeo,[769] they tend to question whether both the words, "article" and "premises" as defined in section 1 includes data, digital files, computers, or any form of an intangible object or evidence and not just tangible objects.[770] They continue to argue that the *CPA* does not adequately explain the position of intangibles involved as an object in a cybercrime or the position of a computer as a prescribed premise.[771] They discuss the very nature and legal position of "data" and define "data" as any information, report or record converted into a digital form or file.[772] According to the aforementioned, section 20 of the *CPA* is then considered questionable regarding its application to cybercrime investigation procedures.[773]

According to the South African Law Commission (SALRC),[774] considering their discussion paper, Computer-Related Crime,[775] the SALRC argues that the stipulations and provisions found in the *CPA* regarding the words, "article" and "premises" were intentionally developed prior to the existence and position of intangible objects or electronic evidence.[776] The SALRC continued to argue that Chapter 2 of the *CPA* cannot be applied to

764 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.
765 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.
766 Van der Merwe *et al Information and Communications Technology Law* 99.
767 Nortjé and Myburgh 2019 *PER/PERLJ* 10.
768 Bouwer 2014 *SACJ* 171.
769 Basdeo 2012 *SACJ* 198, 205.
770 Nortjé and Myburgh 2019 *PER/PERLJ* 11-13.
771 Nortjé and Myburgh 2019 *PER/PERLJ* 11-13.
772 Nortjé and Myburgh 2019 *PER/PERLJ* 11-13.
773 Nortjé and Myburgh 2019 *PER/PERLJ* 11-13.
774 South African Law Commission 1998 *Computer-Related Crime, Project 108*.
775 South African Law Commission 1998 *Computer-Related Crime, Project 108*.
776 South African Law Commission 1998 *Computer-Related Crime, Project 108* 11.

cyber-related matters regarding the search and seizure of intangible objects as the *CPA* is focused on being object-based, specifically regarding "articles" and evidence in criminal proceedings.[777] Throughout the paper, the SALRC continually suggests that the *CPA* should be amended to include and specifically provide for the search-and-seizure procedures as well as the admissibility of intangible objects as authentic evidence in criminal proceedings.[778]

The SALRC refers to the provisions of the *CPA* regulating criminal prosecution procedures of committed offences as well as the position of admissible electronic evidence or objects in the *CPA*;[779] for example, after an intangible object, such as an electronic document, has been searched and seized by an authorised officer, the electronic document must be encrypted immediately to provide a digital trail of authentic evidence to present to the court of law that the intangible object or evidence was never interfered or tampered with from the moment of seizure, leading up to the presentation thereof in court.[780]

According to Schultz,[781] the *CPA* does not provide adequate measures to properly address cybercrime. Although the *CPA* is referred to in criminal proceedings regarding investigations, search-and-seizures procedures and prosecution, it is important to acknowledge that the *CPA* does not specifically provide for offences committed in the cyberspace.[782] Therefore, superior courts recommend that in order to avoid any uncertainty regarding the investigation, the search-and-seizure process and the prosecution procedures in criminal proceedings, the *CPA* must be amended to incorporate modern provisions addressing the investigation, the search-and-seizure process and the prosecution procedures of the cyberspace.[783]

3.5 Protection of Personal Information Act 4 of 2013

777 South African Law Commission 1998 *Computer-Related Crime, Project 108* 11.
778 South African Law Commission 1998 *Computer-Related Crime, Project 108* 11.
779 Van der Merwe *et al Information and Communications Technology Law* 100.
780 Van der Merwe *et al Information and Communications Technology Law* 100.
781 Schultz *Cybercrime: An Analysis of Current legislation in South Africa* 36.
782 Du Toit *The Search Warrant Provisions of the Cybercrimes Act and their Relationship with the Criminal Procedure Act* 778.
783 Du Toit *The Search Warrant Provisions of the Cybercrimes Act and their Relationship with the Criminal Procedure Act* 778.

The South African Parliament assented to the *Protection of Personal Information Act* 4 of 2013 (hereafter the "*POPIA*") on 19 November 2013;[784] however, the *POPIA* was not immediately implemented or signed into law.[785] Nevertheless, the *POPIA* was continually reviewed and amended throughout the years, 2014 and 2020;[786] the latest amendment was commenced and implemented in July 2021.[787] The *POPIA* repealed the former *Protection of Personal Information Bill* [B9], 2009.[788] With the implementation of the *POPIA* South Africa believes it to be one of the key pieces of legislation in assisting national authorities in combatting cybercrime in South Africa.[789]

The main objectives of the *POPIA* include:[790] To promote the protection of personal or private information regarding public and private entities, to establish specific requirements and lawful conditions for the processing of personal or private information, to establish the Information Regulator and its functions in terms of the *POPIA* as well as the *Promotion of Access to Information Act* 2 of 2000, to provide and deliver codes of conduct regarding the processing of personal or private information, to protect the rights of individuals regarding unwanted electronic communications, to regulate the transmission of personal or private information within and outside of South Africa, and to address any additional matters relating to the communication of information.[791]

The *POPIA* also recognizes section 14 of the *Constitution*, i.e. the right to privacy,[792] and strives to uphold and protect any individual, organisation and the government against the unlawful action of retention, collection, use or dissemination of personal or private information.[793] The *POPIA* was originally drafted inspired by the European Union's General Data Protection Regulation framework (hereafter the "GDPR") and predates the GDPR by several years.[794] The GDPR is an international security framework, drafted in the year

784 Preamble of the *Protection of Personal Information* 4 of 2013.
785 Usercentrics 2022 https://usercentrics.com/knowledge-hub/south-africa-popia-protection-of-personal-information-act-overview/.
786 GG 37544 of 11 April 2014; GG 43461 of 22 June 2020.
787 GG 44383 of 1 April 2021.
788 Usercentrics 2022 https://usercentrics.com/knowledge-hub/south-africa-popia-protection-of-personal-information-act-overview/.
789 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.
790 Preamble of the *POPIA*.
791 Preamble of the *POPIA*.
792 Section 14 of the *Constitution*.
793 Section 14 of the *Constitution*.
794 Pinarbasi 2022 https://blog.didomi.io/en/popia-south-africa.

2018.[795] The nature of the GDPR is based on addressing data privacy, data processing and data protection or security in the online environment,[796] it also considers the technological and societal changes and challenges in the online environment,[797] and encourages natural and juristic persons to comply with the available data protection policies and pieces of legislation of the framework.[798]

The *POPIA* comprises 12 chapters, containing 115 sections and 1 schedule.[799] Chapter 1 defines the keywords found in the *POPIA*, and discusses the purpose of the *POPIA*.[800] Keywords to consider in understanding the objective of the *POPIA*,[801]

> "personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to-
> (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
> (b) information relating to the education or the medical, financial, criminal or employment history of the person;
> (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
> (d) the biometric information of the person;
> (e) the personal opinions, views or preferences of the person;
> (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
> (g) the views or opinions of another individual about the person; and
> (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;[802]

and,[803]

> "processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including-
> (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
> (b) dissemination by means of transmission, distribution or making available in any other form; or

795 Mhungu *et al* 2018 *The General Data Protection Regulation*.
796 Mhungu *et al* 2018 *The General Data Protection Regulation*.
797 Mhungu *et al* 2018 *The General Data Protection Regulation*.
798 Mhungu *et al* 2018 *The General Data Protection Regulation*.
799 The *POPIA*.
800 Chapter 1 of the *POPIA*.
801 Section 1 of the *POPIA*.
802 Section 1 of the *POPIA*.
803 Section 1 of the *POPIA*.

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;[804]

Chapter 2 discusses the application and interpretation of the *POPIA*, the lawful monitoring and processing of information, legal rights, responsibilities available to data subjects, and presents a list of specific exclusions.[805] The application of the *POPIA* depends on the position of both entities processing, monitoring and providing personal or private information regardless of being a natural or juristic person.[806] The *POPIA* affects various organisations and the government more than it appears to affect individuals, unless the individual is a victim to an information breach, violating their privacy.[807] Regardless, any and all business-related operations occurring in South Africa are strictly subject to the provisions envisaged in the *POPIA*.[808] The *POPIA* also obligates the implementation of precautionary security measures, for example, installing and securing firewalls to prevent data breaches.[809]

According to the *POPIA* these security measures will navigate and mitigate the possibility of liabilities regarding cybercrime.[810] The provisions envisaged in the *POPIA* regarding the data processing procedure are applied to South African as well as foreign entities.[811] Section 6 of the *POPIA* lists various exclusions regarding its application;[812] these include, non-commercial activities specifically referring to personal activities, the position of presenting data anonymously, the data involves matters of national security, whether the data is processed by law enforcement or government agencies, and whether the data forms part of South Africa's courts of law and their functions.[813]

Section 7 continues listing additional legal exclusions such as journalism, literary-related matters or artistic expression; these exclusions are protected by the right to freedom of

---

804 Section 1 of the *POPIA*.
805 Chapter 2 of the *POPIA*.
806 Usercentrics 2022 https://usercentrics.com/knowledge-hub/south-africa-popia-protection-of-personal-information-act-overview/.
807 Usercentrics 2022 https://usercentrics.com/knowledge-hub/south-africa-popia-protection-of-personal-information-act-overview/.
808 Pinarbasi 2022 https://blog.didomi.io/en/popia-south-africa.
809 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.
810 Gunning and Gabryk 2021 https://www.mondaq.com/southafrica/data-protection/1111854/data-breaches-and-the-interplay-between-popia-ecta-and-the-cybercrimes-act-podcast.
811 Pinarbasi 2022 https://blog.didomi.io/en/popia-south-africa.
812 Section 6 of the *POPIA*.
813 Usercentrics 2022 https://usercentrics.com/knowledge-hub/south-africa-popia-protection-of-personal-information-act-overview/.

expression as envisaged in section 10 of the *Constitution*.[814] Chapter 3 is the data protection chapter; this chapter entails the 8 conditions available for the lawful procedure of processing personal or private information; these conditions include;[815] accountability, limitations, purpose specification, further or additional processing limitations, information quality, transparency and openness, various security safeguards and data subject participation.[816] Chapter 4 continues on the provisions envisaged in Chapter 3 regarding the exemptions from the 8 conditions for the processing of personal or private information.[817]

Chapter 5 addresses supervision; this discusses powers, duties and functions of the Information Regulator and the Information Office regarding the monitoring and enforcement of compliance with the provisions of the *POPIA*.[818] The Information Regulator is empowered to investigate any matter regarding the unlawful infringement or breach of personal or private information.[819] The Regulator's powers include the summoning of parties before the Regulator, the receiving and reviewing of presented evidence, conducting of private interviews with involved parties and entering, searching, or seizing any premises or article in relation to the committed offence in terms of the *POPIA*.[820]

The Information Regulator is also allowed to deliver penalties, such as fines up to ZAR 10 million[821] or imprisonment[822] if there appears to be non-compliance regarding the *POPIA*'s provisions.[823] The Information Regulator reports to the South African Parliament.[824] Chapter 6 entails prior authorisation.[825] Chapter 7 provides the position and procedures for the national codes of conduct.[826] Chapter 8 entails the rights of data subjects regarding unwanted electronic communications.[827] Chapter 9 addresses the transmission of personal

814 Sectioon 7 of the *POPIA*.
815 Chapter 3 of the *POPIA*.
816 Chapter 3 of the *POPIA*; Section 8-25 of the *POPIA*.
817 Chapter 4 of the *POPIA*.
818 Chapter 5 of the *POPIA*.
819 Pillay 2017 https://www.withoutprejudice.co.za/free/article/5659/view.
820 Pillay 2017 https://www.withoutprejudice.co.za/free/article/5659/view.
821 Section 109 of the *POPIA*.
822 Section 107 of the *POPIA*.
823 Snail 2021 https://cyberbrics.info/legal-intersections-between-the-protection-of-personal-information-act-4-of-2013-popia-and-the-cyber-crimes-act-19-of-2020-2/.
824 Usercentrics 2022 https://usercentrics.com/knowledge-hub/south-africa-popia-protection-of-personal-information-act-overview/.
825 Chapter 6 of the *POPIA*.
826 Chapter 7 of the *POPIA*.
827 Chapter 8 of the *POPIA*.

or private information inside and outside of South Africa.[828] Chapter 10 critically discusses the numerous procedures regarding enforcement exercised by the Information Regulator and any legal procedure taking place in terms of the *POPIA*.[829]

Chapter 11 lists different offences and their penalties based on the unlawful infringement or non-compliance with the provisions of the *POPIA*.[830] In the *POPIA*, very few, but specific offences are discussed.[831] Chapter 12 continues with the general provisions, such as the amendment of various laws, arrangements, and commencements.[832] And lastly, the schedule attached to the *POPIA* discusses the relevant laws as amended by section 110 (amendment of laws).[833] As mentioned in Chapter 11 regarding the list of different cyber-offences, it is important to acknowledge that the *POPIA* does not create or establish any new type of cyber-offence.[834]

However, the discussed offences include, the unlawful obstruction or hindrance of the Information Regulator's functions or duties,[835] a breach of confidentiality,[836] the unlawful obstruction regarding the execution of an authorised warrant,[837] failure to comply with information or enforcement notices,[838] offences committed by witnesses presenting evidence,[839] unlawful actions performed by an involved party with an account number,[840] and unlawful actions performed by third parties with an account number.[841] However, when a natural or a juristic person fails to comply with the provisions envisaged the *POPIA*, it does not mean that an offence is automatically committed.[842] The *Cybercrimes Act* provides for the position and offence of non-compliance regarding the *POPIA*.[843]

---

828 Chapter 9 of the *POPIA*.
829 Chapter 10 of the *POPIA*.
830 Chapter 11 of the *POPIA*.
831 Section 100-106 of the *POPIA*.
832 Chapter 12 of the *POPIA*.
833 Schedule of the *POPIA*.
834 Gunning and Gabryk 2021 https://www.mondaq.com/southafrica/data-protection/1111854/data-breaches-and-the-interplay-between-popia-ecta-and-the-cybercrimes-act-podcast.
835 Section 100 of the *POPIA*.
836 Section 101 of the *POPIA*.
837 Section 102 of the *POPIA*.
838 Section 103 of the *POPIA*.
839 Section 104 of the *POPIA*.
840 Section 105 of the *POPIA*.
841 Section 106 of the *POPIA*.
842 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.
843 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.

According to De Wet and Olën[844] as well as Toona,[845] although the newly implemented *Cybercrimes Act* explicitly deals with cybercrime in South Africa, it cannot be considered or applied without direct reference to the *POPIA*.[846] While both the focus of the *Cybercrimes Act* and the *POPIA* appears to be on data, information, and files, these statutes still vary; however, there are similarities regarding cyber-offences, the reporting as well as the investigation thereof.[847] This refers to organisations and individuals reporting any breach or offence occurring in the cyberspace to established cyber-entities or national authorities.[848] Collectively, the various objectives of the *Cybercrimes Act* and the *POPIA* are to provide protection regarding data and the transmission of data regardless of the geographic location.[849]

Toona continues by stating that the connection between the *Cybercrimes Act* and the *POPIA* is based on the safeguarding of personal and private information.[850] Toona adds that during cybercrime investigation procedures, computer forensics and cyber-experts retrieve personal or private information from a device; therefore, the investigation procedure must be conducted according to the provisions envisaged in the *POPIA* to avoid any repercussions.[851] As mentioned, the *POPIA* aims to promote the protection of personal or private information being processed and transmitted by public and private entities.[852] This includes the personal processing scope of information as well as the material scope of information.[853]

Consider the following examples of general data processing in South Africa: Activities such as the disclosure of information, the use or collection of information and the identification

844 De Wet and Olën 2022 https://www.dataguidance.com/opinion/south-africa-cybercrimes-act-its-relationship%C2%A0-popia.
845 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.
846 De Wet and Olën 2022 https://www.dataguidance.com/opinion/south-africa-cybercrimes-act-its-relationship%C2%A0-popia.
847 De Wet and Olën 2022 https://www.dataguidance.com/opinion/south-africa-cybercrimes-act-its-relationship%C2%A0-popia.
848 De Wet and Olën 2022 https://www.dataguidance.com/opinion/south-africa-cybercrimes-act-its-relationship%C2%A0-popia.
849 De Wet and Olën 2022 https://www.dataguidance.com/opinion/south-africa-cybercrimes-act-its-relationship%C2%A0-popia.
850 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.
851 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.
852 Manaleng 2021 https://ewn.co.za/2021/06/03/think-before-you-click-ramaphosa-signs-cybercrimes-act-into-law.
853 Pinarbasi 2022 https://blog.didomi.io/en/popia-south-africa.

of the territorial scope of information.[854] According to Byleveld,[855] the provisions of the *POPIA* clearly set out the position regarding certain documentation, the retention of records and the duty to report a breach of personal or private information in order to assist national authorities in combatting cybercrime in South Africa.[856] The *POPIA* strives to protect data subjects from any form of a data breach,[857] and encourages the integrity and strength of both public and private entities regarding data breaches.[858]

When a breach of personal or private information occurs or a notice of breach is given, it is required that the complainant, regardless of being a public or private entity, must inform the Information Regulator and all involved or affected data subjects.[859] Organisations and businesses are required to comply with the provisions envisaged in the *POPIA*;[860] this includes consideration of the 8 conditions of lawful data processing, informing data subjects about the collection, evaluation and use of data, identification of the legal basis for the processing of personal or private information, for example, contractual obligations, operating in terms of the data collection regulations and rules, focusing on international data transfers, investing in data protection assessments and data processing records, and addressing the position of data retention.[861]

As mentioned, the *POPIA* focuses on upholding the privacy of data.[862] This relates to the obligation of institutions or entities and the aforementioned conditions to collect, process and store personal or private information in a lawful manner.[863] However, if an institution fails to comply with the conditions, the institution or entity will be dealt with in terms of the *POPIA*.[864] Lastly, the *POPIA* also partially addresses website or internet "cookies"; these "cookies" are characterised as micro text files containing unique data (for example,

---

854 Pinarbasi 2022 https://blog.didomi.io/en/popia-south-africa.
855 Byleveld 2022 https://www.fluidrock.co.za/a-brief-overview-of-the-cybercrimes-act-19-of-2020/.
856 Byleveld 2022 https://www.fluidrock.co.za/a-brief-overview-of-the-cybercrimes-act-19-of-2020/.
857 Pillay 2017 https://www.withoutprejudice.co.za/free/article/5659/view.
858 Pillay 2017 https://www.withoutprejudice.co.za/free/article/5659/view.
859 Gunning and Gabryk 2021 https://www.mondaq.com/southafrica/data-protection/1111854/data-breaches-and-the-interplay-between-popia-ecta-and-the-cybercrimes-act-podcast.
860 Pinarbasi 2022 https://blog.didomi.io/en/popia-south-africa.
861 Pinarbasi 2022 https://blog.didomi.io/en/popia-south-africa.
862 Van Deventer 2021 https://www.vandeventers.law/Legal-Articles/entryid/1954/will-the-popi-act-cybercrimes-act-work-well-together.
863 Van Deventer 2021 https://www.vandeventers.law/Legal-Articles/entryid/1954/will-the-popi-act-cybercrimes-act-work-well-together.
864 Van Deventer 2021 https://www.vandeventers.law/Legal-Articles/entryid/1954/will-the-popi-act-cybercrimes-act-work-well-together.

an email or phone number) to identify your smart device in or to a network.[865] When an individual visits a website, the website's browser receives a "cookie" and stores it in a "cookie" file in the browser.[866]

When an individual visits the same website again, the "cookie" will identify the user and load the information from the previous website visit, for example auto-filled information or passwords.[867] These "cookies" must comply with the *POPIA*'s provisions regarding the lawful processing of data.[868] In conclusion, a cybercrime, for example, phishing, can upon occurrence, trigger various pieces of cybercrime legislation such as a breach in terms of the *POPIA*, an offence in terms of the *ECTA* and a crime in terms of the *Cybercrimes Act*.[869] However, the type, circumstances and nature of the cybercrime play an important role in identifying which relevant cybercrime piece of legislation is to be applied.[870]

The collaboration of these South African pieces of cybercrime legislation regarding data protection and data privacy will expectantly bring South Africa up to international standards.[871] The *POPIA* enhances the protection of personal or private information,[872] and enables individuals to enforce and enjoy their fundamental right to privacy as envisaged in the *Constitution*.[873] Section 14 of the *Constitution*, the right to privacy is only considered realistic and achievable if the cyberspace is considered secure, simplified and regulated.[874]

3.6 The Films and Publications Amendment Act 11 of 2019

The *Films and Publications Amendment Act* 11 of 2019 (hereafter the "*FPAA*") is considered a South African statute completely independent from any other type of ICT-related statutes.[875] The *FPAA* was assented to on 19 September 2019,[876] and amended the

865 Nguyen and McNally 2023 https://allaboutcookies.org/what-is-a-cookie.
866 Nguyen and McNally 2023 https://allaboutcookies.org/what-is-a-cookie.
867 Nguyen and McNally 2023 https://allaboutcookies.org/what-is-a-cookie.
868 Nguyen and McNally 2023 https://allaboutcookies.org/what-is-a-cookie.
869 Gunning and Gabryk 2021 https://www.mondaq.com/southafrica/data-protection/1111854/data-breaches-and-the-interplay-between-popia-ecta-and-the-cybercrimes-act-podcast.
870 Gunning and Gabryk 2021 https://www.mondaq.com/southafrica/data-protection/1111854/data-breaches-and-the-interplay-between-popia-ecta-and-the-cybercrimes-act-podcast.
871 Snail 2021 https://cyberbrics.info/legal-intersections-between-the-protection-of-personal-information-act-4-of-2013-popia-and-the-cyber-crimes-act-19-of-2020-2/.
872 Pinarbasi 2022 https://blog.didomi.io/en/popia-south-africa.
873 Pinarbasi 2022 https://blog.didomi.io/en/popia-south-africa.
874 Van Deventer 2021 https://www.vandeventers.law/Legal-Articles/entryid/1954/will-the-popi-act-cybercrimes-act-work-well-together.
875 Van der Merwe *et al Information and Communications Technology Law* 68.

Films and Publications Act 65 of 1996 (hereafter the "*FPA*").[877] The most recent amendment to the *FPAA* and the *FPA* is the *Films and Publications Amendment Regulations*, 2022.[878] The *Regulations* were first published in 2020 with the objective of clarifying specific provisions envisaged in the *FPAA*.[879] These provisions are in relation to online distributors and online streaming services.[880] The *Regulations* comprise 3 amended schedules,[881] and seek to give full effect to the *FPAA*.[882]

The main objectives of the *FPAA* are to address and regulate the procedure of the online distribution of films, videos, games, music and publications in South Africa, to provide the legal process and requirements of distributing content online, and to address user generated content (UGC) on social media or any communication platforms.[883] The *FPAA* also extends the very objective and power of the Film and Publications Board (FPB) in strictly classifying, monitoring, and regulating the conduct and content of general online distributors in South Africa.[884] The FPB also has the power to address online distributors infringing upon the provisions envisaged in the *FPAA*.[885] The *FPAA* also establishes the Enforcement Committee along with its legal obligations and powers.[886]

The *FPAA* considers any natural or juristic person connected to the cyberspace as an online distributor once the natural or juristic person posts content, for example, photographs on social media or communication platforms.[887] The *FPAA* amends and

---

876 *Films and Publications Amendment Act* 11 of 2019.

877 *Films and Publications Act* 65 of 1996; MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force.

878 GG 46839 of 2 September 2022.

879 MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force.

880 MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force.

881 GG 46839 of 2 September 2022.

882 MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force.

883 Preamble of the *FPAA*.

884 MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force.

885 Wrensch 2022 https://www.michalsons.com/blog/alert-the-film-and-publications-amendment-act-is-here-now-what/56248#:~:text=The%20Film%20and%20Publications%20Amendment%20Act%20considers%20everyone%20a%20distributor,and%20a%20commercial%20online%20distributor.

886 Preamble of the *FPAA*.

887 Wrensch 2022 https://www.michalsons.com/blog/alert-the-film-and-publications-amendment-act-is-here-now-what/56248#:~:text=The%20Film%20and%20Publications%20Amendment%20Act%20considers%20everyone%20a%20distributor,and%20a%20commercial%20online%20distributor.

clarifies the 8 chapters and 12 schedules of the former *FPA*.[888] Chapter 1 of the *FPA* provides a list of definitions.[889] Chapter 2 establishes the FPB and the FPB Review Board.[890] Chapter 3 addresses the procedure of required applications and complaints against online publications.[891] Chapter 4 continues with the required applications for, and the distinct classification of films.[892]

Chapter 5 provides for the various types of legal procedures, rights and appeals.[893] Chapter 6 provides the several exemptions available regarding films and publications.[894] Chapter 7 addresses the online code of conduct to classifications and prohibitions.[895] And lastly, Chapter 8 entails the position of regulations, amendments and the repeal of laws.[896] The 12 schedules of the *FPA* discuss the specific type of classifications, the nature of sexual conduct and presents a list of former South African acts.[897] Regarding the *FPAA*, the *FPAA* introduces several definitions in section 1 to assist the *FPA* in defining actions, conduct, online distributors, and content.[898] Some of these definitions include,

"Distribute" is defined as,[899]

> "distribute" [,] in relation to a film, game or a publication, without derogating from the ordinary meaning of that word, includes-
> (a) to stream content through the internet, social media or other electronic mediums;
> (b) to sell, hire out or offer or keep for sale or hire, including using the internet; and[,]
> (c) for purposes of sections 24A and 24B, [includes] to hand or exhibit a film, game or a publication to a person under the age of 18 years, and also the failure to take reasonable steps to prevent access thereof by such a person;"[900]

and,

"Film" is defined as,[901]

---

888 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.
889 Chapter 1 of the *FPA*.
890 Chapter 2 of the *FPA*.
891 Chapter 3 of the *FPA*.
892 Chapter 4 of the *FPA*.
893 Chapter 5 of the *FPA*.
894 Chapter 6 of the *FPA*.
895 Chapter 7 of the *FPA*.
896 Chapter 8 of the *FPA*.
897 Schedule 1 -12 of the *FPA*.
898 Section 1 of the *FPAA*.
899 Section 1 of the *FPAA*.
900 Section 1 of the *FPAA*.
901 Section 1 of the *FPAA*.

> "film" means any sequence of visual images recorded in such manner that by using such recording, such images will be capable of being seen as a moving picture, and includes any picture intended for exhibition through any medium, including using the internet, or device;[902]

Considering the provisions of the *FPAA*, the cyberspace along with all digital or online content will be appropriately addressed through the creation, production, possession and distribution of films, videos, games, music and publications.[903] This relates directly to the *FPAA*'s extensive application regarding UGCs and the access to social media or communication platforms.[904] The *FPAA* created two distinctive categories of online distributors, a commercial online distributor, or a non-commercial online distributor.[905] The objective of a non-commercial online distributor can be defined as, the content posted online does not generate a form of income and the content is exclusively for personal or private use; this type of content is not classified.[906]

Regarding classification, both the *FPA* and the *FPAA* require all online distributors to be registered with the FPB to ensure that all online content must be submitted, classified (or rated) and approved before it is posted to a social media or communication platform.[907] The *FPAA* insists that no game or film may be distributed in South Africa, without being classified according to the distinct provisions of *FPA*.[908] The *FPAA* also provides the option of self-classification to online distributors; this entails that the online distributor must pay a license fee to the FPB to be able to perform a self-classification and be accredited before posting content online.[909]

---

902 Section 1 of the *FPAA*.

903 MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force.

904 MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force.

905 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.

906 Wrensch 2022 https://www.michalsons.com/blog/alert-the-film-and-publications-amendment-act-is-here-now-what/56248#:~:text=The%20Film%20and%20Publications%20Amendment%20Act%20considers%20everyone%20a%20distributor,and%20a%20commercial%20online%20distributor.

907 MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force.

908 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.

909 MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force.

There are, however, certain requirements which the online distributor must adhere to before being able to qualify for or obtain the application of self-classification.[910] Once an online distributor qualifies for the application of self-classification, the FPB is entitled to request details (at any time) regarding the content from the online distributor.[911] The *FPAA* also addresses the position of international content classifications.[912] In terms of the provisions in the *FPAA*, any South African citizen has the right to file a complaint to the FPB, regarding unclassified, prohibited, or potential prohibited content posted on social media or communication platforms.[913]

The FPB will then investigate and consider all merit and evidence of the complaint and will only then react in terms of the *ECTA* and remove or terminate the distributed content.[914] The complainant is required to provide identification to the FPB regarding the online distributor behind the posted content.[915] If, in the case of the posted content, child pornography is displayed, the FPB must refer the case directly to the SAPS.[916] Although smart devices, such as computers, are primarily used for commercial-related matters such as communication or for business purposes, for example, the transfer of money, these devices can also be used in a non-commercial matter, such as cyber-obscenity, specifically child pornography.[917]

Regarding cyber-obscenity, South Africa protects its children (18 years and younger) in section 28 of the *Constitution* (Bill of Rights);[918] this includes being protected from abuse or being degraded.[919] Specifically focused on child pornography, South Africa responded with the provisions envisaged in the *FPA* and the *FPAA* and criminalises, as well as strictly prohibits online child pornography or the distribution thereof.[920]

---

910 Section 18C(2) of the *FPAA*.
911 Section 18C(4) of the *FPAA*.
912 MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force.
913 Section 18E of the *FPAA*.
914 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.
915 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.
916 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.
917 Van der Merwe *et al Information and Communications Technology Law* 86.
918 Section 28 of the *Constitution*.
919 Section 28(d) of the *Constitution*.
920 Maat *Cyber Crime: A Comparative Law Analysis* 251.

"Child pornography" can be defined as,[921]

> "child pornography" means any image, however created, or any description or presentation of a person, real or simulated, who is, or who is depicted or described or presented as being, under the age of 18 years, of an explicit or sexual nature, whether such image or description or presentation is intended to stimulate erotic or aesthetic feelings or not …"[922]

As for the position and powers of the FPB regarding the distribution of private sexual photographs and films,[923] it is argued that the FPB's scope of power and functions fall outside of the aforementioned matter; nevertheless, it appears that the *Cybercrimes Act* addresses the matter extensively.[924] The distribution of private sexual photographs and films on social media or communication platforms is strictly prohibited due to the malicious conduct to intentionally cause harm to another individual.[925] There are, however, exceptions to where such online sexual materials can be referred, for the sole purpose of preventing, detecting or investigating such an offence.[926]

The *FPAA* also addresses the offence of distributing any information, publication, film or game, online, which amounts to the declaration of war, propaganda, violence or hate speech against South Africa or the government.[927] The penalty for such an offence is a fine (not exceeding ZAR 150 000) or imprisonment (not exceeding 2 years).[928] However, it is important to acknowledge that the FPB is not appropriately equipped to assess or review these types of distributed content, and therefore the matter will be directly referred to the appropriate national authority.[929]

The *FPAA* also amends the *FPA* regarding internet access providers; this entails the situation that if any internet access provider services are being used for hosting the distribution of child pornography, war, propaganda, violence or hate speech, the internet

---

921 Section 1 of the *Criminal Law (Sexual Offences and Related Matters) Amendment Act* 32 of 2007.
922 Section 1 of the *Criminal Law (Sexual Offences and Related Matters) Amendment Act* 32 of 2007.
923 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.
924 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.
925 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.
926 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.
927 Section 18H of the *FPAA*.
928 Section 24G of the *FPAA*.
929 MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force.

access provider must be reported to the national authorities and evidence must be presented for the purpose of addressing and investigating the matter.[930] The *FPAA* also amended the *FPA* by establishing the Enforcement Committee.[931] The *FPAA* requires that the Enforcement Committee must operate as impartial and independent, and must perform its functions and objectives without favour, fear, or prejudice, in the same manner as the FPB and Council of Appeal Tribunal.[932]

The functions of the Enforcement Committee are to investigate cases relating to the *FPAA* and the FPB, to adjudicate cases and declare relevant findings, consider evidence under affirmation or oath as presented by an affidavit, impose a fine, suspend a registration certificate or apply to court for the completion and enforcement of certain penalties.[933] The Enforcement Committee is, therefore, considered a quasi-judicial body[934] with judicially empowered characteristics.[935] According to the *FPAA* the powers and functions of compliance officers were also altered and amended.[936]

This includes the classification of information, publications, games and films, to ensure that the distribution of online content is appropriate, to enter a premises or a process of a sale with authorisation, to review or assess articles, to review or assess a list of articles with authorisation, for example, films, to issue a compliance notice, to direct the removal of a film, publication or game and request for proof of a registration certificate as an online distributor.[937] In conclusion, the primary objective of the *FPAA* is to enhance and clarify the provisions envisaged in the *FPA*.[938] The *FPAA* regulates online distributors, the procedure and registration of online distributing in South Africa and entails the rights and

---

930 Section 28 of the *FPAA*.

931 Preamble of the *FPAA*.

932 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.

933 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.

934 According to the Merriam-Webster Dictionary 2023 at https://www.merriam-webster.com/dictionary/quasi-judicial, quasi-judicial can be defined as a legal administrative procedure or body focused and concerned with the adjudication of certain rights rather than promulgated or implemented rules that require specific discretion or a legal review.

935 Preamble of the *FPAA*.

936 Section 15A of the *FPAA*.

937 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.

938 MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force.

responsibilities of distributing and reporting content requirements and establishes the role of the FPB in the online environment.[939]

3.7 Conclusion

It is evident that South Africa has been actively adopting, promulgating, and implementing various pieces of cybercrime legislation, frameworks, and policies over the years regardless of the increased rate of cybercrime in the cyberspace.[940] However, it is imperative to note that the proliferation of national cybercrime legislation, frameworks and policies do not create any additional cyber-related challenges for South Africa regarding cybercrime, especially considering the legal impact and effect of the South African subsidiarity principle, as discussed above.[941]

Considering the discussed cybercrime legislation, frameworks, and policies, one would assume that cybercrime statistics in South Africa would have been reduced quite substantially, nevertheless cybercrime continues to invade the South African cyberspace and national ICTs. This concern leaves the South African legislature with just one question:[942] Will the recently implemented *Cybercrimes Act* be considered as a fundamental breakthrough in addressing and combatting cybercrime inside South African borders? The *Cybercrimes Act* will be critically discussed in the following chapter.

939 Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/.
940 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.
941 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.
942 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.

Chapter 4 The *Cybercrimes Act* 19 of 2020

4.1 The History and Evolution of the Cybercrimes Act 19 of 2020

The history and evolution of cybercrime is as old as the cyberspace and computers themself.[943] Considering that we find ourselves amidst the Fourth Industrial Revolution (4IR),[944] continually confronting the immeasurable extent of the cyberspace, cybercrime is not considered a foreign concept, especially not in South Africa.[945] In the modern world of digitalisation, an international digital revolution led to a great surge of technological and digital advancements in the cyberspace along with considering the adverse impact of the Covid-19 pandemic.[946] The evolutionary nature of the cyberspace is an international concern for numerous countries, regarding the daily demand and increase of the general omnipresent online environment.[947]

These modernistic problems and challenges seek for modernistic solutions and pieces of legislation that will govern and protect South Africans by addressing the legal aspects and implications of these challenges.[948] South Africa has been excessively targeted through cybercrime in the cyberspace due to the lack of the country's cyber-awareness, cybersecurity, and the development and enforcement of cybercrime legislation.[949] According to Mabunda,[950] another reason for South Africa's slow adoption of adequate cybercrime legislation is due to that South Africa is considered a mere consumer of information communication technologies (ICTs) rather than a producer, therefore lacking in cyber-awareness, cybersecurity and the development of cybercrime legislation.[951]

The South African courts dealt with early cases of cybercrime in *Le Roux v Dey* (2011) 3 SA 274 (CC) (hereafter the "*Le Roux* case") and *Manyi v Dlamini* 2018 ZAGPPHC 563

---

943 Mabunda *The South African Legislative Response to Cybercrime* 23.

944 Trevino 2021 https://www.forbes.com/sites/forbestechcouncil/2021/01/29/cyber-attacks-of-the-fourth-industrial-revolution/?sh=2b078b826183.

945 Trevino 2021 https://www.forbes.com/sites/forbestechcouncil/2021/01/29/cyber-attacks-of-the-fourth-industrial-revolution/?sh=2b078b826183.

946 Du Preez 2023 https://www.burgerhuyserattorneys.co.za/the-governance-of-cyber-ict-law-in-south-africa-explained/.

947 Burger-Smidt 2022 https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/.

948 Du Preez 2023 https://www.burgerhuyserattorneys.co.za/the-governance-of-cyber-ict-law-in-south-africa-explained/.

949 Desai 2023 https://www.albaraka.co.za/blogs/legalease-publication-3-2022/impact-of-the-cybercrimes-act-of-financial-institutions.

950 Mabunda *The South African Legislative Response to Cybercrime* 26.

951 Mabunda *The South African Legislative Response to Cybercrime* 26.

(hereafter the "*Manyi* case").[952] These court cases supported the drafting of the *Cybercrimes Act* 19 of 2020 (hereafter the "*Cybercrimes Act*").[953] In the *Le Roux* case,[954] the three applicants, Mr Le Roux, Mr Gildenhuys and Mr Janse van Rensburg sought for leave of appeal against an order and judgement delivered by the Supreme Court of Appeal in awarding compensation and publishing a public apology to the respondent, Dr Dey.[955] The applicants (then schoolchildren) fabricated and disseminated a computer-created image of the respondent (then deputy principal of their high school), Dr Dey.[956] The image revealed two naked men sitting in a sexually suggestive position, with the school crest covering the genital areas of the two men.[957]

At first, the High Court dealt with two claims from the respondent based on defamation and the infringement of his dignity.[958] Progressively, the case was later referred to the Constitutional Court and the Constitutional Court delivered the final judgement of ZAR 25 000 as compensation to the respondent.[959] Nevertheless, there were various elements presented in the case, for example, the applicants applied the defence of freedom of expression (section 16 of the *Constitution*), where the Court had to consider and appropriately address and deliver judgment on the *Le Roux* case.[960] In the *Manyi* case,[961] the plaintiff, Mr Manyi instituted a defamation claim against the defendant, Mr Dhlamini, based on inappropriate statements and allegations made by the defendant about the plaintiff on a mutual WhatsApp group.[962]

The defendant shared and posted inappropriate statements regarding the plaintiff's sexual life and threatened the plaintiff with psychological harm.[963] The Court discussed the infringement of the plaintiff's rights, which included the right to human dignity (section 10 of the *Constitution*) and the right to freedom and security of a person (section 12 of the *Constitution*) and ordered the defendant to pay the plaintiff compensation.[964] Considering

952 Mabeka and Cassim 2023 *Obiter* 20.
953 Mabeka and Cassim 2023 *Obiter* 20.
954 *Le Roux v Dey* (2011) 3 SA 274 (CC) (hereafter the "*Le Roux* case") 3.
955 *Le Roux* case 3.
956 *Le Roux* case 3.
957 *Le Roux* case 3.
958 *Le Roux* case 4.
959 *Le Roux* case 6.
960 Section 16 of the *Constitution*; *Le Roux* case 14.
961 *Manyi v Dlamini* 2018 ZAGPPHC 563 (hereafter the "*Manyi* case").
962 *Manyi* case 2.
963 *Manyi* case 3.
964 Section 12, section 14 of the *Constitution*; *Manyi* case 9.

a more recent case, *Ramokgopa v Nxumalo* [2022] ZAWCHC 175 (hereafter the "*Ramokgopa* case"), the plaintiff, Mr Ramokgopa instituted civil proceedings against the defendant, Miss Nxumalo.[965] The plaintiff's claim was based on both patrimonial and non-patrimonial loss.[966] The rule of law regarding a victim having a choice with the type of legal proceedings they wish to institute, will be discussed.

It appears that the defendant released a list labelled, "Rapists at UCT"[967] on social media platforms and the plaintiff's name was among the many names on the list.[968] This resulted in the plaintiff being removed from various WhatsApp groups and the plaintiff started avoiding social events, attending classes and completely isolated himself due to the adverse effect of the list on his human dignity and reputation.[969] The plaintiff confirmed seeing and working with a psychiatrist regarding the anxiety and depression after the list was released, before deciding to institute any legal proceedings.[970] The Court delivered the judgement and ordered the defendant to compensate the plaintiff based on his damaged reputation, infringed dignity and his medical expenses along with publishing a private and a public apology to the plaintiff.[971]

Despite previous implementation challenges and the extensive procedure of adopting cybercrime legislation,[972] the *Cybercrimes Act* signals South Africa's commitment to the development of national cybercrime legislation, cybersecurity and cyber-awareness.[973] Over the past few years, South Africa has been experiencing several high-profile cyber-attacks against natural and juristic persons.[974] Although various pieces of legislation have already been implemented which address cybercrime to a certain extent, South Africa continues to face numerous challenges regarding cybercrime.[975] As aforementioned, in

965 *Ramokgopa v Nxumalo* [2022] ZAWCHC 175 (hereafter the "*Ramokgopa* case") para [1].
966 *Ramokgopa* case para [1].
967 University of Cape Town.
968 *Ramokgopa* case para [2].
969 *Ramokgopa* case para [10]-[23].
970 *Ramokgopa* case para [23].
971 *Ramokgopa* case para [33]-[35].
972 Pieterse 2021 *AJIC* 15.
973 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.
974 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.
975 Desai 2023 https://www.albaraka.co.za/blogs/legalease-publication-3-2022/impact-of-the-cybercrimes-act-of-financial-institutions.

2021 South Africa was internationally ranked the country with the third highest number of cyber-victims.[976]

South Africa partially addressed cybercrime through the predecessor of the *Cybercrimes Act*, that is the *ECTA*, and although the implementation of the *ECTA* was progressive, for South Africa there is still a lot of room for improvement regarding cybercrime legislation.[977] Considering the international impact and effect of the Council of Europe, Convention on Cybercrime (hereafter the "Budapest Convention") on South African cybercrime legislation, South Africa finally responded to the threat of cybercrime by considering the provisions of the Budapest Convention.[978] During the discussion of this chapter various parallels between the provisions of the *Cybercrimes Act* and the Budapest Convention will be made.[979]

Numerous individuals, organisations, and public and private entities continue to ask why South Africa suddenly needs cybercrime legislation such as the *Cybercrimes Act*?[980] The South African legislature has come to terms with the situation that individuals, organisations and even government departments of South Africa have not yet been made aware of cybercrime and do not understand the threat of cybercrime and the adverse effects thereof.[981] Cybercrime in the cyberspace continues to be on the rise resulting in South Africa being a favourable and easy target.[982] This, therefore, brings the focus of this chapter to the *Cybercrimes Act*. The primary objective of the *Cybercrimes Act* is to keep the South African cyberspace safe and secure and aims to nationally improve the cybersecurity measures of the country.[983]

4.2 The Cybercrimes Act 19 of 2020

976 Burger-Smidt 2022 https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/.

977 Mabunda *The South African Legislative Response to Cybercrime* 18.

978 Mabeka and Cassim 2023 *Obiter* 30.

979 Mabeka and Cassim 2023 *Obiter* 30.

980 Michalsons 2022 https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa#:~:text=The%20Cybercrimes%20Act%20enables%20the,this%20is%20a%20global%20issue.

981 Michalsons 2022 https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa#:~:text=The%20Cybercrimes%20Act%20enables%20the,this%20is%20a%20global%20issue.

982 Mabunda *The South African Legislative Response to Cybercrime* 24.

983 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses; Michalsons 2022 https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa#:~:text=The%20Cybercrimes%20Act%20enables%20the,this%20is%20a%20global%20issue.

4.2.1 Introducing the Cybercrimes Act 19 of 2020

The *Cybercrimes Act* 19 of 2020 (hereafter the "*Cybercrimes Act*") was first introduced and published as the *Cybercrimes and Cybersecurity Bill* [B – 2015] (hereafter the "*Cybercrimes Bill*") (later versions included [B6 – 2017] and [B 6B – 2017]) in August 2015.[984] After its first publication and public commentary, the *Cybercrimes Bill* was reviewed and amended and presented to Parliament once again in February 2017.[985] During the journey of the *Cybercrimes Bill* and the time of public participation (2018-2021), various comments and suggestions, critical considerations and amendments were reviewed and considered by numerous government bodies, including the State Security Agency (SSA).[986]

The *Cybercrimes Act* was finally assented to in May 2021 by Parliament and most of the *Cybercrimes Act*'s provisions were signed into South African legislation by the president in December 2021.[987] It is important to note that the South African *Cybercrimes Act* is an independent piece of legislation and does not appear to have any direct reference to its cyber-predecessor, the *Cybercrimes Bill*.[988] As mentioned, the sudden impact and effect the Covid-19 pandemic had on the South African cyberspace finally convinced Parliament to respond to the threat of cybercrime by implementing the *Cybercrimes Act*.[989] The development and implementation of the *Cybercrimes Act* can only be considered effective when the online privacy of an internet user is achieved, and the cyberspace is safe and secure.[990]

---

984 Michalsons 2022 https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa#:~:text=The%20Cybercrimes%20Act%20enables%20the,this%20is%20a%20global%20issue.

985 Michalsons 2022 https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa#:~:text=The%20Cybercrimes%20Act%20enables%20the,this%20is%20a%20global%20issue.

986 The Law Society of South Africa *Comments By The Law Society of South Africa (LSSA) On The Cybercrimes and Cybersecurity Bill* 1.

987 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses; Michalsons 2022 https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa#:~:text=The%20Cybercrimes%20Act%20enables%20the,this%20is%20a%20global%20issue.

988 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 145.

989 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.

990 Van Deventer 2021 https://www.vandeventers.law/Legal-Articles/entryid/1954/will-the-popi-act-cybercrimes-act-work-well-together.

The *Cybercrimes Act* applies to all South African citizens, whether it be natural or juristic persons, public or private entities, the government, the judiciary and ISP providers.[991] The *Cybercrimes Act* is a voluminous document consisting of 9 chapters, 60 sections and 1 schedule with two substantive criminal law segments.[992] Part 1 addresses the different types of cybercrime and cyber-offences and Part 2 addresses malicious communications.[993] The extensive objectives of the *Cybercrimes Act* are,[994] to recognise and introduce cybercrime as an offence, to criminalise the activity of disclosing or disseminating information to cause damage or harm to another, to regulate and assist the powers and position of specific jurisdictions regarding cybercrime, and to regulate and assist in cyber-investigation procedures.[995]

The *Cybercrimes Act* also introduces and establishes a Point of Contact, implements the reporting of cybercrime, provides for the expansion of South Africa's cyber-capacity and infrastructure, and establishes the position of entering into international safety agreements.[996] However, according to an article written and published by Michalsons,[997] the impact and effect of the *Cybercrimes Act* on South Africa already appears to be quite negative.[998] The article explains that in some cases national legislation tend to restrict the rights of natural and juristic persons and mentions that numerous internet users,[999] for example, ECSPs and financial institutions will, without their knowledge, commit a

---

991 Giles 2021 https://www.michalsons.com/blog/the-practical-impact-of-the-cyber-bill-on-you/25300#:~:text=If%20you%20share%20your%20password,you%20could%20be%20a%20criminal ; Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.

992 The *Cybercrimes Act* 19 of 2020 (hereafter the "*Cybercrimes Act*").

993 Snail 2021 https://cyberbrics.info/legal-intersections-between-the-protection-of-personal-information-act-4-of-2013-popia-and-the-cyber-crimes-act-19-of-2020-2/; Preamble of the *Cybercrimes Act*.

994 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses; The *Cybercrimes Act*.

995 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses; The *Cybercrimes Act*.

996 The *Cybercrimes Act*.

997 A South African law firm located in Cape Town; Giles 2021 https://www.michalsons.com/blog/the-practical-impact-of-the-cyber-bill-on-you/25300#:~:text=If%20you%20share%20your%20password,you%20could%20be%20a%20criminal .

998 Michalsons 2022 https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa#:~:text=The%20Cybercrimes%20Act%20enables%20the,this%20is%20a%20global%20issue.

999 Michalsons 2022 https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa#:~:text=The%20Cybercrimes%20Act%20enables%20the,this%20is%20a%20global%20issue.

cybercrime (by accident) in terms of the list of cyber-offences provided for in the *Cybercrimes Act*.[1000]

A questionable remark to consider regarding the *Cybercrimes Act* is that the *Cybercrimes Act* fails to explicitly define "cybercrime",[1001] as well as other concepts for example, "cyberterrorism" or "cybersecurity", closely related to cybercrime.[1002] This complicates various cyber-related matters such as the identification of cybercrime, the reporting of cybercrime and the investigation and prosecution procedures of cybercrime.[1003] Nevertheless, Chapter 1, section 1 defines various keywords found in the *Cybercrimes Act* to assist in identifying and addressing cybercrime.[1004] These keywords include, "article", "computer", "data", "data message" and "electronic communications service".[1005]

According to the Law Society of South Africa (LSSA), it is crucial to define such concepts to avoid being misunderstood, considering that South Africa is a completely diverse country with various ideological and educational backgrounds.[1006] This section also provides for the manner in which the provisions of the *Cybercrimes Act* must be interpreted and applied.[1007] Chapter 2 comprises of 6 substantive criminal law segments/parts and seeks to introduce and address cybercrime and malicious communications.[1008] Part I addresses the different types of cybercrime;[1009] this includes the unauthorised access[1010] to data, files, information or a computer system.[1011] According to Mabeka,[1012] the cyber-offence of

---

1000 Michalsons 2022 https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa#:~:text=The%20Cybercrimes%20Act%20enables%20the,this%20is%20a%20global%20issue.

1001 Manaleng 2021 https://ewn.co.za/2021/06/03/think-before-you-click-ramaphosa-signs-cybercrimes-act-into-law.

1002 The Law Society of South Africa *Comments By The Law Society of South Africa (LSSA) On The Cybercrimes and Cybersecurity Bill* 3.

1003 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.

1004 Chapter 1 of the *Cybercrimes Act*; Section 1 of the *Cybercrimes Act*.

1005 Chapter 1 of the *Cybercrimes Act*; Section 1 of the *Cybercrimes Act*.

1006 The Law Society of South Africa *Comments By The Law Society of South Africa (LSSA) On The Cybercrimes and Cybersecurity Bill* 4.

1007 Chapter 1 of the *Cybercrimes Act*; Section 1 of the *Cybercrimes Act*.

1008 Snail 2022 *Obiter* 545; Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 48.

1009 Chapter 2, part 1 of the *Cybercrimes Act*; Article 8 of the Budapest Convention.

1010 According to Mabunda at *The South African Legislative Response to Cybercrime* 72, the concept of unauthorised access refers to the unlawful intentional conduct which directly threatens the confidentiality of a computer operating system through access.

1011 Section 2 of the *Cybercrimes Act*; Chapter 3 of the *POPIA*; Chapter 2 of the Budapest Convention.

1012 Mabunda *The South African Legislative Response to Cybercrime* 74.

unauthorised access consists of three distinct elements, (a) unlawfulness, (b) intention and (c) the access to a smart device/computer.[1013]

Part I continues with addressing the unlawful interception or acquiring of data, files, information or a computer system,[1014] the unlawful and intentional action to access data, files, information or a computer system through the use of advanced software or hardware tools,[1015] the unlawful interference with data, files, information or a computer system,[1016] the unlawful interference and intentional access to a data storage medium of a computer or a computer system,[1017] the unlawful and intentional use, possession or provision of an access code or password,[1018] cyber fraud,[1019] cyber forgery and uttering,[1020] cyber-extortion,[1021] aggravated offences[1022] and incorporeal (intangible) property or object theft.[1023] It is safe to assume that South Africa has never been immune against any form of hacking[1024] or hacktivist attacks.[1025]

According to Mabeka,[1026] to interpret and understand the implications of section 8, cyber fraud,[1027] one must consider the following two key elements.[1028] The two key elements are, (a) the unlawful, intentional action, without any consent and (b) the action of misrepresenting.[1029] Mabeka continues to explain that cyber fraud is generally based on a cyber-criminal obtaining personal or private information about a cyber-victim to commit a crime accordingly, for example identity fraud.[1030] Other examples of cyber fraud are fraudulent online sales and fraudulent investments.[1031] However, this ultimately leads

1013 Mabunda *The South African Legislative Response to Cybercrime* 74.
1014 Section 3 of the *Cybercrimes Act*; Article 3-5 of the Budapest Convention; Section 86 of the *ECTA*; Chapter 3 of the *POPIA*.
1015 Section 4 of the *Cybercrimes Act*.
1016 Section 5 of the *Cybercrimes Act*; Article 5 of the Budapest Convention.
1017 Section 6 of the *Cybercrimes Act*; Article 3-5 of the Budapest Convention.
1018 Section 7 of the *Cybercrimes Act*; Chapter 7 of the *POPIA*.
1019 Section 8 of the *Cybercrimes Act*; Article 8 of the Budapest Convention.
1020 Section 9 of the *Cybercrimes Act*; Article 7 of the Budapest Convention.
1021 Section 10 of the *Cybercrimes Act*.
1022 Section 11 of the *Cybercrimes Act*.
1023 Section 12 of the *Cybercrimes Act*.
1024 According to Mabunda in *The South African Legislative Response to Cybercrime* 80*,* hacktivism is a combination of hacking and activism.
1025 Mabunda *The South African Legislative Response to Cybercrime* 89.
1026 Mabeka 2022 *IJLPA* 14.
1027 Section 8 of the *Cybercrimes Act*.
1028 Mabeka 2022 *IJLPA* 14.
1029 Mabeka 2022 *IJLPA* 14.
1030 Mabeka 2022 *IJLPA* 14.
1031 Mabunda *The South African Legislative Response to Cybercrime* 130-137.

Mabeka and others[1032] to asking whether cyber-victims are allowed to claim patrimonial and non-patrimonial compensation via legal proceedings in terms of the *Cybercrimes Act*?[1033]

Mabeka concludes with the suggestion that section 8 of the *Cybercrimes Act* should consider and incorporate an additional legal clause which enables cyber-victims to institute either civil or criminal proceedings in fraud-related matters.[1034] Mabunda[1035] also states that cyber fraud does not appear to vary much from traditional common law fraud.[1036] Mabunda explains and discusses that the elements of cyber fraud and common law fraud are identical, both consisting of (a) unlawfulness; (b) intention; (c) misrepresentation and (d) prejudice.[1037] The key element to consider regarding on-/ offline fraud is, misrepresentation.[1038]

As for section 9,[1039] cyber forgery is the production and presentation of false data, files, or documents (that appear genuine) to another individual with the intention to cause harm.[1040] Cyber-uttering on the other hand is the act of distributing and disseminating false data, files, or computer programmes to another individual with the intention to cause harm.[1041] A combined example of cyber forgery- and uttering is when a cyber-criminal uses an illegal software programme to forge an online signature of an individual in order to commit a cybercrime.[1042] Upon becoming aware of this, the cyber-victim will then have the exclusive option to refer the case to criminal or civil proceedings in terms of the *Cybercrimes Act*. [1043] This matter will be critically discussed.

Regardless, the cyber-victim will have the responsibility to present the *facta probanda* and *facta probantia* to prove the cause of action in the case.[1044] Regarding section 10, cyber-

---

1032 Mabeka 2022 *IJLPA* 14; Mabeka and Cassim 2023 *Obiter* 27; Burger-Smidt 2022 https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/.
1033 Mabeka 2022 *IJLPA* 14.
1034 Mabeka 2022 *IJLPA* 18.
1035 Mabunda *The South African Legislative Response to Cybercrime* 128.
1036 Mabunda *The South African Legislative Response to Cybercrime* 128.
1037 Mabunda *The South African Legislative Response to Cybercrime* 129.
1038 Mabunda *The South African Legislative Response to Cybercrime* 129.
1039 Cyber forgery- and uttering.
1040 Mabunda *The South African Legislative Response to Cybercrime* 95.
1041 Mabunda *The South African Legislative Response to Cybercrime* 95.
1042 Mabeka and Cassim 2023 *Obiter* 23.
1043 Mabeka and Cassim 2023 *Obiter* 23.
1044 Mabeka and Cassim 2023 *Obiter* 23.

extortion,[1045] the different key elements of cyber-extortion are (a) unlawfulness, (b) intention, (c) threats, blackmailing or bullying and (d) confidential data or information.[1046] Cyber-extortion directly relates to the objective of taking advantage of a natural or a juristic person in the online environment.[1047] Examples of cyber-extortion are ransomware attacks and DDoS attacks.[1048] Section 11, aggravated offences,[1049] entails any cyber-offence involving a "restricted computer system".[1050]

Aggravated offences include offences committed in terms of financial institutions or protected organs of state (as envisaged in section 239 of the *Constitution*).[1051] These offences are considered quite serious and are prosecuted by the authorised Director of Public Prosecutions.[1052] Part II of Chapter 2 addresses malicious communications.[1053] Malicious communication offences are always focused on one of two targets: (a) a specific individual or (b) a group of individuals.[1054] This part also introduces keywords and their definitions; the keywords include, "damage to property", "disclose" and "violence".[1055]

Part II continues with listing various offences, such as the dissemination or distribution of data messages causing damage to property (corporeal or incorporeal) or the incitement to violence against an individual or a group,[1056] the dissemination of data messages threatening or blackmailing an individual or a group with the damaging of property (corporeal or incorporeal) or the inflicting of violence[1057] and lastly, the disclosure or

---

1045 According to Higgins 2022 at https://nordvpn.com/blog/cyberextortion/, "Cyber extortion attacks involve hackers attempting to convince, trick, or bully a victim into giving up money or confidential data (or both). Hackers can do so through phishing emails, ransomware attacks, and other extortion methods. The result of a successful cyber extortion attack could be a data breach, financial theft, or even cyber espionage.".

1046 Mabunda *The South African Legislative Response to Cybercrime* 104.

1047 Mabunda *The South African Legislative Response to Cybercrime* 104.

1048 Higgins 2022 https://nordvpn.com/blog/cyberextortion/.

1049 Section 11 of the *Cybercrimes Act*.

1050 According to Mabunda at *The South African Legislative Response to Cybercrime* 105, a restricted computer system is any computer program or file under the control of or used by a financial institution or an organ of state (section 239 of the *Constitution*), for example a court.

1051 Snail 2021 https://cyberbrics.info/legal-intersections-between-the-protection-of-personal-information-act-4-of-2013-popia-and-the-cyber-crimes-act-19-of-2020-2/.

1052 Mabunda *The South African Legislative Response to Cybercrime* 105.

1053 Part II of the *Cybercrimes Act*; Article 8 of the Budapest Convention.

1054 Mabunda *The South African Legislative Response to Cybercrime* 115.

1055 Section 13 of the *Cybercrimes Act*.

1056 Section 14 of the *Cybercrimes Act*.

1057 Snail 2021 https://cyberbrics.info/legal-intersections-between-the-protection-of-personal-information-act-4-of-2013-popia-and-the-cyber-crimes-act-19-of-2020-2/; Section 15 of the *Cybercrimes Act*.

dissemination of data messages involving intimate or explicit images without the consent of the individual involved.[1058]

As discussed in the aforementioned cases, the intentional disclosure or dissemination of data messages (without consent) containing an intimate or explicit image (also known as non-consensual pornography or revenge pornography) which directly infringes upon the right to human dignity,[1059] and the right to privacy,[1060] can result in an established cybercrime.[1061] The *Cybercrimes Act* defines an "intimate image" as any photograph or picture,[1062] real or simulated, revealing an individual's nude body, this includes their breasts, genital organs or the anal region.[1063] This also includes images where the individual cannot be clearly identified, but is mentioned in the sub-text or caption of the explicit image.[1064] The *Criminal Law (Sexual Offences and Related Matters) Amendment Act* 32 of 2007 can be referred to, to additionally assist in such matters.[1065]

Considering the above-mentioned, the rule of law and position regarding defamation can also be referred to section 16 of the *Cybercrimes Act* to assist and,[1066] allow a victim to exclusively institute civil proceedings rather than criminal proceedings.[1067] Defamation can be defined as the unlawful and intentional publication or dissemination of data or information, regardless of the type, defamatory of nature which injures an individual's reputation.[1068] There are four key elements of defamation, (a) unlawfulness; (b) intention; (c) dissemination and (d) defamatory.[1069] The first two elements are self-explanatory, but the third element requires that the dissemination must be made by an individual other than the victim.[1070]

1058 Section 16 of the *Cybercrimes Act*.
1059 Section 10 of the *Constitution*.
1060 Section 14 of the *Constitution*.
1061 Burger-Smidt 2022 https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/; Snail 2022 *Obiter* 552.
1062 Burger-Smidt 2022 https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/.
1063 Section 16(2)(b) of the *Cybercrimes Act*.
1064 Manaleng 2021 https://ewn.co.za/2021/06/03/think-before-you-click-ramaphosa-signs-cybercrimes-act-into-law.
1065 Mabunda *The South African Legislative Response to Cybercrime* 123.
1066 Mabunda *The South African Legislative Response to Cybercrime* 119; Article 9 of the Budapest Convention.
1067 Mabeka and Cassim 2023 *Obiter* 27.
1068 Mabunda *The South African Legislative Response to Cybercrime* 119.
1069 Mabunda *The South African Legislative Response to Cybercrime* 119.
1070 Mabunda *The South African Legislative Response to Cybercrime* 119.

The fourth element requires that the published information must be defamatory, meaning that the information exposes hatred towards the victim.[1071] Considering the option of legal proceedings, according to Mabeka and Cassim,[1072] the *Cybercrimes Act* does not (yet) provide for additional compensation remedies available to a cyber-victim regardless of their preferred option of legal proceedings.[1073] They continue to discuss that the *Cybercrimes Act* must be reviewed and amended to include the option for additional compensation remedies.[1074]

According to South Africa's Minister of State Security, Mr David Mahlobo,[1075] the *Cybercrimes Act* also addresses malicious communications that refer to "fake news" or "false narratives".[1076] This also includes any information that is "inherently false".[1077] However, Mahlobo continues to argue and question the following,[1078] (a) who will have the authority to decide what type of information is considered false or not?[1079] (b) what legal requirements must be evident or applied to determine or classify that the information is indeed false information?[1080] And, (c) will the regulation of this "false information" not lead to the censorship and the prohibition of freedom of expression of South African citizens in the cyberspace?[1081]

Part III addresses the direct or indirect action regarding the assistance of attempting, aiding, conspiring, abetting, instigating, inciting, inducing, instructing, procuring, or commanding to commit a cybercrime.[1082] A natural or juristic person found guilty in terms of section 17 will be convicted and prosecuted in terms of the *Cybercrimes Act*.[1083] Part IV addresses the objective and legal position of competent verdicts,[1084] which often assists South African courts in presenting their declarations regarding cybercrime.[1085] This also

---

1071 Mabunda *The South African Legislative Response to Cybercrime* 119.
1072 Mabeka and Cassim 2023 *Obiter* 26.
1073 Mabeka and Cassim 2023 *Obiter* 26.
1074 Mabeka and Cassim 2023 *Obiter* 26.
1075 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 49.
1076 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 49.
1077 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 49.
1078 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 49.
1079 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 49.
1080 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 117.
1081 Section 16 of the *Constitution*; Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 49.
1082 Part III of the *Cybercrimes Act*; Section 17 of the *Cybercrimes Act*; Article 11 of the Budapest Convention.
1083 Section 17 of the *Cybercrimes Act*.
1084 Part IV of the *Cybercrimes Act*.
1085 Snail 2022 *Obiter* 545.

provides for the option and position of alternatives regarding evidence presented in legal proceedings before court and the position of contraventions to the provisions in the *Cybercrimes Act*.[1086] Section 18 is considered quite extensive and broad.[1087]

Part V primarily addresses sentencing, the position of liability and provides for the different conviction and prosecution procedures regarding a contravention of the provisions in the *Cybercrimes Act*.[1088] The *Cybercrimes Act* prescribes a sentence of a monetary fine or imprisonment, or both to a committed cybercrime.[1089] Section 19 also provides for the option of referring to section 276 of the *Criminal Procedure Act* 51 of 1977 (hereafter the "*CPA*") to deliver an appropriate sentence within the court's legal jurisdiction or discretion.[1090] The competent court must, however, consider all elements and facts when delivering an appropriate sentence to a cyber-criminal in terms of the *CPA*.[1091]

However, the *Cybercrimes Act* should be amended to authorise national law enforcement to legally close an individual's or organisation's website which contravenes the regulations and requirements of the *Financial Intelligence Centre Act* 38 of 2001.[1092] Part VI is not yet signed into South African legislation, however it addresses the authority and application of protection and interim protection orders regarding complainants in pending criminal proceedings.[1093] This part also sets out the legal procedure of particulars presented in court from ECSPs,[1094] assists in the finalisation of orders in criminal proceedings[1095] and imposes the different penalties and prosecutions available upon conviction of a cybercrime in terms of the *Cybercrimes Act*.[1096]

The *Cybercrimes Act* also addresses and recognises the right to freedom of expression[1097] and the application of this constitutional right as a factor to consider and investigate in

---

1086 Section 18 of the *Cybercrimes Act*.
1087 Section 18 of the *Cybercrimes Ac*t.
1088 Part V of the *Cybercrimes Act*.
1089 Section 19(3) of the *Cybercrimes Act*.
1090 Section 19(4) of the *Cybercrimes Act*.
1091 Snail 2022 *Obiter* 554.
1092 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 134.
1093 Section 20 of the *Cybercrimes Act*.
1094 Section 21 of the *Cybercrimes Act*.
1095 Section 22 of the *Cybercrimes Act*.
1096 Section 23 of the *Cybercrimes Act*; Article 13 of the Budapest Convention.
1097 The right to freedom of expression is envisaged in section 16 of the *Constitution*.

legal proceedings such as cyberbullying.[1098] The severity of the prosecution or penalty is based on the type of cybercrime and aims to provide protection and compensation for the cyber-victim.[1099] Chapter 3 of the *Cybercrimes Act* discusses the jurisdiction of South African courts in addressing cybercrime committed both in- and outside the Republic.[1100] The jurisdictions of courts and national authorities are a crucial element to consider when addressing and prosecuting cybercrime.[1101] The general rule of law regarding jurisdiction is envisaged in the *Cybercrimes Act*, and provides that every state has the legal jurisdiction and authority to exercise control over what crime occurs in that specific state's jurisdiction and territory (principle of territoriality).[1102]

The law regarding jurisdiction also considers elements such as, where the cybercrime was committed, in what country the cyber-criminal resides and the country where the cyber-victim resides (principle of nationality).[1103] According to Erasmus and Bowden[1104] regarding the jurisdiction provisions of the Budapest Convention,[1105] in the case of a committed cybercrime; the country where the cybercrime was committed from, has the legal jurisdiction to prosecute the cybercrime, however, this approach is not without fault considering that there are still numerous countries operating without any or inadequate cybercrime legislation.[1106] Chapter 3 also delegates certain powers to the National Commissioner, the National Head of the Directorate, and the National Director of Public Prosecutions regarding the issuing of legal directives and execution orders.[1107]

Chapter 4 of the *Cybercrimes Act* is considered extensive as it entails the legal procedures and powers of investigation including the search, access and seizure of articles related to a committed cybercrime.[1108] The keywords to consider in this chapter are, "access", "investigator" and "seize".[1109] The SAPS is considered the leading national authority to

[1098] Mabeka and Cassim 2023 *Obiter* 21.
[1099] Mabeka and Cassim 2023 *Obiter* 21.
[1100] Chapter 3 of the *Cybercrimes Act*; Article 22 of the Budapest Convention.
[1101] Mabunda *The South African Legislative Response to Cybercrime* 141.
[1102] Mabunda *The South African Legislative Response to Cybercrime* 142
[1103] Mabunda *The South African Legislative Response to Cybercrime* 142.
[1104] Erasmus and Bowden 2020 *Obiter* 322.
[1105] Erasmus and Bowden 2020 *Obiter* 322.
[1106] Erasmus and Bowden 2020 *Obiter* 322.
[1107] Section 24(4)-(5) of the *Cybercrimes Act*.
[1108] Chapter 4 of the *Cybercrimes Act*; Article 19 of the Budapest Convention.
[1109] Section 25 of the *Cybercrimes Act*.

address and cooperate in these investigation procedures,[1110] along with South Africa's National Commissioner, the National Head of the Directorate, the National Director of Public Prosecutions and the involved Cabinet member responsible for the administration of justice.[1111] In short, Chapter 4 entails the cybercrime investigation procedures along with considering the extent and provisions of the *CPA* without the *CPA* being inconsistent with the *Cybercrimes Act* or the *Constitution* (considering the subsidiarity principle).[1112]

According to Chapter 4,[1113] the investigation procedures regarding cybercrime consist of standard operating procedures.[1114] This includes the required content and submission of legal applications, the submission of oral applications, the content and issuing of search-and-seizure warrants by a national official, the lawful execution of the search-and-seizure warrant, the position of searched and seized articles, and the lawful position of investigating without a search-and-seizure warrant but with legal consent from national authorities.[1115] According to Du Toit,[1116] the lawfulness of a search-and-seizure investigation conducted both in terms of the *CPA* and the *Cybercrimes Act*, depends on the individual's expectation of their right to privacy being upheld.[1117]

Chapter 4 continues with addressing the position of an individual or party concerned to a cybercrime,[1118] the position of an arrested individual or party to a cybercrime and delegates the position and powers of police officials and cyber-investigators.[1119] It is important to regulate the legal position and powers of police officials and cyber-investigators regarding cyber-investigations and search-and-seizure procedures to prevent the misuse or abuse of powers due to the lack of cyber-expertise.[1120] The chapter also recognises and regulates offences committed in terms of investigation procedures and addresses wrongful search and seizure.[1121]

1110 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.
1111 Snail 2022 *Obiter* 556.
1112 Du Toit 2022 *Obiter* 764.
1113 Section 27 of the *CPA* applies to chapter 4 of the *Cybercrimes Act*.
1114 Du Toit 2022 *Obiter* 767.
1115 Du Toit 2022 *Obiter* 764-778.
1116 Du Toit 2022 *Obiter* 764.
1117 Du Toit 2022 *Obiter* 764; Section 14 of the *Constitution*.
1118 This can either be the victim, cyber-criminal or a third person connected to the cybercrime.
1119 Section 32-36 of the *Cybercrimes Act*.
1120 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 141.
1121 Section 35-37 of the *Cybercrimes Act*.

Chapter 4 concludes with addressing the unlawful intention of providing false information through an affidavit or under oath (not signed into legislation yet), the prohibition of disclosing information, the unlawful interception of indirect communication, data and evidence preservation (not signed into legislation yet), data direction regarding search-and-seizure procedures and finally, the lawful procedure for obtaining any form of data (not signed into legislation yet).[1122] As mentioned, Chapter 4 of the *Cybercrimes Act* can be referred to or assisted by the *CPA*,[1123] unless the provisions of the *CPA* are inconsistent with the provisions of the *Cybercrimes Act*.[1124] However, there already appear to be several inconsistencies between the *CPA* and the *Cybercrimes Act*.[1125]

The first inconsistency is the position of an "appointed issuing official".[1126] According to the provisions of the *CPA*, an appointed issuing official is a magistrate or a justice of peace.[1127] The *CPA* excludes a regional magistrate unless the regional magistrate is explicitly mentioned in the provisions of the *CPA*.[1128] However, in terms of the *Cybercrimes Act*, an issuing official can be a magistrate.[1129] This includes a regional magistrate and a judge of the High Court, however, the *Cybercrimes Act* does not empower a justice of peace.[1130] The second inconsistency concerns the type of article that may be seized.[1131] According to section 20 of the *CPA* "article" can be defined as "anything" directly or indirectly connected, relevant or used as an object or subject to commit a crime.[1132]

However,[1133] the *Cybercrimes Act* explicitly defines an "article" as any "data", "computer program", "computer data storage medium" or a "computer system",[1134] along with the requirement that an article must be connected or relevant to the committed cybercrime to be seized.[1135] Other examples of inconsistencies refer to the content of applications,[1136]

1122 Section 38-45 of the *Cybercrimes Act*.
1123 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.
1124 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime; Du Toit 2022 *Obiter* 764.
1125 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime; Du Toit 2022 *Obiter* 767.
1126 Du Toit 2022 *Obiter* 767.
1127 Du Toit 2022 *Obiter* 767.
1128 Du Toit 2022 *Obiter* 767.
1129 Du Toit 2022 *Obiter* 768.
1130 Du Toit 2022 *Obiter* 768.
1131 Du Toit 2022 *Obiter* 769.
1132 Section 20 of the *CPA*.
1133 Section 1 of the *Cybercrimes Act*.
1134 Section 1 of the *Cybercrimes Act*.
1135 Du Toit 2022 *Obiter* 769.
1136 Du Toit 2022 *Obiter* 770.

the position of oral applications regarding a search warrant,[1137] the content of a search warrant[1138] and the lawful execution of a search warrant.[1139] Chapter 5 of the *Cybercrimes Act* addresses mutual assistance.[1140]

This chapter entails the lawful disclosure of cyber-related information by the National Commissioner or the National Director of Public Prosecutions to foreign states,[1141] provides for the assistance and cooperation from foreign states,[1142] ensures that juristic persons comply with orders issued by a designated judge,[1143] provides information regarding the outcome of a foreign state's mutual assistance or cooperation,[1144] and sets out the procedure of issuing a direction request for assistance from a foreign state.[1145] The application of the direction request must include, (a) reasonable grounds regarding the committed cybercrime; (b) provide that the investigation is on-going and (c) mention the reason(s) for the direction request.[1146]

This chapter also refers to the *International Co-operation in Criminal Matters Act* 75 of 1996 for additional assistance.[1147] Mabunda[1148] comments on this chapter by stating that the *Cybercrimes Act* does indeed address and regulate the international assistance and cooperation from foreign states appropriately, and that South African courts have a broad scope in the exercising of jurisdiction regarding cybercrime.[1149] However,[1150] Mabunda criticizes the lengthy and time consuming chain of command for requesting mutual assistance or a direction request considering the rapid, evolutionary nature of cybercrime and continues to discuss another important factor being that the *Cybercrimes Act* must continually consider the process of its legal checks and balances.[1151]

1137 Du Toit 2022 *Obiter* 771.
1138 Du Toit 2022 *Obiter* 772.
1139 Du Toit 2022 *Obiter* 775.
1140 Chapter 5 of the *Cybercrimes Act*; Article 23-27 of the Budapest Convention.
1141 Section 47 of the *Cybercrimes Act*.
1142 Section 48 of the *Cybercrimes Act*.
1143 Section 49 of the *Cybercrimes Act*.
1144 Section 50 of the *Cybercrimes Act*.
1145 Section 51 of the *Cybercrimes Act*.
1146 Mabunda *The South African Legislative Response to Cybercrime* 155.
1147 Chapter 5 of the *Cybercrimes Act*.
1148 Mabunda *The South African Legislative Response to Cybercrime* 160.
1149 Mabunda *The South African Legislative Response to Cybercrime* 160.
1150 Mabunda *The South African Legislative Response to Cybercrime* 161.
1151 Mabunda *The South African Legislative Response to Cybercrime* 161.

Chapter 6 establishes and provides for the powers and functions of the designated Point of Contact (previously cybercrime unit, for example,[1152] the Cybersecurity Hub).[1153] The South African National Police Commissioner must designate a Point of Contact (previously the 24/7 Point of Contact)[1154] in terms of the SAPS regulations.[1155] The National Police Commissioner must also administer and equip the designated Point of Contact.[1156] The Minister of Police is also entitled to regulate cyber-related matters along with the designated Point of Contact.[1157] The main objective of the designated Point of Contact is to assist in cyber-investigations and legal proceedings;[1158] this includes-, providing technical advice and legal assistance, facilitating in terms of the *Cybercrimes Act*, identifying locations, articles and suspects in cyber-investigations and cooperating with other international legal authorities regarding cybercrime.[1159]

According to Mabunda,[1160] the designated Point of Contact can also be considered a national independent agency or a "capable guardian".[1161] A "capable guardian" is a cybersecurity operative resource with the objective and ability to protect a cyber-target or victim from a motivated cyber-offender.[1162] According to Mabunda,[1163] the designated Point of Contact would act as the perfect capable guardian if it is educated, prepared and expanded appropriately, and operates as an independent private organisation legally registered in terms of the *Companies Act 71* of 2008.[1164] Although the *Cybercrimes Act* provides for Chapter 5 (Mutual Assistance) and Chapter 6 (Point of Contact), these establishments have not yet been implemented.[1165]

Nevertheless, it appears that reporting resources and mechanisms, for example a national website, cybercrime.org.za have been established while South Africa awaits the

---

1152 Pillay 2017 https://www.withoutprejudice.co.za/free/article/5659/view.
1153 Chapter 6 of the *Cybercrimes Act*; Article 35 of the Budapest Convention.
1154 Later discussed in this chapter.
1155 Section 52 of the *Cybercrimes Act*.
1156 Section 52 of the *Cybercrimes Act*.
1157 Mabunda *The South African Legislative Response to Cybercrime* 181.
1158 Byleveld 2022 https://www.fluidrock.co.za/a-brief-overview-of-the-cybercrimes-act-19-of-2020/.
1159 Byleveld 2022 https://www.fluidrock.co.za/a-brief-overview-of-the-cybercrimes-act-19-of-2020/; Article 35 of the Budapest Convention.
1160 Mabunda *The South African Legislative Response to Cybercrime* 162.
1161 Mabunda *The South African Legislative Response to Cybercrime* 162.
1162 Mabunda *The South African Legislative Response to Cybercrime* 162.
1163 Mabunda *The South African Legislative Response to Cybercrime* 162.
1164 Mabunda *The South African Legislative Response to Cybercrime* 162.
1165 Burger-Smidt 2022 https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/.

commencement of Chapter 5 and Chapter 6.[1166] However, this leaves questions unanswered regarding the *Cybercrimes Act* and the process of reporting cybercrime and what happens to the reported cybercrime, pending the commencement of Chapter 6?[1167] Chapter 7 provides for the presenting of evidence and the proof of facts by sworn statements, for example an affidavit.[1168] This chapter also addresses the functions and powers of a cyber-expert in the different examination procedures of evidence,[1169] regulates affidavits providing false information, and regulates the requesting of oral evidence, admissibility and the evidentiary value of a signed affidavit before a competent court.[1170]

Chapter 8 imposes the obligation and duty of ECSPs and financial institutions to report cybercrime, addresses the expansion of South Africa's cybercrime capacity and infrastructure regarding the investigation and prosecution of cybercrime and obligates the National Director of Public Prosecutions to record cyber-related matters and statistics.[1171] The obligation and duty of reporting cyber-offences to the SAPS within seventy-two hours of becoming aware of the cyber-offence rests on ECSPs and financial institutions.[1172] Failing to report such an offence will result in prosecution based on non-compliance with the provisions of the *Cybercrimes Act* through a monetary fine.[1173]

These types of organisations are also required to provide national authorities with the necessary or required assistance to access, search or seize any article or retained data relevant to the committed cybercrime.[1174] However, the *Cybercrimes Act* fails to state the specific type of assistance.[1175] These organisations are not obligated or required to implement cybersecurity measures within the organisation's network domain, or to

---

1166 Burger-Smidt 2022 https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/.
1167 Burger-Smidt 2022 https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/.
1168 Chapter 7 of the *Cybercrimes Act*.
1169 Snail 2022 *Obiter* 559.
1170 Section 53 of the *Cybercrimes Act*.
1171 Chapter 8 of the *Cybercrimes Act*.
1172 Section 54 of the *Cybercrimes Act*; Section 21-22 of the *POPIA*.
1173 Gunning and Babryk 2021 https://www.mondaq.com/southafrica/data-protection/1111854/data-breaches-and-the-interplay-between-popia-ecta-and-the-cybercrimes-act-podcast.
1174 Desai 2023 https://www.albaraka.co.za/blogs/legalease-publication-3-2022/impact-of-the-cybercrimes-act-of-financial-institutions.
1175 Desai 2023 https://www.albaraka.co.za/blogs/legalease-publication-3-2022/impact-of-the-cybercrimes-act-of-financial-institutions.

monitor the stored data in their systems.[1176] This section does not include financial institutions such as the Financial Sector Conduct Authority or the South African Reserve Bank.[1177] As mentioned earlier, the SAPS are obligated to provide a 24/7 point-of-contact network available to assist and facilitate in the reporting and investigation of cybercrime.[1178]

Section 55 of the *Cybercrimes Act* addresses South Africa's capacity to detect, prevent and investigate cybercrime,[1179] where section 56 obligates the National Director of Public Prosecutions to keep record of cyber-related matters and statistics.[1180] Chapter 9 entails the general provisions of the *Cybercrimes Act*; this includes executive authority, entering into agreements, the repeal, amendment and inclusion of laws and regulations and the commencement of the *Cybercrimes Act*.[1181] The *Cybercrimes Act* is considered post-incident by nature and clearly defines the various types of cybercrime and the manner in which these cybercrimes are investigated and prosecuted.[1182]

An important remark regarding the *Cybercrimes Act* is, for the *Cybercrimes Act* to be considered effective, it cannot operate with an overly broad or extensive mandate.[1183] Regarding the impact and effect of previous cybercrime legislation in South Africa, the *POPIA* created and established various cyber-related offences for non-compliance to the *Cybercrimes Act*.[1184] Therefore, the *POPIA* generally acts as an additional resource to the *Cybercrimes Act*,[1185] for further interpretation and additional assistance in cybercrime investigation procedures as well as the position of liability and prosecutions regarding personal or private information.[1186] It is important for natural and juristic persons to

---

1176 Byleveld 2022 https://www.fluidrock.co.za/a-brief-overview-of-the-cybercrimes-act-19-of-2020/; Desai 2023 https://www.albaraka.co.za/blogs/legalease-publication-3-2022/impact-of-the-cybercrimes-act-of-financial-institutions.

1177 Desai 2023 https://www.albaraka.co.za/blogs/legalease-publication-3-2022/impact-of-the-cybercrimes-act-of-financial-institutions.

1178 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses; Article 35 of the Budapest Convention.

1179 Section 55 of the *Cybercrimes Act*.

1180 Section 56 of the *Cybercrimes Act*.

1181 Section 57-60 of the *Cybercrimes Act*.

1182 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.

1183 Mabunda *The South African Legislative Response to Cybercrime* 138.

1184 Pillay *A Privacy Perspective on the Cybercrimes Act, 2020 – Aspects to consider in your Privacy Programme* 1.

1185 Snail 2022 *Obiter* 552.

1186 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.

understand that they may have obligations to both the *Cybercrimes Act* and the *POPIA*, but to different degrees.[1187]

During cybercrime investigations cyber-investigators often retrieve personal or private information about a natural or juristic person from a smart device or computer system and are then required to address this information in a specific manner in order to avoid legal repercussions.[1188] The *POPIA* assists in this specific area of cybercrime investigation procedures.[1189] The *Cybercrimes Act* does also encourage, but not require, an individual or organisation to adopt the provisions set out in the *POPIA* as baseline cybersecurity measures and maintain the cybersecurity system.[1190] Regarding the position of legal proceedings; Section 38 of the *Constitution* entails the enforcement of rights;[1191] this includes the right of an individual to approach a competent court when they are convinced that their rights in the Bill of Rights have been infringed upon.[1192]

It is important to acknowledge that the *Cybercrimes Act* does not explicitly provide for the option of selective proceedings or prosecutions as mentioned earlier.[1193] However, the *Cybercrimes Act* does not explicitly resort to the single option of criminal proceedings, but also to the possible option of civil proceedings.[1194] For example, when a cybercrime results in the intentional dissemination of explicit images or defamatory material, the targeted cyber-victim has the choice for the best suitable option available to either enter into a civil proceedings lawsuit rather than choosing a criminal proceedings lawsuit, for example in the matter of a defamation case.[1195] The manner of compensation regarding the civil

---

1187 Byleveld 2022 https://www.fluidrock.co.za/a-brief-overview-of-the-cybercrimes-act-19-of-2020/.

1188 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.

1189 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.

1190 Pillay *A Privacy Perspective on the Cybercrimes Act, 2020 – Aspects to consider in your Privacy Programme* 3.

1191 Section 38 of the *Constitution*.

1192 Section 38 of the *Constitution*.

1193 The *Cybercrimes Act*; Du Toit *The Search Warrant Provisions of the Cybercrimes Act and their Relationship with the Criminal Procedure Act* 764-767; Giles 2021 https://www.michalsons.com/blog/the-practical-impact-of-the-cyber-bill-on-you/25300#:~:text=If%20you%20share%20your%20password,you%20could%20be%20a%20criminal.

1194 Burger-Smidt 2022 https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/.

1195 Burger-Smidt 2022 https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/.

proceedings lawsuit claim will then (also) be based on either, patrimonial or non-patrimonial loss (similar to the claim of a criminal proceedings lawsuit).[1196]

However, according to Mabeka,[1197] the gap regarding the institution of civil proceedings rather than criminal proceedings is evident when one refers to the two common law principles of *lis pendens* and *res judicata*.[1198] The principle of *lis pendens* was thoroughly discussed in the case of *Mofokeng v Motloung* (4472/19) [2022] ZAGPJHC 546 (hereafter the "*Mofokeng* case").[1199] The court defined and discussed the four requirements of the principle of *lis pendens*,[1200] (a) pending litigations; (b) between the same involved parties; (c) based on the same cause of action; (d) regarding the same subject matter.[1201]

The principle of *res judicata* was thoroughly discussed in the case of *Molaudzi v S* (CCT42/15) [2015] ZACC 20 (hereafter the "*Molaudzi* case").[1202] The court defined and discussed *res judicata* based on the statement, "a matter already judged".[1203] The court continued by discussing four requirements regarding the principle,[1204] (a) a case before court in which final judgement was delivered and is no longer subject to appeal; (b) the principle means to preclude or bar litigation of a case on the same issues between the involved parties; (c) the principle precludes a suit from being discussed subjected to previous litigation and a delivered judgement; and (d) precludes re-litigation of facts and issues already decided before court.[1205]

It is evident that the two common law principles share similarities, which is that there should be finality in litigation and when a competent court delivers judgement, the litigation must conclude.[1206] However, according to Mabeka,[1207] considering the position of the plaintiff when the defendant institutes the defence of *lis pendens* or *res judicata* in litigation, it appears that the plaintiff will not have any legal response to the defendant's

---

1196 Section 10, section 14 of the *Constitution*; Burger-Smidt 2022 https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/.
1197 Mabeka 2022 *IJLPA* 19.
1198 Mabeka 2022 *IJLPA* 19.
1199 *Mofokeng v Motloung* (4472/19) [2022] ZAGPJHC 546 (hereafter the "*Mofokeng* case").
1200 *Mofokeng* case para [39].
1201 *Mofokeng* case para [39].
1202 *Molaudzi v S* (CCT42/15) [2015] ZACC 20 (hereafter the "*Molaudzi* case").
1203 *Molaudzi* case para [9].
1204 *Molaudzi* case para [10]–[11].
1205 *Molaudzi* case para [10 –[11].
1206 *Mofokeng* case para [40].
1207 Mabeka 2022 *IJLPA* 19.

defence.[1208] Therefore, the South African legislature should consider this matter in the future.[1209] In general, the *Cybercrimes Act* fails to properly address, amend and clarify numerous South African pieces of cybercrime legislation and sections, for example the surveillance and monitoring provisions in the (declared unconstitutional) *RICA*.[1210] It is also argued that the *Cybercrimes Act* only addresses cybercrime and not cybersecurity in South Africa as well.[1211]

4.3 The Constitution of the Republic of South Africa, 1996 and the Cybercrimes Act 19 of 2020

Over the past few years, both South Africa's legislative and judicial branches of government recognised the lack of national legislation addressing cybercrime and cybersecurity.[1212] South Africa responded by investigating, promulgating, and implementing various pieces of legislation and frameworks partially addressing cybercrime and cybersecurity.[1213] However, considering the cyber-measures taken by the South African government, it is inevitable that these cyber-measures might have implications on the constitutional rights of citizens, especially the right to privacy found in section 14 of the *Constitution*.[1214] In recent years, numerous human rights groups, civil society movements and the national media have voiced their strong opposition to the increase of cybersecurity measures undertaken by the South African government.[1215]

These groups and movements do not only focus on one primary piece of cybercrime legislation, but rather on numerous pieces of cybercrime legislation including the *RICA* and the *ECTA*.[1216] In addition, South Africa is known for being a democratic country.[1217] This specifically focuses on the right to privacy and the right to freedom of expression as envisaged in the *Constitution*.[1218] According to Molwantwa,[1219] the right to freedom of

---

1208 Mabeka 2022 *IJLPA* 19.
1209 Mabeka 2022 *IJLPA* 19.
1210 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 118.
1211 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 120.
1212 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* ii.
1213 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* ii.
1214 Section 14 of the Constitution; Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* ii.
1215 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 2.
1216 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 3.
1217 Karlsson *Democracy in South Africa* 1; Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 3.
1218 Karlsson *Democracy in South Africa* 1; Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 3; Section 14, section 16 of the *Constitution*.

expression also refers to the right of obtaining, storing, and sharing information.[1220] While the cyberspace continues to develop at a rapid pace, it is understandable that the South African government would want to promulgate and implement cybercrime legislation and cybersecurity measures and resources to protect the country and its citizens in the cyberspace.[1221]

Although cybersecurity is an extremely comprehensive concept with various definitions and interpretations,[1222] every country, government, organisation, and individual has the duty and responsibility to protect themselves in the cyberspace.[1223] Cybersecurity in terms of the South African cyberspace means online protection for South African citizens against the various risks encountered in the cyberspace by the use of protected civil or military cyberspaces.[1224] It is important to define the concept of cybersecurity to understand the need for cybersecurity measures in South Africa.[1225] The interpretation of cybersecurity is based on the five different sectors of a country, being the political, military, environmental, economic, and societal sectors.[1226]

Although these sectors differ in function and power, the main objective of each of these sectors is to enforce security by focusing on what the different 'referent object' of the implemented security is.[1227] The referent object of security is a specific object under the protection of the relevant sector, therefore, each sector's referent object varies.[1228] An example of a referent object can be statistics, databases or confidential information.[1229] The current approach of the *Cybercrimes Act* to cybersecurity measures in South Africa is considered state-centric; this simply means that the national security of the country appears more essential than individual security.[1230] According to Mahlobo,[1231]

1219 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 3.
1220 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 3.
1221 Terrina *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 7; Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 4.
1222 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 11.
1223 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 14.
1224 Sutherland *Governance of Cybersecurity* 84; Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 25.
1225 Sutherland *Governance of Cybersecurity* 84; Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 11.
1226 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 11.
1227 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 12.
1228 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 12.
1229 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 12.
1230 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 49.

> "finding a balance between security and respecting human rights in the field of information security and communication technologies continue to be a contentious matter internationally".[1232]

For a democratic South Africa, the principle of "Constitutional Supremacy" is the fundamental principle when it comes to the country's national rule of law.[1233] This principle entails the fact that the supreme law of the country is the *Constitution*, meaning that all laws, legislation, policies, institutions, and actions performed by the South African government are subject to, and must be consistent with the *Constitution* and when it is proven that it is not, the law or action will be declared unconstitutional (taking into consideration the subsidiarity principle).[1234] The *Constitution* enforces equality and justice to all along with considering the rest of the provisions in the Bill of Rights.[1235]

According to Molwantwa,[1236] there are numerous fundamental rights of citizens which might be affected by national cybersecurity measures; these rights include,[1237] the right to equality (section 9), the right to human dignity (section 10), the right to privacy (section 14), the right to freedom of religion, belief and opinion (section 15), the right to freedom of expression (section 16) and the right of access to information (section 32).[1238] As mentioned earlier,[1239] constitutional rights, for example section 14 of the *Constitution*, the right to privacy,[1240] is not considered absolute and can be limited by section 36 of the *Constitution*, the limitation clause.[1241] The requirements of limiting such a right must be justified and reasonable according to the *Constitution*.[1242]

This entails the situation that the decision to limit a right must be made in good faith and be beneficial to society and the country.[1243] However, the *Cybercrimes Act* fails to explicitly

---

1231 South African Government 2016 https://www.gov.za/speeches/minister-david-mahlobo-state-security-agency-dept-budget-vote-201617-26-apr-2016-0000.
1232 South African Government 2016 https://www.gov.za/speeches/minister-david-mahlobo-state-security-agency-dept-budget-vote-201617-26-apr-2016-0000.
1233 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 17.
1234 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 18.
1235 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 18.
1236 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 18.
1237 Section 9, section 10, section 14, section 15, section 16 of the *Constitution*.
1238 Sections found in the *Constitution*; Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 18.
1239 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 29.
1240 Section 14 of the Constitution.
1241 Section 14, section 36 of the *Constitution*.
1242 The *Constitution of the Republic of South Africa*, 1996; Sutherland *Governance of Cybersecurity* 95.
1243 Sutherland *Governance of Cybersecurity* 95; Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 30.

state in which manner the right to privacy and cybersecurity measures will be balanced;[1244] therefore, the *Cybercrimes Act* does not establish or provide for the necessary checks and balances regarding cybercrime and cybersecurity measures, increasing the power of the state to regulate the cyberspace.[1245] Therefore, cybersecurity in South Africa must be approached in a balanced manner to not infringe or violate these fundamental rights of citizens while combatting and addressing cybercrime in the cyberspace.[1246]

With the implementation of the *Cybercrimes Act*, one of South Africa's political parties, the Democratic Alliance (DA), reasoned and proposed an amendment to the *Constitution* of South Africa regarding the establishment of an office for a national Cyber Commissioner to diligently protect and regulate South Africa's cyber-related matters.[1247] The DA's supporting statement explained that the threat of cybercrime and the lack of appropriate cybersecurity measures in South Africa did not appear important when the 1996 *Constitution* was promulgated and implemented;[1248] therefore, the proposal to amend Chapter 9 of the *Constitution* (State institutions supporting constitutional democracy) will result in the establishment of a Cyber Commissioner.[1249]

The role and functions of the Cyber Commissioner will be to support and strengthen constitutional democracy in South Africa by establishing, implementing, monitoring, and advising cybersecurity measures and capabilities in the public and private sector.[1250] The Cyber Commissioner will also be responsible for creating and providing cybercrime and cybersecurity awareness.[1251] The proposed amendments were published by Member of Parliament, Advocate Glynnis Breytenbach in the Government Gazette on Wednesday, 9 November 2022.[1252] The proposed amendments also state that ICTs are central to

---

1244 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 50.
1245 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 50.
1246 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 26.
1247 Breytenbach 2022 https://www.da.org.za/2022/12/da-welcomes-public-reception-to-the-cyber-commissioner-bill.
1248 Breytenbach 2022 https://www.da.org.za/2022/12/da-welcomes-public-reception-to-the-cyber-commissioner-bill.
1249 Breytenbach 2022 https://www.da.org.za/2022/12/da-welcomes-public-reception-to-the-cyber-commissioner-bill.
1250 Vermeulen 2022 https://mybroadband.co.za/news/security/468359-proposal-to-amend-south-africas-constitution-for-cyber-commissioner.html.
1251 Vermeulen 2022 https://mybroadband.co.za/news/security/468359-proposal-to-amend-south-africas-constitution-for-cyber-commissioner.html.
1252 Vermeulen 2022 https://mybroadband.co.za/news/security/468359-proposal-to-amend-south-africas-constitution-for-cyber-commissioner.html.

democratic government functioning, national infrastructure, and the protection of rights as well as the delivery of services to South African citizens.[1253]

The proposal[1254] continues by explaining that the personal and private information of individuals, organisations or the government are not protected enough, which will ultimately result in exposed information and financial loss due to cybercrime.[1255] The proposal also mentions that public and private organisations are often not financially stable enough to implement high-profile cybersecurity measures or that they lack the appropriate expertise to implement cybersecurity, leaving the individual, organisation or government vulnerable and exposed.[1256] The question remains, is the *Cybercrimes Act* in line with the *Constitution* or not?

In Molwantwa's opinion,[1257] there appear to be certain sections in the *Cybercrimes Act* that are considered to be in line with the *Constitution*, however, there are also certain sections that are not.[1258] According to Molwantwa,[1259] the certain sections of the *Cybercrimes Act* not in line with the *Constitution* include, delegating too much unregulated power to the SSA and the SAPS, not explicitly stating the balance between combatting cybercrime and protecting the constitutional rights of South African citizens, allowing for the transfer of personal or private information to another country by the government, and that the *Cybercrimes Act* operates from a state-centric approach.[1260]

For South Africa to be able to ensure that cybercrime and cybersecurity legislation do not oppose constitutional rights, the government must seek to define, as already mentioned, what cybersecurity means and how they aim to implement it; this includes clarifying the concepts of cybercrime and cybersecurity and balancing the constitutional rights of citizens and cybersecurity measures.[1261] The cybersecurity approach must focus on being more

---

1253 Vermeulen 2022 https://mybroadband.co.za/news/security/468359-proposal-to-amend-south-africas-constitution-for-cyber-commissioner.html.

1254 In process; Available to be read by the public.

1255 Vermeulen 2022 https://mybroadband.co.za/news/security/468359-proposal-to-amend-south-africas-constitution-for-cyber-commissioner.html.

1256 Vermeulen 2022 https://mybroadband.co.za/news/security/468359-proposal-to-amend-south-africas-constitution-for-cyber-commissioner.html.

1257 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 53.

1258 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 53.

1259 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 53.

1260 State-centric approach in this context refers to the power of the government; Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 54.

1261 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 67.

human-centric rather than state-centric.[1262] The government must establish and empower cybersecurity services supervising the interception of South African communications.[1263] Cybercrime and cybersecurity matters must be reviewed and evaluated by the SSA as well as include the South African Human Rights Commission (SAHRC).[1264]

The government must ensure that state security and intelligence services do not abuse their powers to unlawfully infringe upon any constitutional rights.[1265] For the *Cybercrimes Act* to achieve its main objective, it must be constantly reviewed to ensure that it falls within the provisions of the *Constitution*.[1266] An example of an independent body to review the *Cybercrimes Act* would be the SAHRC because of their objective interest in public matters, especially regarding the protection of rights.[1267] The constitutional rights of South African citizens are only as important as their security; therefore security in the cyberspace can only be achieved when the constitutional rights of citizens are upheld and protected and at times, limited.[1268] While the *Cybercrimes Act* does address and provide for cybersecurity measures and cybercrime committed inside and outside South Africa, there is still much room for improvement.[1269]

4.4 Conclusion

The *Cybercrimes Act* appears to have an extensive reach and impact in South Africa regarding cybercrime and cybersecurity, considering the protection of information in the cyberspace.[1270] According to Justice Minister Ronald Lamola,[1271] the *Cybercrimes Act* is in fact, the first big step to a safe and secure South African online environment considering that the *Cybercrimes Act* consolidates national cybercrime legislation.[1272] Lamola continues

---

1262 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 67.
1263 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 68.
1264 Sutherland *Governance of Cybersecurity* 87; Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 68.
1265 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 68.
1266 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 66.
1267 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 66.
1268 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 58.
1269 Mabeka and Cassim 2023 *Obiter* 19.
1270 Emma-Iwuoha 2021 https://www.michalsons.com/blog/the-cybercrimes-act-is-here-now-what/46362.
1271 Grealy *et al* 2021 https://businesstech.co.za/news/technology/543432/south-africas-new-cybercrime-laws-have-been-partially-introduced-heres-what-comes-next/#:~:text=The%20Cybercrimes%20Act%20defines%20three,damage%20to%20property%20or%20violence.
1272 Grealy *et al* 2021 https://businesstech.co.za/news/technology/543432/south-africas-new-cybercrime-laws-have-been-partially-introduced-heres-what-comes-next/#:~:text=The%20Cybercrimes%20Act%20defines%20three,damage%20to%20property%20or%20violence.

by stating that the implemented provisions aim to ensure among others, that the cyber-infrastructure of South Africa is extended, capacitated and trained to address cybercrime appropriately, that national verifiable statistics of the impact of the *Cybercrimes Act* will be analysed and reviewed for feedback, and that cybercrime investigation procedures will be evaluated to determine the effectiveness of the *Cybercrimes Act*.[1273]

Lamola reassuringly concludes that the rest of the provisions will be implemented in due course once the ancillary regulations have been considered and finalised.[1274] According to Rughoonandan,[1275] the realistic effects of the *Cybercrimes Act* on South African individuals and organisations are considerable.[1276] However, Rughoonandan states that not all issues regarding cybersecurity in South Africa have been resolved, and that the enforcement of cybersecurity is becoming an infraction on an individual's freedom regarding who owns or uses a computer or smart device or whoever is connected to the internet and cyberspace.[1277] For South Africa to be able to effectively combat cybercrime, the government must firstly understand cybercrime and secondly analyse the number of cyber-resources available to identify, report and prosecute cybercrime.[1278]

The *Cybercrimes Act* repeals certain pieces of cybercrime legislation; the aim of the *Cybercrimes Act* is to achieve controlled codification regarding computer crimes and the cyberspace.[1279] However, it is important to note that the *Cybercrimes Act* cannot be the only piece of cybercrime legislation implemented in South Africa.[1280] South Africa must continue to develop cybercrime legislation and policies considering the rapid pace of advanced technology and the procedural requirements of national law promulgation and implementation.[1281] Therefore, it is of the utmost importance for South Africa and its

---

1273 Grealy *et al* 2021 https://businesstech.co.za/news/technology/543432/south-africas-new-cybercrime-laws-have-been-partially-introduced-heres-what-comes-next/#:~:text=The%20Cybercrimes%20Act%20defines%20three,damage%20to%20property%20or%20violence.

1274 Grealy *et al* 2021 https://businesstech.co.za/news/technology/543432/south-africas-new-cybercrime-laws-have-been-partially-introduced-heres-what-comes-next/#:~:text=The%20Cybercrimes%20Act%20defines%20three,damage%20to%20property%20or%20violence.

1275 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 54.

1276 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 55.

1277 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 55.

1278 Mabunda *The South African Legislative Response to Cybercrime* 139.

1279 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 106.

1280 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 140.

1281 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 140.

cybercrime legislation to be precise and focused on addressing cybercrime and cybersecurity to avoid any hindrances or uncertainties in the cyberspace.[1282]

[1282] Mabunda *The South African Legislative Response to Cybercrime* 192.

Chapter 5 Conclusion and Recommendations

5.1 Conclusion

The history and evolution of cybercrime in South Africa has been quite a journey throughout the past few years.[1283] Cybercrime, previously referred to as "hacking",[1284] first became evident in the early 1970's and since then, progressed significantly to become an international concern for numerous countries and their governments due to the lack of a controlled and secure online environment.[1285] Although there appears to be no precise definition of the concept of cybercrime,[1286] as cybercrime is still considered a relatively new crime, cybercrime can be defined as an illegal online action or activity committed by a cyber-attacker (usually protected by advanced software) in terms of gaining unauthorised access to or confidential information from an independent individual, organisation or a country's government.[1287]

However, it is important to note that a cybercrime can be committed offline as well.[1288] Regarding the progressive nature and objective of ICTs and the impact and effect of the Fourth Industrial Revolution (4IR) on modern technology,[1289] it has become quite clear that countries and their governments do not have the option to simply ignore or neglect the process of promulgating and implementing appropriate cybercrime legislation to properly address and combat cybercrime in the cyberspace.[1290] The cyberspace along with international ICTs play fundamental roles in the development of a country's social and economic infrastructure.[1291] Cybercrime has been evident in South Africa since the 1990's and for over thirty years South Africa has been challenged to appropriately identify, address and combat cybercrime within its borders.[1292]

1283 Mabunda *The South African Legislative Response to Cybercrime* 23.
1284 GOOSEVPN 2015 https://goosevpn.com/blog/origin-cybercrime.
1285 Kaspersky 2020 https://www.kaspersky.co.za/resource-center/threats/what-is-cybercrime.
1286 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 7.
1287 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 7.
1288 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 8; Writer's definition of cybercrime.
1289 Snail 2021 https://cyberbrics.info/legal-intersections-between-the-protection-of-personal-information-act-4-of-2013-popia-and-the-cyber-crimes-act-19-of-2020-2/.
1290 Schultz *Cybercrime: An Analysis of Current legislation in South Africa* 40.
1291 Allen 2021 https://issafrica.org/iss-today/critical-infrastructure-attacks-why-south-africa-should-worry.
1292 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 4.

As mentioned in Chapter 1,[1293] South Africa secured itself as country number six with the most cyber-attacks in the year, 2021.[1294] Shortly after the Covid-19 pandemic, South Africa responded by implementing the fundamental piece of cybercrime legislation, the *Cybercrimes Act* 19 of 2020 (hereafter the "*Cybercrimes Act*").[1295] However, for South Africa it is important to understand that the battle against cybercrime cannot be won without an understanding of the extensive nature and various elements that make up cybercrime and the cyberspace.[1296] The impact and effect of the lack of understanding the nature of cybercrime and its various elements are seen throughout both the public- and private sectors of South Africa.[1297]

As mentioned, the Covid-19 pandemic played a remarkable role in the history and evolution of cybercrime as "remote working" became the new international operating standard for educational institutions as well as national and international organisations.[1298] The impact and effect of the Covid-19 pandemic held severe consequences for countries and their cyber-infrastructure due to an overly engaged online environment.[1299] Shortly after the impact and effect of the Covid-19 pandemic, South Africa actively invested in promulgating and implementing the *Cybercrimes Act*.[1300] The *Cybercrimes Act* is considered a fundamental breakthrough for South African cybercrime legislation in combatting, addressing, and prosecuting cybercrime in South Africa.[1301] According to Allen,[1302] the *Cybercrimes Act* proved itself and can be considered an international piece of cybercrime legislation.

There are four distinct factors to consider when identifying cybercrime.[1303] These factors include (a) the target of the cybercrime, (b) the instrument or smart device used to

---

1293 As discussed in chapter 1.3.

1294 Ernest 2022 https://www.timeslive.co.za/news/south-africa/2022-05-04-sa-ranked-6th-country-most-affected-by-cybercrime-research-finds/.

1295 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.

1296 Gumbi *Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom* 92.

1297 Gumbi *Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom* 92.

1298 Olofinbiyi and Singh 2020 *IJCS* 221.

1299 Olofinbiyi and Singh 2020 *IJCS* 221.

1300 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.

1301 Giles 2021 https://www.michalsons.com/blog/the-practical-impact-of-the-cyber-bill-on-you/25300#:~:text=If%20you%20share%20your%20password,you%20could%20be%20a%20criminal ; Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.

1302 Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.

1303 Casey *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 14.

commit the cybercrime, (c) the specific role of the smart device in the cybercrime and in general, (d) considering crimes involving smart devices.[1304] According to Cassim,[1305] smart devices or instruments used to commit a cybercrime can either be used as an object or a subject.[1306] An object to a cybercrime is when the smart device or instrument is used to physically perform and carry out the crime by itself, for example, through a software programme to commit online identity theft.[1307] A subject to a cybercrime is when the smart device or instrument is used as an instrument by the cyber-attacker to perform or commit a traditional crime, for example, fraud.[1308]

The different types of cybercrime can be divided into several categories;[1309] these categories include cybercrime against an individual, cybercrime against society, cybercrime against organisations or companies, cybercrime against the government (cyber-terrorism), and lastly, intellectual property cybercrime.[1310] As discussed in Chapter 2,[1311] examples of the most common types of cybercrime include, phishing attacks, email harassment, DDoS attacks, viruses and worms, identity theft, online fraud and extortion, and web-jacking.[1312] Considering the different categories of cybercrime, there are several different categories of cyber-attackers based on the objective and the outcome of the cybercrime;[1313] these categories include script kiddies, organised hackers, professional hackers and discontented employees.[1314]

Regardless of the recent implementation of the *Cybercrimes Act*, cybercrime remains a progressive challenge.[1315] It is important for South Africa to continue to develop national cybercrime legislation along with implementing cybercrime terminology and create national awareness regarding cybercrime and cybersecurity measures in the

---

1304 Casey *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 14.
1305 Cassim 2009 *PER/PELJ* 59.
1306 Cassim 2009 *PER/PELJ* 59.
1307 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 7.
1308 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 7.
1309 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
1310 Coolidge 2021 https://coolidgelawfirmaz.com/what-are-the-major-types-of-cybercrime/.
1311 As discussed in chapter 2.1.
1312 As discussed in chapter 2.1.
1313 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
1314 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
1315 Cassim 2011 *CILSA* 126.

cyberspace.[1316] As mentioned above,[1317] cybercrime is considered a relatively new crime, therefore introducing unfamiliar types of challenges to South Africa.[1318] These challenges include,[1319] the detection of cybercrime, the investigation procedure of cybercrime, the reporting of cybercrime and the effective combatting of cybercrime.[1320]

According to Cassim,[1321] South Africa has been too focused and occupied with its national legislation regarding traditional crimes for example, homicide,[1322] resulting in a neglected cybercrime state.[1323] Although cybercrime is considered far more complex than any other traditional crime,[1324] there are numerous distinguishable elements to determine and separate cybercrime from traditional crimes.[1325] These elements include,[1326] the cyber-medium involved in the crime, the speed of the crime, the evidence of the crime, the reach of the crime, and lastly, the scale of the crime.[1327] Other elements include, the consequences of the crime and the country's national infrastructure to respond to the committed crime.[1328]

Regarding the previous position of cybercrime in South Africa;[1329] South Africa faced numerous cyber-attacks through the years, which ultimately resulted in tremendous financial losses.[1330] South Africa has been victim to many cyber-attacks including the attacks on TransUnion,[1331] and Transnet.[1332] These cyber-attacks ultimately led to the promulgation and implementation of numerous pieces of cybercrime legislation and the

1316 Gumbi *Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom* 92.
1317 As discussed in chapter 1.3.
1318 Grobler, Zaaiman and Van Vuuren 2013 *CSIR* 34.
1319 Dlamini and Mbambo 2019 *ISSN* 6.
1320 As discussed in chapter 2.
1321 Cassim 2011 *CILSA* 127.
1322 Cassim 2011 *CILSA* 127.
1323 Cassim 2011 *CILSA* 127.
1324 Pinto 2022 https://www.eatmy.news/2022/11/how-cyber-crimes-differ-from.html.
1325 UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis.
1326 PGI 2018 https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/.
1327 PGI 2018 https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/.
1328 Leukfeldt and Malsch 2019 https://nscr.nl/en/gevolgen-cybercrime-zeer-ingrijpend-voor-slachtoffers/.
1329 See chapter 2.2.
1330 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com.
1331 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com.
1332 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com.

NCPF.[1333] Regarding the current position of cybercrime in South Africa;[1334] South Africa continues to battle against the threat and impact of cybercrime;[1335] however, since the implementation of the *Cybercrimes Act* South Africa might possibly rest assured and enjoy a safe and secure cyberspace along with knowing that investigation procedures are at hand were an internet user to fall victim to a cybercrime or a cyber-attack.[1336]

Regarding the history and evolution of cybercrime legislation in South Africa, Chapter 3 thoroughly discussed and examined the extensive pieces of cybercrime legislation available in South Africa, prior to the implementation of the *Cybercrimes Act*.[1337] Each of the selected pieces of cybercrime legislation was discussed based on their origin, their objective, and their shortcomings.[1338] The selected pieces of legislation were, the *RICA*, the *ECTA* along with the *CPA*, the *POPIA*, the *FPAA*, the National Cybersecurity Policy Framework (NCPF) and the two international cybercrime conventions, the Budapest Convention, and the AU Convention.[1339] This chapter partially focused on the two international cybercrime conventions and both cybercrime conventions were discussed in terms of the impact they had on South Africa's cybercrime legislation.[1340]

The Budapest Convention played a remarkable role in the history and evolution of South Africa's cybercrime legislation.[1341] The objective of the Budapest Convention is to address, regulate and explain cybercrime and cybersecurity to different countries.[1342] As mentioned,[1343] South Africa was the only African country to sign the Budapest Convention but never ratified it, nevertheless the Budapest Convention did convince South Africa to invest more in promulgating and implementing cybercrime legislation.[1344] The promulgation and implementation of the *ECTA* was the result of one of the first pieces of

1333 Pieterse *Electronic Crime Unit* 9.
1334 See chapter 2.3.
1335 Dlamini and Mbambo 2019 *ISSN* 5.
1336 Dlamini and Mbambo 2019 *ISSN* 5.
1337 As discussed in chapter 3.
1338 As discussed in chapter 3.
1339 As discussed in chapter 3.
1340 As discussed in chapter 3.
1341 Sutherland 2019 https://www.itweb.co.za/content/lwrKxv3JLOJqmg1o.
1342 Council of Europe 2001 Convention on Cybercrime *ETS* 1-3.
1343 Sutherland 2019 https://www.itweb.co.za/content/lwrKxv3JLOJqmg1o.
1344 Sutherland 2019 https://www.itweb.co.za/content/lwrKxv3JLOJqmg1o.

legislation to specifically address cybercrime in South Africa, originating from the Budapest Convention.[1345]

Although the AU Convention was signed by South Africa, South Africa never ratified it.[1346] The AU Convention encourages cybersecurity and personal data protection, along with focusing on the protection of online transactions.[1347] The AU Convention played a less remarkable role in the history and evolution of South Africa's cybercrime legislation.[1348] Chapter 3 also discussed the development of cybercrime legislation in South Africa over the past few years. This chapter further discussed the extent and depth of the selected cybercrime legislation and the impact it had on the South African legislature prior to the *Cybercrimes Act*.[1349] The impact and effect of the *Constitution* was also discussed, especially regarding certain sections found in the Bill of Rights.[1350]

The first piece of legislation discussed was the *RICA*. The *RICA* was first implemented in 2005, after the NCPF was introduced as the fundamental cybercrime policy framework of South Africa.[1351] However, in the case *AmaBhungane Centre for Investigative Journalism*[1352] the Constitutional Court declared the *RICA* unconstitutional due to numerous reasons.[1353] Therefore, the *RICA* is no longer considered applicable in South Africa.[1354] The second piece of legislation discussed was the *ECTA*. The most relevant chapters of the *ECTA* are Chapter XII and Chapter XIII. Chapter XII addresses and establishes the objective, functions, and powers of "Cyber Inspectors".[1355]

Chapter XIII addresses cybercrime and lists a few cyber-offences recognisable in terms of the *ECTA*; some of these cyber-offences include the unauthorised access or unlawful

---

1345 Eboibi 2020 *Commonwealth Law Bulletin* 6.
1346 Sutherland 2017 *AJIC* 92.
1347 African Union Convention on Cyber Security and Personal Data Protection 1-2.
1348 Sutherland 2017 *AJIC* 92.
1349 As discussed in chapter 3.
1350 Chapter 2 of the *Constitution*; Hakmeh, Naylor and Wallace 2022 https://www.chathamhouse.org/2022/02/what-cyber-attack; Karlsson *Democracy in South Africa* 1.
1351 Maat *Cyber Crime: A Comparative Law Analysis* 10.
1352 *AmaBhungane Centre for Investigative Journalism NCP v Minister of Justice and Correctional Services and Others*; *Minister of Police and Others v AmaBhungane Centre for Investigative Journalism NCP Case* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021).
1353 Ongeso 2021 https://bowmanslaw.com/insights/mergers-and-acquisitions/south-africa-constitutional-court-upholds-declaration-of-invalidity-of-rica/.
1354 *AmaBhungane Centre for Investigative Journalism* 61.
1355 Eboibi 2020 *Commonwealth Law Bulletin* 6.

interference with data.[1356] Certain sections of the *ECTA* will be amended regarding the implementation of the *Cybercrimes Act*.[1357] The third piece of legislation read along with the *ECTA* is the *CPA*. The *CPA* addresses the manner in which investigation procedures are conducted along with addressing the issuing of warrants, the functions of authorised officials, and the procedure of accessing, searching, and seizing articles in the process of investigation procedures.[1358] The fourth piece of legislation is the *POPIA*. The *POPIA* is known for promoting the protection of personal or private information in both the public and private sectors.[1359]

The *POPIA* also addresses data protection and data supervision and lists different offences recognisable in terms of the *POPIA*.[1360] The *POPIA* and *Cybercrimes Act* share similar objectives in terms of safeguarding communications within the Republic.[1361] The last piece of legislation was the *FPAA*. The *FPAA* was implemented to address and regulate online distribution in South Africa.[1362] This includes films, games, videos, and publications.[1363] The *FPAA* also established the Film and Publications Board.[1364] Throughout the chapter, shortcomings of the previous pieces of cybercrime legislation can be found.[1365]

The last chapter, Chapter 4, critically discussed and examined the history and evolution of the recently implemented *Cybercrimes Act*. The main objective of the *Cybercrimes Act* is to establish a safe and secure cyberspace for South African citizens and improve the national cybersecurity of the country.[1366] Since the implementation of the *Cybercrimes Act* the South Africa government and legislature have been evaluating the impact and effect of the *Cybercrimes Act* on the South African cyberspace.[1367] However, no official statements

---

1356 Chapter XIII of the *ECTA*.
1357 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 40.
1358 Preamble of the *CPA* 51 of 1977.
1359 Preamble of the *POPIA*.
1360 The *POPIA*.
1361 Pinarbasi 2022 https://blog.didomi.io/en/popia-south-africa.
1362 Preamble of the *FPAA*.
1363 MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force.
1364 MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force.
1365 Schultz *Cybercrime: An Analysis of Current legislation in South Africa* 36.
1366 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.
1367 Manaleng 2021 https://ewn.co.za/2021/06/03/think-before-you-click-ramaphosa-signs-cybercrimes-act-into-law; Michalsons 2022 https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa#:~:text=The%20Cybercrimes%20Act%20enables%20the,this%20is%20a%20global%20issue.

or reviews have been released other than the statements regarding the delays with certain chapters or sections envisaged in the *Cybercrimes Act*.[1368] Chapter 4 also discussed the position regarding jurisdiction, lawful investigation procedures, mutual assistance, and established (not yet commenced) the designated Point of Contact.[1369]

Cybercrime is considered multi-jurisdictional due to its borderless nature and the way numerous countries and governments result in becoming the cyber-victim of the same cyber-attack launched from a specific geographical location.[1370] With the implementation of the *Cybercrimes Act* certain pieces of legislation will be amended or repealed.[1371] The chapter continued by addressing the position and effect of the *Constitution* versus the position and effect of the *Cybercrimes Act* and addressed whether the *Cybercrimes Act* appears to be in line with the *Constitution*.[1372] The premise of this study was focused on the primary objective and legal extent of the recently implemented *Cybercrimes Act* in properly responding to cybercrime.[1373]

The primary objective of the *Cybercrimes Act* is to develop and establish a secure online environment for South African citizens, organisations, and the government, and it appears that the impact and effect of the *Cybercrimes Act* has been positive.[1374] Although the *Cybercrimes Act* appears to be quite extensive, according to this study, the *Cybercrimes Ac*t is not considered extensive enough to solely address or combat cybercrime in South Africa. The *Cybercrimes Act* responds to cybercrime occurring in South Africa; however, South Africa must focus on implementing additional cybercrime legislation or policies to establish a safe and secure cyberspace.[1375]

Regarding the assumption of the study,[1376] the duty and responsibility of the South African government and legislature to protect the country and its citizens as envisaged in section

---

[1368] Burger-Smidt 2022 https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/.
[1369] Chapter 3 – chapter 6 of the *Cybercrimes Act*.
[1370] Gumbi *Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom* 93.
[1371] Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 106.
[1372] As discussed in chapter 4.3.
[1373] See chapter 1.5.
[1374] The *Cybercrimes Act*.
[1375] This refers to amendment acts, and international treaties or conventions addressing and filling the gaps of the reach of the *Cybercrimes Act*.
[1376] See chapter 1.5.

7 and section 14(d) of the *Constitution* are crucial.[1377] This duty and responsibility are regularly exercised with great diligence; however, it appears that this duty and responsibility can be lawfully limited or compromised considering the complex nature of cybercrime and that cybercrime investigation procedures often require access, search and seizure of the targeted device, which can infringe section 14(d) of the *Constitution*.[1378] The South African government and national authorities must focus on establishing a lawful balance between cybercrime investigation procedures and section 14 of the *Constitution*.[1379]

Therefore, it is crucial for additional cybercrime legislation and resources to assist the *Cybercrimes Act* in addressing cybercrime in South Africa, as the *Cybercrimes Act* cannot be solely considered adequate while cybercrime in South Africa is still on the rise.[1380] Therefore, as the rate of cybercrime continues to increase,[1381] the South African government must act briskly to ensure that the *Cybercrimes Act* is implemented and applied correctly to ensure a safe online environment for internet users. The hypothesis of the study was,[1382] although the recently implemented *Cybercrimes Act* of South Africa appears quite promising and the legal impact thereof, quite positive, the *Cybercrimes Act* cannot solely be regarded as effective or advanced enough in addressing and combatting cybercrime to the crime's greatest extent.[1383]

As mentioned,[1384] the study presented not only previous cybercrime legislation shortcomings but also the shortcomings of the *Cybercrimes Act*, some of these shortcomings include defining the concept of cybercrime, balancing the restrictions of the *Cybercrimes Act* with other pieces of legislation, addressing inconsistencies between the *Cybercrimes Act* and the *CPA*, the lengthy timeframe of requesting mutual assistance, etc.[1385] Therefore, the *Cybercrimes Act* cannot be considered as the only cybercrime

---

1377 Section 7, section 14 of the *Constitution*.
1378 Sutherland 2017 *AJIC* 94.
1379 Sutherland 2017 *AJIC* 94.
1380 Mcanyana and Brindley 2020 https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa.
1381 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 4.
1382 See chapter 1.5.
1383 As discussed in chapter 1.5.
1384 As discussed in chapter 1.5.
1385 As thoroughly discussed in chapter 4.1.

legislation in South Africa.[1386] The *Cybercrimes Act* must be supported through additional cybercrime legislation.[1387] The discussion and results support the hypothesis. In conclusion, the main research question of this study was:[1388] To what extent does the recently implemented *Cybercrimes Act* effectively address and deal with the extensive and complex nature of cybercrime to combat cybercrime in South Africa?

The sub-question of this study was:[1389] Does the *Cybercrimes Act* have any shortcomings regarding investigation procedures, the delegation of powers of national authorities or prosecution procedures? In the writer's view, the *Cybercrimes Act* is a considerable start regarding adequate cybercrime legislation in South Africa. The *Cybercrimes Act* is an exquisite piece of national cybercrime legislation which South Africa and its citizens will greatly benefit from. The *Cybercrimes Act* is an informative and international standard piece of cybercrime legislation effectively addressing various components and elements that make up the cyberspace.

The extensive reach of the *Cybercrimes Act* is considered national (and in rare cases international), comprehensive, and effective for individuals, organisations, several government departments, and the public and private sectors of South Africa, regardless of the fact that some of its sections still need to be amended to include specific stipulations and that some of the sections of the *Cybercrimes Act* must still be signed into law.[1390] The *Cybercrimes Act* addresses citizens, organisations and the government with immense diligence and is educational in nature.[1391] However, regarding the shortcomings of the *Cybercrimes Act*: Yes, there already appear to be a few concerns and recommendations regarding the *Cybercrimes Act* and the manner in which it determines and delegates the powers of national authorities or national officials.

Cyber-experts believe that if the *Cybercrimes Act* fails to explicitly address the delegation of powers, the abuse of powers can easily undermine the entire objective of the C*ybercrimes Act*.[1392] Other shortcomings and concerns include the manner in which the

---

1386 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 140.
1387 The additional cybercrime legislation must focus on addressing the shortcomings as discussed above; Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 140.
1388 See chapter 1.3.3.
1389 See chapter 1.3.3.
1390 As discussed in chapter 4.
1391 As discussed in chapter 4.
1392 Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa* 141.

Cybercrimes Act regulates lawful cyber-investigation and prosecution procedures without infringing upon any privacy matter or right found in the Bill of Rights, specifically referring to section 10, the right to human dignity and section 14, the right to privacy of the *Constitution*.[1393] It is therefore important to remark that the *Cybercrimes Act* cannot solely combat cybercrime in South Africa, and must be assisted by additional cybercrime legislation, for example, the *POPIA*.[1394] The few concerns and recommendations regarding the shortcomings of the *Cybercrimes Act* will be discussed under the Recommendations heading below.

5.2 Recommendations

In the writer's opinion, the *Cybercrimes Act* is an inspired and well-written piece of national cybercrime legislation; however, the analysis and effectiveness of the recently implemented *Cybercrimes Act* can be refined by considering the following: The few concerns and recommendations regarding the shortcomings of the *Cybercrimes Act* can be divided into two categories, legislative recommendations, and practical recommendations.

5.2.1 Legislative recommendations

(a) The first recommendation I believe to be of utmost importance is that the *Cybercrimes Act* must be reviewed and amended to include and define simple academic definitions of the following concepts, "cybercrime", "cybersecurity" and "cyberterrorism".[1395] I believe the lack of simple definitions for these concepts can easily question the legal competence of national authorities or create confusion in the South African legislature regarding the identification of cybercrime.[1396]

(b) The second recommendation is that the *Cybercrimes Act* fails to address the concept of cybersecurity or cybersecurity measures.[1397] Although the *Cybercrimes Act* focuses on addressing and combatting cybercrime, the concept of cybersecurity must not be neglected.[1398] Cybersecurity is one of the fundamental prevention components of

---

1393 Hakmeh, Naylor and Wallace 2022 at https://www.chathamhouse.org/2022/02/what-cyber-attack.
1394 Madziwa and Snail 2021 https://www.hg.org/legal-articles/cyber-crime-in-south-africa-5351.
1395 Section 1 of the *Cybercrimes Act*.
1396 Michalsons 2022 https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa#:~:text=The%20Cybercrimes%20Act%20enables%20the,this%20is%20a%20global%20issue.
1397 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 18.
1398 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 18.

cybercrime, and cybercrime cannot be understood without the referral to cybersecurity. South Africa must additionally focus on cybersecurity as one of the crucial elements present in the cyberspace and disassemble the concept of cybersecurity until they understand how to use cybersecurity to their advantage.[1399] Implementing advanced cybersecurity measures[1400] as first defence will mitigate the countless threats of cybercrime in South Africa.

(c) The third recommendation is the specific role of regularly monitoring cybercrime investigation and prosecution procedures.[1401] This recommendation must be explicitly stipulated in the *Cybercrimes Act* to prevent the abuse of evidence and powers by national authorities or national officials and prevent these procedures from being conducted unlawfully.[1402] Implementing this specific section will diminish problems such as the erasing or altering of evidence and ensure that the investigation and prosecution procedures are executed with diligence and discretion.[1403]

(d) The fourth recommendation, as discussed in Chapter 4, is where the *Cybercrimes Act* fails to provide cyber-victims with the option of instituting civil proceedings in cybercrime cases rather than criminal proceedings.[1404] Often the institution of civil proceedings rather than criminal proceedings will benefit the cyber-victim more,[1405] bringing the investigation and prosecution procedure to an accomplished level of executing fair justice.

(e) The fifth recommendation is that the *Cybercrimes Act* also fails to explicitly address the legal requirement from a cyber-victim to give consent to the processing of any personal or private information during the investigation procedure.[1406] Legal consent is one of the fundamental requirements needed to lawfully conduct an investigation procedure, especially a cybercrime investigation procedure.[1407] Without the legal requirement of

---

1399 Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* 18.
1400 As thoroughly discussed in chapter 2.1, p 33.
1401 As thoroughly discussed in chapter 4.1; Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 78.
1402 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 78.
1403 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 78.
1404 Mabeka and Cassim 2023 *Obiter* 23; Mabeka 2022 *IJLPA* 14.
1405 Mabeka and Cassim 2023 *Obiter* 23; Mabeka 2022 *IJLPA* 14.
1406 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.
1407 Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses.

consent, national authorities or cyber-investigators will face severe legal repercussions based on section 14 (right to privacy) of the *Constitution*.

(f) The sixth recommendation: Govender[1408] approaches the legal process in which investigation procedures are conducted.[1409] Govender states that the investigation procedure consists of four distinct elements, identification, preservation, analysis, and presentation.[1410] She continues by suggesting that the security precautions of the investigation procedure must be cyber-advanced making it impossible to expose, damage or alter any electronic evidence during the investigation procedure.[1411] This includes storing electronic evidence on third-party servers, placing electronic evidence under 24/7 cybersecurity and surveillance, avoiding the exposure of the electronic evidence to magnetic fields or extreme temperatures, for example heat, and avoiding the exposure of the electronic evidence to too many computer programmes, resources or databases.[1412]

(g) The seventh recommendation, as discussed in Chapter 4: the establishment and operation of a 24/7 Point of Contact has not yet been commenced and South Africa appears to be eagerly waiting on its commencement date.[1413] The 24/7 Point of Contact will act as an independent cyber-entity focusing on the reporting of cybercrime, providing legal assistance and the expansion of South Africa's cyber-infrastructure.[1414] Various cyber-incident response teams along with the 24/7 Point of Contact will encourage cyber-awareness and cybersecurity and support the commitment South Africa made to provide a safe and secure cyberspace.[1415] The reasons for the delay in implementing or commencing the 24/7 Point of Contact and cyber-incident response teams remain unknown.

1408 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 78.

1409 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 78.

1410 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 78.

1411 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 78.

1412 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 78.

1413 Burger-Smidt 2022 https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/.

1414 Pillay 2017 https://www.withoutprejudice.co.za/free/article/5659/view.

1415 Pillay 2017 https://www.withoutprejudice.co.za/free/article/5659/view.

(h) The eighth recommendation: Adam[1416] states that South Africa lacks any specific or established cryptocurrency legislation.[1417] Although cryptocurrencies are rooted in finances rather than in cyber, the *Cybercrimes Act* can be used as a national standard to introduce and encourage the South African legislature to focus on promulgating and implementing cryptocurrency legislation. The *Cybercrimes Act* does not have to dedicate an entire chapter to cryptocurrencies, a simple section would suffice. Since cryptocurrencies take place in the online environment, it would not be completely uncommon for the *Cybercrimes Act* to address cryptocurrencies in a section.

(i) The last legislative recommendation: Although the Budapest Convention appeared as one of the fundamental cybercrime conventions that inspired the promulgation and implementation of the *Cybercrimes Act*, it is quite clear that the *Cybercrimes Act* does not consider or address all the principles envisaged in the Budapest Convention.[1418] For example, Article 13 of the Budapest Convention addresses sanctions and measure; this section includes "non-criminal sanctions" which often refers to civil litigation or remedies.[1419] Article 13 is closely related to section 23 of the *Cybercrimes Act*, however section 23 does not include any form of "non-criminal sanctions".[1420] Therefore the *Cybercrimes Act* fails to provide the explicit option (meaning it is not envisaged in the *Act*) of civil litigation or proceedings (as discussed in chapter 4) to those affected by cybercrime.[1421]

5.2.2 Policy/Practical recommendations

(a) The first practical recommendation, according to Jideani:[1422] South Africa must focus on improving national awareness regarding cybercrime and especially cybersecurity to prevent cybercrime from occurring in the first place.[1423] Jideani discussed three important elements regarding raising cyber-awareness in South Africa; these elements are,[1424] strategic planning, experienced skills, and the involvement of the government.[1425] The first

1416 Adam 2021 *PSLR* 378.
1417 Adam 2021 *PSLR* 378.
1418 Mabeka and Cassim 2023 *Obiter* 30.
1419 Mabeka and Cassim 2023 *Obiter* 30.
1420 Mabeka and Cassim 2023 *Obiter* 30.
1421 Mabeka and Cassim 2023 *Obiter* 30; As discussed in chapter 4.
1422 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 113.
1423 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 113.
1424 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 113.
1425 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 113.

element, strategic planning, refers to natural and juristic persons implementing cybersecurity measures apart from adhering to national cybercrime legislation.[1426] This includes cybercrime and cybersecurity policies or campaigns within South Africa's national security structures.[1427]

The second element, experienced skills refer to the need of developing and regularly upgrading South Africa's cyber-infrastructure and expanding its cyber-capacity.[1428] This element is focused on responding to cybercrime in an appropriate manner by implementing a Cybersecurity Hub.[1429] This is directly referenced to Chapter 6 of the *Cybercrimes Act*, the designated Point of Contact.[1430] The third element, the involvement of the government refers to the role the government plays in developing and implementing national cybercrime legislation or cybersecurity measures.[1431] This can be done through both public or private organisations and educational institutions.[1432] Financial support and resource guidance can also be implemented by the government in developing and addressing cybercrime in South Africa.[1433]

(b) The second recommendation considers the availability of international resources. Schultz[1434] is of the opinion that South Africa fails to invest or engage in the option of international cooperation from different countries in addressing and combatting cybercrime.[1435] Schultz states that it is crucial for South Africa to collaborate with other countries and implement a holistic cybercrime legislation.[1436] She continued by stating that the established cybercrime legislation in South Africa is too inadequate to holistically address or combat cybercrime, and that national cybercrime legislation must also focus on preventing cybercrime instead of just prosecuting cybercrime, which South Africa will simply benefit from.[1437]

1426 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 113.
1427 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 113.
1428 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 113.
1429 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 113.
1430 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 113.
1431 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 114.
1432 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 114.
1433 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 114.
1434 Schultz *Cybercrime: An Analysis of Current legislation in South Africa* 42.
1435 Schultz *Cybercrime: An Analysis of Current legislation in South Africa* 42.
1436 Schultz *Cybercrime: An Analysis of Current legislation in South Africa* 43.
1437 Schultz *Cybercrime: An Analysis of Current legislation in South Africa* 43.

(c) The third recommendation addresses the concern that the South African government fails to encourage cyber-awareness or facilitate cyber-training for national authorities, national officials, or cyber-staff in terms of responding to cybercrime.[1438] The South African government must focus on implementing cyber-awareness to protect all internet users, including citizens, organisations, and the government. Cyber-awareness will generate and encourage internet users to participate in cyber-training programmes and campaigns. Although the objective of the *Cybercrimes Act* is not addressing cyber-awareness, the *Cybercrimes Act* can be used as a national framework to implement cyber-awareness.

(d) The fourth recommendation: Govender,[1439] similar to Jideani,[1440] also argues that South Africa and the government must focus on developing and expanding their cyber-resources, cyber-response infrastructure and their cyber-incident capacity.[1441] The cyber-resources, cyber-response infrastructure and cyber-incident capacity refers to the ability South Africa has, to protect its citizens and to respond to cybercrime.[1442] Govender in support of Jideani states that the educating and equipping of national law enforcement officers, for example the police and agencies are crucial in the fight to respond appropriately to cybercrime.[1443] Govender also mentions that the educating and equipping process must be progressive in nature considering the evolving nature of cybercrime and the cyberspace.[1444]

(e) The fifth recommendation builds on the recommendation made at recommendation (b), but focuses more on a national level of cooperation than on an international level; as discussed earlier by Schultz:[1445] the necessity of international cooperation against cybercrime must not be ignored; however, Schultz recommends that South Africa should also encourage a national cyber-resource network between the public- and private sector of South Africa for cooperation and form a partnership against cybercrime. In the writer's

---

1438 Leukfeldt and Malsch 2019 https://nscr.nl/en/gevolgen-cybercrime-zeer-ingrijpend-voor-slachtoffers/.
1439 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 77.
1440 Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations* 113.
1441 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 77.
1442 Leukfeldt and Malsch 2019 https://nscr.nl/en/gevolgen-cybercrime-zeer-ingrijpend-voor-slachtoffers/.
1443 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 77.
1444 Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* 77.
1445 Schultz *Cybercrime: An Analysis of Current Legislation in South Africa* 43.

opinion, the public and private sector of South Africa appear to have no network or relation regarding the national problem of cybercrime and the effect cybercrime has on South Africa as a country. Surely there are certain cybersecurity measures that can be taken by both the public and private sector to assist each other in addressing and combatting cybercrime.

BIBLIOGRAPHY

Literature

Adam 2021 *PSLR*

Adam Z "An overview of the regulation of cryptocurrency in South Africa" 2021 *PSLR* 370-386

Alkaabi *Combatting Computer Crime: An International Perspective*

Alkaabi AOS *Combatting Computer Crime: An International Perspective* (PhD theses Queensland University of Technology 2010)

Arce 2018 *JOC*

Arce DG "Malware and market share" 2018 *JOC* 1-6

Basdeo 2012 *SACJ*

Basdeo V "The Legal Challenges of Search and Seizure of Electronic Evidence in South African Criminal Procedure: A Comparative Analysis" 2012 *SACJ* 198-211

Bote *The South African National Cyber Security Policy Framework: A critical analysis*

Bote D *The South African National Cyber Security Policy Framework: A critical analysis* (LLM-dissertation North-West University 2019)

Bouwer 2014 *SACJ*

Bouwer GP "Search and Seizure of Electronic Evidence: Division of the Traditional One-Step Process into a New Two-step Process in South African Context" 2014 *SACJ* 156-171

Brierly 1952 *YILC*

Brierly JL "Third Report on the Law of Treaties – Articles Tentatively Adopted by the Commission at the Third Session with Commentary Thereon" 1952 *YILC* 50-56

Casey *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*

Casey E *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 3rd ed (Elsevier Inc. Unites States of America 2011)

Cassim 2011 *CILSA*

Cassim F "Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players" 2011 *CILSA* 123-138

Cassim 2012 *PER/PELJ*

Cassim F "Addressing the spectre of cyber terrorism: a comparative perspective" 2012 *PER/PELJ* 381-415

Cassim 2009 *PER/PELJ*

Cassim F "Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study" 2009 *PER/PELJ* 36-79

Chigada and Madzinga 2021 *SAJIM*

Chigada J and Madzinga R "Cyber-attacks and threats during COVID-19: A systematic literature review" 2021 *SAJIM* 1-11

Dashora 2011 *JAPSS*

Dashora K "Cyber Crime in the Society: Problems and Preventions" 2011 *JAPSS* 240-257

Dlamini and Mbambo 2019

Dlamini S and Mbambo C "Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses" 2019 *ISSN* 1-13

Du Toit *The Search Warrant Provisions of the Cybercrimes Act and their Relationship with the Criminal Procedure Act*

Du Toit P "The Search Warrant Provisions of the Cybercrimes Act and their Relationship with the Criminal Procedure Act" 2022 *Obiter* 764-778

Du Toit, Hadebe and Mphatheni 2018 *CRIMSA*

Du Toit R, Hadebe PN and Mphatheni M "PUBLIC PERCEPTIONS OF CYBERSECURITY: A SOUTH AFRICAN CONTEXT" 2018 *CRIMSA* 111-131

Eboibi 2020 *Commonwealth Law Bulletin*

Eboibi FE "Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and institutional accountability" 2020 *Commonwealth Law Bulletin* 1-32

Erasmus and Bowden 2020 *Obiter*

Erasmus D and Bowden S "A Critical Analysis of South African Anti-money Laundering Legislation with Regard to Cryptocurrency" 2020 *Obiter* 309-327

Govender *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa*

Govender TF *A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa* (LLM-dissertation University of KwaZulu-Natal 2018)

Grobler, Zaaiman and Van Vuuren 2013 *CSIR*

Grobler M, Zaaiman J and Van Vuuren J.C. "Preparing South Africa for Cyber Crime and Cyber Defense" 2013 *CSIR* 32-41

Gumbi *Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom*

Gumbi D *Understanding the treat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom* (LLM-dissertation University of Cape Town 2018)

Hart *The Concept of Law*

Hart HLA *The Concept of Law* (Duke University School of Law 1963)

Heselman and Warren "Cyber Crime Influencing Business in South Africa"

Heselman M and Warren M "Cyber Crime Influencing Business in South Africa" in *InSITE 2004: Informing Science + IT Education* (January 2004) 253-266

Jansen van Rensburg *The human element in information security: An analysis of social engineering attacks in the greater Tswane area of Gauteng, South Africa*

Jansen van Rensburg SK *The human element in information security: An analysis of social engineering attacks in the greater Tshwane area of Gauteng, South Africa* (PhD-dissertation University of South Africa 2017)

Jideani 2018 *Towards a cybersecurity framework for South Africa e-retail organisations*

Jideani PC *Towards A Cybersecurity Framework for South African E-Retail Organisations* (LLM-dissertation Cape Peninsula University of Technology 2018)

Justice, Crime Prevention and Security Cluster (JCPS) Delivery Agreement, 24 October 2010

Justice, Crime Prevention and Security Cluster (JCPS) Delivery Agreement, 24 October 2010

Karlsson *Democracy in South Africa*

Karlsson P *Democracy in South Africa* (LLM-dissertation Linnaeus University 2021)

The Law Society of South Africa *Comments By The Law Society of South Africa (LSSA) On The Cybercrimes and Cybersecurity Bill*

Law Society of South Africa *Comments By The Law Society of South Africa (LSSA) On The Cybercrimes and Cybersecurity Bill* (2015) available at https://www.lssa.org.za/wp-content/uploads/2020/01/LSSA-CYBERCRIMES-AND-CYBERSECURITY-BILL-Comment-30-Novemeber-2015.pdf accessed 12 June 2023

Maat *Cyber Crime: A Comparative Law Analysis*

Maat SM *Cyber Crime: A Comparative Law Analysis* (LLM-dissertation University of South Africa 2009)

Mabeka 2022 *IJLPA*

Mabeka NQ "The Application of Section 8 of Cybercrimes Act 19 of 2020 in Civil Procedure in South Africa is a Hailing Snow: A Comparative Studies between South Africa and United Kingdom" 2022 *IJLPA* 13-20

Mabeka and Cassim 2023 *Obiter*

Mabeka NQ and Cassim F "Interpreting the Provisions of the Cybercrimes Act 19 of 2020 in the Context of Civil Procedure: A Future Journey" 2023 *Obiter* 19-32

Mabunda *The South African Legislative Response to Cybercrime*

Mabunda SM *The South African Legislative Response to Cybercrime* (PhD-dissertation University of the Western Cape 2021)

Mbanaso and Dandaura 2015 *IOSR*

Mbanaso U and Dandaura E "The Cyberspace: Redefining A New World" 2015 *IOSR* 17-24

Minnaar and Herbig 2022 *AC:AJCV*

Minnaar A and Herbig FJW "Cyber-attacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic" 2022 *AC:AJCV* 155-185

Molwantwa *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa*

Molwantwa DM *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* (LLM-dissertation North-West University 2019)

Nkanyane *Subsidiarity in the Context of Administrative Law*

Nkanyane NI *Subsidiarity in the Context of Administrative Law* (LLM-dissertation University of Pretoria 2018)

Nortjé and Myburgh at *PER/PELJ*

Nortjé JGJ and Myburgh DC "The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa" 2019 *PER/PELJ* 1-42

Ntsaluba *Cybersecurity Policy and Legislation in South Africa*

Ntsaluba N *Cybersecurity Policy and Legislation in South Africa* (LLM-dissertation University of Pretoria)

Olofinbiyi and Singh 2020 *IJCS*

Olofinbiyi SA and Singh SB "The Role and Place of Covid-19: An Opportunistic Avenue for Exponential World's Upsurge in Cyber Crime" 2020 *IJCS* 221-230

Pieterse *Electronic Crime Unit*

Pieterse BNT *Electronic Crime Unit* (2015) available at http://www.nstf.org.za/wp-content/uploads/2015/10/BrigPieterse.pdf accessed 13 May 2023

Pieterse 2021 *AJIC*

Pieterse H "The Cyber Threat Landscape in South Africa: A 10-Year Review" 2021 *AJIC* 1-21

Pillay *A Privacy Perspective on the Cybercrimes Act, 2020 – Aspects to consider in your Privacy Programme*

Pillay L *A Privacy Perspective on the Cybercrimes Act, 2020 – Aspects to consider in your Privacy Programme* (2021) available at https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za-Deloitte-Cybercrimes-Privacy-POV.pdf accessed 20 May 2023

Poonia 2014 *IJETTCS*

Poonia AS "Cyber Crime: Challenges and its Classification" 2014 *IJETTCS* 119-121

Prakash and Rajan 2018 *IJPAM*

Prakash GA and Rajan A "A Comparative Study on the Difference Between Conventional Crime and Cyber Crime" 2018 *IJPAM* 1452-1464

Ramages *Capacities and Rights of the Legal Subject*

Ramages J *Capacities and Rights of the Legal Subject* 2018 available at *chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ru.ac.za/media/rhodesuniversity/content/law/documents/courseoutlines2018/Introduction_to_Law_-_JR.pdf* accessed 10 June 2023

Rughoonandan *Cybercrime and its impact on extraditions in the Republic of South Africa*

Rughoonandan PH *Cybercrime and its impact on extraditions in the Republic of South Africa* (LLM-dissertation University of South Africa 2021)

Schultz *Cybercrime: An Analysis of Current Legislation in South Africa*

Schultz CB *Cybercrime: An Analysis of Current Legislation in South Africa* (LLM-dissertation University of Pretoria 2016)

Snail 2008 *Juta's Business Law*

Snail S "Cyber crime in the context of the ECT Act" 2008 *Juta's Business Law* 63-69

Snail *Legal Development in Cyber Crime Law in South Africa*

Snail S *Legal Development in Cyber Crime Law in South Africa* (2021) available at http://www.nstf.org.za/wp-content/uploads/2015/10/Cybercrime.pdf accessed 26 July 2023

South African Law Commission 1998 *Computer-Related Crime, Project 108*

South African Law Commission *Computer-Related Crime, Project 108* (1998) available at https://www.justice.gov.za/salrc/ipapers/ip14_prj108_1998.pdf accessed 23 July 2023

Sutherland 2017 *AJIC*

Sutherland E "Governance of Cybersecurity" 2017 *AJIC* 20, 83-112

Van der Merwe *et al Information and Communications Technology Law*

Van der Merwe D *et al* (eds) *Information and Communications Technology* 3rd ed (LexisNexis South Africa 2022)

Van Niekerk 2017 *AJIC*

Van Niekerk B "An Analysis of Cyber-Incidents in South Africa" 2017 *AJIC* 113-132

Case law

AmaBhungane Centre for Investigative Journalism NCP v Minister of Justice and Correctional Services and Others; *Minister of Police and Others v AmaBhungane Centre for Investigative Journalism NCP Case* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021)

Le Roux v Dey (2011) 3 SA 274 (CC)

Manyi v Dlamini 2018 ZAGPPHC 563

Minister of Police v AmaBhungane Centre for Investigative Journalism NPC CCT 279/19

Mofokeng v Motloung (4472/19) [2022] ZAGPJHC 546

Ramokgopa v Nxumalo [2022] ZAWCHC 175

R v Secretary of State for the Home Department, Ex parte Ruddock [1987] 2 All ER 518 (QB)

Legislation

Civil Proceedings Evidence Act 25 of 1965

Computer Evidence Act 57 of 1983

Companies Act 71 of 2008

Constitution of the Republic of South Africa, 1996

Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007

Criminal Procedure Act 51 of 1977

Criminal Procedure Amendment Act 9 of 1968

Cybercrimes Act 19 of 2020

Cybercrimes and Cybersecurity Bill [B – 2015]

Cybercrimes and Cybersecurity Bill [B6 – 2017]

Cybercrimes and Cybersecurity Bill [B 6B – 2017]

Electronic Communications and Transactions Act 25 of 2002

Electronic Communications and Transactions Amendment Bill of 2012

Films and Publications Act 65 of 1996

Films and Publications Amendment Act 11 of 2019

Films and Publications Amendment Regulations, 2022

Financial Intelligence Centre Act 38 of 2001

Interception and Monitoring Prohibition Act 127 of 1992

International Co-operation in Criminal Matters Act 75 of 1996

Police Service Act 68 of 1995

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

Protection of Personal Information Bill [B9], 2009

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

Regulation of Interception of Communications and Provision of Communication Related Information Amendment Bill [B 9B 2006]

International law instruments

African Union Convention on Cyber Security and Personal Data Protection EX.CL/846

Council of Europe *Convention on Cybercrime* 23 November 2001

European Union's General Data Protection Regulation 2016/679

Government publications

GG 37544 of 11 April 2014

GN 609 in GG 39475 of 4 December 2015

GG 43461 of 22 June 2020

GG 44383 of 1 April 2021

GG 46839 of 2 September 2022

Internet sources

Allen 2021 https://issafrica.org/iss-today/critical-infrastructure-attacks-why-south-africa-should-worry

Allen K 2021 *Critical infrastructure attacks: Why South Africa should worry* https://issafrica.org/iss-today/critical-infrastructure-attacks-why-south-africa-should-worry accessed 26 April 2022

Allen 2021 https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime

Allen K 2021 *South Africa lays down the law on cybercrime* https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime accessed 19 April 2022

Bandakkanavar 2020 https://krazytech.com/technical-papers/cyber-crime Bandakkanavar R 2020 *Causes of CyberCrime and Preventive Measures* https://krazytech.com/technical-papers/cyber-crime accessed 23 May 2022

Bhangattjee, Govuza and Sebanz *Technology* 2020 https://www.cliffedekkerhofmeyr.com/export/sites/cdh/en/news/publications/2020/technology/downloads/Technology-Media-and-Telecommunications-Alert-18-February-2020.pdf

Bhangattjee P, Govuza A and Sebanz L 2020 *Technology, Media & Telecommunications Alert* https://www.cliffedekkerhofmeyr.com/export/sites/cdh/en/news/publications/2020/technology/downloads/Technology-Media-and-Telecommunications-Alert-18-February-2020.pdf accessed 18 February 2023

Bischoff 2022 https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

Bischoff P 2022 *Which countries have the worst (and best) cybersecurity?* https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/ accessed 13 June 2023

Borges 2019 https://securitytrails.com/blog/types-of-cyber-crime

Borges 2019 *Types of Cybercrime and How to Protect Yourself Against Them* https://securitytrails.com/blog/types-of-cyber-crime accessed 22 February 2023

Breytenbach 2022 https://www.da.org.za/2022/12/da-welcomes-public-reception-to-the-cyber-commissioner-bill

Breytenbach MP 2022 *DA welcomes public reception to the Cyber Commissioner Bill* https://www.da.org.za/2022/12/da-welcomes-public-reception-to-the-cyber-commissioner-bill accessed 10 July 2023

Britannica 2022 https://www.britannica.com/technology/software

Britannica 2022 *Software computing* https://www.britannica.com/technology/software accessed 19 July 2022

Burger-Smidt 2022 https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/

Burger-Smidt A 2022 *Think twice before hitting retweet: major clampdown on digital abuse in South Africa* https://businesstech.co.za/news/internet/652563/think-twice-before-hitting-retweet-major-clampdown-on-digital-abuse-in-south-africa/ accessed 13 May 2023

BusinessTech 2022 https://businesstech.co.za/news/property/637305/south-africas-real-estate-industry-is-worried-about-this-type-of-crime/

BusinessTech 2022 *South Africa's real estate industry is worried about this type of crime* https://businesstech.co.za/news/property/637305/south-africas-real-estate-industry-is-worried-about-this-type-of-crime/ accessed 27 February 2023

BusinessTech 2022 https://businesstech.co.za/news/technology/639277/the-world-faces-a-cybercrime-catastrophe-including-south-africa/

BusinessTech 2022 *The world faces a cybercrime catastrophe – including South Africa* https://businesstech.co.za/news/technology/639277/the-world-faces-a-cybercrime-catastrophe-including-south-africa/ accessed 12 February 2023

Buxton 2022 https://www.minclaw.com/how-avoid-being-extorted-online/

Buxton D 2022 *How to Avoid Becoming a Victim of Extortion on the Internet* https://www.minclaw.com/how-avoid-being-extorted-online/ accessed 20 July 2022

Byleveld 2022 https://www.fluidrock.co.za/a-brief-overview-of-the-cybercrimes-act-19-of-2020/

Byleveld R 2022 *A Brief Overview Of The Cybercrimes Act 19 of 2020* https://www.fluidrock.co.za/a-brief-overview-of-the-cybercrimes-act-19-of-2020/ accessed 16 July 2023

Campbell 2021 https://businesstech.co.za/news/cloud-hosting/546856/how-south-africas-cybercrimes-act-will-change-how-you-use-the-internet/

Campbell M 2021 *How South Africa's Cybercrimes Act will change how you use the internet* https://businesstech.co.za/news/cloud-hosting/546856/how-south-africas-cybercrimes-act-will-change-how-you-use-the-internet/ accessed 16 July 2022

Cheng 2021 https://www.ringcentral.com/us/en/blog/what-is-cloud-communications

Cheng A 2021 *What is cloud communication?* https://www.ringcentral.com/us/en/blog/what-is-cloud-communications accessed 26 September 2022

Clark 2019 https://greatergood.berkeley.edu/article/item/what_makes_technology_good_or_bad_for_us

Clark J 2019 *What Makes Technology Good or Bad for Us?* https://greatergood.berkeley.edu/article/item/what_makes_technology_good_or_bad_for_us accessed 12 February 2023

Coolidge 2021 https://coolidgelawfirmaz.com/what-are-the-major-types-of-cybercrime/

Coolidge T 2021 *What are the Major Types of Cybercrime?* https://coolidgelawfirmaz.com/what-are-the-major-types-of-cybercrime/ accessed 10 June 2023

Council of Europe 2022 https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

Council of Europe 2022 *Chart of signatures and ratifications of Treaty 185* https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 accessed 12 July 2022

Cutler 2022 https://terrycutler.com/the-malicious-hacking-employee/

Cutler T 2022 *The malicious hacking employee* https://terrycutler.com/the-malicious-hacking-employee/ accessed 16 April 2023

defenceWeb 2022 https://www.defenceweb.co.za/cyber-defence/siu-csir-collaborate-to-fight-cybercrime/

defenceWeb 2022 *CSIR and SIU team up to fight cybercrime* https://www.defenceweb.co.za/cyber-defence/siu-csir-collaborate-to-fight-cybercrime/ accessed 21 February 2023

Desai 2023 https://www.albaraka.co.za/blogs/legalease-publication-3-2022/impact-of-the-cybercrimes-act-of-financial-institutions

Desai J 2023 *Impact of the Cybercrimes Act on Financial Institutions* https://www.albaraka.co.za/blogs/legalease-publication-3-2022/impact-of-the-cybercrimes-act-of-financial-institutions accessed 17 July 2023

Dikgole 2022 https://www.moneyweb.co.za/news/south-africa/cyber-security-threats-to-real-estate/

Dikgole P 2022 *Cyber security threats to real estate* https://www.moneyweb.co.za/news/south-africa/cyber-security-threats-to-real-estate/ accessed 24 May 2023

Docrat 2022 https://isite.co.za/ransomware-attacks-south-africa/

Docrat 2022 *Ransomware Attacks in South Africa: What You Need to Know* https://isite.co.za/ransomware-attacks-south-africa/ accessed 17 April 2023

Trevino 2021 https://www.forbes.com/sites/forbestechcouncil/2021/01/29/cyber-attacks-of-the-fourth-industrial-revolution/?sh=2b078b826183

Trevino M 2021 *Cyber-attacks Of The Fourth Industrial Revolution* https://www.forbes.com/sites/forbestechcouncil/2021/01/29/cyber-attacks-of-the-fourth-industrial-revolution/?sh=2b078b826183 accessed 14 August 2023

Daskal and Kennedy-Mayo 2020 https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/?cn-reloaded=1

Daskal J and Kennedy-Mayo D 2020 *Budapest Convention: What is it and how is it being updated?* https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/?cn-reloaded=1 accessed 14 May 2022

De Wet and Olën 2022 https://www.dataguidance.com/opinion/south-africa-cybercrimes-act-its-relationship%C2%A0-popia

De Wet PR and Olën D 2022 *South Africa: The Cybercrimes Act, its relationship with POPIA, and compliance* https://www.dataguidance.com/opinion/south-africa-cybercrimes-act-its-relationship%C2%A0-popia accessed 14 July 2023

Domains 2022 https://companies.mybroadband.co.za/domains/2022/11/01/cybercrime-in-south-africa-what-every-sme-needs-to-know/

Domains 2022 *Cybercrime in South Africa: What every SME Needs to Know* https://companies.mybroadband.co.za/domains/2022/11/01/cybercrime-in-south-africa-what-every-sme-needs-to-know/ accessed 24 February 2023

DSC Attorneys 2021 https://www.dsclaw.co.za/articles/when-does-legal-professional-privilege-not-apply-in-south-africa/

DSC Attorneys 2021 *When Does Legal Professional Privilege NOT apply in South Africa?* https://www.dsclaw.co.za/articles/when-does-legal-professional-privilege-not-apply-in-south-africa/ accessed 28 August 2023

Du Preez 2023 https://www.burgerhuyserattorneys.co.za/the-governance-of-cyber-ict-law-in-south-africa-explained/

Du Preez N 2023 *The Governance of Cyber & ICT Law in South Africa Explained* https://www.burgerhuyserattorneys.co.za/the-governance-of-cyber-ict-law-in-south-africa-explained/ accessed 4 April 2023

Ellerbeck 2022 https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business/

Ellerbeck S 2022 *Nearly half of businesses are being hit by economic crime, with cybercrime the gravest threat. What can they do about it?* https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business/ access 13 May 2023

Ellis 2022 *What Makes a Smart Device Smart?* https://www.makeuseof.com/smart-device-meaning/ accessed 8 May 2022

Ellis M 2022 *What Makes a Smart Device Smart?* https://www.makeuseof.com/smart-device-meaning/ accessed 8 May 2022

Ernest 2022 https://www.timeslive.co.za/news/south-africa/2022-05-04-sa-ranked-6th-country-most-affected-by-cybercrime-research-finds/

Ernest M 2022 *SA ranked 6th country most affected by cybercrime, research finds* https://www.timeslive.co.za/news/south-africa/2022-05-04-sa-ranked-6th-country-most-affected-by-cybercrime-research-finds/ accessed 14 May 2022

Federal Bureau of Investigation 2018 https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

Federal Bureau of Investigation 2018 *30 Years Since First Major Attack on the Internet* https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218 accessed 13 August 2023

Giles 2009 https://www.michalsons.com/blog/cyber-crime-explained/2667

Giles J 2009 *Cybercrime law in South Africa explained* https://www.michalsons.com/blog/cyber-crime-explained/2667 accessed 23 May 2023

Giles 2021 https://www.michalsons.com/blog/the-practical-impact-of-the-cyber-bill-on-you/25300#:~:text=If%20you%20share%20your%20password,you%20could%20be%20a%20criminal

Giles J 2021 *The practical impact of the Cybercrimes Act on you* https://www.michalsons.com/blog/the-practical-impact-of-the-cyber-bill-on-you/25300#:~:text=If%20you%20share%20your%20password,you%20could%20be%20a%20criminal accessed 17 June 2023

Giles 2022 https://www.michalsons.com/blog/what-is-ict/2525

Giles J 2022 *What is ICT? What is the Meaning or Definition of ICT?* https://www.michalsons.com/blog/what-is-ict/2525 accessed 19 May 2023

GOOSEVPN 2015 https://goosevpn.com/blog/origin-cybercrime

GOOSEVPN 2015 *The Origin of Cybercrime* https://goosevpn.com/blog/origin-cybercrime accessed 24 April 2022

Grealy *et al* 2021 https://businesstech.co.za/news/technology/543432/south-africas-new-cybercrime-laws-have-been-partially-introduced-heres-what-comes-next/#:~:text=The%20Cybercrimes%20Act%20defines%20three,damage%20to%20property%20or%20violence

Grealy P *et al* 2021 *South Africa's new cybercrime laws have been partially introduced – here's what comes next* https://businesstech.co.za/news/technology/543432/south-africas-new-cybercrime-laws-have-been-partially-introduced-heres-what-comes-next/#:~:text=The%20Cybercrimes%20Act%20defines%20three,damage%20to%20property%20or%20violence accessed 28 July 2023

Gunning and Gabryk 2021 https://www.mondaq.com/southafrica/data-protection/1111854/data-breaches-and-the-interplay-between-popia-ecta-and-the-cybercrimes-act-podcast

Gunning E and Gabryk N 2021 *South Africa: Data Breaches And The Interplay Between POPIA, ECTA And The Cybercrimes Act (Podcast)* https://www.mondaq.com/southafrica/data-protection/1111854/data-breaches-and-the-interplay-between-popia-ecta-and-the-cybercrimes-act-podcast accessed 14 July 2023

Hakmeh, Naylor and Wallace 2022 https://www.chathamhouse.org/2022/02/what-cyber-attack

Hakmeh J, Naylor E and Wallace J 2022 *What is a cyber attack?* https://www.chathamhouse.org/2022/02/what-cyber-attack accessed 10 July 2022

Higgins 2022 https://nordvpn.com/blog/cyberextortion/

Higgins M 2022 *What is cyber extortion?* https://nordvpn.com/blog/cyberextortion/

ITWeb 2023 https://www.itweb.co.za/content/8OKdWqDXg92qbznQ

ITWeb 2023 *Interpol, SAPS warn of online jobs, social media scams* https://www.itweb.co.za/content/8OKdWqDXg92qbznQ accessed 25 February 2023

Jigsaw Academy 2022 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/

Jigsaw Academy 2022 *20 Important Types of Cyber Crimes To Know in 2022* https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/ accessed 10 February 2023

Kaspersky 2020 https://www.kaspersky.co.za/resource-center/threats/what-is-cybercrime

Kaspersky 2020 *Tips on how to protect yourself against cybercrime* https://www.kaspersky.co.za/resource-center/threats/what-is-cybercrime accessed 19 May 2022

Kleijssen and Perri 2016 https://rm.coe.int/cybercrime-evidence-and-territoriality-issues-and-options/168077fa98

Kleijssen J and Perri P 2016 *Cybercrime, Evidence and Territoriality: Issue and Options* https://rm.coe.int/cybercrime-evidence-and-territoriality-issues-and-options/168077fa98 accessed 13 June 2022

Latto 2020 https://www.avast.com/c-worm-vs-virus

Latto N 2020 *Worms vs. Virus: What's the Difference and Does It Matter?* https://www.avast.com/c-worm-vs-virus accessed 19 April 2023

Leukfeldt and Malsch 2019 https://nscr.nl/en/gevolgen-cybercrime-zeer-ingrijpend-voor-slachtoffers/

Leukfeldt R and Malsch M 2019 *Cybercrime has serious consequences for its victims* https://nscr.nl/en/gevolgen-cybercrime-zeer-ingrijpend-voor-slachtoffers/ accessed 12 February 2023

Linkedin 2023 https://www.linkedin.com/in/jenna-clark-b0221a132 accessed 23 May 2023

Lutkevich 2021 https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie

Lutkevich B 2021 *What is a script kiddie?* https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie accessed 20 April 2023

MacKenzie 2022 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force

MacKenzie J 2022 *South Africa: Films and Publications Amendment Act comes into force* https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/south-africa-films-and-publications-amendment-act-comes-into-force accessed 24 April 2023

Madziwa and Snail 2021 https://www.hg.org/legal-articles/cyber-crime-in-south-africa-5351

Madziwa S and Snail S 2021 *Cyber Crime In South Africa* https://www.hg.org/legal-articles/cyber-crime-in-south-africa-5351 accessed 14 May 2023

Mahlobo 2015 https://www.politicsweb.co.za/politics/on-cybersecurity-in-south-africa--david-mahlobo

Mahlobo D 2015 *On cybersecurity in South Africa – David Mahlobo* https://www.politicsweb.co.za/politics/on-cybersecurity-in-south-africa--david-mahlobo accessed 27 February 2023

Manaleng 2021 https://ewn.co.za/2021/06/03/think-before-you-click-ramaphosa-signs-cybercrimes-act-into-law

Manaleng P 2021 *Think Before You Click – Ramaphosa Signs Cybercrimes Act Into Law* https://ewn.co.za/2021/06/03/think-before-you-click-ramaphosa-signs-cybercrimes-act-into-law accessed 17 June 2023

Mcanyana, Brindley and Seedat 2020 https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf

Mcanyana W, Brindley C and Seedat Y 2020 *Insight into the Cyberthreat Landscape in South Africa* https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf accessed 20 February 2023

Merriam-Webster Dictionary 2023 https://www.merriam-webster.com/dictionary/fundamentalism#:~:text=%3A%20a%20movement%20or%20attitude%20stressing,Islamic%20fundamentalism

Merriam-Webster Dictionary 2023 *Definition of fundamentalism* https://www.merriam-webster.com/dictionary/fundamentalism#:~:text=%3A%20a%20movement%20or%20attitude%20stressing,Islamic%20fundamentalism accessed 20 August 2023

Merriam-Webster Dictionary 2023 https://www.merriam-webster.com/dictionary/Internet

Merriam-Webster Dictionary *Definition of internet* 2023 https://www.merriam-webster.com/dictionary/Internet accessed 25 July 2023

Merriam-Webster Dictionary 2022 https://www.merriam-webster.com/dictionary/malicious

Merriam-Webster Dictionary 2022 *Definition of malicious* https://www.merriam-webster.com/dictionary/malicious accessed 13 July 2022

Merriam-Webster Dictionary 2023 https://www.merriam-webster.com/dictionary/quasi-judicial

Merriam-Webster Dictionary 2023 *Definition of quasi-judicial* https://www.merriam-webster.com/dictionary/quasi-judicial accessed 13 July 2023

Mhungu *et al* 2018 https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-deloitte-gdpr-report.pdf

Mhungu R *et al* 2018 *The General Data Protection Regulation* https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-deloitte-gdpr-report.pdf accessed 19 July 2023

Michalsons 2022 https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa#:~:text=The%20Cybercrimes%20Act%20enables%20the,this%20is%20a%20global%20issue

Michalsons 2022 *Cybercrimes Act in South Africa Overview and Read* https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa#:~:text=The%20Cybercrimes%20Act%20enables%20the,this%20is%20a%20global%20issue accessed 6 May 2023

Morgan 2022 https://cybersecurityventures.com/our-company/

Morgan S 2022 *Cybersecurity Ventures* https://cybersecurityventures.com/our-company/ accessed 24 March 2023

Mukherjee 2023 https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/#:~:text=Cybercrimes%20include%20phishing%2C%20hacking%2C%20spoofing,%2C%20i.e.%2C%20mainly%20offline%20crimes

Mukherjee A 2023 *Difference Between Cyber Crime and Conventional Crime in Tabular Form* https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/#:~:text=Cybercrimes%20include%20phishing%2C%20hacking%2C%20spoofing,%2C%20i.e.%2C%20mainly%20offline%20crimes accessed 5 May 2023

NATO Cooperative Cyber Defence Centre of Excellence 2020 https://ccdcoe.org/organisations/au/

NATO Cooperative Cyber Defence Centre of Excellence 2020 *African Union* https://ccdcoe.org/organisations/au/ accessed 30 March 2023

Nguyen and McNally 2023 https://allaboutcookies.org/what-is-a-cookie

Nguyen SJ and McNally C 2023 *What Are Internet Cookies and How Are They Used?* https://allaboutcookies.org/what-is-a-cookie accessed 16 July 2023

Norwich University Online 2020 https://online.norwich.edu/academic-programs/recources/types-of-cyber-crime

Norwich University Online 2020 *5 Types of Cyber Crime: How Cybersecurity Professionals Prevent Attacks* https://online.norwich.edu/academic-programs/recources/types-of-cyber-crime accessed 15 July 2022

Ongeso 2021 https://bowmanslaw.com/insights/mergers-and-acquisitions/south-africa-constitutional-court-upholds-declaration-of-invalidity-of-rica/

Ongeso JP 2021 *South Africa: Constitutional Court Upholds Declaration of Invalidity of RICA* https://bowmanslaw.com/insights/mergers-and-acquisitions/south-africa-constitutional-court-upholds-declaration-of-invalidity-of-rica/ accessed 14 June 2023

Ongeso 2022 https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/

Ongeso JP 2022 *South Africa: Films and Publications Amendment Act Comes into Operation* https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/ accessed 17 February 2023

PGI 2018 https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/

PGI 2018 *What is the difference between cyber crime and traditional crime?* https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/ accessed 12 February 2023

Pieterse 2015 http://www.nstf.org.za/wp-content/uploads/2015/10/BrigPieterse.pdf

Pieterse BNT 2015 *Electronic Crime Unit* http://www.nstf.org.za/wp-content/uploads/2015/10/BrigPieterse.pdf accessed 15 February 2023

Pietrangelo 2019 https://www.healthline.com/health/negative-effects-of-technology#positive-effects

Pietrangelo A 2019 *What Are The Negative and Positive Effects of Technology?* https://www.healthline.com/health/negative-effects-of-technology#positive-effects accessed 8 April 2022

Pillay 2017 https://www.withoutprejudice.co.za/free/article/5659/view

Pillay K 2017 *The Cybercrime and Cybersecurity Bill and POPIA: Prioritising Data Protection* https://www.withoutprejudice.co.za/free/article/5659/view accessed 15 July 2023

Pinarbasi 2022 https://blog.didomi.io/en/popia-south-africa

Pinarbasi AT 2022 *How to be compliant with South Africa's POPIA act* https://blog.didomi.io/en/popia-south-africa accessed 18 July 2023

Pinto 2022 https://www.eatmy.news/2022/11/how-cyber-crimes-differ-from.html

Pinto M 2022 *How Cyber Crimes Differ from Traditional Crimes* https://www.eatmy.news/2022/11/how-cyber-crimes-differ-from.html accessed 20 May 2023

Reyers 2023 https://blog.reputationx.com/digital-footprint

Reyers N 2023 *What is a digital footprint?* https://blog.reputationx.com/digital-footprint accessed 17 August 2023

Rouse 2013 https://www.techopedia.com/definition/610/end-user

Rouse M 2013 *What Does End User Mean?* https://www.techopedia.com/definition/610/end-user accessed 27 May 2024

Seger 2016 https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/#:~:text=The%20Budapest%20Convention%20is%20a,more%20effective%20and%20subject%20to

Seger A 2016 *The Budapest Convention on Cybercrime: a framework for capacity building* https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/#:~:text=The%20Budapest%20Convention%20is%20a,more%20effective%20and%20subject%20to accessed 30 March 2023

Shea and Lutkevich 2021 https://www.techtarget.com/searchsecurity/definition/cracker

Shea S and Lutkevich B 2021 *Computer Cracker* https://www.techtarget.com/searchsecurity/definition/cracker accessed 25 April 2023

Sheldon and Hanna 2022 https://www.techtarget.com/searchsecurity/definition/cyberterrorism

Sheldon R and Hanna KT 2022 *What is cyberterrorism?* https://www.techtarget.com/searchsecurity/definition/cyberterrorism accessed 14 April 2023

Smiley 2019 https://blog.thinkreliability.com/case-study-the-morris-worm-brings-down-the-internet

Smiley K 2019 *Case Study: The Morris Worm Brings Down the Internet* https://blog.thinkreliability.com/case-study-the-morris-worm-brings-down-the-internet accessed 14 June 2023

Snail 2021 https://cyberbrics.info/legal-intersections-between-the-protection-of-personal-information-act-4-of-2013-popia-and-the-cyber-crimes-act-19-of-2020-2/

Snail S 2021 *Legal Intersections Between The Protection Of Personal Information Act 4 Of 2013 (POPIA) And The Cyber Crimes Act 19 Of 2020* https://cyberbrics.info/legal-intersections-between-the-protection-of-personal-information-act-4-of-2013-popia-and-the-cyber-crimes-act-19-of-2020-2/ accessed 18 June 2023

South African Government 2016 https://www.gov.za/speeches/minister-david-mahlobo-state-security-agency-dept-budget-vote-201617-26-apr-2016-0000

South African Government 2016 *Minister David Mahlobo: State Security Agency Dept Budget Vote 2016/17* https://www.gov.za/speeches/minister-david-mahlobo-

state-security-agency-dept-budget-vote-201617-26-apr-2016-0000 accessed 30 June 2023

South African Government News Agency 2021 https://www.sanews.gov.za/south-africa/lamola-welcomes-ramping-cybercrimes-act

South African Government News Agency 2021 *Lamola welcomes ramping of Cybercrimes Act* https://www.sanews.gov.za/south-africa/lamola-welcomes-ramping-cybercrimes-act accessed 20 July 2022

Surfshark 2021 https://surfshark.com/research/data-breach-impact/statistics

Surfshark 2021 *Cybercrime statistics* https://surfshark.com/research/data-breach-impact/statistics accessed 20 February 2023

Sutherland 2019 https://www.itweb.co.za/content/lwrKxv3JLOJqmg1o

Sutherland C 2019 *History of South African cyber legislation* https://www.itweb.co.za/content/lwrKxv3JLOJqmg1o accessed 30 March 2023

Toona 2022 https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com

Toona M 2022 *What is the purpose of the Cybercrimes Act?* https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses?utm_referrer=https://www.google.com accessed 13 February 2023

Townsend 2022 https://www.securityweek.com/cyber-insights-2022-improving-criminal-sophistication/

Townsend K 2022 *Cyber Insights 2022: Improving Criminal Sophistication* https://www.securityweek.com/cyber-insights-2022-improving-criminal-sophistication/ accessed 18 June 2023

UKEssays 2018 https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis

UKEssays 2018 *Distinction Between Conventional And Cyber Crime Information Technology Essay* https://www.ukessays.com/essays/information-

technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php?vref=1#citethis accessed 12 February 2023

Upadhyay 2020 https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/

Upadhyay 2020 *20 Important Types of Cyber Crimes To Know in 2021* https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/ accessed 12 July 2022

Usercentrics 2022 https://usercentrics.com/knowledge-hub/south-africa-popia-protection-of-personal-information-act-overview/

Usercentrics 2022 *South Africa's Protection of Personal Information Act – an overview* https://usercentrics.com/knowledge-hub/south-africa-popia-protection-of-personal-information-act-overview/ accessed 10 April 2023

Van Deventer 2021 https://www.vandeventers.law/Legal-Articles/entryid/1954/will-the-popi-act-cybercrimes-act-work-well-together

Van Deventer C 2021 *Will The POPI Act & Cybercrimes Act Work Well Together?* https://www.vandeventers.law/Legal-Articles/entryid/1954/will-the-popi-act-cybercrimes-act-work-well-together accessed 25 July 2023

Vermeulen 2022 https://mybroadband.co.za/news/security/468359-proposal-to-amend-south-africas-constitution-for-cyber-commissioner.html

Vermeulen J 2022 *Proposal to amend South Africa's constitution for Cyber Commissioner* https://mybroadband.co.za/news/security/468359-proposal-to-amend-south-africas-constitution-for-cyber-commissioner.html accessed 28 July 2023

Von Solms 2022 https://theconversation.com/five-things-south-africa-must-do-to-combat-cybercrime-186089

Von Solms B 2022 *Five things South Africa must do to combat cybercrime* https://theconversation.com/five-things-south-africa-must-do-to-combat-cybercrime-186089 accessed 12 February 2023

Williams, Fourie and Siyaya 2021 https://www.golegal.co.za/newly-enacted-cybercrimes-act/

Williams G, Fourie T and Siyaya S 2021 *The newly enacted Cybercrimes Act and what it means for South Africans* https://www.golegal.co.za/newly-enacted-cybercrimes-act/ accessed 25 April 2022