A HISTORICAL-LEGAL ANALYSIS OF SEARCH AND SEIZURE OF ELECTRONIC RECORDS FOR THE PROSECUTION OF FINANCIAL CRIMES IN SOUTH AFRICA

by

UNATHI POYO

submitted in accordance with the requirements

for the degree of

MASTER OF LAWS (LLM)

In the subject

CRIMINAL AND PROCEDURAL LAW

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF VM BASDEO

CO-SUPERVISOR: PROF F CASSIM

TABLE OF CONTENTS

CHAPTER FOUR

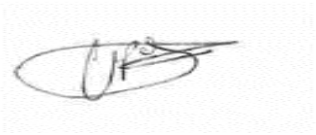
ELECTRONIC EVIDENCE

ACADEMIC HONESTY DECLARATION

Declaration: Unathi Poyo

1. I understand what academic dishonesty entails and I am aware of Unisa's policies in this regard.
2. I declare that this Dissertation is my own, original work. Where I have used someone else's work, I have indicated this using the prescribed style of referencing. Every contribution to, and quotation in, this dissertation from works or works of other people has been referenced according to this style.
3. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.
4. I did not make use of another student's work and submitted it as my own.

Name: Unathi Poyo

Signature: 

Student number: 43715613

Date: 01 September 2020

ACKNOWLEDGEMENTS

1. I would like to thank my mother. She has been my rock, my biggest supporter and fan. She has stepped in and helped me take care of my daughter while I concentrated on my research. Without her, I would not be where I am in life.
2. I would like to thank Prof V.M. Basdeo, who told me I could do it. Your knowledge, advice and supervision have been invaluable and I appreciate it.
3. I would like to thank Prof F. Cassim who is my mentor and always gave me information and took an interest in my success. Your kindness and generosity is amazing.
4. I would like to thank my Colleagues in the Department of Criminal and Procedural Law for always encouraging me.

SUMMARY

Crime has been around since the beginning of time. In an evolving society, and the methodology of crime also changes. The methodology of combating and preventing crime should aim to match the speed at which crime occurs. Criminal procedure deals with the powers of the police to investigate crimes.[1] The Criminal Procedure Act 51 of 1977 (CPA) contains the principles of search and seizure in chapter 2. The promulgation of the CPA was during a period where the computer was a new phenomenon. At this time, it was inconceivable that technology would ever advance and become so ubiquitous, to the point that technology would infiltrate every aspect of our lives, and laws. There has since been many developments in our law, especially a new Constitutional dispensation.[2] There have been developments and technological advancements that have had a direct and indirect bearing on the CPA. People use technology to communicate, transact, and unfortunately, to commit crime. These developments require there to be amendments in the CPA. There has been no specific amendments relating to search and seizure which are of significance in addressing technological advances. It is recommended that the amendments to the CPA include definitions and guidelines for procedural aspects of collection of electronic evidence.

1 South African Police Service Official website "About Us" https://www.saps.gov.za/about/about.php (accessed on 31 July 2019).

2 The Constitution of the Republic of South Africa, 1996 (hereinafter referred to as the Constitution). s 2 of the Constitution states, "The Constitution is the supreme law and any law or conduct inconsistent with it is invalid".

KEYWORDS

Search and seizure; financial crimes; commercial crime; cybercrime; technology; electronic evidence, computer, digital, analogue, Information age, investigation.

LIST OF ABBREVIATIONS

AFU	Asset Forfeiture Unit
BAC	Businesses Against Crime
CILSA	*The Comparative and International Law Journal of Southern Africa*
CPA	Criminal Procedure Act
Crim Just	*Criminal Justice*
CSIRT	Computer Security Incident Response Team
DoJCD	Department of Justice and Constitutional Development
ECT Act	Electronic and Communication Transaction Act
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act
IEA	Institute of Economic Affairs
IJLIT	*International Journal of Law and Information Technology*
IJDE	*International Journal of Digital Evidence*
JILT	*Journal of Information, Law and Technology*
LEAA	Law of Evidence Amendment Act
NCPF	National Cybersecurity Policy Framework

NDPP National Director of Public Prosecutions

NPA National Prosecuting Authority

PAIA Promotion of Access to Information Act

PER *Potchefstroom Electronic Law Journal*

PFMA Public Finance Management Act

POPI Protection of Personal Information Act

SABRIC South African Banking Risk Information Centre

SACJ *South African Computer Journal*

SALRC South African Law Reform Commission

SAPS South African Police Service

SAPS ACT South African Police Service Act

SARS South African Revenue Service

SIU Special Investigating Unit

SOP Standard Operating Procedure

Tax Act Tax Administration Act

UNCITRAL United Nations Commission on International Trade Law

CHAPTER ONE

INTRODUCTION AND GENERAL OVERVIEW

1.1 Introduction

The object of this research is the search and seizure of electronic records for the prosecution of financial crimes in South Africa. The research will examine the history of the Criminal Procedure Act 51 of 1977 (CPA) relating to the investigation of financial crimes and electronic evidence, therefore are several aspects to this research. This research encompasses the following: the right to privacy, requirements of a valid search warrant, collecting electronic evidence, investigating financial crime, and establishing that a crime was committed. The rate at which financial crimes are committed using technological means requires the serious attention of the legislature.

Authorities and the Government have no sense of urgency with regard to the search and seizure of electronic evidence, in the investigation of financial crimes. There are, however, numerous institutions, task teams, organisations and laws pertaining to the investigation of financial crimes, regardless of the medium used to commit them. None has proven to be significantly successful in combating financial crime. Rather, there are inconsistencies in combating financial crimes committed with electronic mediums.

The investigation of those who contravene the law is in terms of criminal procedure.[3] Criminal procedure seeks to establish the parameters in the investigation of crime. It therefore regulates the powers and duties of the police.[4] This topic is very wide and there is various legislation promulgated regarding search and seizure, specifically the search of objects. The task of the South African Police Service (SAPS) is the investigation of crime. The objectives are set out in the Constitution of the Republic of South Africa, 1996 as follows:[5]

> The objects of the police service are to prevent, combat and investigate crime, to maintain public order, to protect and secure the inhabitants of the Republic and their property, and to uphold and enforce the law.[6]

---

3 Mudaly L Search and seizure of documents in the investigation of tax-related cases (M Tech University of South Africa 2011) 49.

4 Joubert JJ *Criminal procedure handbook* 12th ed (Juta 2016) 7.

5 The Constitution of the Republic of South Africa, 1996 (hereinafter referred to as "the Constitution").

6 s 205(3) of the Constitution.

The task of the SAPS is to search for evidence that relates to the commission of a crime and the seizure of such evidence. This is to provide evidence in the court of law for the prosecution of those charged.[7] The main legislation in regards to the principle of search and seizure has been the CPA.[8]

The CPA refers to every aspect of search and seizure including the requirements for a search with and without a warrant. Since its promulgation, the CPA has been the core piece of legislation that governs the principle of search and seizure. However, in recent years, there have been many developments in the law and advancements in technology that have a bearing on criminal procedure, thus there is a constant need to amend and update the CPA accordingly. The CPA came at a time when it was inconceivable that location would be outside the scope of the physical realm and that when we refer to an object it can be something intangible.[9]

Over the years, it has become evident the State in the form of the police[10] as a single institution are unable to carry out the task of investigating financial crimes. This includes gathering electronic evidence in its original capacity and requires specialised skills by computer forensic personnel.[11] The CPA stipulates that it is the task of the SAPS to carry out search and seizure. Thus, this is made the primary duty of the police. The CPA does make provision for other statutes to conduct search and seizure.[12] This is all the more evident in that the developments in Constitutional law place a limit on the authority of the police in executing their duties. This limitation is the right to privacy.[13]

A central theme of this research is how technology has advanced since the enactment of the CPA. Technology has radically changed the world in which we live, and it has changed how we interact and transact in everyday life. However, with every positive

---

7 Joubert *Criminal procedure handbook* 19 "For the purpose of this research this means an accused person who has appeared in court and has pleaded".

8 ch 2 of the CPA.

9 South African Law Reform Commission Issue Paper 14 (Project 108) "Computer-related crime: options for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects" (1998) 11.

10 s 205(3) of the Constitution "The objects of the police service are to prevent, combat and investigate crime, to maintain public order, to protect and to secure the inhabitants of the Republic and their property, and to uphold and enforce the law".

11 Ndara V *Computer seizure as technique in forensic investigation (*M Tech University of South Africa 2013) defines computer forensic investigation as "A branch of digital forensic science pertaining to legal evidence found in computers and digital storage media" 35.

12 s 19 of the CPA.

13 s14 of the Constitution.

contribution that technology has brought into modern day society, it has also brought with it a state of vulnerability, as many transactions are now electronic, or wireless.[14]

The investigation of financial crimes further complicates and burdens investigations, as there is no coherent law. The personal nature of finances creates many barriers. The financial sector is highly regulated, there are several statutes that protect the personal information of individuals. Though South Africa is progressing in terms of investigating financial crimes by using electronic evidence, there is still a great deal of uncertainty. South Africa is making very slow progress regarding the investigation of financial crimes using electronic evidence. An important institution in relation to investigation of a crime is the prosecuting unit. In South Africa there is a single prosecuting authority[15] and the State prosecutes all crimes.[16] There are provisions in the National Prosecuting Authority Act (NPA Act)[17] that deal with search, seizure and the obtaining of warrants.[18] There is no doubt regarding the importance of the provisions of search and seizure in preparatory investigations especially in the fight against crime.[19]

The promulgation of the CPA was in a period when technology was not considered as affecting the law. There has been little if any change affecting electronic evidence made since its promulgation. This is more so in relation to the search and seizure of electronic evidence.

This research examines the different components of the law, evaluates them separately, and subsequently combines them in order to establish how to regulate search and seizure of financial crimes using electronic evidence. This analysis will examine the promulgation of the CPA. It will also consider the current information and technological era. It asks the question as to why the CPA has not been updated

---

14 Papadopoulos S and Snail S *Cyberlaw @ SA III: The law of the internet in South Africa* 3rd ed (Van Schaik 2012) 333.

15 National Prosecuting Authority has the following duties:
Power to institute and conduct criminal proceedings
(1) The power, as contemplated in s 179(2) and all other relevant sections of the Constitution , to -
(a) institute and conduct criminal proceedings on behalf of the State;
(b) carry out any necessary functions incidental to instituting and conducting such criminal proceedings; and (c) discontinue criminal proceedings, vests in the prosecuting authority and shall, for all purposes, be exercised on behalf of the Republic.

17 National Prosecuting Authority Act 32 of 1998 (hereinafter referred to as the NPA Act).

18 s 29 of the NPA Act.

19 *Thint (Pty) Ltd v National Director of Public Prosecutions and Others; Zuma v National Director of Public Prosecutions and Others* 2008 (2) SACR 421.

adequately to reflect the changes and updates regarding the advancement of technology and the increase in crimes committed for financial gains.

Criminal procedure seeks to regulate the legal requirements for search and seizure. The research poses the question: what are the parameters of the process used by law enforcement, legal practitioners, and all those involved in the fact-finding mission once there has been the commission of a crime? This is the general and broad scope of criminal procedure. This research seeks to narrow the aspects of crime to the scope of search and seizure of electronic evidence for prosecuting financial crimes. A timeline of the history of the CPA and electronic evidence is fundamental to this research. This research will examine the promulgation of the CPA at a time when technology was not a factor, and looks at the CPA in the current technological age in which electronic evidence is not clearly defined in South Africa. Search and seizure for the collection of electronic evidence is regulated by current legislation, where technological advances have not been given due diligence in regards to developing legislation.[20] The CPA confers powers on the State to search and seize only if the object is to find certain persons or seize an article.[21] The object and scope of this research has three elements, which are, search and seize; electronic records; and crimes committed for financial gain. For analysis, there is a separate consideration of the three elements including the component of the historical aspects. The research considers the integration of these three elements as aspects in the legal process of criminal justice system, and progress made for the effectiveness of investigation and prosecution thereof.

1.2 Purpose of study

The purpose of this research is to establish whether there are sufficient mechanisms in place to combat the surge in criminal activities arising from the use of computers. This research aims to show that the CPA lags behind in addressing the need for investigative tools required by law enforcements agencies when collecting electronic evidence, especially those of a financial nature. This is because such crimes not only affect the victim, but also have an effect on the economy. The reason for this research focus area is that there needs to be new developments that directly address the

---

20 Basdeo VM, Montesh M and Lekubu BK "Search and seizure of evidence in cyber environments: A law enforcing the detection rate of commercial crime" 2017 *JLSD* 48.

21 s 20 of the CPA.

problem of insufficient legislation pertaining to electronic evidence used in computer and cybercrime in South Africa. It is no secret that there is a lack of confidence by the public in the ability of law enforcement agencies to combat crime, as there is such a high crime rate in the country.[22] This lack of confidence trickles down to the courts and the entire justice system.[23]

There are numerous laws relating to financial crime, electronic evidence, and criminal procedure. At issue, however, is the way in which these laws remain disconnected and do not offer coherent, concise, and strategic engagement for the investigation of crime. Furthermore, the private sector simply does not have the financial resources and capacity to fight the surge of financial and cybercrime.[24] Criminal procedure requires that an article must fall strictly within the parameters of the definition of "article" for search and seizure.[25] There is no specific definition for financial crimes. This is the apparent conundrum. The investigation of financial crime is a specialist field. Having to identify whether or not there is even a reasonable suspicion of a crime requires specialist knowledge. Institutions need to have mechanisms in place to help combat and fight potential threats. The investigation of financial crimes requires the consideration of several factors. These factors inevitably lead to questions that need to be asked in order to understand what is required of a successful investigation. These questions are: what would constitute reasonable suspicion? How to establish that certain evidence might be contained in electronic records, and the most difficult would be identifying a suspect?

---

22 Business Tech "South Africa crime states" https://businesstech.co.za/news/government/270689/south-africa-crime-stats-2018-everything-you-need-to-know/ (accessed on 15 March 2019).

23 Statistics South Africa "While crime increases, fear rises and trust in criminal justice system drops" http://www.statssa.gov.za/?p=11627 (accessed 15 March 2019).

24 Jackson D "Financial crime - driven by opportunity, technology and greed" 2015 *SAIPA* 9.

25 s 20 of the CPA;
The state may, in accordance with the provision of this chapter, seize anything (in this chapter referred to as an article) -
(a) Which is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within the republic of elsewhere;
(b) Which may afford evidence of the commission or suspected commission of an offence, whether within the republic or elsewhere; or
(c) Which is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence.

1.3 Hypothesis and research question

The South African legislature promulgated the CPA in 1977. More than forty years on from the enactment of the CPA, enforcement agencies need to follow the correct procedure to avoid acting outside the scope of the law. When searching a person, law enforcement agencies also need to take cognisance of the Constitutional right afforded to people including but not limited to the right to freedom and security of person.[26] Law enforcement agencies need to have a valid search warrant that sets out the article, place or persons that needs to be searched when conducting search and seizure. Acting outside a search warrant is *ultra vires*. Therefore, there is a question as to whether the CPA adequately defines provisions of a demanding and growing technological era. This ought to be considered in light of the significant increase in crimes committed using a computer and the use of technological instruments.[27]

The following questions should be considered. How is the current legislation a barrier in the investigation of crimes where the object is to seize electronic evidence? This is seen in light of the fact that the current legislative framework proves itself to be insufficient. Law enforcement agencies are not equipped with enough knowledge and skills. The view is that the financial sector is a separate institution that regulates itself outside the ambit of the general SAPS. There is a lack of a definition of electronic evidence. The courts, who are insufficiently equipped, are tasked with dealing with electronic evidence on a case-by-case basis. The answers to these questions need to be put in relation to how the Constitutional rights to privacy impact on connecting search and seizure of evidence in electronic form.

Our Constitution determines that every law and conduct inconsistent with it is invalid; this is because it is the supreme law of the land.[28] However, it is important to note that not every right in the Constitution is absolute. Every right in the Constitution is subject to the limitation clause.[29] The Constitution's limitation clause is one of the legislative checks and balances put in place to ensure that there is no autocracy in the investigation of crimes. Similarly, the requirements for a valid search and seizure is in

---

26 s 12(1)(e) "Everyone has the right to freedom and security of the person, which includes the right – not to be treated or punished in a cruel, inhuman or degrading way".

27 Jackson 2015 *SAIPA* 9. Financial crime is often closely linked to cybercrime, with developing technology and markets presenting new opportunities for miscreants to exploit business and society.

28 s 2 of the Constitution.

29 s 36 of the Constitution.

place to ensure compliance with an individual's fundamental right envisaged in the Constitution. A crime is a violation of the victim's right to safety and security of person.[30] Unfortunately, in order for the State to investigate and prosecute, there is a further violation of Constitutional rights. Even so, criminal procedure deals with suspected and accused persons, and everyone has the right be regarded as innocent until proven guilty in a court of law.[31] The criminal justice systems needs to find a delicate balance between the rights of the accused and those of the victims.[32] The State needs to properly investigate crimes and ensure the vindication of victims, and ensure a successful prosecution of criminals. Achieving this balance is important in making sure that there is a decrease in criminal activity.

South Africa is behind in dealing with the increase of technology. Technology is the biggest threat to combating crime, because it gives criminals the platform to inflict harm, with little possibility of being apprehended.[33] South Africa already has a mounting problem with combating crime. The country is constantly painted as being violent and having high a number of crimes committed.[34] The elusive element of technology contributes another layer to the immense problem South Africa is facing. There is a need for positive action to be taken regarding the issue of crime in South Africa, especially with technology moving and growing at a rapid pace. In addition, technology is fast becoming a tool used to commit crime, this it more difficult to catch and prosecute criminals.[35]

South Africa needs to improve its skills in order to improve its commitment to combating crime and providing a safe and secure environment for all South Africans.

> Strong laws addressing phishing scams are necessary to restore consumer confidence in the internet.[36]

South Africa's current Electronic and Communications Transaction Act[37] has introduced cyber inspectors. As a specialised skill to further assist law enforcement in

---

30 s 12 of the Constitution.
31 s 35 (3) (h) of the Constitution.
32 Joubert *Criminal procedure handbook* 9.
33 Goodman MD and Brenner SW "The merging consensus on criminal conduct in cyberspace" 2002 *IJLIT* 144.
34 South African Police service "Crim Statistics 2017/2018" https://www.saps.gov.za/services/crimestates.php (accessed on 18 December 2018).
35 Jackson 2015 *SAIPA* 9.
36 Cassim F "Addressing the spectra of phishing: are adequate measures in place to protect victims of phishing?" 2014 *CILSA* 405.
37 Electronic and Communications Act 25 of 2002 (hereinafter referred to as the "the ECT Act").

the battle against computer and cybercrime, there is the Special Investigating Unit whose mandate is forensic investigation.[38] This research does not dispute that there are indeed investigators and skilled personnel available to conduct search and seizure. However, it aims to reveal that this is insufficient to deal with this particular area of law.

In South Africa, there are several role players involved in the investigation of crimes committed with a financial motive. However, it seems to be a scattered effort. There needs to be more of a collaborative effort in combating crime, as it is so complex.[39] This also includes educating internet users who are vulnerable, as their ignorance makes them an easy target.[40] South Africa has institutions and organisations that seek to combat the constantly increasing criminal activities relating to financial and commercial crime. However, this is always done retroactive. One of the more glaring characteristics of technology is that it is constantly changing. There are new ways of committing crimes using technology, and thus, police and State officials require those skills that are invaluable to the investigation of these crimes committed with advancing technology. There furthermore needs to be constant training and upgrading of the necessary skills. The State can no longer be reactive, but it needs to make a proactive effort to fight and combat crimes of this nature.

> Law enforcement agencies who are involved in the investigation and prosecution of cases should be technically savvy and receive adequate technical training and education to fight cybercrime.[41]

1.4 Chapter overview

1.4.1 Chapter Two - The general principles of search and seizure

This encapsulates a discussion of the principle of search and seizure and its relation to the procedure of collecting electronic evidence. The wording of the CPA is not conducive to the collection of electronic evidence. The courts have rejected the argument that there can be one umbrella provision to address the collection of

---

38 Special Investigating Unit "Our Mandate" https://www.siu.org.za/our-mandate/ (accessed on 20 November 2018).

39 Cassim 2014 *CILSA* 406. The article discusses phishing, which is a cybercrime. It falls within the scope of "financial crime" for the purpose of this research. Phishing is where scammers trick bank customers into entering their usernames and passwords.

40 The South African Banking Risk Information Centre "Digital Banking Crime Statistics" https://www.sabric.co.za/media-and-news/press-release/digital-banking-crime-statistics/ (accessed on 20 February 2019).

41 Cassim 2014 *CILSA* 405.

electronic evidence as a “document” when it is not.[42] The provisions of search and seizure cannot be seen in isolation of the Constitution that states that the right to privacy is paramount and may only be limited in terms of the law of general application.

There is an expansion on the various elements of search and seizure, the most important of which being reasonableness. Reasonableness is the starting point to investigation, as the police need to have a reasonable suspicion that a crime has been committed in order to conduct a search. The cognitive value of the principle of search and seizure as designed when it was enacted is not the same in modern day society. This is due to the nature of the modern criminal. The modern criminal is no longer just a physical threat. Modern day technology always allows criminals to commit crimes from remote areas.[43] This needs to be addressed with the same skill set and tools, including devices and software needed. However, in South Africa, this is not the case. There is insufficient advancement in the law to fight these remote criminals or inadequate skilled officials to conduct the required search and investigation to prosecute these criminals successfully.

1.4.2 Chapter Three - Financially motivated crimes

This research delves specifically into crimes committed for financial gain. When the police are investigating a crime, they need to bear in mind the nature of the crime committed in order to determine what kind of evidence they need to collect and present in court.

The South African financial industry is highly regulated. There are numerous laws pertaining to it and regulatory bodies that are there to ensure that the various financial institutions comply with the numerous laws. There is also a significant difference in laws regulating the private and public financial sector. The public sector needs to function in line with the principles of government accountability, whereas the private sector is profit-driven.

This chapter discusses the various institutions that investigate financial crime. The discussion centres on the capacity and ability to investigate and combat financial crime. In South Africa, reference is made to both financial and commercial crimes and

---

42 *Beheermaatscappij Helling I NV v Magistrate, Cape Town and others* [2005] JOL 13758 37.
43 Goodman *IJLIT* 144.

for the purpose of this research, financial crime shall be the terminology used. Institutions and organisations that are tasked with investigating financial crimes are not statutorily mandated to do so, thus they have to work efficiently and assist the police.

1.4.3 Chapter Four - General principles of evidence: Electronic evidence

In South Africa, the law of evidence is not codified. The content of admissible evidence is determined on a case-by-case basis. The courts use common law in South Africa to deal with electronic evidence. South Africa has made little progress in the promulgation of legislation that deals specifically with electronic evidence. This is despite the fact that the South African Law Reform Commission (SALRC) has conducted research and made recommendations in regards to the law of evidence.[44] Therefore, knowledge of the principles of evidence is required in order to deal with electronic evidence, as the courts have not made a determination on how to deal with electronic evidence. The courts rely on the ECT Act, which is the only piece of legislation that regulates electronic evidence, by providing a definition for "data messages" and admissibility of data messages. The courts have primarily dealt with computer printout and their admissibility in terms of section 15 of the ECT Act.[45]

This chapter will discuss the principles of evidence and provide a discussion on how it relates to electronic evidence. It does not engage in the analysis and presentation of evidence in court but it is limited to the nature in which it can be collected or investigated. Unfortunately, it is a common theme that South Africa has made very little progress in providing clear processes and procedures to regulate electronic evidence.

The urgency of providing legislation for the admission of electronic evidence in court proceedings is hastened by the alarming rate in which financial crimes are committed. The financial crimes that are committed not only affect victims but also affect the financial sector including financial institutions and the government who need to regulate the economy. Thus, there needs to be a determination made in order for the successful prosecutions of those who commit financial crimes and to regain

---

44 South African Law Reform Commission Issue Paper 27 (Project 126) "Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues" (2010) 3.

45 *S v Ndiki and others* [2007] 2 All SA 185 (ck) 191.

confidence in those law enforcement agencies tasked with the responsibility of investigating and prosecuting these crimes.

1.5 Summary

The law serves as an invisible security blanket for the public. This 'blanket' thus needs to ensure that it covers where it needs to, in order to fulfil its mandate of providing safety and security to the public. This is, however, not the case when it comes to crimes of a financial nature. There is a lack of coherent direction in regards to the search and seizure of elements that would serve as evidence in a court of law to prosecute those who commit crimes with a motive of financial gain. This chapter seeks to serve as an indication that the current *status quo* does not serve the developing needs of consumers and the public in offering protection from financial crime. It is also lacking in providing mechanisms to prove the commission of such crimes with sufficient evidence to prosecute it.

South Africa needs to act more swiftly to deal with the increase in financial crimes with the use of technology. It is no longer sufficient to play catch-up. The advanced nature of technology means that criminals are constantly ahead of investigators. The lack of adequate and relevant laws with skilled persons is undermining the efforts of law enforcement in the effort to fight crime.

> The internet has created a vibrant marketplace for business and consumers to interact, but it has also provided criminals with new avenues to commit crime.[46]

This research therefore seeks to highlight the glaring inconsistencies and gaps in South Africa relating to search and seizure of electronic evidence for prosecuting financial crimes. The law relating to search and seizure in general is outdated and it does not effectively address the changing structure of how current crimes are committed. People no longer use physical means nor do they need to have human contact to unlawfully appropriate funds. The efforts by law enforcement agents in their investigation of crimes, needs to match the intensity of the criminals.

---

46 Cassim 2014 *CILSA* 402.

The following chapter will examine and discuss the fundamental principles of search and seizure, their origins and whether there has been sufficient development to facilitate their relevance in an increasing world of advancing technology.

CHAPTER TWO

THE GENERAL PRINCIPLES OF SEARCH AND SEIZURE

2.1 Introduction

Crime is a reality of life in South Africa.[47] The courts have highlighted this, and particularly how it effects everything, including the economy.[48] It is thus incumbent on the State that there be rules to combat the surge of crime in the country. The main theme of this research is that the design of criminal investigation as a model of combating and preventing crime was aimed at crimes committed in a physical territory.

The physical nature of crime has been at the crux of criminal investigation with the crime being physical and the perpetrator also being physically present at the crime scene.[49] The CPA is the principle legislation that governs the search and seizure of objects. This chapter will discuss the rules pertaining to search and seizure. This will also include a discussion of other statutes, as the CPA includes provision for other statutes that may search and seize objects for investigations.[50] The various statutes discussed include elements of electronic evidence and financial crime. These include the ECT Act, which was essentially promulgated for the purpose of addressing technological advancements, the NPA Act, which provides for a special directorate, the Financial Intelligence Centre Act (FICA) that primarily investigates financial crimes, the investigation of any contravention in terms of the Income Tax Act, and the POCA which deals with organised crime. There is no uniformity on the aspects of search and seizure of electronic evidence, all the more so because this requires a specialist eye. The SALRC noted that there is a need for an investigation into whether there is sufficient legislation to deal with electronic evidence.[51]

---

47 Joubert *Criminal procedure handbook* 6.

48 *Langa DP in Investigating Directorate: Serious Economic Offences v Hyundai Motors Distributors (Pty) Ltd v Smith* 200 BCLR 1079 (CC) 37, it is a notorious fact that the rate of crime in South is unacceptably high. There are frequent reports of violent crime and incessant disclosure of fraudulent activity. This has a seriously adverse effect not only on the security of citizens and the morale of the community but also of the country's economy. The need to fight crime is thus an important objective in our society, and the setting up of special Investigating Directorates should be seen in that light.

49 Papadopoulos *Cyberlaw* 334.

50 s 19 of the CPA "The provisions of this chapter shall not derogate from any power conferred by any other law to enter any premises or to search any person, container or premises or to seize any matter, to declare any matter forfeited, or to dispose of any matter."

51 South African Law Reform Commission Issue Paper 27 (Project 126) "Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues" (2010) 5.

The importance of officials who have the latest digital equipment when investigating criminal activity cannot be understated. The SAPS does have a division that investigates priority crimes.[52] However, what is important with regard to this division and various other institutions is that not every case is investigated and there is specific criteria on which a case is investigated.[53] This does not allow there to be a conclusive fight against criminal activity of financial crimes using technology. In South African law, the duty of combating crime is the task of the government; this includes the investigating and collecting of evidence for the prosecution of accused persons.[54] The South African police service is the main institution that investigates crime. However, there are certain crimes that require a specialised investigating unit. The courts have said,

> The need to fight crime is thus an important objective in our society, and the setting up of special Investigating Directorates should be seen in that light.[55]

The CPA[56] makes provisions for the investigation of crime with and without a search warrant. This chapter looks at the requirements for a valid search warrant and will not be discussing search without a search warrant, as this aspect will require a broad generalisation regarding the commission of a crime. The chapter will discuss the powers to search for and seize objects, authorised by a valid search warrant.[57] It is imperative that those exercising these powers remain strictly within the limits of the law; this is because a warrant that is too wide and vague will be regarded as invalid by a court of law.[58]

The police must also be cognisant of an individual's fundamental rights in the Constitution. These fundamental rights includes the rights of both the victim and the accused. The requirements of search and seizure are there to ensure law enforcement

---

52 The South Africa Police Service "Directorate for priority crime investigation" https://www.saps.gov.za/dcpi/index.php (accessed on 02 February 2019).

53 Public Service Commission South Africa August 2001 "A review of South Africa's national anti-corruption agencies https://www.psc.gov/za/documents/reports/corruption/03.pdf (accessed on 19 February 2019).

54 South African Government official website "How does the criminal justice system work?" https://www.gov.za/faq/justice-and-crime-prevention/how-does-criminal-justice-system-work (accessed 01 March 2019).

55 *Investigating Directorate: Serious Economic Offences and others v Hyundai Motors Distribution (Pty) Ltd v Smit* 2000 BCLR 1079 (CC) 37.

56 s 22 of the CPA.

57 Joubert *Criminal procedure handbook* 178.

58 *Beheermaatscappij v Magistrate, Cape Town and others* 30.

does not abuse their powers, and conducts investigation in light of these fundamental rights. Law enforcement agencies need to be cognisant of their overall duty to combat crime. There needs to be a balance between investigating crimes and ensuring adherence to an individual's Constitutional rights.

Section 21 of the CPA includes several key role players involved in the execution of a search warrant. When dealing with the investigation of crimes that are committed for financial gain, other parties have to be involved as there are other provisions that regulate the investigations of financial crimes. In South Africa, financial institutions are highly regulated. When you include the element of crime committed with a computer, you enter into an electronic sphere of evidence. Electronic evidence further requires a specialist manner in which it is collected.

South Africa is still behind when it comes to the combating of crimes committed with technological means that have as their sole purpose financial gain. The combating and prosecution of criminals who commit such crimes is important, as it not only affects the confidence of the public in law enforcement, but it also directly affects the economy of the country.

This research seeks to discuss the principle of search and seizure in light of all the relevant legislation and procedures relating to it. This discussion will also encompass the role of technological advances particularly relating to electronic evidence used in computers and cybercrime as a collective.

2.2 Criminal Procedure Act 57 of 1977

2.2.1 The general rule

The general rule concerning search and seizure is that it must be conducted in terms of a search warrant. This important provision is found in section 21(1) of the CPA and it states:

> Subject to the provisions of sections 22, 24 and 25, an article referred to in section 20 shall be seized only by virtue of a search warrant issued -
> a) by a magistrate or justice, if it appears to such magistrate or justice from information on oath that there are reasonable grounds for believing that any such article is in the possession or under the control of or upon any person or upon or at any premises within his area of jurisdiction; or

> by a judge or judicial officer presiding at criminal proceedings, if it appears to such judge or judicial officer that any such article in the possession or under the control of any person or upon or at any premises is required in evidence at such proceedings.

The power given to law enforcement to search for and seize objects in an investigation is for obtaining evidence. This evidence will subsequently be used in the prosecution of the accused person.[59] A warrant will be valid if it is issued by an impartial and unbiased magistrate or judicial officer. The judicial officers must ensure that there are reasonable grounds for the warrant. An important provision for the purpose of this research is that the warrant must also readily indicate the object or person that must be searched and seized.

2.2.2 Search with a warrant

A warrant is a document by which searches are judicially authorised and legitimated.[60] The courts have provided that,

> A warrant is not a mere formality. It is a mechanism employed to balance an individual's right to privacy with public interest in compliance with and enforcement of regulatory provisions. A warrant guarantees that the state must be able, prior to an intrusion, to justify and support intrusions upon individuals' privacy under oath before a judicial officer. Further, it governs the time, place and scope of the search. This softens the intrusion on the right to privacy, guides the conduct of the inspection, and informs the individual of the legality and limits of the search. Our history provides evidence of the need to adhere strictly to the warrant requirement unless there are clear and justifiable reasons for deviation.[61]

The wording of a warrant is central to whether or not it will later be valid or invalid. The court can declare invalid a warrant that is too wide or vague.[62] For a warrant to be valid, the items to be searched and seized need to be sufficiently, specifically defined.[63] Such a requirement makes sense when the object of search and seizure is physical and readily ascertainable. However, the nature of computer evidence is such that it limits the ability of law enforcement agencies being able to name specifically the

---

59 South African Law Reform Commission Issue Paper 14 (Project 108) "Computer-related crime: options for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects" *(*1998*)* 4.

60 Basdeo VM *A Constitutional perspective of police powers of search and seizure in the criminal justice system* (LLM University of South Africa 2009) 59.

61 *Minister of Police and others v Kunjana* [2016] ZACC 21.

62 *Powell and Others v Van der Merwe NO and Others* 2005 (5) SA 62 (SCA) 35.

63 *Beheermaatscappij v Magistrate, Cape Town and Others* 1.

item to be searched. The search and seizure of electronic evidence is explained as follows:

> Search and seizure of electronic evidence is concerned with data that has been recorded or registered in the past, either in tangible or in intangible form; and the gathering of this data takes place at a single moment in time.[64]

The characteristics of electronic evidence has raised several issues relating to the search of and seizure, and the inadequacy of the CPA to deal with this matter. One such character is that electronic evidence is not traditional and is unique. Therefore this requires a unique procedure to be followed when collecting electronic evidence. The evaluation of electronic evidence has turned into a two-step process, where there is the seizure of the computer and the information on the physical computer.[65] It can no longer be seen as one act. However, several questions arise from the second process in relation to the second step. When can the search of the information on a computer be said to take place? Who seizes such information and are they specifically mentioned in the search warrant? These questions were answered as follows: the actual seizure of electronic evidence occurs only when it is discovered in the subsequent off-site search and seizure.[66]

The search warrant is very important for carrying out an investigation. However, this should not minimise the significance of a search warrant but should rather show the need for legislation to be updated regarding the search for computer evidence. The ECT Act tried to remedy this with section 82(4) that states that the concept of "premises" and "article" includes information systems and data messages. [67]

A warrant is such that a person cannot challenge the validity of the facts presented by law enforcement to a judicial officer; therefore it has the potential to damage one's reputation and business interest. That is why it is essential that the information provided is "adequate and objectively" based.[68]

---

64 Basdeo 2017 *JLSD* 50.

65 Bouwer GP "Search and seizure of electronic evidence: Division of traditional one-step process into a new two-step process in a South African context" 2014 *SACJ* 156.

66 Bouwer 2014 *SACJ* 168.

67 s 1 of the ECT Act defines "information system" as a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the internet.

68 *Powell and Others v Van der Merwe* 49.

2.2.3 Requirements for a valid search warrant

The courts have established[69] what must be included in a search warrant in order for it to be valid:

> What emerges from this analysis is that a valid warrant is one that, in a reasonably intelligible manner:
> (a) States the statutory provision in terms of which it is issued;
> (b) Identifies the searcher;
> (c) Clearly mentions the authority it confers upon the searcher;
> (d) Identifies the person, container or premises to be searched;
> (e) Describes the article to be searched for and seized, with sufficient particularity; and;
> (f) Specifies the offence which triggered the criminal investigation and the names of the suspected offender.

This list of requirements is not open-ended as there are other considerations to be taken into account, particularly the relevant legislation pertaining to search and seizure. Other such considerations include the naming of the offence in a warrant.[70]

The warrant governs the time, place, and scope of the search, limiting the privacy intrusion guiding the State in the conduct of the inspection and informing the subject of the legality and limits of the search. Our history provides much evidence for the need to adhere strictly to the warrant requirement.[71]

2.2.3.1 Judicial discretion

In the South Africa criminal justice system, the key role-players are both the criminal investigators in the form of the police, and the courts who prosecute crimes. The judiciary in the Republic needs to be fair and impartial and cannot be held ransom to any external influence. This is more so the case as the courts are seen as the guardians and custodians of the Constitution.

The courts' abilities to apply their minds in the decision process is a crucial check and balance to effective and efficient running of the criminal justice system. A judicial officer must account for their decision, this needs to be reasonable and to consider all relevant facts because no two cases will be similar.[72]

---

69 *Minister of Safety and Security v Van der Merwe* 2011 (5) 61 (CC) 25.
70 *Goqwana v The Minister of Safety NO and others* (20668/14) [2015] ZASCA 186.
71 *Minister of Police and Others v Kunjana* [2016] ZACC 21.
72 Joubert *Criminal procedure handbook* 179.

The judicial officer in signing a warrant must apply his mind to the facts. The courts need to establish that there are reasonable grounds for the suspicion, and that there is a suspected commission of a crime. A judicial officer is to apply his mind to whether or not a suspicion arises which sufficiently justifies the invasion of a person's right to privacy.[73]

As there are no rules but just guidelines in determining "reasonableness",[74] the judicial officer has to exercise a discretion, which must be exercised in a judicial manner.[75] Judicial discretion is not an exact science and therefore leaves substantial room for error, particularly where it is justified based on a rule or principle that has no legal basis in itself:

> The warrant may only be issued where the judicial officer has concluded that there is a reasonable suspicion that such an offence has been committed, that there are reasonable grounds to believe that objects on the relevant premises and, in the exercise of his or her discretion, the judicial officer considers it appropriate to issue a search warrant.[76]

The exercise of police powers in the investigation of a crime must be done in the strictest sense bearing in mind a person's right to privacy and the need to balance the right to privacy and investigating a crime. This is important because even though we are moving away from the unfair and discriminatory past in South Africa, this has laid the foundation for the fundamental rights that South Africans enjoy. The rights in the Constitution must be enjoyed without fear of arbitrary limitation and abuse from the State in the name of fighting crime.

These rights are also not absolute and maybe limited in terms of section 36 of the Constitution. An interesting consideration would be the recognition of human rights in relation to developing technology. The need to regulate the internet where people are free to act as they wish, but less accountable for their actions.

---

73 *Powell and Others v Van der Merwe* 68.
74 Joubert *Criminal procedure handbook* 125.
75 Joubert *Criminal procedure handbook* 139.
76 *Powell and Others v Van der Merwe* 30.

Section 25 of the CPA stipulates that there should be reasonable grounds based on information given on oath that an offence is or is likely to be committed, for a magistrate to issue a warrant.[77] Many other considerations must be taken into account when a warrant is issued. These were discussed by the Court in *Powell and Others v Van der Merwe and other*,[78] where the Court said it has been established that:

(a) Because of the great danger of misuse in the exercise of authority under search and seizure warrants, the courts examine their validity with a jealous regard for the liberty of the subject and his or her rights to privacy and property.
(b) This applies to both the authority under which a warrant is issued, and the ambit of its terms.
(c) The terms of a search warrant must be construed with reasonable strictness. Ordinarily there is no reason why it should be read otherwise than in the terms in which it is expressed.
(d) A warrant must convey intelligibly to both the searcher and searched the ambit of the search it authorises.
(e) If a warrant is to general, or if its terms go beyond those of the authorising statue permits, the courts will refuse to recognise it as valid, and it will be set aside.
(f) It is no cure for an overbroad warrant to say that the subject of the search knew or ought to have known what was being looked for: the warrant must itself specify its object, and must do so intelligibly and narrowly within the bounds of the empowering statue.

A warrant must be strictly interpreted to protect the rights of the individual against excessive interference by the State[79], and the warrant must clearly define the purpose of the search and the article that must be seized.

---

77 (1) If it appears to a magistrate or justice from information on oath that there are reasonable grounds for believing -
(b) that an offence has been or is being or is likely to be committed or that preparations or arrangements for the commission of any offence are being or are likely to be made in or upon any premises within his area of jurisdiction, he may issue a warrant authorising a police official to enter the premises in question at any reasonable time for the purpose -
(i) of carrying out such investigations and of taking such steps as such police official may consider necessary for the preservation of the internal security of the Republic or for the maintenance of law and order or for the prevention of any offence;
(ii) of searching the premises or any person in or upon the premises for any article referred to in s 20 which such police official on reasonable grounds suspects to be in or upon or at the premises or upon such person;
(iii) of seizing any such article.

78 2005 (1) SACR 317 (SCA) 41.

79 Joubert *Criminal procedure handbook* 180.

In addition to providing the requirements for a valid warrant, the court also stipulated the guidelines that must be observed by a judicial officer in considering the validity of the warrant.[80]

The courts have repeatedly referred to the importance of a warrant not being vague, and have stipulated that it must contain sufficient information that a reasonably intelligible person might understand. A judicial officer issuing or signing a warrant is an essential party to the procedure and must ensure that they take careful consideration and care in doing so.[81]

2.2.3.2 Object to be seized

The purpose of search and seizure is to obtain evidence that will assist the police in identifying a perpetrator and subsequently serve as evidence in the ensuing trial. The CPA refers to this as "articles". The prosecutor is required to adduce evidence of the commission of a crime, identify the perpetrator, and convince the court beyond a reasonable doubt that the person before the court is in fact guilty. In *National Union of South African Students v Divisional Commissioner, South African Police, Cape Western Division and Other,* the Court rejected the argument that a warrant that contains a list of items to be seized can be interpreted in such a manner as to include any or all the items in the position of the applicant.[82] The search and seizure must also be relevant for proving a case. It is clear from the use of the words "article" and "premises" that the provisions of the criminal act are intended to be applied in respect of physical items.[83]

---

80 (a) The person issuing the warrant must have the authority and jurisdiction;
(b) The person authorising the warrant must satisfy herself that the affidavit contains sufficient information on the existence of the judicial facts;
(c) The terms of the warrant must neither be vague nor overbroad
(d) A warrant must be reasonably intelligible to both the searcher and the searched person;
(e) A warrant must always consider the validity of the warrant with a jealous regard for the searched person's Constitutional rights; and
(f) The terms of the warrant must be construed with reasonable strictness.

81 *Goqwana v Minister of Safety NO and others* (20668/14) [2015] ZASCA 186.

82 *National Union of South African Students v Divisional Commissioner, South African Police, Cape Western Division and Others* 624.

83 South African Law Reform Commission discussion paper 99 (Project 108) "Computer related Crime: Preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software appliances and related procedural aspects" (2001) 14.

In *Ntoyakhe v Minister of Safety and security*,[84] the Court determined that the seizure of an article during an investigation extends to the subsequent detention of it. The CPA protects investigators who detain articles, as long as the article is kept within a reasonable period.[85] However, once it has been established that the article will not be used, or that there will not be a subsequent trial, it must be returned to the lawful possessor. This provision is relevant when the article details comprise of a physical nature. Computer evidence, the investigator seizes a computer and can make a mirror copy of the computer. This will speak to the originality and authenticity of the evidence. It is necessary to take into consideration the nature of computer evidence due to it being so fragile. Computer evidence is easily corrupted and is susceptible to a variety of viruses, and it may be deleted or destroyed.

Electronic evidence is still treated as a stepchild in South Africa; this is further amplified by the Court's definition of electronic evidence.[86] It is hard to ignore the fact that the CPA was enacted in a time where technological advances was not even something that would have been a factor. The use of a computer has become very popular nowadays. This forces us to view the concept of an article as being outdated and lacking the characteristics to encapsulate the changing conditions governing the investigation of crimes.

A warrant must clearly state the purpose of the search and the articles to be seized.[87] A warrant must seize only certain articles. In terms of the CPA, articles susceptible to seizure must fall within the following three categories in section 20 of the CPA.[88]
Evidentiary material

> Section 20(a) Articles which are concerned in or are on reasonable grounds believed to be concerned in the commission or suspected commission of an offence whether within the Republic or elsewhere.

The court in *Cine Films v Commissioner*[89] held that a warrant can only be issued for securing articles that are reasonably believed to be concerned in the commission of

84 *Ntoyakhe v Minister of Safety and security* 2000 (1) SA 257 354.
85 *Ntoyakhe v Minister of Safety and Security* 354.
86 Bouwer 2014 *SACJ 156*.
87 Basdeo *Constitutional Perspective of police powers of search and seizure* 79.
88 s 20 of the CPA.
89 *Cine Films v Commissioner* 1972 (2) SA 254 (A) 95.

an offence, and are to be used in the subsequent criminal proceedings in order to prove such offence. Proof of a crime consist of:

> Section 20(b) Articles which may afford evidence of the commission or suspected commission of an offence, whether within the Republic or elsewhere.

The advent of a computer virus designed by a Hong Kong national that crossed multiple borders and jurisdictions has brought awareness to this threat.[90] Though the American government wanted to prosecute him, they could not extradite him, as his actions were not criminal in Hong Kong.[91] The object identified in a warrant must aid as the subject of the crime:

> Section 20(c) Articles which are intended to be used or are on reasonable grounds believed to be intended to be used in the commission of an offence.

Though it is noted that it is not always possible to know exactly what article is used in the commission of a crime, a warrant cannot be termed too generally,[92] where this instance was inevitably discretionary. The courts have said that a warrant must specify its object, and that it must do so intelligibly and narrowly.[93] It is also important for the person being searched to be able to understand the warrant when it is produced to him.

The CPA does not place a limitation on the type of item to be seized in a search warrant, it just needs to fall within the category.[94] The matter for consideration is whether the physical component and the information contained in a computer can be regarded as a single article justifying its seizure as evidence.

The court rejected the idea that computers and other electronic items may be seized, when the warrant only authorised the seizure of "documentation".[95] It further stated that this could not be accepted as a common practice, where Section 20 of the CPA is clear in its wording. It was also recognised that for the purpose of collecting information from a computer, the police do not need to physically remove the computer

---

90 Goodman 2002 *IJLIT* 139.
91 Goodman 2002 *IJLIT* 140.
92 *Beheermaatscappij v Magistrate, Cape Town* 30.
93 *Powell and Others v Van der Merwe 42.*
94 South African Law Reform Commission Issue Paper 14 (Project 108) "Computer-related crime: options for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects" *(*1998*)* 10.
95 *Beheermaatscappij v Magistrate, Cape Town 37*.

or electronic items, but may copy and download information in the premises in which the items are, with little intrusion and disruption to the business.[96] This is of importance because a warrant was set aside, based on these grounds alone.

2.2.3.3 Reasonableness

When a suspected offence is being investigated, the police need to establish elements of the case. They need to ascertain whether there was a crime or offence committed, who the likely perpetrators might be, and need to collect evidence that will enable them to prove their case against the accused person. In the initial stages of an investigation, the police need to seize evidence. However, in order for them to do so they rely on different sources to provide them with information. The police thus do not have concrete evidence at the beginning of their investigation and would have to build a case based on the principle of "reasonable suspicion". Reasonable suspicion is not an abstract concept that is conjured up by police. Though there are no hard and fast rules to determine reasonableness, it has a factual basis[97] rather than an emotional one. Reasonable suspicion is the starting point for the collection of evidence. The Court in *Powell* has stated that,

> Suspicion in its ordinary meaning is a state of conjecture or surmise where proof is lacking; I suspected but cannot prove. Suspicion arises at or near the starting point of an investigation of which the obtaining of prima facie proof is the end.[98]

A judicial officer's decision to issue a warrant is based on the oath or information provided by a police officer requesting the warrant. The information provided is based on "reasonable grounds" for believing that a certain article is at a certain place or is in the possession of a particular person. It is also important that the information relied on be obtained *bona fide* and not in violation of the Constitution.[99] There is no single way of determining what exactly constitutes reasonable grounds.

---

96 *Beheermaatscappij v Magistrate, Cape Town* 37.

97 *Powell and Others v Van der Merwe* 35. The court said "A reasonable suspicion, he found, was an impression formed on the basis of diverse factors, including facts and pieces of information falling short of fact such as allegations and rumours. It is the total picture that is relevant".

98 *Powell and Others v Van der Merwe* 38.

99 Basdeo VM "The Constitutional validity of search and seizure powers in South African criminal procedure" 2009 *PER* 74.

Even though the point of departure in establishing grounds for search and seizure is reasonableness, this has to be determined on a case-by-case basis. The Court in *Mnyungula v Minister of Safety and security and others* discussed the meaning of sections 20 and 22 of the CPA, in order to establish what would constitute "reasonable belief".[100] There are certain principles that can be deduced from the provisions of section 21 of the CPA. A warrant must be strictly interpreted to protect the rights of the individual against excessive interference by the State,[101] and the warrant must clearly define the purpose of the search and the article that must be seized.

The Court in *Beheermaatscappij* specified that a warrant authorising a search of documents must only seize documents, not computers and other equipment.[102] The significance of this judgment is that warrants must specifically provide for the seizure of a computer, bearing in mind that the computer is only one component of the investigation.

2.3 Concluding remarks on search and seizure

The CPA provides for legislative requirements in regards to search and seizure. It also provides for the requirements of a valid search warrant. These provisions have been tested ample times by the courts. The courts have also included what it deems necessary for a warrant to be valid. It has done this cognisant of the need to investigate crime and preserve the Constitutional rights of individuals. The courts have dealt with the search and seizure of electronic evidence on a case-by-case basis. The difficulty faced by law enforcement in regards to electronic evidence does not allow there to be a detraction from the requirements for search and seizure. Police powers must still be exercised within the limits of the law.

The gap in providing legislative framework for the search and seizure of electronic evidence is becoming a pressing issue that needs to be addressed with urgency. The provisions of the CPA in regards to search and seizure do not operate in vacuum or isolation. The following is a discussion of other legislative provisions, where the Court indicated that a warrant must include the legislative authority in which it is issued.

---

100 *Mnyungula v Minister of Safety and security and others* 2004 (1) SACR 219.

101 *National Union of South African Students v Divisional Commissioner, South African Police, Cape Western Division and Others* [1971] 2 All SA 620 (C) 626.

102 *Beheermaatscappij v Magistrate Cape Town* 37.

2.4 The Electronic Communications and Transactions Act 25 of 2002

The ECT Act regulates electronic communication and transactions.

> The main aim of the ECT Act is to provide for the facilitation and regulation of electronic communication and transactions in the public interest.[103]

The ECT Act is important as it clearly provides for definitions of various terminology pertaining to the technological sphere. One important definition in regards to electronic evidence provided for by the ECT Act is the definition of “data messages”.[104]

The ECT Act also makes provision for the appointment of cyber-inspectors in terms of section 80. The powers of cyber-inspectors include to inspect and monitor web activity.[105] The powers of cyber-inspectors do not relate specifically to the investigation of cybercrime, as they are regulated by the Department of Communication, however they provide a skill that is invaluable. The SAPS needs to apply to the Department of Communication in order to receive the assistance of a cyber-inspector. Though this may be seen as a move in the right direction, it should also be noted that there has never been a cyber-inspector appointed.[106] This raises the question as to how effective the ECT Act is in dealing with computer investigations and cybercrime. The fact that there are dormant provisions in the main legislation dealing with computer evidence is not progressive in dealing with emerging and advancing technology. This might also be attributable to the fact that the ECT Act is not the brainchild of the Department of Justice and Constitutional Development (DoJCD).

This research pertains strictly to the collection of electronic evidence that is used in committing offences targeted at financial gain. Therefore, one of the more important pieces of legislation regarding this is the ECT Act. The ECT Act has as its objectives the following, which are relevant for the purpose of this research:

a. to recognise the importance of the information economy for the economic and social prosperity of the Republic;

---

103 Cassim 2014 *CILSA* 414.

104 s 1 of the ECT Act defines "data message" as 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.

105 s 81 of the ECT Act.

106 Papadopoulos *Cyberlaw* 328.

b. promote the understanding and, acceptance or and growth in the number of electronic transactions in the Republic;
c. remove and prevent barriers to electronic communications and transactions in the Republic;
d. promote and provide legal certainty and confidence in respect of electronic communication transactions;
e. develop a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions; and
f. ensure that the national interest of the Republic is not compromised through the use of electronic communication.[107]

The ECT Act is not primarily made to address issues with crime, especially cybercrime. It is enacted to work in conjunction with other legislation. This is due to the cumbersome processes that needs to be followed. The ECT Act focuses more on the issues relating to the promotion of access to electronic communication and preventing abuse, and does not criminalise certain behaviour that is in contravention to it, playing more of an administrative role in regards to electronic communication.

2.5 Cybercrimes Act, 2019

South Africa has several draft bills of cybercrimes legislation. The most recent Cybercrimes Bill, 2017 was accepted by the National Council of Provinces, and has been sent to the President to assent.[108] In terms of the short title, this Bill will be referred to as the Cybercrimes Act, 2019.[109]

All previous drafts included, that the aim of the Bill is to "create offences and impose penalties which have a bearing on Cybercrime".[110] CPA included that the law did not intend to include a computer, electronic material, or other items that fall outside the scope of what can be regarded as a document for the purposes of evidence. The Cybercrimes Act, 2019 provides for definitions in Section 1 of the Act. Chapter 4 refers to the "powers to investigate, search, access or seizure", this section also provides for definitions. In terms of section 1 the following definitions are provided for "article",

> Any data, computer programme, computer data storage medium, or computer system which—

---

107 s 2(1) (a), (c), (d), (e), (j) and (r).
108 Official website of the South African National CSIRT "Home" https://www.cybersecurityhub.gov.za (accessed on 03 July 2019).
109 s 60(1) of the Cybercrimes Act, 2019.
110 Cybercrime and Cybersecurity Bill 2015 and 2017 respectively.

> *(a)* is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission;
> *(b)* may afford evidence of the commission or suspected commission; or
> *(c)* is intended to be used or is, on reasonable grounds, believed to be intended to be used in the commission, of—
> (i) an offence in terms of Part I or Part II of Chapter 2: or
> (ii) any other offence, whether within the Republic or elsewhere.

This definition affords clarity in regards to the provision of the CPA as to whether or not computer programmes and data messages fall within the scope of what is regarded as an article for the purpose of search and seizure. This definition of "article" is not found in the 2015 Bill but it is discussed under section 29 of the 2017 Bill.

Section 25 of the Cybercrime Act, 2019 provides the definition for "access",

> to make use of data, a computer program, a computer data storage medium or a computer system or their accessories or components or any part thereof or any ancillary device or component to the extent necessary to search for and seize an article

The definition of seizure is as follows,

> Includes to -
> (a) remove a computer data storage medium or any part of a computer system;
> *(b)* render inaccessible, data, a computer programme, a computer data storage medium or any part of a computer system in order to preserve evidence;
> *(c)* make and retain a copy of data or a computer program; or
> *(d)* make and retain a printout of output of data or a computer program.

The definition of access is important, due to the need of law enforcement to have access to a computer in order to conduct a search and seizure. This poses a problem in such cases where law enforcement cannot conduct a search when they do not have access. The sensitive nature of electronic evidence becomes apparent when access is not granted due to computer files being corrupted or deleted.[111] It has been suggested that the terms "search" and "seizure" should in fact be substituted for more suitable terms such as "access".[112]

---

111 *African Cash and Curry (Pty) Limited v Commissioner for the South African Revenue Service [*2020] 1 All SA 1 (SCA) 105.

112 Nortjé JGJ and Myburgh DC "The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa" *PER / PELJ* 2019(22) – DOI 6 http://dx.doi.org/10.17159/1727-3781/2019/v22i0a4886 (accessed on 25 June 2020)

The Cybercrimes Act, 2019 stipulates that the provision in the Act must be applied in conjunction with the CPA. [113]

The Cybercrimes Act, 2019 has very similar provisions to those of the CPA, especially in regards to the requirement of a search warrant. Articles may only be seized in terms of a search warrant with the exception of certain provisions.[114]

The Cybercrimes Act, 2019 also provides for the scope and limits of carrying out the search warrant by the police official.[115]

The Cybercrimes Act, 2019 makes mention of a police official[116] applying for a warrant and subsequently carrying it out. This is important because there is no mention of any specialised skills that are necessary and required for the carrying out of a warrant for the seizure of computers, computer storage media and data.

There is a positive duty placed on the private sector to assist police officials technically, or render otherwise necessary assistance[117] in order for them to carry out a search and seizure of articles falling within the definition in section 1 of the Cybercrimes Act, 2019. Failure to act when requested by the police constitutes a crime.[118]

The Cybercrimes Act, 2019 is long-awaited. It has been a slow journey to reach a statute that regulates the domain of information technology, and the crimes that are committed in this space. There is an obligation created forcing the public and the private sector to work together so as to address the increase in cybercrime. It has also set up structures to respond to incidents relating to cybercrime.[119]

The Cybercrimes Act, 2019 has drastically changed the ECT Act, in terms of the schedule, the ECT Act excludes cybercrimes.[120] The ECT Act no longer deals with cybercrimes and section 85–88 of the ECT Act was deleted, while section 89 of the ECT Act was substituted.

---

113 s 27 of the Cybercrimes Act, 2019.
114 s 29(1) of the Cybercrimes Act, 2019.
115 s 29(2) of the Cybercrimes Act, 2019.
116 Definition in terms of s 1 of the Cybercrimes Act, 2019 “a member of the South African Police Services as defined in s 1 of the SAPS Act”.
117 s 34(1) of the Cybercrimes Act, 2019.
118 s 34(2) of the Cybercrimes Act, 2019.
119 s 54(1) (a) the Cybercrimes Act, 2019.
120 S 58 of the Cybercrimes Act, 2019

2.6 National Prosecuting Authority Act 32 of 1998

The Republic of South Africa has a single prosecuting authority established in terms of the Constitution.[121] The NPA Act establishes a national prosecuting body with the main function of prosecuting crimes. The NPA Act makes provisions for the function of the office of the Investigating Directorate,

> The National Prosecuting Authority Act makes provision for the search and seizure of property by an Investigating Director in the office of the National Director of Public Prosecutions, to facilitate the investigation of certain specified offences. The power to search and seize property may be exercised on the authority of a warrant by a judicial officer. [122]

The Investigation of serious Economic Offences Act 46 of 1995 was established. It has since been repealed and consequently replaced by the NPA Act. The Investigating Directorate was established in the office of the National Director of Public Prosecutions (NDPP). There are different categories of crime, and not all are investigated by the NDPP. Those that are more serious necessitate the formation of an investigation directorate in terms of section 7(1) of the NPA Act.[123] The investigation of crimes is done in respect of economic crimes.[124] The National Prosecuting Authority has the discretion to institute criminal proceedings once it has been established that a criminal offence has been committed. The NPA therefore plays an important role in the process of investigating crime. There are two types of investigation in terms of the NPA Act, namely an inquiry,[125] and a preparatory investigation.[126] These two types of investigation speak to the element of reasonableness. The NPA Act differentiates what

---

121 s 179(1) of the Constitution "There is a single national prosecuting authority in the Republic, structured in terms of an Act of Parliament, and consisting of –
(a) a National Director of Public Prosecutions, who is head of the prosecuting authority, and is appointed by the President, as head of the national executive; and
(b) Directors of Public Prosecutions and prosecutors as determined by an Act of Parliament.

122 *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd v Smith* 2000 BCLR 1079 (CC) 2.

123 (1) The President may, by proclamation in the Gazette, establish one or more Investigating Directorates in the Office of the National Director, in respect of such offences or criminal or unlawful activities as set out in the proclamation.

124 Proclamation R123 (GG 19579, 4 December). The specific crimes are also defined in this proclamation.

125 s 28(1) of the NPA Act. An inquiry is held if the Investigating Director –
has reason to suspect that a specified offence has been or is being committed or that an attempt has been or is being made to commit such an offence.

126 Is held if the investigating Director –
Considers it necessary to hear evidence in order to enable him or her to determine if there are reasonable grounds to conduct an investigation in terms of ss (1)(a), the Investigating Director may hold a preparatory investigation.

reasonableness is for the purpose of investigation by the directorate, where one states there are already reasonable grounds to suspect an offence and the other deals with there being a suspicion, but there is uncertainty as to whether there are reasonable grounds. The powers of the Investigating Directorate to investigate a crime in terms of the NPA Act was discussed extensively by the courts.[127] The Investigating Directorate is a special unit established under the NPA Act to conduct investigation into serious and complex offences.[128] "The need to fight crime is thus an important objective in our society, and the setting up of special investigating directorates should be seen in that light".[129]

The office of the investigating directorate has been re-established by the President in terms of section 7(1) of the NPA Act. The President includes a list of offences that will be investigated by the directorate, including high priority complex crimes.[130] The Investigating Directorate has three offices and the offences are separated according to three categories.[131] The Powers of the Investigating directorate are set out extensively in section 29.[132] Section 29 of the NPA Act gives the investigating directorate powers to enter premises, with or without notice, for the purpose of investigation. The section allows them to search the premises, examine objects and make copies or extracts from any book or document. The use of the words "book or document" sets a limitation, where it is conceivable that people have information stored in a computer rather than a book or hardcopy document. Therefore, there needs to be an appropriate update of legislation, as it cannot be assumed that the words "book" and "document" are synonymous with data on a computer. The CPA in section 19 makes provision for there to be other statutes dealing with the principle of search and seizure. The NPA Act also mirrors the CPA in that it contains the requirement of judicial

127 *Powell and Others v Van der Merwe* 5.
128 *Investigating Directorate: Serious Economic Offences v Hyundai Motors Distributors (Pty) Ltd v Smith* 44.
129 *Investigating Directorate: Serious Economic Offences v Hyundai Motors Distributors (Pty) Ltd v Smith* 53.
130 President proclaims NDPP Investigating Directorate to strengthen fight against corruption http://www.thepresidency.gov.za/press-statements/President-proclaims-ndpp-investigating-directorate-strengthen-fight-against (accessed on 14 May 2019).
131 Proclamation R123, Government Gazette 19579, 4 December 1998.
132 s 29 of the NPA Act.

authorisation.[133] Section 29(5) of the NPA Act stipulates that the warrant must be granted on information given under oath based on reasonable grounds.[134]

A search warrant is an expeditious investigating tool that grants law enforcement considerable amount of powers to invade a person's right to privacy; hence, it is important that the requirements for a valid warrant apply, and that there are checks and balances in place to ensure accountability. Law enforcement agents conducting themselves in regards to a warrant must do so bearing in mind that they must act within the limits and confines of the law in order that justice be seen to be met. The NPA establishes investigating bodies that are not necessarily there for the purpose of the pre-trial investigation. This is the Asset Forfeiture Unit (AFU), which conducts investigation for the purpose of forfeiture.[135]

Another body that falls under the NPA is the Special Investigation Unit (SIU). This unit is specifically mandated to investigate financial misappropriation and maladministration by the state.[136] According to the SIU:

> We are the State's preferred provider of forensic investigating and litigation services working together with other agencies in the fight to eradicate corruption, malpractice and maladministration from society.[137]

The primary focus of this research is financial crimes. This legislation is therefore important because Government needs to establish priority means of combating crimes that affect the economy.

---

133 s 29(5) of the NPA Act.

134 (5) A warrant contemplated in ss (4) may only be issued if it appears to the magistrate, regional magistrate or judge from information on oath or affirmation, stating -
(a) the nature of the investigation in terms of s 28;
(b) that there exists a reasonable suspicion that an offence, which might be a specified offence , has been or is being committed, or that an attempt was or had been made to commit such an offence; and
(c) the need, in regard to the investigation, for a search and seizure in terms of this section that there are reasonable grounds for believing that anything referred to in ss (1). Is on or in such premises or suspected to be on or in such premises.

135 Montesh M "An analysis of the role of the South African asset forfeiture unit and the special investigating unit" *Acta Criminologica* 2009 33.

136 The SIU will be discussed in general as their specific powers relate to the public sector when there is financial misconduct by public institutions. This topic is beyond the scope of what is covered in this research.

137 Special Investigating Unit https://www.siu.org.za (accessed on 02 July 2018).

Section 2 of the SIU Act enables the president to establish the Unit.[138] This section states that the function of the SIU is to investigate within its framework as per the terms of reference in the prescribed proclamation. This includes investigating and collecting evidence.[139]

A Special Investigating Unit must, as soon as practically possible after it has obtained evidence referred to in subsection (1)(d), inform the relevant prosecuting authority thereof, whereupon such evidence must be dealt with in the manner which best serves the interests of the public. [140]

The SIU Act also makes provisions for search and seizure;[141] these are similar to those of the CPA. It requires that a person's dignity be respected and that they may search, examine, extract, make copies and request information.[142]

> Any member of a Special Investigating Unit or a police officer authorised thereto by a member of the Special Investigating Unit may, for the purpose of performing the functions and exercising the powers mentioned in sections 4 and 5, and subject to the provisions of this section, enter and search any premises on or in which anything connected with an investigation is or is suspected to be.[143]

The search and seizure in terms of the SIU Act also stipulates that it must be done with a search warrant that is signed by a member of the special tribunal or judicial officer.[144]

2.7 The Financial Intelligence Centre Act 38 of 2001

The Financial Intelligence Centre (FIC) was promulgated in terms of the FICA.[145] It is established within the public administration sector as a juristic person that is outside the public service.[146] The centre's principle object is to act as a watchdog for money

---

138 (1) The President may, whenever he or she deems it necessary on account of any of the grounds mentioned in ss (2), by proclamation in the Gazette -
(i) establish a Special Investigating Unit in order to investigate the matter concerned;
(ii) refer the matter to an existing Special Investigating Unit for investigation.

139 s 2(a) - (b) of the SIU Act.

140 s 4(2) of the SIU Act.

141 s 6 of the SIU Act.

142 s 6(3) of the SIU Act.

143 s 6(1) of the SIU Act.

144 s 6(5) (a) of the SIU Act.

145 Financial intelligence Centre Act 38 of 2001 (hereinafter referred to as FICA).

146 s 2 of FICA.

laundering activity and other unlawful activities used by individuals to clean ill-gotten gains.

> (1) The principal objective of the Centre is to assist in the identification of the proceeds of unlawful activities and the combating of money laundering activities and the financing of terrorist and related activities.
> (2) The other objectives of the Centre are -
> (a) to make information collected by it available to investigating authorities, the intelligence services and the South African Revenue Service to facilitate the administration and enforcement of the laws of the Republic.

The centre's function is limited to that of an investigatory body and does not have formal powers as those of the SAPS. The functions of the centre are to identify and analyse information relating to the unlawful activity of suspects.[147] The FIC is there to curb activities of commercial crimes, combating money and financing of terrorist activities. The relevance of including the FICA in this research is to show that there are indeed various institutions that work to combat commercial crimes, but work in isolation to other such institutions. The FIC publish a media report to clarify the role it places as a crime preventing institution.[148]

2.8 The Income Tax Act 58 of 1962

The Income Tax Act is relevant in this research as tax contraventions fall within the scope of financial crime. People and citizens who work or conduct business in South Africa are obligated to pay taxes accordingly. However, it is undoubtedly common that there are people who evade disclosing correctly, their earning in order not to pay taxes or to pay a lesser amount.[149] The Income Tax provides that the Commissioner[150] may search and seize items relating to any information it might need. We will look at Section

---

147 To achieve its objectives the Centre must - (a) process, analyse and interpret information disclosed to it, and obtained by it, in terms of this Act; (b) inform, advise and cooperate with investigating authorities, supervisory bodies, the South African Revenue Service and the intelligence services; (c) monitor and give guidance to accountable institutions, supervisory bodies and other persons regarding the performance by them of their duties and their compliance with the provisions of this Act; (d) retain the information referred to in paragraph (a) in the manner and for the period required by this Act.

148 Financial Intelligence Centre "Media Release Financial Intelligence Reports: FIC Role Clarified" https://www.fic.gov.za/Documents/Media%20Release%20%204%20Sept%202019%20(003).pdf (accessed on 16 September 2019).

149 *Feruccio Ferucci and Others v The Commissioner for The Revenue Service and Another* 2002 (6) SA 219 (c) 3.

150 **"Commissioner"** means the Commissioner for the South African Revenue Service appointed in terms of s 6 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997), or the Acting Commissioner designated in terms of s 7 of that Act.

74D of the Income Tax Act. The Tax Administration Act has since repealed this Act,[151] but we will look at it in comparison to the current provision and the general provision of the CPA in regards to search and seizure.

(1) The Act empowers the Commissioner of revenue services to obtain and verify information using search and seizure. This Act allows for the application and issuing of a judicial warrant or the purpose of search and seizure.
A judge may, on the application of the Commissioner or a person authorised by him issue a warrant authorising the officer or officers specified therein without prior notice at and] any time to:

(i) Enter and search any premises; and

(ii) Search any person present on such premises, provided that such search is conducted by an officer of the same gender as the person being searched. For an information, documents or things which may afford evidence as to the non-compliance or any taxpayer of his obligation in terms of the Income Tax act, and to seize any documents or things authorised by the warrant.[152]

Application to the judge for issue of such warrant shall be supported by information supplied under oath or declaration "establishing the facts on which the application is based".[153] The Income Tax Act is succeed by the Tax Administration Act 28 of 2011.[154] The Tax Act stipulates that an application for a warrant may be authorised by a senior official[155] and that an *ex parte* application may be made to a judge for a search warrant. The application for a warrant must be made under oath or declaration containing information relevant and sufficient information.[156]

The Tax Act makes provision for a search without a warrant if there are reasonable grounds to believe that the material contains relevant information to their investigation will be found there but it is not mentioned in the warrant.[157]

2.9 The Prevention of Organised Crime Act 121 of 1998

The Prevention of Organised Crime Act[158] is established to combat crimes and ensure that criminals do not benefit from crime. The PCOA also recognised the Constitution as placing a duty on the police to protect and promote the rights enshrined in the Bill

151 28 of 2011. s 74D was repealed by s 271 of the Tax Administration Act.
152 *Feruccio Ferucci and Others v The Commissioner for The Revenue Service* 5.
153 *Feruccio Ferucci and Others v The Commissioner for The Revenue Service* 5.
154 Hereinafter referred to as "the Tax Act".
155 s 59(1) of the Tax Act.
156 s 59(2) of the Tax Act.
157 s 63 of the Tax Act.
158 Prevention of Organised Crime Act 121 of 1998 (hereinafter referred to as the PCOA).

of Rights. In its preamble, the PCOA recognises that South Africa is lacking in legislation relating to the combat of organised crimes. [159] It has as its objective:

> to introduce measures to combat organised crimes, money laundering and criminal gang activity.

Also important is the fact that the Tax Act has the effect of providing for the recovery of proceeds of unlawful activity.[160] However, this does not fall within the ambit of this research and thus will not be discussed. The purpose of including this legislation is to show that there are measures in place to recover monies and assets that are obtained by illegal means.

2.9.1 Concluding remarks

There are several statutes that have provisions relating to search and seizure. These all assist in the investigation of crime. These do not overlap as the CPA makes provision for search and seizure in section 19. As discussed in the introductory chapter, this is a scattered effort. There are a plethora of institutions and laws to combat crime. There is, however, no structure in place to determine jurisdiction in regards to fighting crime. There is potential to bring these statutes and institutions together to form a uniform structure to combat financial crimes. All the provisions above have similar provisions to the CPA in regards to search and seizure. These essentially amount to a duplication.

It is not clear as to which of these constitutes the leading provision in regards to search and seizure of electronic evidence. These laws apply as and when there is a crime investigated. These provisions are subject to the Constitution, where the right to privacy must be protected, and thus the requirements of a search warrant must be adhered to regardless of the legislation relied upon. For this reason, it is important to discuss the Constitution and the scope of the limitation in regards to the fight against crime.

---

159 Whereas the South African common law and statutory law fail to deal effectively with organised crime, money laundering and criminal gang activities, and also fail to keep pace with international measures aimed at dealing effectively with organised crime money laundering and criminal gang activities.

160 ch 5 of the PCOA.

2.10 The Constitution of the Republic of South Africa, 1996

The Constitution establishes a new order in South Africa.[161] Section 2 the of the Constitution states:

> This Constitution is the supreme law of the Republic, law or conduct inconsistent with it is invalid, and the obligations imposed by it must be fulfilled.

The Constitution contains the Bill of Rights in Chapter 2. The rights in the Bill of Rights are fundamental and important. This is established in terms of section 7:

> This Bill of Rights is a cornerstone of democracy in South Africa. It enshrines the rights of all people in our country and affirms the democratic values of human dignity, equality and freedom.

Section 8(1) addresses the application of the Bill of Rights and states that "The Bill of Rights applies to all law, and binds the legislature, the executive, the judiciary and all organs of state*."* All laws need to ensure that they are not in conflict with the Constitution including the CPA, which provides for the procedures and process in place when a crime has been committed. This establishes that, in principle, the investigation of a crime cannot fall outside the ambit of the Constitution. In the investigation of crime, the police must take cognisance of the right to privacy enshrined in section 14 of the Constitution.

The State is tasked with the duty of enforcing criminal law and conducts investigation to collect evidence as part of the pre-trial process. This is, however, subject to the provisions of the Constitution. Criminal procedure seeks to ensure that there is a balance between the rights of the accused and those of the victims. The investigation requires that the State take cognisance of both the need to solve the crime and not infringe on the rights of the suspect.[162]

The courts tend to jealously safeguard individual rights because of the persuasive nature of these powers of search and seizure in the hands of the State.[163] The courts are tasked with interpreting the law to give it effect, and they must do so with the supremacy of the Constitution in mind, and the object and purport of the fundamental

---

161 *S v Makwanyane* 1995 (6) BCLR 665.

162 For the purpose of this research "suspect" refers to both a suspect and an accused person.

163 Joubert *Criminal procedure handbook* 122.

rights. An important provision in the Bill of Rights that relates to search and seizure is a person's right to privacy:

> 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 possession seized;
> (d) The privacy of their communication infringed.

2.10.1 The right to privacy

The right to privacy is an important fundamental right in the Constitution and it is afforded to all citizens of South Africa.

> Section 14 of the Constitution guarantees that everyone has the right to privacy, including the right not to have their person or home searched, their property searched, their possessions seized or the privacy of their communications infringed.[164]

However, it should be noted that the rights in the Constitution are not absolute and they can be limited in terms of section 36 of the Constitution.[165] The role of crime in South Africa is such that there needs to be measures in place for the police to investigate criminal offences effectively.

> The truism that no right is to be considered absolute implies that from the outset of interpretation each right is always already limited by every other right accruing to another citizen. In the context of privacy this would mean that it is only the inner sanctum of a person, such as his/her family, life, sexual preference and home environment, which is shielded from erosion by conflicting rights of the community.[166]

The right to privacy is intimate to a person. However, it is conceivable that the rights of human beings coincide, including the right to privacy. This is because human beings do not live in isolation of one another. The Constitution governs the relationship between government officials in their dealings with the public and the relationship where the public interact with one another. The courts have discussed the relativity in

---

164 *Minister of Police and Others v Kunjana* [2016] ZACC 21.

165 The rights in the Bill of Rights may be limited only in terms of a law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, and taking into account all relevant factors, including –
(a) The nature of the right;
(b) The importance of the purpose of the limitation;
(c) The nature and extent of the limitation;
(d) The relationship between the limitation and its purpose; and
(e) Less restrictive means to achieve the purpose.

166 *Minister of Police and Others v Kunjane* [2016] ZACC 21 8.

relation to the right to privacy, the more a person interacts with the general public their right to privacy dwindles.[167] The Court is noting that there is a limitation to the degree of privacy that is protected when an individual is in constant contact with the public.

It has been established that a search warrant and the seizure of objects in terms of a search warrant are a direct violation of a person's right to privacy.[168] A warrant therefore needs to ensure that it meets all the requirements discussed above. A warrant that is too widely worded and is vague will be considered invalid and put aside. The Constitution aims to advance an ethical criminal justice system that is accountable to society.[169]

> Although the section[170] authorises seizure of "anything" the powers are not all embracing. There are items that are not susceptible to seizure, such as in the case of privilege. Also of importance is the consequences of unlawful searches and seizures.

It is essential, therefore, that law enforcement officials stay strictly[171] within the confines of the law when they are investigating crimes in order not to abort justice. Law enforcement officials must be skilled in the use of investigative tools and extremely knowledgeable about the intricacies of the law.[172] The focus of criminal procedure cannot be solely on the infringement of rights. There needs to be cognisance of the fact that when a crime has been committed the victim has also been violated.

There needs to be a balance between the rights of those accused of crime, and that of society to be safe.[173] The Court decided that the extent to which the privacy of the accused had been infringed has of lesser importance to achieving the purpose of the search in the case.[174]

> Any entry upon or search of any premises in terms of this section shall be conducted with strict regard to decency and order, including - (c) the right of a person to his or her personal privacy.[175]

---

167 *Investigating Directorate: Serious Economic Offences v Hyundai Motors Distributors (Pty) Ltd v Smith* 2000 BCLR 1079 (CC) 5.
168 Basdeo *Constitutional Perspective of police powers of search and seizure* 5.
169 *Beheermaatschappij v Magistrate, Cape Town* 49.
170 s 20 of the CPA.
171 *National Director of Public Prosecutions v Mahomed* [2007] SCA 138 36.
172 Basdeo *Constitutional Perspective of police powers of search and seizure* 7.
173 s 12 of the Constitution.
174 *S v Madiba 1998* (1) BCLR 38 (D) 37.
175 s 29(2) (c) of the NPA Act.

The courts in *Bernstein and another v Bester and others NO* said,

> Nevertheless it seems to be a sensible approach to say that the scope of a person's privacy extends a *fortiori* only to those aspects in regard to which a legitimate expectation of privacy can be harboured.[176]

In dealing with a person's right to privacy, this should not just end at meeting the requirements for a valid search warrant. It should be clearly communicated to the party being searched or whose items are being seized why they are being searched.[177] The court[178] cited another case with approval, emphasising:

> The sanctity of the right to privacy and said that the existence of safeguards to regulate the way in which state officials may enter the private domains of ordinary citizens is one of the features that distinguish a Constitutional democracy from a police state.[179]

2.10.2 The limitation clause

The courts need to balance the interest of two competing rights in the Constitution in order to establish that the limitation of a right is justifiable.[180]

> The balancing of different interest must still take place. On the one hand, there is the right infringed; its nature; its importance in an open and democratic society based on human dignity, equality and freedom; and the nature and extent of the limitation. On the other hand, there is the purpose of the importance of the limitation. In the balancing process and in the evaluation of the proportionality one is enjoined to consider the relation between the limitation and its purpose as well as the existence of less restrictive means to achieve this purpose. [181]

The conundrum regarding the right to privacy as envisaged in the Constitution and that of the need for pre-trial investigation, relating to search and seizure is best explained by the following statement,

> The law jealously protects the personality and property rights of individuals. These rights include every person's right to his or her body, freedom, honour, dignity, and privacy, as well as his rights with regard to property. Accordingly, these interests are fully protected by the Constitution. Sometimes, however, society's wider interest in the combating of crime necessitates the limitation of these rights. It may,

176 *Bernstein and another v Bester and others NO* 1996 (4) BCLR 449 75.
177 "It is desirable that a person whose premises are being invaded should know the reason why". As stated in *Minister for Safety and Security and Van der Merwe* 54.
178 *Minister of Police and Others v Kunjane* [2016] ZACC 18.
179 *Mistry v interim National Medical and Dental Council of South Africa* [1998] ZACC 25.
180 *Johncom media investment LTD V M and PD and another* CCT 08/08 [2009] ZACC 1.
181 *Johncom media investment LTD V M and PD and another* CCT 08/08 [2009] ZACC 24.

> for instance, be necessary to arrest a person and thereby encroach upon their freedom of movement, or to seize property. Despite this, the law constantly strives towards achieving a balance between society's demands, on the one hand, to bring offenders to justice, and, on the other hand, to uphold the personality and property rights of the individual. To achieve this, the law lays down strict rules with regard to the circumstances in which the limitation of these rights will be permissible to investigate crime or to bring offenders to justice. The Constitutionality of these limitations can only be determined by measuring them against the limitation clause in section 36 of the Constitution.[182]

It has been established that every person has the right to privacy as envisaged in the Constitution and that the principal of search and seizure is a direct violation of this right. It is understood that it would be cumbersome for law enforcement to conduct an investigation if it was constantly in violation with the law. Therefore, the Constitution makes provision for the limitation of rights. Section 36 of the Constitution determines limitation of rights.

The law of general application that enables the limitation of the right to privacy is the CPA. The CPA limits the individuals' right to privacy in terms of search and seizure contained in section 20 of this Act. The court is also tasked with the duty of having to strike a balance between the right to privacy and the need for search and seizure in investigating crimes.[183]

> The importance of the purpose of the limitation is crucial to the analysis, as it is clear that the Constitution does not regard the limitation of a Constitutional right as justified unless there is a substantial state interest requiring the limitations.[184]

2.11 Summary

Crimes that have financial gain as their sole motivation require an intense investigation by the police. The investigation includes the search and seizure of evidence. Technological advances have also meant that there are new ways in which people commit crimes.[185] It is therefore important that the police or any institution tasked with

---

182 Joubert *Criminal procedure handbook* 122.

183 *Investigating Directorate: Serious Economic Offences v Hyundai Motors Distributors (Pty) Ltd v Smith* 24.

184 *Minister of Police and Other v Kunjane* [2016] ZACC 19.

185 Cassim 2014 *CILSA* 401.

the investigation of these crimes be adequately skilled and have the correct and necessary resources to deal with the advancement of technology.

This chapter concludes that an essential element to a police investigation includes search and seizure. There are so many elements to this principle of search and seizure for this research and the author looks at the use of electronic evidence when the crime is that of financial gain, and the various legislation that pertain to the search and seizure of electronic evidence.

The South African law is very clear about the requirements for a valid search warrant. The requirements are that it must be signed by a judicial officer based on information provided by a State official on oath on reasonable grounds and the objects to be seized must clearly be identifiable. Concerning the object to be seized, the court have made it clear that a warrant must intelligibly set out the specific items to be seized.

The Court in *Powell* set aside the warrant, which was said to be broadly worded and vague. The Court noted that it amounted to a general ransacking. This goes against the spirit of the Constitution in protecting individuals.[186] The courts have also expressed clearly, what is required for a valid search and seizure and the scope of each requirement. The Court[187] has described a warrant as being similar to a weapon. The successful prosecution of crimes require that there be a limitation of the right to privacy.[188] The following chapter will discuss what a financial crime is, how it can be established that there has been a crime in which there was misappropriation of funds, and the different legislative frameworks that deal with finances.

186 *Powell and Others v Van der Merwe* 62.
187 *Goqwana v Minister of Safety NO and others* (20668/14) [2015] ZASCZ 186.
188 *Minister of Police and Other v Kunjane* [2016] ZACC 21.

CHAPTER THREE

FINANCIALLY MOTIVATED CRIME

3.1 Introduction

The law is divided into public law and private law, respectively. Public law governs the relationship between the State and the public, whereas private law governs the relationship between individuals.[189] The second element of this research that needs to be discussed is criminal activities that result in financial loss to the victim. These criminal activities are committed with a computer as an instrument.

Financial crimes are no different to any other crime that have an element of being physical, and thus they need as much attention. Financial crimes not only affects the victim, but also the economy. Financial crimes directly affect the growth of the economy, investment potential and confidence of the public.[190]

Historically crimes that involved the unlawful appropriation of another's money or funds were physical in nature; these include crimes such as theft[191] and robbery.[192] The fact that a computer is used to commit these crimes from a remote location does not make it less traumatic than the common law crimes of theft or robbery that are more personal. As humans, we place certain trust in the internet and tend to be naïve when it comes to the true extent of the dangers of technology. Our defences, are down and we are less guarded when transacting in the comfort of our home with no regard that a computer can thus become the subject of a crime when used as an instrument to commit these crimes.[193]

---

189 Snyman CR *Criminal law* 6th ed (LexisNexis 2016) 3.

190 The South African Banking Risk Information Centre "SAPS and SABRIC Recommit to Intensify Fight against Bank Robberies https://www.sabric.co.za/media-and-news/press-release/saps-and-sabric-recommit-to-intensify-fight-against-bank-robberies/ (accessed on 20 February 2019).

191 Snyman *Criminal law* 475 defines theft as "A person commits theft if he unlawfully and intentionally appropriated movable, corporeal property which (a) belongs to, and it is in the possession of, another, (b) belongs to another but is in the perpetrator's own possession; or (c) belongs to the perpetrator but is in another's possession.

192 Snyman *Criminal law* 508. Provides the definition of Robbery; "Robbery consists in theft of property by unlawfully and intentionally using: (a) violence to take the property from somebody else; or (b) threats of violence to induce the possessor of the property to submit to the taking of the property.

193 Cassim F "Addressing the spectra of cybercrime in Africa: Evaluating measures adopted by South Africa and other regional role players" 2011 *CILSA* 124.

The evolution of technology has meant that one does not have to physically steal from another or be present. Technology has introduced a new kind of thief, one that is remote and cannot be easily identified. The purpose of this chapter is to illuminate the fact that the economy is at risk in our burgeoning technological era. We live in the information age where our lives are computerised into either a device or a cloud, the internet is not synonymous with the concept of the cloud.[194] Banks and other financial institutions rely heavily on technology. Yet, the average person is unaware of the dangers and criminals lurking in the cyberspace.

What is of greater concern is the fact that South Africa is still behind in regulating and fighting such crimes. The statutes that are in place are reactive; action taken when there is a crime committed or when there is an event that requires the attention of the police, Government, and relevant stakeholders. This is unacceptable when it comes to combating crimes committed using computers. This is because technology is fast evolving. There is a need to have specialised and sophisticated legislation to combat these crimes.[195]

The fight against crimes committed with technology needs to be proactive.[196] South Africa has many different institutions and organisations even within the police force and other governmental departments that investigate crimes separately. There is no uniformity. We lack a single unit that is tasked with the investigation of financial crimes, a unit that has influence nationally, is skilled and is capacitated to deal decisively with this type of criminal activity. Various institutions within the SAPS and NPA have been found to be ineffective due to the political influence and constant media scandals.

> In general, South Africa's laws are sufficiently robust and comprehensive to address financial crime. The real weakness lies in the structures that are required to implement the laws. Law enforcement is hamstrung by the lack of expertise, resources and co-ordination.[197]

---

194 The cloud is a general metaphor that is used to refer to the internet. Initially, the internet was seen as a distributed network and then, with the invention of the World Wide Web, as a tangle of interlinked media. As the internet continued to grow in both size and the range of activities it encompassed, it came to be known as "the cloud." https://www.techopedia.com/definition/26514/cloud (accessed on 22 February 2019).

195 Cassim 2011 *CILSA* 124.

196 Wille C *et al Principles of financial law* (LexisNexis 2007) 211: "Perpetrators of financial crimes are scholars in the latest development in electronic commerce, business practices, legislation and law enforcement measure, with the regulators and crime fighters battling to keep up with the latest ingenious schemes to steal, cheat, defraud and embezzle."

197 De Koker L "Financial crime in South Africa" 2007 *IEA* 37.

The ECT Act introduced cybercrime inspectors in terms of section 80 of the ECT Act. This provision requires the director general of the Department of Communications to appoint cyber inspectors. It is not a step forward to have electronic evidence, cybercrime and regulating of cyber inspectors under the Department of Communication. The SAPS need to apply to the Department of Communications to receive assistance from cyber inspectors.[198]

3.2 Definition of a crime

Substantive law dictates what constitutes a crime.[199] In court, the prosecutor would have to establish that all the elements of a crime are there and thus there has been a crime committed. This includes proving the element of unlawfulness of the perpetrator's actions. The nature of financial crimes committed with technological means, however, makes it difficult to simply put it into one category of a crime, and this includes cybercrime. This is especially so because the international community has determined that there cannot be one universal definition of cybercrime. In addition, you can have criminal activities such as tax invasion or crimes committed using a computer, as an instrument but these do not necessarily constitute cybercrime,

> Any offence may involve important evidence located on a computer (including mobile devices), even if this offence is otherwise un-related to computer systems. While this is not cybercrime, the criminal justice system nevertheless needs to be able to recognise and handle electronic evidence.[200]

Determining the elements of the crime for this purpose would also be a difficult task especially with the complexity of financial crimes. The fact is that the world is constantly revolving and there are new ways of committing these crimes. There are always new ways in which criminals outsmart the system and find new ways to commit crimes.[201]

---

198 (2) Any statutory body, including the SAPS, with powers of inspection or search and seizure in terms of any law may apply for assistance from a cyber-inspector to assist it in an investigation: Provided that (a.) the requesting body must apply to the Department for assistance in the prescribed manner; and (b.) the Department may authorise such assistance on certain conditions.

199 Joubert *Criminal procedure handbook* 7. The author defines substantive law as comprising legal rules that determine the rights and duties of individuals.

200 Council of Europe "Cybercrime@IPA specialised cybercrime unit - good practice study" www.coe.int/cybercrime (accessed on 01 July 2020).

201 Interpol "Summary - Global cybercrime strategy" https://www.interpol.int/content/download/5586/file/Summary_CYBER_Strategy_2017_01_EN%20LR.pdf?inLanguage=eng-GB (accessed on 25 July 2020).

There is a constant need to regulate human interaction or human exchange. We currently live in a technological age, where the exchange of information has become a precious and expensive commodity. Information is so important, to the extent that it is regulated in South Africa in terms of the Promotion of Access to Information Act 2 of 2000 (PAIA).[202] PAIA stipulates that a person has the right to access to information held by the State and information held by any other person for exercising his or her right or for the protection of his or her right.[203]

The relevance of this is to show the invaluable nature of information. However, the prevalence of cybercrime and technology-related crimes is that, at the core of it is the theft of information. Criminals use the information that is stored in technological devices and the cloud to commit other crimes. The information age has presented itself as a platform that makes the public vulnerable to those criminals that are lurking around waiting to take advantage and exploit this vulnerability. Criminals use technology to access clients' personal information so that they can steal from them.[204]

The term "financial crimes" is not generally used in South Africa. South African law and law enforcement agencies normally use the terms "commercial crime" and economic "crime" or refer to offences such as theft, fraud, insider trading, money laundering, and terrorist financing.[205]

3.3 Financial crimes

An element of the definition of theft is the unlawful appropriation of money belonging to somebody else.[206] Generally, when one thinks of the illegal or unlawful appropriation of another's property they think of theft. Theft is the common law crime that is defined as follows:

> A person commits theft if he unlawfully and intentionally appropriates movable, corporeal property which
>
> (a) Belongs to, and it is in the possession of, another;
> (b) Belongs to another but is in the perpetrators' own possession; or

202 Hereinafter referred to as "PAIA".
203 s 32 of PAIA.
204 The South African Banking Information Centre (SABRIC) warms consumers to beware of phishing and malware. https://www.sabric.co.za/media-and-news/press-release/sabric-warms-consumers-to-beware-of-phishing-and-malware/ (accessed 20 February 2019).
205 De Koker 2007 *IEA* 34.
206 Snyman *Criminal law* 476.

(c) belongs to the perpetrator but is in another's possession and such other person has a right to possess it which legally prevails against the perpetrator's own right to possession provided that the intention to appropriate the property includes an intention permanently to deprive the person entitled to the possession of the property, of such property.

Financial crime is the act of stealing, when a person unlawfully takes money that does not belong to him or her. Such crimes can be carried out in various ways. The SAPS formally uses various terms associated with criminal acts of financial gain such as fraud, embezzlement, theft, corruption, cybercrime and computer-related offences.[207] Financial crime occurs when, there is an act of unlawful appropriation of another's patrimonial property, and it further define illicit financial activity as:

> Illicit financial activity as conducting any financial transaction, whether formally or informally, which, if done during the normal course of business, could be prosecuted under the laws of the land.[208]

The researcher notes for the purpose of this research, that there is a difference between cybercrime and financial crime. The Cybercrimes Act, 2019 does not provide a definition for cybercrime in section 1. However, Chapter 2 of the Cybercrimes Act, 2019 provides several crimes that fall within the scope of financial crime. The main reason this research does not focus solely on cybercrime is that not all cybercrimes are committed with a financial motive. In addition, it is possible to have a crime committed with a computer as an instrument that does not necessarily fall within the scope of cybercrime. There are provisions from various legislation that criminalises certain actions that relate to economic activity. The NPA Act provides that the provisions of Chapter 5 be specifically for the,

> Powers, duties and functions relating to the investigating directorate.[209]

There was a surge in organised crimes in South Africa, which included international crimes syndicates. This prompted the government to act accordingly and thus the POCA was introduced. POCA provides for the definition of "unlawful activity" in section 1 of the Act as,

---

207 Budhram T and Geldenhuys N "A losing battle? Assessing the detection rate of commercial crime" 2017 *SA Crime Quarterly* 7.

208 Jordaan J *Analysis of bank account statements to establish evidence of illicit financial activity (*M Tech University of South Africa 2007) 4.

209 s 26(1) of the NPA Act.

> conduct which constitutes a crime or which contravenes any law whether such conduct occurred before or after the commencement of this Act and whether such conduct occurred in the Republic or elsewhere.

Financial crime would require the skills of a financial investigator, and this task falls within the arena of auditing and accountancy.[210] South Africa is still at a disadvantage, in its attempt to combat financial crimes because it lacks adequate specialised skills.

The search and seizure of electronic evidence in financial crimes is viewed as a task for external people and it has been practiced as such. Financial investigations are defined as:

> Financial investigation as investigations in which, on behalf of law enforcement, financial expertise is used in order to gather, check, refine, process and analyse financial information.[211]

On the face of it, financial investigation seems synonymous with the broad spectrum of things however, this is not the case. It can be further defined as follows:

> Financial investigation is the identification and documentation of the movement of money during the course of and after a crime. It establishes the link between where the money comes from, who gets it, when it was received, and where it was stored or deposited.[212]

Financial crimes, as previously stated, encapsulate a broad definition of crimes committed with financial gain as a motive. Even though this includes both the public and the private sector, there is a difference between the two. Within the public sector, such crimes are commonly related to the act of corruption by government institutions or officials who partake in activities that amount to the theft of State funds for personal gain. There will not be an in-depth discussion on corruption in South Africa in this dissertation, but rather, a discussion relating to the regulation of corruption as it relates to State funds, and that of the private sector. The POCA was introduced as a means of combating organised crime and money laundering. In terms of Section 1, property is defined as:

> Money or any other movable, immovable, corporeal or incorporeal thing and includes any rights, privileges, claims and securities and any interest therein and all proceeds thereof.

The public sector has several legislative provisions dedicated to ensuring checks and balances when dealing with State funds, one such provision is the Public Finance

---

210 Jordaan *Analysis of bank account statements* 17.
211 Jordaan *Analysis of bank account statements* 17.
212 Jordaan *Analysis of bank account statements* 18.

Management Act (PFMA).[213] The PFMA deals with how State funds are managed and spent in relation to the duty of the country to provide service delivery. The public sector is unfortunately also vulnerable to the risk of unlawful misappropriation of funds with the use of technology and computers. [214]

Most companies have internal measures, such as auditors, who are used to account for the funds or finances of that company. Auditing can shed light on any unlawful activity regarding the misuse of funds. However, for the purpose of this research, the discussion of financial crimes is limited to the public arena, with the victim being the ordinary person on the street, who does not have sophisticated mechanism in place to secure and track his/her financial activity. Individuals rely on the financial institutions and government in the form of law enforcement to protect them.

The private sector also has different regulatory bodies depending on the type of financial institution. The overall body that deals with the finance sector is the Financial Service Boards.[215] Financial crimes have a direct bearing on individuals, organisations, business and the government who suffer loss from acts such as fraud, theft, corruption, tax evasion, and money laundering, facilitating, receiving and possessing the proceeds of crime.[216] In the first instance involving electronic evidence, the courts rejected the use of bank statements as evidence.[217] However, in terms of section 236 of the CPA, bank statements are not allowed to be used as evidence in criminal proceedings.

3.4 Reporting financial crimes

3.4.1 Introduction

The right to privacy is guaranteed in the Constitution and has been discussed extensively in the previous chapter. The courts have stated that in relation to search and seizure, the right to privacy maybe limited in terms of section 36.[218]

The Court has expressed the view that a person's right to privacy is less likely to be infringed upon the more a person delves into the world, in their business activities and

213 Public Finance Management Act 1 of 1999 (hereinafter referred to as the PFMA).
214 Cassim 2011 *CILSA* 124.
215 Established in terms of the Financial Service Board (hereinafter referred to as the FSB).
216 Budhram Budhram 2017 *crime quarterly* 7.
217 *Narlis v South Africa Bank of Athens* 1976 (2) SA 573 (A) 158.
218 The Constitution of the Republic, 1996.

social interactions.[219] South Africa is moving towards an era where there is a mechanism in place that limits society's right to privacy in order to fight crime. However, society is struggling with the idea that communication will be monitored. This was done under the auspices that it would help the police investigate crimes better and allow for the interception of criminals before they even commit crimes.

The South African government even introduced the concept of "whistle blowing"[220] to aid in combating criminal and corrupt activates in both the public and private sector. Information has become a precious commodity, personal information is stolen and used by thieves to steal from unsuspecting victims.[221] Information is commonly referred to as data.[222] It is not just any information that is at risk of being misappropriated and used for criminal acts. However, because there is no certainty regarding what information can be used it is important to protect one's personal information in its entirety, there are several statutes that offer protection relation to information. This includes the Constitution, which guarantees a person's right to "freedom and security of person".[223] However, a discussion needs to be had about whether information can be used in a positive manner, to fight against crimes.

These are important for several reasons, bringing forth the question of whether or not it amounts to a crime when someone with knowledge of a crime intentionally withholds such information from the police. The Constitution also protects a person from self-incrimination;[224] just as the right to privacy can be limited so can any other right in the Constitution. The CPA makes provision for a judicial officer to compel a person to provide information needed for the investigation of a crime.[225]

3.4.2 The South African Police Service

The role of the SAPS is very important and cannot be understated. The Constitution notes the following about the police service:

---

219 *Bernstein and others v Bester NO and others* 85.

220 "Whistle blower" is the term used to describe a person who discloses information in terms of s 1 of the Protected Disclosure Act 26 of 2002 (as amended).

221 Cassim F "Protecting personal information in the Era of identity theft: Just how safe is our personal information from identity thieves?" 2015 *PER* 70.

222 s 1 of the Cybercrimes Act, 2019 definition of "data" means electronic representation of information in any form.

223 s 12 of the Constitution.

224 s 35(3) (j) of the Constitution.

225 s 185 of the CPA.

> (1) The national police service must be structured to function in the national, provincial and, where appropriate, local spheres of government. (2) National legislation must establish the powers and functions of the police service and must enable the police service to discharge its responsibilities effectively, taking into account the requirements of the provinces. (3) The objects of the police service are to prevent, combat and investigate crime, to maintain public order, to protect and secure the inhabitants of the Republic and their property, and to uphold and enforce the law.[226]

In terms of the preamble to the South African Police Service Act (SAPS Act),[227] the police must ensure co-operation with other services and communities in efforts to combat crime. This does not take away the primary duty of the Police service, which is to protect fundamental rights in the Constitution.

However, it is noted that the very nature of financial crimes may go beyond the scope of the SAPS and delve into the arena of specialisation of forensic accounting and auditing. Therefore, the SAPS is tasked with establishing a Directorate to investigate and prevent priority crimes including commercial crimes.[228]

3.4.3 The Protected Disclosure Act 26 of 2002

The aim of the Protected Disclosure Act[229] is to provide for the procedure in which an employer or worker may inform the police of criminal activities or other activities that are irregular or unethical. The Protected Disclosure Act is an avenue for those with information relating to unlawful activates to be able to disclose anonymously.[230] This is formally known as whistle blowing.[231] The Protected Disclosure Act has been amended to include protection of those who want to come forward with information relating to their former employers, this includes previous employment in a government agency. It is recognised in the preamble that criminal activities and corruption are detrimental to an economy. The significance of the Protected Disclosure Act is that it provides a channel for police to investigate information given to it by the public. Financial crimes need to be brought to the attention of the police in order for them to be investigated; this is because a person's finances are private and confidential. When

226 s 205 of the Constitution.
227 South African Police Service Act 68 of 1995.
228 Preamble to the SAPS Act.
229 26 of 2002 (hereinafter the Protected Disclosure Act).
230 The preamble to the FICA.
231 For the purpose of this research, persons who disclose information will be referred to as "whistle blowers".

a crime is committed, it is not obvious to the police and thus it needs to be brought to the attention of officials. The same principle applies when crimes are committed within companies, institutions and government organisations. Therefore, the Protected Disclosure Act allows for the anonymous release of information to the police, this is important because people should not be forced to deal with the repercussions of "doing the right thing".

3.4.4 The Protection of Personal Information Act 4 of 2013

The South African Constitution protects a person's right to privacy in terms of section 14.[232] The Protection of Personal Information Act (POPI)[233] seeks to give effect to this provision of the Constitution.[234]

> It promotes *inter alia*, the protection of personal information processed by private and public bodies and provides for the protection of the rights of persons regarding unsolicited electronic communication the new legislation places a responsibility on companies to respect the personal information of clients and to handle such information with utmost care and responsibility.[235]

A person's personal information needs to be protected. This is because one of the dangers of emerging technology is the impact on the identity of a person with the subsequent consequence of criminal activity using a person's information. The protection of personal information is not the sole responsibility of law enforcements and financial institutions. Consumers are constantly cautioned to be careful in regards to who they give their information. Criminals go as far as even targeting victims' home computers and disguise themselves as legitimate businesses.[236]

3.4.5 The Financial Intelligence Centre Act 38 of 2001

The FIC is established in terms of the FICA.[237] The FIC is established as an anti-money laundering centre and creates a duty on the private sector and other agencies to report on unlawful activities. It provides a list of definitions in section 1 that include the following:

---

232 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.

233 4 of 2013 (hereinafter referred to as POPI).

234 Hereinafter, referred to as the POPI.

235 s 19 of the POPI.

236 Cassim 2015 *PER* 76.

237 38 of 2001.

a. Bearer negotiable instrument - means any instrument that may on demand by the bearer thereof be converted to the currency of the Republic or that of another country, and includes, amongst, others, cheques, promissory notes or money orders;
b. Cash - (a) coin and paper money of the Republic or of another country that is designated as legal tender and that circulates as, and is customarily used and accepted as, a medium of exchange in the country of issue; (b) travellers' cheques;
c. Inspector - means a person appointed in terms of section 45A; and
d. Property - has the meaning attributed to that term in section 1 of the Prevention Act.[238]

The FICA states that it is the superior act, should there be any conflict with other legislations save the Constitution.[239] In terms of the Constitution, there needs to be accountability and transparency relating to any function of public administration.[240] The FIC is one such institution that is operating under public administration but must be autonomous from any government influence. It operates as a juristic person operating outside the public service but within the public administration.[241] This simply means that it is publicly funded. The FIC needs to ensure that it does all that is expected and necessary in order to fulfil its function and mandate, which includes engaging in any lawful activity with other relevant bodies to promote its objectives.[242] The FICA does not explicitly say or make provision for the search and seizure of items or evidence for prosecution but the above provision indicates that there can be a working relationship formed with relevant investigating bodies to ensure that the objectives of anti-money laundering are met. This therefore clearly makes provision for the operation of various institutions in order to fulfil its mandate. The FICA requires accountable institutions[243] to require documentation from prospective clients that prove the legitimacy of the client as an individual or otherwise business entity.[244]

The FIC may require information or additional information for the purpose of their investigation.[245] Much like the Protected Disclosure Act, FICA promotes the disclosure of information relating to unlawful or criminal activities and it provides for the protection

238 In terms of s 1 of the Prevention Act, this term means "money or any other movable, immovable, corporeal or incorporeal thing, and includes any rights, privileges, claims and securities and any interest therein and all proceeds thereof".
239 s 1A of the FICA.
240 s 195(1) (g) of the Constitution.
241 s 2 of the FICA.
242 s 3 of FICA.
243 This means a person referred to in Schedule 1 of FICA.
244 s 21 of FICA.
245 s 32 of FICA.

against criminal and civil action of those who come forward with the information.[246] The provisions of this Act are in no way a means of limiting the powers of other investigating or supervisory bodies:

> This Act does not detract from – (a) an investigating authority's power in terms of other legislation to obtain information for the purpose of criminal investigations.

Due to the powers of the FIC being limited, it is obligated to make available information held by it that was reported to it, to other investigating bodies.[247] The FICA also makes provision for search in section 70, and states that

> (1) A police official or person authorised by the Minister to receive a report under section 30(1), who has reasonable grounds to suspect that an offence under section 54 has been or is about to be committed, may at any time search any person, container or other thing in which any cash contemplated in section 30(1) is suspected to be found.

The FICA also makes provision for the seizure in terms of subsection 2 and stipulates that,

> A police official or person authorised by the Minister referred to in subsection (1) may seize any cash contemplated in section 30(1).

3.5 The European Convention on Cybercrime

The protocol that was published in 2001 has as its mandate the international co-operation in combating cybercrime. This is because member states and the international community recognise that the world is becoming more digitised, and this means that there is an opportunity for the risk of crimes being committed through this medium.[248]

> The Convention is the only binding international instrument on this issue. It serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between state parties to this treaty.[249]

South Africa is a non-member of the European council and signatory to the treaty. South Africa has however not ratified it.[250] South Africa took over a decade to include

---

246 s 4 of FICA.
247 s 3(2) (a) of FICA.
248 Council of Europe *Convention on Cybercrime* Budapest 2001 2.
249 Council of Europe *Convention on Cybercrime* Budapest 2001 2.
250 Ratification or accession signifies an agreement to be legally bound by the terms of the convention https://www.unicef.org/crc/index_30207.html (07 February 2019).

legislation that deals with cybercrime after it had become a signatory to the Convention. This Convention will be discussed in its capacity as providing guidelines for legislative framework that was to be promulgated for the regulation of cybercrime.

3.6 Cybercrime

The Cybercrimes Act, 2019 does not contain provision relating to the definition of cybercrime. However, the Cybercrimes and Cybersecurity Bill[251] states that there is no universal definition of cybercrime; however it does attempt to define it as follows:

> Crimes which are committed by means of, or which were facilitated by or which involve date, a computer programme, a computer data storage medium or a computer system.[252]

Cybersecurity is however, defined in the Cybercrimes Bill, 2017 as:

> Technologies, measures and practices designed to protect data, computer programmes, computer data storage medium or a computer system against cybercrime, damage or interference.[253]

The same definition is not provided for in the Cybersecurity Act, 2019. In terms of the National Cybersecurity Policy Framework (NCPF) it seeks to provide coordination in regards to cybersecurity through the cybersecurity hub. [254]

There are, additionally, other definitions of cybercrime:

> Cybercrime (computer crime) can be defined as any criminal activity that involves a computer.[255]

> Any unlawful conduct involving a computer or computer system or computer network, irrespective of whether it is the object of the crime or instrumental in the commission of the crime or incidental to the commission of the crime.[256]

It is important to reiterate that authors who provide definitions for “cybercrime” in no way intend for these to constitute a universal definition. There is a consensus that it is practically impossible to have one definition of cybercrime that encapsulates its every essence. Cybercrime is an umbrella term used for the crimes that are committed over the internet. However, an important element of cybercrime is that it is committed within

---

251 Cybercrimes Bill, 2017.
252 Memorandum on the objects of the Cybercrimes and Cybersecurity Bill, 2017.
253 Memorandum on the objects of the Cybercrimes and Cybersecurity Bill, 2017.
254 National Cybersecurity Policy Framework GG 39475 4 December 2015 (hereinafter the NCPF).
255 Snail S “Cybercrime in the context of the ECT” 2009 63.
256 Papadopoulos *Cyberlaw* 336.

the sphere of the World Wide Web. The ECT Act governs cybercrime in South Africa and criminalises the unlawful interception of information.[257] This should be considered however, in light of the Cybercrimes Act, 2019 that will drastically amend the ECT Act when it comes into law.

The growing phenomenon of the digitisation of information has led to various developments in today's life, communication and business.[258] This has, however, not come with aspects that affect the individual and community at large. The biggest threat on the internet is the target of information, and regardless of where a person is a criminal can illegally appropriate important information from a remote location. The phenomenon of cybercrime emerged in the 1990s.[259]

> Cybercrime has become the fastest growing crime in the world with resourceful crime syndicates preying on millions of unsuspecting and gullible victims. Cybercrime also undermines consumer confidence in e-commerce transactions.[260]

Criminals use tactics that fool innocent people because of how authentic they seem. The ECT Act was developed under the Department of Communication.[261] It therefore has to be interpreted by the courts to have a criminal law and criminal procedural law element and influence. The commercialisation of the internet has led to a broader problem that was never anticipated.[262] This is primarily the reason the author does not specifically and exclusively refer to cybercrime, but will include an array of financial crimes committed with electronic use. Cybercrime and cyber-attacks are not limited to crimes that are for financial gain. The use of electronic commerce has led to problems relating to the admissibility and evidentiary weight of electronic evidence.[263] The Cybercrimes Act, 2019 has deleted chapter of the ECT Act dealing with cybercrime. The Cybercrimes Act, 2019 now therefore deals exclusively with cybercrime. Central to this research, especially in this chapter, is that computer crime and cybercrime are not synonymous. The evidence of this is in the "Harmonization of ICT Policies in Sub-

---

257 s 86(1) of ECT Act.

258 Harmonization of ICT Policies in Sub-Saharan Africa "Electronic Transactions and Electronic Commerce: Southern African Development Community Model" 2013.

259 Snail 2009 *JILT* 63.

260 Wille C *Principles of financial law* 222.

261 Department of Communication.

262 Papadopoulos *Cyberlaw* 333.

263 Harmonization of ICT Policies in Sub-Saharan Africa "Electronic Transactions and Electronic Commerce: Southern African Development Community Model" 2013.

Saharan Africa Computer Crime and Cybercrime: Southern African Development Community Model law" 2013,' made recommendations relating to "Computer crime and cybercrime legislation".[264] The potential Cybercrimes Act, 2019 needs to be discussed in light of current legislation and common law dealing with crimes that have the element of financial misappropriation. The Cybercrimes Bill, 2015 directly mimics the Harmonization of ICT Policies in Sub-Saharan Africa "Computer Crime and Cybercrime: Southern African Development Community Model law" of 2013. The 2017 Cybercrimes Bill is an improved version to the Cybercrimes Bill, 2015, which has included other offences that were not previously included. However, there are also provisions that were excluded that made a positive contribution to the combating of cybercrime and computer crimes. There are certain crimes that have become widely known and easily identifiable. These include crimes such as phishing, which "refer […] to criminal act that are carried out online to coerce victims to disclose personal secretive information about themselves".[265] The Cybercrimes Act, 2019 has also included crimes that are familiar but have a different element that is cyber, such as cyber fraud. The common law definition of fraud is:

> The unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another.

Fraud is not only committed in terms financial crime, however, the element of actual or potential prejudice maybe proved in terms of monetary loss.[266]

Cyber fraud is defined as, any person who unlawfully and with the intention to defraud, makes a misrepresentation—

> Any person who unlawfully and with the intention to defraud makes a misrepresentation—
> *(a)* by means of data or a computer programme; or
> *(b)* through any interference with data or a computer programme as contemplated in subsection 5(2)(*a*), (*b*) or (*e*) or interference with a computer data storage medium or a computer system as contemplated in section 6(2)(*a*),
> which—
> (i) causes actual prejudice; or
> (ii) is potentially prejudicial,
> to another person, is guilty of the offence of cyber fraud.

---

264 Harmonization of ICT Policies in Sub-Saharan Africa "Computer Crime and Cybercrime: Southern African Development Community Model law" 2013.

265 Cassim 2014 *CILSA* 402.

266 Snyman *Criminal law* 527.

Thus, this definition has included a definition of an act being committed using a computer programme or data.[267] The Cybercrimes Bill, 2015 does not make specific reference to defining cybercrimes including that of cyber fraud. The Cybercrimes Act, 2019 includes an element of theft of incorporeal property to the common law offence,

> The common law offence of theft must be interpreted so as not to exclude the theft of an incorporeal.[268]

The nature of corporeal property is that it is a thing. The common law definition of theft exclude the possibility of being able to misappropriate something that is not tangible. However, the Cybercrimes Act, 2019 has remedied this by updating the definition of theft.

Different departments and institutions have dealt with cybercrime as though it were an internal housekeeping issue. Cybercrime is investigated in terms of the CPA and more specifically Chapter 2. However, it is not sufficient in that the scope of the CPA are not broad enough to tackle the nature of cybercrime adequately.

This research aims to show that the law relating to the investigation of electronic evidence is scattered, and that this is confirmed in the Cybercrimes Bill, 2017.[269] Its memorandum stipulates that,

> There is no coherent and organised approach in South Africa to deal with cybercrime and cybersecurity. Different Government Departments enacted legislation to protect their own interest.

The Cybercrimes Bill, 2017 also states that there is no adequately skilled person to deal with the growing phenomenon of cybercrime.[270] There is enough protection for the physical sphere, however, this cannot be said to extend to information infrastructures. The ECT Act made an attempt in this regard, but it does not sufficiently

---

267 s 1 of the Cybercrimes Act, 2019 defines "data" as electronic representation of information in any form.

268 Snyman *Criminal law* 475. Definition of *theft;*
A person commits theft if he unlawfully and intentionally appropriates movable, corporeal property which,
(a) belongs to, and is in the possession of, another; or
(b) belongs to another but is in the perpetrator's own possession; or
(c) belongs to the perpetrator but is in another's possession and such other person has a right to possess it which legally prevails against the perpetrator's own right of possession.
Provided that he intention to appropriate the property includes an intention permanently to deprive the person entitled to the possession of the properly of such property.

269 Memorandum on the objects of the Cybercrimes and Cybersecurity Bill, 2017 point 10.

270 Memorandum on the objects of the Cybercrimes and Cybersecurity Bill, 2017 point 11.

protect it.[271] South Africa is not without its efforts to combat the surge of cybercrime. This is evident with laws such as the POCA and FICA, South Africa was able to join the Financial Action Task Force.[272]

3.7 Relevant investigating bodies and strategic partnerships

South Africa has a history of various bodies investigating crimes. It is not a history that paints a good picture in regards to the effectiveness of these investigating bodies. This clearly goes to show a lack of uniformity and consistency in the investigation of crime. There are also organisations that work with the "government" to assist in the combating of financial crimes with the use of technological means.[273] These are commendable, and a very necessary part of fighting crime, but create an imbalance regarding who is tasked with the fighting of financial crimes. This can lead to loopholes in the fight against financial crimes.

Over the past decade, South Africa has introduced several forms of legislation to fight the surge of criminal activities that have a financial gain as the motive, including cash heist, money laundering and organised crimes. This legislation encompasses and addresses the following:

3.7.1 Financial Action Task Force

South Africa went on to adopt FICA and together with the Prevention of Organised Crime Act created a money laundering control framework in South Africa that then qualified the country to be the first African State to join the Financial Action Task Force.[274]

3.7.2 Directorate: Special Operations

The South African government long recognised that there has been an increase[275] in financial crimes, and knew that this had to be dealt with by a specialised unit. This

---

271 Memorandum on the objects of the Cybercrimes and Cybersecurity Bill, 2017 point 13.

272 Is an intergovernmental policy making body that has a ministerial mandate to establish international standards for combating money laundering and terrorist financing https://www.fatf-gafi.org (7 February 2019).

273 The South African Banking Risk Information Centre "SAPS and SABRIC Recommit to Intensify Fight against Bank Robberies https://www.sabric.co.za/media-and-news/press-release/saps-and-sabric-recommit-to-intensify-fight-against-bank-robberies/ (accessed on 20 February 2019).

274 De Koker 2007 *IEA* 35.

275 *Bogoshi and Another v Director: Office for Serious Economic Offences and others* 1995 (SCA) 543/93 3.

initially came in the form of the Serious Crimes Unit, which has since been repealed and replaced by the Directorate: Special Operations (DSO).[276] The DSO was formally known as the Scorpions. The DSO was tasked with the investigation of matters that fall outside the scope of the SAPS, but are high impact cases, which threaten national security and economic stability.[277]

As a branch of the NPA, the Directorate: Special Operations was established in terms of the NPA Act. In terms of its founding provision the Directorate: Special Operations has as its purpose to "combat corruption within the criminal justice system and serious economic crimes". This branch was able to fight crime proactively.[278] A member of the DSO has equal powers to those of a police official in the SAPS in terms of investigation of crimes and the powers of search and seizure of evidence.

3.7.3 Commercial branch of the SAPS

This branch has as its main objective to ensure the effective gathering, management, use and dissemination of the information on commercial crime, in order to meet the legal responsibility of the SAPS.[279] The task of this branch is to investigate fraud and other related crimes.[280] One of the problems identified by the commercial branch is that although modern technology offers benefits in regards to collection of evidence, this is also a hindrance due to the sensitive nature of such evidence that can be easily destroyed. The SAPS recognises the need for special skills in investigating commercial crimes and thus has groups within the unit that have the skills set required. The electronic group also deals with e-crimes.[281] Since its inception the commercial

276 Administration of Justice: Input for the SA yearbook 2003/2004 "Directorate: Special Operations. The DSA is committed to the investigation of matters that are national in scope, and concentrate on those crimes that threaten national security and economic stability" https://www.GCIS.co.za (accessed on the 19 January 2019).

277 Administration of Justice: Input for the SA yearbook 2003/2004 https://www.GCIS.co.za (accessed on the 19 January 2019).

278 Public Service Commission South Africa August 2001 "A review of South Africa's national anti-corruption agencies" https://www.psc.gov/za/documents/reports/corruption/03.pdf (accessed on 19 February 2019).

279 Public Service Commission South Africa August 2001 "A review of South Africa's national anti-corruption agencies https://www.psc.gov/za/documents/reports/corruption/03.pdf (accessed on 19 February 2019).

280 South African Government "The South African Police Service on Commercial branch success" https://www.gov.za/South-african-police-service-commercial-branch-success (accessed on the 19 February 2019).

281 South African Government "The South African Police Service on Commercial branch success" https://www.gov.za/South-african-police-service-commercial-branch-success (accessed on the 19 February 2019).

crimes branch identified problems and barriers to the fight against commercial crimes. These include lack of skilled and experienced personnel. The branch has to employ external personnel in order to assist with forensic accounting. There are also constraints in this regard, as there is insufficient technology in terms of both hard- and software for conducting investigations. This is a serious problem, especially where criminals are always using the latest technology and "know how" on computers to commit crimes.[282] Currently, the SAPS has established a branch to investigate priority crimes in South Africa known as the Hawks.[283] The Hawks were established in terms of section 17C of the SAPS Act.[284] The Hawks are responsible for combating, investigating and preventing priority crimes such as organised crime, commercial crime, and corruption.[285] The founding provisions for this is found in section 17B,

> The need to establish a Directorate [as a Division of] in the Service to prevent, combat and investigate national priority offences, in particular serious organised crime, serious commercial crime and serious corruption.[286]

3.7.4 South African Banking Risk Information Centre

The fight against crime is a collective battle with various stakeholders even though the police have a duty to prevent, combat and investigate crime.[287] The individual person has a responsibility to himself or herself to try to make sure that they do not fall victim or prey to criminal masterminds.[288] One such partnership is the South African government, and the South African Banking Risk Information Centre (SABRIC).[289] SABRIC reports on crimes that affect the commercial and financial sector and works closely with the SAPS. SABRIC has identified an increase in criminal activities in the use of technological devices such as the banking app, as well as online, and mobile

---

282 Public Service Commission South Africa August 2001 "A review of South Africa's national anti-corruption agencies https://www.psc.gov/za/documents/reports/corruption/03.pdf (accessed on 19 February 2019).

283 The South Africa Police Service "Directorate for priority crime investigation" https://www.saps.gov.za/dpco/index/php (accessed 26 February 2019).

284 Establishment and composition of Directorate for Priority Crime Investigation.

285 https://www.saps.gov.za/dpci/index.php (accessed on 26 February 2019).

286 s 17D of the SAPS Act.

287 s 205(3) of the Constitution.

288 "You wouldn't leave your house open, so you should be equally proactive with your devices" Kalyani Pillay SABRIC CEO. South African Banking Risk Information Centre "Sabric encourages consumers to take care of their cybersecurity" https://sabric.co.za/media-and-newsroom/press-release/sabric-encourages-bank-consumers-to-take-care-of-their-cyber-security (accessed on the 20 February 2019).

289 Hereinafter referred to as "SABRIC".

banking.[290] The organisation has noted that criminals use both their knowledge of technology and social engineering skills to con innocent and unsuspected victims to hand over information. This is also complicated by the fact that clients are not well versed in the workings of technological devices.[291] This has led to the SAPS and SABRIC working together to educate the public about the dangers of technology and being malformed consumers.[292] The establishment of this non-profit organisation is a step in the right direction for South Africa in its effort to fight cybercrime and bank related crimes. These partnerships are a positive move and are necessary to fight financial crimes.[293]

3.7.5 Business Against Crime in South Africa

The police constantly address the importance of strategic partnerships in the fight against commercial crime.[294] Much like SABRIC, the Businesses Against Crime (BAC) in South Africa[295] is one such partnership. The role of the BAC is to ensure that businesses adequately secure themselves and have sufficient preventative measures to fight cybercrime and partner up with government to share expertise and information.[296] The government has to invite the BAC in order for them to offer assistance and their skills in the fight against commercial crimes.[297]

3.8 Public Finance Management Act 1 of 1999

The PFMA is responsible for the regulation of financial management in the national government and provincial government. The objective of the PFMA is to "secure transparency, accountability and sound management" of State entities.[298] This is in line with the provisions of accountability and efficiency as envisaged in the

290 https://www.sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics (accessed on 20 February 2019).
291 https://www.sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics (accessed on 20 February 2019).
292 https://www.sabric.co.za/media-and-news/press-release/saps-and-sabric-recommit-to-intensify-fight-against-bank-robberied/ (accessed on 20 February 2019).
293 Cassim 2011 *CILSA* 131.
294 https://www.saps.gov.za/newsroom (accessed 27 February 2019).
295 Hereinafter referred to as the "BAC".
296 Businesses against Crime South Africa "Working towards a safe and secure South Africa: About us" https://www.bac.org.za/ (accessed 20 February 2019).
297 Businesses against Crime South Africa "Working towards a safe and secure South Africa: About us" https://www.bac.org.za/ (accessed 20 February 2019).
298 s 2 of the PFMA.

Constitution.[299] Public institutions must therefore ensure compliance with the PFMA in their use of public funds. The PFMA includes actions, whether intentional or negligent, that amount to misconduct in Chapter 10.[300] The PFMA itself does not criminalise financial misconduct by accountable institutions. Therefore, there would be an investigation once it has been established that there is misconduct. Such investigation would fall within the jurisdiction of the Hawks.

3.9 Commercial Crime Court

In South Africa, the DoJCD is primarily responsible for the administration of the courts. In terms of the Constitution, the judicial system consists of a hierarchy of courts, and courts that are established in terms of an Act of Parliament, including those with similar status to the High Court.[301] One such court is the Commercial Crimes Court. The Commercial Crimes Unit was established in 1999 under the NPA as part of one of the structures within the NPA to fight crime. The aim was to bring specialisation to the investigation and prosecution of commercial crimes.

The lack of a specialised court to deal with commercial criminal matters was identified as a major weakness in South Africa's fight against financial crimes.[302] The DoJCD thus took the initiative and introduced the commercial crimes court, which prosecutes serious economic infringements. The DoJCD is responsible for resources for the proper functioning of the criminal justice system.

The successful prosecution of financial crime in terms of common law or statutory provisions will carry a punishment in relation to the particular provision. The ECT Act contains penalties for those found to be in contravention of it. However, these do not seem too sufficiently address the severity of the impact of cybercrime on victims and

---

299 s 195(1) (b) "public administration must be governed by the democratic values and principles enshrined in the Constitution, including the following principles: efficient, economic and effective use of resources must be promoted." s 195(1) (g) "transparency must be fostered by providing the public with timely, accessible and accurate information".

300 Financial misconduct by officials in Department and Constitutional institutions. –(1) An accounting officer for a Department or Constitutional institution commits an act of financial misconduct if that accounting officer willfully or negligently –

(a) Fails to comply with a requirement of s 38, 38, 40, 41 or 42; or
(b) Makes or permits an unauthorised expenditure, an irregular expenditure or fruitless and wasteful expenditure.

(2) An official misconduct by treasury officials of a Department. Trading entity or a Constitutional institution to whom power or duty is assigned in terms of s 44 commits an act of financial misconduct if that official willfully or negligently fails to exercise that power or perform that duty.

301 s 166 of the Constitution.

302 De Koker 2007 *IEA* 36.

the economy of the country. Section 89 of the ECT Act calls for a person to be fined or imprisoned for a period not exceeding five years depending on the particular section they have contravened.[303] There needs to be harsher and more stringent penalties to deter cybercriminals.[304] The Cybercrimes Act, 2019 impose a maximum sentence of 15 years.

3.10 Summary

The object of the discussion in this chapter was crimes committed for financial gain. This chapter examined criminal activity where the main element is the misappropriation of funds. Though this research seeks to highlight the use of the computer to accelerate criminals committing this crime, it looks at this in a broader perspective rather than just discussing cybercrime. This is a means of committing a crime but it is not the only means of misappropriating money with the use of a computer.

There is no specific legislation that deals with crime for financial gain exclusively; even though the financial sector is highly legislated and regulated. This is not always beneficial as it places a burden on the financial sector rather than alleviates it. There is a need to put additional measures in place to fight the surge of crimes committed with a computer and other financial cybercrime.

An increase in financial crimes despite the financial sector being highly legislated and even having a specialised, indicates that there is insufficient measures in place to deal specifically with the problem of financial crimes. There must be a collective effort of the country to take the profit out of crime and ensure that people do not benefit from their illegal activities.[305] The following chapter discusses the law of evidence and provides a historical background of the law of evidence as captured by the SALRC.

---

303 According to s 89 of the ECT Act, (1) A person convicted of an offence referred to in s 37(3), 40(2), 58(2), 80(5), 82(2) or 86(1), (2) or (3) is liable to a fine or imprisonment for a period not exceeding 12 months. (2) A person convicted of an offence referred to in s 86(4) or (5) or s 87 is liable to a fine or imprisonment for a period not exceeding five years.

304 Cassim 2011 *CILSA* 128.

305 Kempen A "Taking the profit out of crime - the Asset Forfeiture Unit" https://www.npa.gov.za/sites/files/files/FAQs%20on%20AFU.pdf (accessed on 26 October 2016).

CHAPTER FOUR

ELECTRONIC EVIDENCE

4.1 Introduction

The law of evidence is not regulated, and this has posed many challenges. The SALRC issued a paper with the aim of combining its efforts to codify the law of evidence.[306] The immense issues relating to the law of evidence became noticeable. The rise of technology and electronic evidence presented its own more complex set of problems. The first recorded instance of electronic evidence is a case in which the determination of electronic print-outs were presented in court, and the court needed to make a decision whether they fell within the scope of evidence for court proceedings.[307] However, electronic evidence is not well established, and it is regarded as a new field.[308] There needed to be further calls and investigations for the introduction of electronic evidence in criminal proceedings.[309]

The use of electronic evidence was confined to computer printouts. Moreover, these needed to fit the definition provided in the CPA that largely refers to documents.[310] The process of regulating electronic evidence has been one of trial and error. In this research, electronic evidence will be discussed in regards to the element of search and seizure and how electronic evidence is presented in criminal proceedings in court.

Electronic evidence in criminal proceedings was regulated in terms of the Computer Evidence Act,[311] the CPA, the ECT Act and more recently the Cybercrimes Act, 2019. The nature of electronic evidence has been acknowledged as a difficult concept to grasp or master. The definition of electronic evidence needs to be discussed in-depth to provide a foundation for applying the relevant legal principles. The definition of a computer and data is constantly affected by developing technology. The process of search and seizure in regards to electronic evidence has become a double function

306 South African Law Reform Commission Issue Paper 27 (Project 126) "Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues" (2010) 3.

307 *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A) 155.

308 Bouwer 2014 *SACJ* (2) 156.

309 South African Law Reform Commission Issue Paper 27 (Project 126) "Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues" (2010) 20.

310 South African Law Reform Commission Issue Paper 27 (Project 126) "Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues" (2010) 18.

311 57 of 1983.

for investigators.[312] This research will examine two important aspects of electronic evidence. The first being how it is searched for and seized. The second is how it will be presented in court. The CPA determines the manner in which police may search and seize evidence.[313] There are no set rules to collecting electronic evidence. This chapter will establish what evidence is and more specifically, deal with what is electronic evidence. It will also look at what the courts have established in terms of the search and seizure of electronic evidence. The law is so behind in the area that we have still not even dealt decisively with the issue of electronic evidence. There is various legislation, institutions, and entities that regulate search and seizure of evidence; this is mainly dependent on the manner of evidence required. When there is a crime of a financial nature committed, there are even more laws and entities involved, again this would have to depend on the nature of the crime. Crimes of a financial nature need to be addressed expeditiously because they affect more than just the victim. They also affect the economy of the country. Therefore, it is necessary that the means to combat this is up to date and effective.

4.2 The law of evidence

Evidential material only become evidence once it is formally admitted, therefore prior to the court formally admitting in material as evidence it is only regarded as having potential of being evidence.[314] The law of evidence governs the proof of facts in a court of law.[315] The main function of the law of evidence is to determine what facts are "legally receivable".[316] It calls for the rules of evidence and governs the admissibility and evaluation of evidence.[317] In the South African law of evidence, there is primary and secondary evidence.[318] The principles to be discussed are relevance,[319] admissibility, and proof of facts, prejudicial effect, burden of proof, and evidentiary burden. There needs to be a distinction between burden of proof and evidentiary burden.

---

312 Bouwer 2014 *SACJ* 162.
313 s 20 of the CPA.
314 Bellengere A *et al The law of evidence in South Africa* (Oxford 2013) 3.
315 Schwikkard PJ and Van der Merwe SE *Principles of evidence* 4th ed (Juta).
316 Schwikkard *Principles of evidence* 4.
317 Bellengere *Law of evidence* 4.
318 Schwikkard *Principles of evidence* 23.
319 Bellengere *Law of evidence* 25"A piece of evidence is considered relevant if it might help prove or disprove the probable existence or non-existence of a fact in issue."

The information and material collected by the police during their investigation must be such that it would be presented in court. This evidence is presented to persuade the court of the facts in issue.[320] In the law of evidence, there are several important principles that are used, some are similar, and thus need to be discussed further, defined and distinguished. These will be discussed as a foundation for the rest of the research. The view amongst scholars is that

> Evidence must be relevant to the matter being investigated, to have value. It must have a direct bearing on the perpetrated crime, and a logical connection is presumed between the evidence discovered and the actual facts of the matter.[321]
>
> One party's duty to produce sufficient evidence for a judge to call on the other party to answer and it also encompasses the duty cast upon a litigant to adduce evidence in order to combat a prima facie case made by his opponent.[322]

This is the burden required to establish there is enough evidence to prove a case that the other party will have to answer. This is not equated with burden of proof that is essentially the standard of proof required to prove a case completely.

Evidentiary burden can also be defined as:

> The duty or burden that rests on a party at any particular point in a trial to lead enough evidence to force the other side to respond. [323]

In terms of criminal procedure, a burden rests on the prosecuting authority to prove beyond a reasonable doubt the accused person is guilty of the crime with which he has been charged. Burden of proof refers to "the obligation of a party to persuade the trier of facts by the end of the case of the truth of certain propositions."[324] The prosecutor is the one that carries this burden in terms of the Constitution[325] and in terms of the NPA Act.[326] To establish this burden the prosecutor presents its evidence that must establish guilt beyond a reasonable doubt. The accused person has a Constitutional right to answer and challenge such evidence.[327] Evidence is not necessarily proof, the court will still need to analyse evidence in order to establish

---

320 Bellengere *Law of evidence* 23.
321 Jordaan *Analysis of bank account statements* 25.
322 Schwikkard *Principles of evidence* 602.
323 Bellengere *Law of evidence* 36.
324 Schwikkard *Principles of evidence* 602.
325 s 35 of the Constitution.
326 s 2 of the NPA Act 32 of 1998.
327 s 35(3) (i) of the Constitution.

whether it provides proof of a fact.[328] When an inference may be drawn from the facts as to the existence of facts in dispute, this makes them relevant.[329] We therefore cannot say that evidence is in itself proof. Evidence is admitted and tested, and thus can be referred to as proof.[330] There needs to be a discussion regarding the terminology used for the purpose of electronic evidence in order to enable a further understanding of it. In South African law, the words digital and electronic are understood as synonymous.[331] Evidence is placed into different categories based on how it is presented in court. This forms the basis of how evidence is presented in court. The commonly recognised categories are real evidence, hearsay evidence and documentary evidence.

4.2.1 Real evidence

> Real evidence is an object, upon which proper identification becomes of itself, evidence. The party who wishes to produce real evidence for inspection by the court must call a witness who can identify the object. [332]

In *Mdlongwa v The State,* the court confirmed that video film and tape recordings are real evidence.[333] Real evidence is a thing or object that is presented in court and it is inspected to enable the court to make inference on the facts in issue.[334]

4.2.2 Hearsay evidence

The ECT Act in section 15 deals with admissibility of data messages. It is, however, noted that the courts have different interpretations of section 15. There is still no certainty regarding whether electronic evidence ought to be heard in terms of the ECT Act or in terms of the common law principle of hearsay. However, if it is that the evidence presented is to ascertain the contents of the evidence then the rules of hearsay evidence apply. The person who created the evidence would thus have to testify.[335] Section 3 of the Law of Evidence Amendment Act (LEAA) governs hearsay. The court recognises printouts where the credibility is dependent on the person giving

---

328 Schwikkard *Principles of evidence* 21.
329 Schwikkard *Principles of evidence* 52.
330 Bellengere *Law of evidence* 35.
331 Bouwer 2014 *SACJ* 158.
332 Schwikkard *Principles of evidence* 421.
333 *Mdlongwa v The State quoting judgment from S v Mpumlo and others* 1986 (3) SA 485 (E) 490 *H –I; Motata v Nair NO* 2009 (2) SA 575 (T) 21 "is real evidence, as distinct from documentary evidence, and, provided it is relevant, it may be produced as admissible evidence, subject of course to any dispute that may arise either as to its authenticity or the interpretation thereof".
334 Bellengere *Law of evidence* 65; Schwikkard *Principles of evidence* 421.
335 Papadopoulos *Cyberlaw* 324.

such evidence. This would therefore be admissible in terms of section 15(1) of the ECT Act.[336] It was determined that the use of electronic evidence in court proceedings and the provisions of the ECT Act do not seek to override the rules of section 3 of the LEAA, and as such the rules of the latter statute in regards to hearsay evidence apply. However, where the probative value does not depend on the credibility of a person, section 3 of the LEAA does apply. The Court found that section 3 gives it a discretion whether or not to admit certain evidence.[337] The court must evaluate such evidence and take into account all relevant factors to determine whether it is admissible in terms of the ECT Act.

4.2.3 Documentary evidence

When dealing with documentary evidence, it is important to note the purpose of which the documentary evidence is presented in court. It is either to prove the existence of the contents in the document, or to prove that the document itself exists.

The first instance is such that, when the object of presenting the document is to prove the contents, the material of the documents is immaterial. Therefore, whether it is a paper or a electronic printout it is documentary evidence. The electronic printouts then becomes a matter of real evidence as the object itself becomes the issue in the court proceedings.[338] In terms of the CPA, a document is defined as,

> The document is or forms part of a record relating to any trade or business and has been complied in the course of that trade or business, from information supplied, directly or indirectly, by persons who have or may reasonably be supposed to have personal knowledge or the matters dealt with in the information supplied.[339]

In order to be recognised as evidence, a document must be original, it must be authenticated, and be relevant.[340] The court recognises printouts where the credibility is dependent on the person giving such evidence. This would therefore be admissible

---

336 (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence
a. on the mere grounds that it is constituted by a data message; or
b. if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

337 *Ndlovu v Minister of Correctional Services and another* [2006] 4 All SA 165 (W) 174.

338 Bellengere *Law of evidence* 60.

339 s 221 of the CPA.

340 Schwikkard *Principles of evidence* 432.

in terms of section 15(1) of the ECT Act.[341] It was determined that the use of electronic evidence in court proceedings and the provisions of the ECT Act do not seek to override the rules of section 3 of the LEAA, and as such, the rules of the latter statute in regards to hearsay evidence apply. However, where the probative value does not depend on the credibility of a person, section 3 of the LEAA does apply. The court found that when evaluating evidence that might be seen as hearsay evidence against the principle of best evidence, section 3 provides for discretion as to whether or not it is admissible.[342]

4.3 Electronic Evidence

One of the central themes of this research is that technology has become a main feature in our everyday lives. We have turned to technology to communicate and transact, whether in business dealings or financial matters. Therefore, the computer has become a source of generating evidence of such communication and transaction.[343] For the purpose of this research, electronic record means evidence that is generated from a computer as a source. There is currently only one legislation regulating electronic evidence in South Africa that is the ECT Act.[344] The ECT Act is based on the UNCITRAL model law on electronic Commerce. It has been established that electronic evidence is not conventional, and therefore, that conventional laws are inadequate. This is especially the case in cybercrime, "in cybercrime cases, much of the evidence is digital – which means that it is not tangible evidence".[345]

The SALRC acknowledged that the codification of the law of evidence is too enormous a task, and therefore abundant it.[346] The courts have been reluctant when addressing the issue of evidence, and have been relying on common law rules to decipher electronic evidence. There is also reliance on scholarly writing and research on what is electronic evidence, such as Stephen Mason who defines electronic evidence as:

---

341 In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of data messages, in Evidence.
a. On the mere grounds that it is constituted by a data message; or
b. If it is the best evidence that the person adducing it could reasonably expected to obtain.

342 *Ndlovu v Minister of Correctional Services* 174.

343 Ndara *Computer seizure as technique in forensic investigation* 49.

344 Papadopoulos *Cyberlaw* 317.

345 Ndara *Computer seizure as technique in forensic investigation* 34.

346 South African Law Reform Commission Report (project 6) "Admissibility in Civil Proceedings of evidence generated by computers" (1986).

> Electronic evidence is data that is created, manipulated, stored or communicated by any device, computer system or transmitted over a communication system that is relevant to the process of adjudication.[347]

However, it is also pertinent to understand what is meant by the term electronic in order to fully comprehend the nature of the evidence, where

"The term electronic may be considered to be a generic term which encompasses all forms of data, whether produced by an analogue device or in digital form".[348] The use of electronic devices has increased and has subsequently changed the way we communicate.[349] This has a direct bearing on the rule of law. Even though it is acknowledged that the law of search and seizure concerning electronic evidence is lagging behind: "These changes with each technological advancement, the pace of which far outstrips the slow machinery of legal change".[350]

There needs to be a discussion regarding the terminology used in of electronic evidence in order to enable a further understanding of it. In South African law, the words digital and electronic are synonymous.[351] The definition of digital is:

> Any data stored or transmitted using a computer that support or refute a theory of how an offence occurred or that address critical elements of the offence such as intent and alibi.[352]

The research of electronic evidence requires there to be a definition of certain terminology in order to clearly grasp the terms without creating confusion. This includes distinguishing between electronic evidence and digital documents, "which [are] documents that exist in a format other than on paper".[353] Electronic is a useful shorthand to describe the nature of the medium.[354] Digital evidence information of probative value is stored or transmitted in binary form that may be relied on in court.[355] So far, the discussion has addressed the different elements in isolation to one another. At no point have we been able to conclusively link all these elements to adequately address the disparities that are lacking in dealing with the issue. The ECT Act is the

---

347 Mason S Electronic evidence Disclosure, Discovery and admission (LexisNexis 2007) 22.
348 Mason *Electronic evidence* 21.
349 Cassim 2014 *CILSA* 402.
350 Bellengere *Law of evidence* 73.
351 Bouwer 2014 *SACJ* 158.
352 Casey E *Digital evidence and computer crime: Forensic science, computers and the internet* 3rd ed (Elsevier 2010) 7.
353 Mason *Electronic evidence* 23.
354 Mason *Electronic evidence* 22.
355 Casey *Computer crime* 12.

closest and most recent piece of legislation to deal with electronic evidence. In terms of this Act, data messaging includes all forms of electronic material.[356] Electronic documents are documents that exist in a format other than paper.[357]

A common feature in defining electronic evidence is the inclusion of “data”. As with many of the terms used in relation to technology there is no one single definition. In terms of the Convention on Cybercrime Article 1 provides a definition for “computer data” that states,

> Any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

There are other definitions that are more technical,

> Computer data maybe broadly classified into binary data, where information is handled as a number represented in binary form, and text data, including alphanumeric punctuation data.

4.3.1 Admissibility

Admissibility is the key requirement to determining what is regarded as evidence.[358] Once evidence is admitted it will be tested and examined by the opposing party.[359] The Constitution protects the accused’s right to challenge evidence that forms part of the overall right to a fair trial.[360] The ECT Acts provides for the automatic admission of data messaging.[361]

There are varying decisions in regards to the admissibility of electronic evidence. Evidence is either admissible or not, and once it is admissible, it will be presented.[362] In a reported case, the Court noted there to be two types of electronic evidence, that is, evidence that is admissible and not subject to the rules of hearsay in terms of the LEAA,[363] which is evidence that was made without human intervention, this evidence is regarded as real evidence;[364] and electronic evidence that is subject to the rules of hearsay whose authenticity and accuracy will need to be collaborated by a witness

---

356 s 1 of the ECT Act, "data" means electronic representations of information in any form.
357 Mason *Electronic evidence* 21.
358 Bellengere *Law of evidence* 3.
359 Bellengere *Law of evidence* 23.
360 s 35(3) (i) “Every accused person has a right to a fair trial, which includes the right – to adduce and challenge evidence.
361 s 15(1) (a) of ECT Act.
362 Bellengere *Law of evidence* 25.
363 s 3 of the LEAA.
364 *S v Ndiki and others* 195.

testimony. [365] The Court only has a discretion in regards to the weight of the evidence.[366]

The Court also stated that there might be doubts cast on regarding the reliability of computer evidence being presented as real evidence that depends on the proper functioning of the operating system.[367] A discussion of admissibility is important for the purpose of this research, because in terms of the rules of evidence, evidentiary material becomes evidence in court once it has been admitted. It helps establish the fact that the current legislative framework is still not in line with technological advances. Evidence is either admissible or not admissible; there are no varying levels of degrees of admissibility.[368] The CPA in section 210 governs the admissibility of evidence:

> No evidence as to any fact, matter or thing shall be admissible which is irrelevant or immaterial and which cannot conduce to prove or disprove any point or fact at issue in criminal proceedings.

The courts also examines the relevance of the evidence as a factor in determining whether it is admissible.[369] All irrelevant evidence is inadmissible,[370] and it is thus important that the evidence be admissible in terms of the requirements of the courts. There are several factors that have to be considered when determining whether evidence is admissible, such as the fact that the prosecutor must prove its case beyond a reasonable doubt.[371] The Constitution makes provision for the protection of rights of the accused person; therefore, evidence that is unconstitutionally obtained is inadmissible.[372]

It also makes provision for the exclusion of evidence obtained unconstitutionally.[373]

---

365 *S v Ndiki and others* 189.
366 *S v Ndiki and others* 199.
367 *S v Ndiki and others* 191.
368 Schwikkard *Principles of evidence* 23.
369 Schwikkard *Principles of evidence* 23.
370 Schwikkard *Principles of evidence* 49.
371 These are important aspects to consider, but for the purpose of this research they will not be discussed in detail.
372 s 35(5) of the Constitution.
373 In regards to the exclusion of evidence, it is important to qualify when evidence may be excluded. It will only be excluded if
1. The admission of such evidence would render the trial unfair or
2. Be detrimental to the administration of justice. Thus, the evidence obtained unconstitutionally is not automatically excluded.

> Evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice. [374]

Therefore, the test is as to whether the admission of unconstitutionally obtained evidence would be detrimental to the administration of justice. The courts also look at the "prejudicial effect", what this essentially means is that evidence which even though may prove or disprove facts in dispute may be excluded if it will be prejudice the affected party.[375] The prejudicial effect of admitting evidence outweighs its probative value.

> In the pre-constitutional era, the courts generally admitted all evidence, irrespective of how it was obtained, if it was relevant. The only qualification was that the judge always (had) a discretion to disallow evidence if the strict rules of admissibility would operate unfairly against the accused" as where an accused was compelled to incriminate him or herself through a confession or otherwise. However, real evidence which was obtained by improper means was more readily admitted. The reason was that such evidence usually bore the hallmark of objective reality compared with narrative testimony that depends on the say so of a witness. Real evidence is an object which, upon proper identification, becomes, of itself, evidence (such as a knife, firearm, document or photograph or the metal box in this case). Thus, where such evidence was discovered as result of an involuntary admission by an accused, it would be allowed because of the circumstantial guarantee of its reliability and relevance to guilt the principal purpose of a criminal trial. As a rule, evidence relating to the "fruit of the poisonous tree" was not excluded.[376]

However, the exclusionary clause lies outside the scope of this dissertation. Admissibility should not be confused with weight. The weight of the evidence is determined once the court decides whether such evidence is admissible of not.[377]

The court establishes whether the burden of evidence has been set off by looking at the weight. There are several authorities governing evidence in South Africa, the most relevant being the CPA, which stipulates the provision of search and seizure for the purpose of obtaining evidence. The CPA was not enacted for collecting physical evidence and it could not foresee a future where documents would become obsolete

---

374 s 35(5) of The Constitution: "Evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice."

375 Schwikkard *Principles of evidence* 56.

376 *Mthembu v S* [2008] JOL 21609 (SCA) 10.

377 Schwikkard *Principles of evidence* 23.

and the world would be digital.[378] The nature of electronic evidence is complex, and requires specialised skills to collect and analyse it. Hearsay evidence occurs when the probative value of it depends on a person's credibility other than the person giving evidence.[379] The rule when it comes to hearsay evidence is that it is generally inadmissible.[380] This is due to the best evidence rule in which the original declarant must be called when adducing evidence. Hearsay evidence may also be seen to be in conflict with the Constitutional principles of the right to a fair trial; this is because an accused person cannot argue against this type of evidence. This thus goes against the principle is Section 35(3) (i) of the Constitution which is the right to challenge evidence in terms of the right to a fair trial.

> Every accused person has a right to a fair trial, which includes the right to challenge evidence as a component of the right to a fair trial.[381]

This same principle is also be found in other statutes including section 3 of the LEAA.[382] To illustrate,

> Documentary evidence is any written thing capable of being evidence and it does not matter what is written on it.[383] The CPA defines a document in section 221(5) as "any device by means of which information is recorded or stored".

Documentary evidence can either be admitted for proving what the document contains or whether its admission is to prove the facts in the document are true.[384] The requirements of documentary evidence are that it must be the original document that is produced in court and the document must be authenticated.[385] The determination of

---

378 Bouwer 2014 *SACJ* 157. "Criminal Procedure Act 51 of 1977 was enacted for application in a physical environment and for the seizure of tangible objects in a tangible world, and not for search and seizures in the virtual world of cyberspace."

379 s 3(4) of LEAA 45 of 1988.

380 Schwikkard *Principles of evidence* 287.

381 s 35(3) (i) of the Constitution.

382 (1) Subject to the provisions of any other law, hearsay evidence shall not be admitted as evidence at criminal or civil proceedings, unless -
(a) each party against whom the evidence is to be adduced agrees to the admission thereof as evidence at such proceedings; (b) the person upon whose credibility the probative value of such evidence depends, himself testifies at such proceedings; or (c) the Court, having regard to - (i) the nature of the proceedings; (ii) the nature of the evidence; (iii) the purpose for which the evidence is tendered; (iv) the probative value of the evidence; (v) the reason why the evidence not given by the person upon whose credibility the probative value of such evidence depends;
(vi) any prejudice to a party which the admission of such evidence might entail; and
(vii) any other factor which should in the opinion of the court be taken into account, is of the opinion that such evidence should be admitted in the interests of justice.

383 Schwikkard *Principles of evidence* 421.

384 Schwikkard *Principles of evidence* 437.

385 Schwikkard *Principles of evidence* 432.

how a document must be authenticated is, however, not clear. The CPA provides direction in regards to what constitutes proof of the document being an original.[386]

As was made clear in all the cases to which reference has been made, the present case and all cases similar to it which deal with the admissibility of evidence obtained by automatic machines, relates to the admissibility of the evidence concerned, not to the weight of such evidence.[387]

4.3.2 Originality

The law of evidence determines that for evidence to be admissible it must meet both general requirements of admissibility, as well as the requirements set for the admission of specific type of evidence.[388] The requirement of originality deals specifically with documentary evidence. There thus needs to be a discussion of these requirements due to the nature of how electronic evidence is mainly presented as computer printouts in court. The principle of this rule, though ancient, is attached to the best evidence rule,[389] and relates to the source of recording.[390] The ECT Act provides that electronic data should be admitted if it is found to be the best evidence even though it is not in its original form.[391]

The courts however also recognised that it is probable for there to be instances in which it is not possible to use the original document and thus there needs to be reliance on secondary document.[392] The admissibility of the latter depends on the circumstances of the case and what needs to be proven. The courts have stated that:

> the general rule of the law of evidence is that, when the purpose is to establish the terms of the writing, the writing itself must be produced but that secondary evidence may be given of the contents when the original has been destroyed, lost and proper search has been made for it.[393]

There has been different reactions by the courts to the provisions of section 15, where the courts have interpreted it to mean that electronic data should not be excluded due

386 s 233 of the CPA.
387 *Ex parte Rosch* [1998] 1 All SA 319 (W) 3.
388 Schwikkard *Principles of evidence* 432.
389 Schwikkard *Principles of evidence* 432.
390 Schwikkard *Principles of evidence* 432
391 s 15(1) (b) of the ECT Act.
392 *Ndlovu v Minister of Correctional Services* 171.
393 Schwikkard *Principles of evidence* 433.

to the format in which it is presented.[394] There has been different interpretations that require there to be an examination into the reliability of the computer or electronic device before it can be outright included or rather admitted as evidence in court proceedings.[395]

The ECT Act does make provision for instances in which there are laws that are unwavering of the requirement of originality. In terms of section 14, the information should remain intact and should be capable of being displayed and be presented in proceedings. There can be evidence that a data message has remained intact by providing an audit trail and showing how the company or person dealing with the evidence limits or restricts access.[396]

4.3.3 Authenticity

The Commission indicated that one of the hindrances and concerns relating to Electronic Evidence is "authenticity" and "admissibility".[397] This was due to the cumbersome nature of electronic evidence and ever-changing technology. This leads to courts having to use various legislation to deal with the issue of admissibility, such as the CPA, ECT Act and the LEAA. Electronic evidence is authenticated due to its "capacity to prove the digital object is what it purports to be".[398] The document must be authenticated.[399] A document can be authenticated in several different ways, by calling a witness, or a person who signs the document and can identify it.[400] The originality would appear to correspond with the original source of recording. Authenticity means tendering evidence of authorship or possession depending on the purpose for which it is tended.[401] These requirements clearly speak to evidence, which

394 Bellengere *Law of evidence* 76, "Some courts, for example *Ndlovu v Minister of Correctional Services and Another,* have, accordingly interpreted s 15 of the ECT Act as facilitating the admissibility of electronic evidence in that it disallows the rejection of such evidence merely on the basis that it is electronic evidence.

395 Bellengere *Law of evidence* 76*,* In *S v Ndiki* 188, the courts interpreted s 15 as distinguishing between two types of electronic evidence: first, evidence that depends solely upon the reliability and accuracy of the computer itself and its operating systems programs, which is real evidence. Second, computer recorded data, the probative value of which depends on someone who is not a witness in the proceedings.

396 Papadopoulos *Cyberlaw* 322.

397 South African Law Reform Commission Issue Paper 27 (Project 126) "Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues" (2010) 7.

398 Mason *Electronic evidence* 22.

399 Schwikkard *Principles of evidence* 432.

400 *Ndlovu v Minister of Correctional Services* 174.

401 Schwikkard *Principles of evidence* 434.

is in its physical form. There is no mention of how electronic evidence will meet these requirements. This would have to be investigated through an analysis of case law.

4.3.4 Conclusion

The common law provision is that "evidence that tends to prove or disprove an allegation which is in issue is admissible unless a specific ground for exclusion operates."[402]

When the courts are faced with the less conventional forms of evidence, there is a great deal of uncertainty, and they have to pronounce on whether or not such evidence may be admissible in court, taking into account all relevant factors relating to it. Electronic evidence is not conventional, and cannot simply be placed in a category like those already established in terms of the rules of evidence. Electronic evidence is not a fully established field, and it is still underdeveloped.[403] The use of computers has become the defining character of the modern world.[404] The use of electronic material is unavoidable.[405] Evidence in judicial proceedings is increasingly taking the form of electronic evidence.[406]

Electronic evidence is described as being unique because it is not physical in nature.[407] Thus, there would be a need for unique procedures in collecting and presenting electronic evidence. Currently, in regards to the principles of evidence, search and seizure is based mainly on the evidence being physical and tangible in nature.

4.4 Search and seizure of electronic evidence

The working of electronic evidence for the purpose of a criminal investigation is complex. It is seldom that a computer itself is the object of the search. It is the information that is contained within the computer that is the object of the search. Thus, this has created a scenario where investigators need to first seize a computer and subsequently access whatever information is stored on the computer.

---

402 *R v Trupedo* 1920 AD 58 62.
403 Bouwer 2014 *SACJ* 156.
404 Schwikkard *Principles of evidence* 437.
405 Schwikkard *Principles of evidence* 437.
406 Mason *Electronic evidence* 1.
407 Bouwer 2014 *SACJ* 157.

> The physical dynamics of search and seizure of electronic evidence differ from traditional search and seizure in that two seizures take place. Firstly, the seizure of the hardware, namely the computer or computer components, takes place and secondly, information is seized after the computer or computer components have been searched.[408]

It is important that the search of computers and or electronic items be clearly stated as that in a search warrant. It is insufficient that a warrant stipulates that the object of the search is for documents, but computers and electronic equipment are seized in that warrant. The court dismissed this as being common practice.[409] Even though there have been many developments including those relating to electronic evidence, there has been little development in the CPA of how non-conventional evidence is collected.[410]

4.4.1 Procedure in collecting electronic evidence

The search of evidence is confined to that of an object. This, however, is not enough to cover the scope of the search of and seizure of electronic evidence.[411] What is required in this regard is uniform procedure to regulate search and seizure of electronic evidence.[412] With electronic evidence, there is a split into two processes: the first process is to gather the physical component of the computer and the second is the analysis of the computer to obtain information for getting information for investigation.[413]

The fact that search and seizure is now a two-step process necessitates a different approach to the wording of a warrant.[414] The sensitivity of electronic evidence is such that it must be handled with care and skill. Electronic evidence would need to be collected by forensic investigators.[415] Law enforcement agencies need to have a formal and correct way of collecting evidence. A failure of justice due to lack of proper procedures would lead to a state of lawlessness in which criminals perceive

---

408 Bouwer 2014 *SACJ* 156.

409 By no stretch of the imagination could all the computer hardware, software and "peripheral" mentioned in Annexure "A" to the Mowbray and Table View search warrants be classified as "documentation". *Beheermaatschappij v Magistrate, Cape Town* 37.

410 Bouwer GP "Search and Seizure of electronic evidence: Division of traditional one-step process into a new two-step process in a South African context" 2014 *SACJ* 157.

411 *Beheermaatschappij v Magistrate, Cape Town* 39.

412 South African Law Reform Commission Discussion paper 131 (Project 126) "The review of evidence" (2015) 63.

413 Bouwer 2014 *SACJ* 158.

414 Bouwer 2014 *SACJ* 166.

415 Mason *Electronic evidence* 484.

themselves as untouchable.[416] The nature of electronic evidence is such that it is essential that the collection of electronic evidence must be regulated and there must be procedural laws to identify what needs to be done in investigations.[417]

4.5 South African Law Reform Commission

The SALRC is established by an Act of Parliament.[418] The SALRC acts as an advisory body to the Minister of Justice.[419] Its objectives are set out in the SALRC Act and these include the investigating of branches of the law to make recommendations for the "development, modification or reform of the law".[420] The powers and duties of the Commission are such that they include the drawing of a draft legislation after investigations are concluded that this is necessary for reform.[421] The Minister of Justice must approve programmes of interest for the purpose of consideration by the SALRC.[422] One of the core competencies of the Commission is to conduct research for investigation of "the existing legal position and to identify shortcomings or deficiencies that needs to be rectified".[423]

The first step in the process is a compilation of an issue paper. An issue paper outlines the problem identified and a particular branch of law and therefore clarifies the aim of an investigation.[424] An issue paper was published for public comment and suggestion in the investigation of the Law of Evidence. The project investigated by the SALRC was identified as Issue Paper 27 Project 126 "Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues" 2010. This project is a long-standing

---

416 Myburgh DC *Developing a framework for the search and seizure of digital evidence forensic investigators in South Africa* (MCom in Forensic Accountancy North - West University 2016) 5.

417 Goodman 2002 *IJLIT* 142.

418 South African Law Reform Commission Act 29 of 1973 (SALRC Act).

419 s 1 of the SALRC Act.

420 s 4 of the SALRC Act.
The objects of the Commission shall be to do research with reference to all the branches of the law of the Republic and to research and to investigate all such branches of the law in order to make recommendations for the development, improvement, modernisation or reform thereof, including–
(a) The repeal of obsolete or unnecessary provisions;
(b) The removal of anomalies;
(c) The bringing about of uniformity in the law in force in the various parts of the Republic;
(d) The consolidation or codification of any branch of the law; and
(e) Steps aimed at making the common law more readily available.

421 s 5(5) of the SALRC Act.

422 s 5(2) of the SALRC Act.

423 The South African Law Reform Commission "Objects" https://www.justice.gov.za/salrc/objects.htm (accessed on 1 May 2019).

424 The South African Law Reform Commission "SALRC Objects, Constitution and Function" https://www.justice.gov.za.salrc/objects.htm (accessed on 1 May 2019).

matter. The Report to the project as officially released as “Review of the Law of Evidence” 2019.

The finalisation of an issue paper leads to a discussion paper. A discussion paper is for informing the public of the background and the Commission’s intention. Project 126 has several discussion papers that relate to the investigation of The Law of evidence, including Discussion Paper 113 Project 126 “Review of the Law of Evidence: Hearsay and Relevance” 2008. Project 126 issue paper was established with the view of codifying the South African law of Evidence.[425] However, the Commission realised the magnitude of this undertaking and that it was too immense a task. This task therefore was subsequently abandoned.[426]

The SALRC had embarked on investigating several issues relating to evidence.[427] However, it later recognised that it was more beneficial to merge project 126 and project 113, the initial intention for the project was to codify the law of evidence. This was in line with the view that it would be more expedient to look at electronic evidence in its entirety. The Commission would thus look at technological developments holistically rather than in segments. Therefore, the project would look at the procedural aspects of collecting evidence, presenting it in court and storing it.[428]

A significant point put forward by the Commission in project 126 was, whether technology-related evidentiary questions can be sufficiently dealt with under existing rules of evidence and procedure. [429]

The Commission finally released the report on project 126.[430] This report chronicles the journey taken by the SALRC in its effort to bring effective change to the law of evidence. One of the outcomes of this is the need to review the ECT Act on an urgent basis. The ECT Act has many provisions that are not implemented and others that are obsolete. A revision of the ECT Act revealed concerns of how emerging technology

---

425 South African Law Reform Commission Issue Report, Project 126 “Review of the Law of Evidence” 2019 1.

426 South African Law Reform Commission Issue Paper 27 (Project 126) “Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues” (2010) 3.

427 South African Law Reform Commission Report (Project) 113 “The Use of Electronic Equipment in Court Proceedings (Postponement of Criminal Cases via audiovisual link)” (2003) 1.

428 South African Law Reform Commission Issue Paper 27 (Project 126) “Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues” (2010) 4.

429 South African Law Reform Commission Issue Paper 27 (Project 126) “Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues” (2010) 5.

430 South African Law Reform Commission Report, Project 126 Review of the law of evidence.

poses a challenge to existing legal concepts that are inadequate to deal with the advances.[431]

4.6 Case law

The courts have developed case law relating to electronic evidence since the first case of *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A). The purpose of discussing this case was not to highlight the reasons the court put forward in its judgment as to the admissibility of the electronic printouts. [432] In *Narlis*, the evidence presented in court was not merely produced by a computer but there was human intervention. The nature of the evidence was such that there was no accountability or any means of safeguarding the accuracy of the information being entered in the computer. The manager who was providing evidence on behalf of the respondent was unable to provide conclusive evidence of the accuracy of the records, as he did not compile them personally.[433] The object was to establish the historical strides made in regards to the admission of electronic evidence and whether or not there has been significant development in this regard. This is still a moot point, as the courts remain undecided about the correctness of this case and there are different judgments.

It is important to note that evidence in a form other than the traditional forms of evidence or conventional evidence is still privy to the same rules. Thus, a discussion of the law of evidence in general preceding a discussion of the law of evidence is important. There are varying decisions on how to apply the various law regulating electronic evidence. The courts have determined that the ECT Act governs electronic evidence.[434] However, the courts are undecided regarding the interpretation of the specific provisions relating to electronic evidence. There are contradicting judgments and the courts have not dealt decisively with the matter.

When determining admissibility of evidence in court, the court needs to determine whether electronic evidence is real evidence or hearsay evidence. Prior to the ECT Act, reference to electronic evidence was mainly for computer-generated documents.

---

431 South African Law Reform Commission Issue Paper 27 (Project 126) "Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues" (2010) 28.

432 *Narlis v South African Bank of Athens* 158. "To sum up in the present case, the respondent, suing the appellant for R2 000 on a deed of suretyship, failed to prove that the alleged principal debtor owed the bank any money as at the date averred in the summons a matter which was put in issue in the pleadings".

433 *Narlis v South African Bank of Athens* 156.

434 *Ndlovu v Minister of correctional services* 177.

Therefore, the courts used the Computer Evidence Act to deal with electronic evidence.[435] In *Ex parte Rosch*,[436] the court had to deal with the admissibility of computer-generated printouts from a telephone company. It was established during the proceedings that these were records that were made by a computer and that there was no human intervention. The Court determined that firstly, the law regarding hearsay was not applicable as there was no human input and thus "no room for dishonesty or human error".[437] The court went on to state that section 3(4) of the LEAA does not apply.

In *Ndlovu v Minister of correctional services*, the court had to make a determination on the admissibility of printouts of electronic evidence.[438] A summary of the facts of the case are that the plaintiff was convicted on robbery and subsequently released on parole. During his parole, the plaintiff was arrested on another charge. While in prison, he was detained stating that he had violated his parole. The plaintiff was claiming damages for his unlawful detention. The defendant relied on computer print-outs as evidence that the plaintiff had violated his parole and thus his detention was lawful as he was serving out the reminder of his sentence. The court had to first deal with the evidentiary matter. The plaintiff contended that the printouts were not originals and the best evidence rule was not placed before the court.[439]

The Court determined that in the particular case no allegation was made regarding the original being different to the copy, should this have been the case then the original should have been presented to the Court.[440] It mentioned that it was also common practice that parties included copies in the court bundle. This was, however, subject to the other party lodging an objection. The plaintiff in this regard tacitly waived having the originals presented in court, and therefore could not argue this point during the trial.[441]

The Court first dealt with admissibility in terms of section 15 of the ECT Act. The Court clarified that section 15(1) includes evidence without further scrutiny; it further stated that electronic evidence is not seen to be more prevalent than an ordinary

435 Computer Evidence Act 57 of 1983.
436 [1998] 1 All SA (W).
437 *Ex parte Rosch* [1998] 1 All SA (W) 321.
438 [2006] 4 All SA 165 (W).
439 *Ndlovu v Minister of Correctional Services* 171.
440 *Ndlovu v Minister of Correctional Services* 171.
441 *Ndlovu v Minister of Correctional Services* 171.

document.[442] The Court made a determination that in regard to computer printouts, section 15 of the ECT Act is relevant.[443] When dealing with evidence, three important rules of evidence must be mentioned. These include the relevance of the evidence, its authenticity, and the originality. Section 15(1) does not preclude these important rules from electronic evidence. It "must be relevant and otherwise admissible, be proved to be authentic and the original must be produced".[444] Evidence is admissible when it was made in the course of ordinary business or when an authorised person certifies a copy as being correct.[445] The Courts came to a different conclusion regarding electronic evidence, where it said that computer documents are not synonymous with being documents for the purpose of evidence. This case demonstrated the fact there is insufficient legislation dealing with electronic evidence. The court called for a *lacunae* in our law to be filled and for new legislation relating specifically to computer evidence in criminal cases to be considered and promulgated.[446] The Court relied on common law to deal with the admission of electronic evidence as computer printouts. It held that "in terms of the prevailing law, it could not admit the disputed documents which contained information that has been processed and generated by a computer into evidence."

4.7 Academic opinion in the international community

The Constitution of the Republic recognises that there is a need to recognise international laws and the contributions they make in our legal system. The

---

442 *Ndlovu v Minister of Correctional Services* 172.

443 (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence.
a. on the mere grounds that it is constituted by a data message; or
b. if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.
(2) Information in the form of a data message must be given due evidential weight.
(3) In assessing the evidential weight of a data message, regard must be had to.
a. the reliability of the manner in which the data message was generated, stored or communicated;
b. the reliability of the manner in which the integrity of the data message was maintained;
c. the manner in which its originator was identified; and
d. any other relevant factor.
(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

444 *Ndlovu v Minister of Correctional Services* 172.

445 *Ndlovu v Minister of Correctional Services* 173.

446 *S v Mashiyi and another* [2002] JOL 9894 (Tk) 18.

interpretation clause requires that the Constitution be interpreted in such a manner that it must consider internal law.[447]

One of the biggest challenges that emanates from electronic evidence is the issue of jurisdiction. Electronic information that constitutes an offence may be saved in a different server or remote location, or cloud that is far from the actual location of the author.[448] At an international level, there is a lack of interest in a Convention dealing with electronic evidence due to its complexity and various components.[449]

There is a consensus within the international community that the judicial and legal community are very slow in adapting to the vastly progressive change that is brought about by technological advancement. The vast use of technology in criminal-related activities, require the courts and judicial system to recognise the need to move in the same direction. This scepticism is not without merit. The use of computers is technical in nature, and a thorough understanding of the law is required. A computer admitted as electronic evidence in Court must be scrutinised, and the use of computers in court as evidence also raises questions of its reliability, authenticity, and originality.[450]

A computer has the potential to carry volumes of information depending on the nature of the storage. The submission of digital evidence can be overwhelming to a trial attorney. It is more advisable to have a computer forensic expert collect information for preserving it as evidence in court proceeding. This will also mean that a forensic investigator will have to be used as an expert in court when the computer or digital evidence is presented.[451]

---

447 s 39(1) (b) When interpreting the Bill of Rights, a court, tribunal or forum – must consider international law.

448 Bellengere *Law of evidence* 78.

449 Stephen Mason "A convention on electronic evidence: helping to provide for certainty in international trade" http://www.uncitral.org.pdf/english/congress/Papers_for_Congress/38-MASON-A_Convention_on_Electronic_Evidence.pdf (accessed on 13 November 2018).

450 Mason S "Electronic Evidence: A proposal to reform the presumption of reliability and hearsay" https://www.sciencedirect.com/science/article/pii/S0267364913002057 (accessed on 12 April 2019).

451 Luehr PH "Real evidence, virtual crimes - the Role of Computer Forensic Experts" *20 Crim.* Just (2005) 17.

4.8 Summary

It needs to be noted that technological advances and the new era of information technology do not take away from the pre-determined and pre-established rules of evidence that have been tried and tested in our courts.

> In dealing with computer evidence it must be recognised that computers are not infallible and that the dangers inherent in this type of evidence must be acknowledged and the necessary safeguards put into place.[452]

There is no statute regulating the law of evidence, and the courts have thus been dealt with it on a case-by-case basis. The first project by the SALRC commenced regarding the review of the law of evidence commenced in 1973. Since the inception of this project, there has been minimal progress made regarding the regulating evidence, especially electronic evidence. There has been many developments in technology and increase in the commission of crime using the computer. The ECT Act was enacted after recommendation by the SALRC. However, the Act is the brainchild of the Department of Communication. It is documented that the DoJCD had little influence with regard to the ECT Act.[453] The ECT Act is currently the leading Act in regulating the admissibility of electronic evidence in the court of law. The courts have still not settled the admission in terms of section 15 of the ECT Act and deal with such evidence on a case-by-case basis. The Cybercrimes Act, 2019 is noted as having the effect of drastically changing and amending the ECT Act. However, this Act has not been passed in Parliament. The current principles of the law of evidence are still considered, such as the rules governing hearsay in terms of the LEAA. The collection of evidence is primarily for the presentation of it in court in order to establish a *prima facia* case for proving guilt. With the advancement of technology, it cannot be accepted electronic evidence be reduced to computer printouts. As argued here, the rules of evidence need to be updated to ensure that they are in line with emerging technology and the fight against crime.

---

452 *S v Ndiki and others* 200.

453 Mason *Electronic evidence* 460.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

The CPA is the leading legislation in regards to “provisions for procedures and related matters in criminal proceedings”.[454] It details matters of how the search for and seizure of objects may be done for the process of pre-trial investigations. Therefore it needs to be the main legislation relied upon by all investigators in regards to search and seizure.

Chapter 2 of this research establishes the following important points, firstly, the parameters of the investigation of a crime, including requirements set out by statute and the courts. This was done by examining the CPA, as the leading legislation regarding investigation of crimes. It further demonstrates the various laws that deal with search and seizure and the different investigating bodies. A discussion of these institutions indicated a lack of cohesion that has caused more of a barrier to the fight against financial crime.

In 2.2.3 above search and seizure was discussed as a tool in criminal investigation. The courts require, a clearly defined warrant in order for the process of search and seizure to be valid. The right to privacy is a constitutionally guaranteed fundamental right. Requirements for a valid search warrant are there to ensure a limit of police powers. Therefore, the provisions of search and seizure must be in line with the Constitution and the limitations set by it. The Constitution also provides consequences for illegal search which is beyond the scope of this research.

There is no clear definition for electronic evidence. The consequence is the inability of lawmakers to sufficiently regulate the search for electronic evidence. This is further complicated by electronic evidence relating to financial crime. Chapter 3 establishes that there is a vacuum, which has a direct bearing on the progress of combating crime. 2.1 above demonstrates that there has been no developments in the CPA regulating search and seizure in light of emerging technological advances. The summary in chapter 4 concluded that electronic evidence in South Africa is still making slow strides. This is despite the fact that the SALRC had a Project 126. Project 126 was

454 Preamble to the CPA.

initiated shortly after the establishment of the SALRC, and was only concluded in 2019, this is not a positive step. The issue of addressing technological advances, cybercrime, financial crime and the law of evidence has proven to be an elusive, enigmatic and cumbersome task.

The research aim and hypothesis seek to show the flagrant, glaring need to address the issue of developments in search and seizure of electronic evidence relating to financial crimes. In light of the stringent requirements of search and seizure and the consequences of invalid warrants, the importance of legislation, which is up to date, is important. Particularly important for this research is establishing recommendations regarding legislative reform of search and search.

5.2 Conclusion

A key requirement for a search warrant, which is also pinnacle to an investigation is identifying an object. Both the collection of computer and online evidence poses a problem in that it is not readily or easily identifiable. What is most apparent from this research is that new technology has resulted in new ways of committing crime. Therefore, the fight to combat crime must move at the same pace as criminal activity and behaviour.

The ECT Act demonstrates that South Africa has made notable strides in regulating computer evidence. It is recognised that there is a two-part element in the search and seizure of electronic evidence. A computer is a physical component and the information in it is intangible data.[455] The ECT Act tried to remedy the gap between the CPA's requirement of an object and the new form of an object in an electronic form,

> For purposes of this Act, any reference in the Criminal Procedure Act, 1977, to "premises" and "article" includes an information system as well as data messages.[456]

In determining whether the ECT Act did in fact provide a remedy, two things will be evaluated against this section. The first is the court's interpretation of a search warrant and the effect of the Cybercrimes Act, 2019 on the provisions of the ECT Act. The courts have always considered that a search warrant must be

455 Papadopoulos *Cyberlaw* 328.
456 s 82(4) of the ECT Act.

interpreted with “reasonable strictness” and that in determining the object of the search articles to be seized must be in line with the articles described in a search warrant.[457]

The principle of “reasonable strictness” has been further monitored by a constitutional democracy. In view of Constitutionality, a warrant must also be interpreted and carried out in light of an individual’s constitutional rights.[458] The courts are strict regarding what objects maybe seized in terms of a search warrant. This is because of the ease that came with evidence that was tangible and readily identifiable. However, in cases of electronic evidence the question is whether the term “data” proves sufficient. A computer as a physical component would be described effortlessly in a search warrant. The information in a computer would prove to be laborious. The courts interpret a search warrant with reasonable strictness even relating to electronic evidence.

> The search warrant authorises only a search for, and seizure of, “documentation”. On the authorities which I have mentioned above, it must be construed with reasonable strictness and, ordinarily, in terms in which it is expressed. By no stretch of the imagination could all the computer hardware, software and “peripherals” mentioned in annexure “A” to the Mowbray and Table View search warrants be classified as “documents”.[459]

The Cybercrimes Act, 2019 stipulates that for the purpose of the Act, an object maybe seized under a search warrant.[460] The court must ensure that the object searched for and seized is or on reasonable grounds believed to offer assistance in proving the commission of a crime.[461] Another important requirement for a search warrant, which specifically requires the searcher to be identified, the person who carries the off-site search of the information and computer data must be identified. It would need to be clearly stated whether investigation would be conducted by an investigator as defined in the Cybercrimes Act, 2019 or the SAPS.

The provisions in 3.4 is an indication that there is guidance from the international community regarding legislation dealing with computer and cybercrime. Despite the

---

457 *National Union of South African Students v Divisional Commissioner, South African Police, Cape Western Division and Others* 626.

458 *The Investigating Directorate: Serious Economic Offences v Hyundai Motors Distributors (Pty) Ltd v Smith* 40.

459 *Beheermaatschappij v Magistrate, Cape Town* 37.

460 s 29(2) (g) of the Cybercrimes Act, 2019.

461 Basdeo 2009 *PER* 316.

global rise of computer and cybercrime there are no adequate laws.[462] Currently there is a reliance on judicial interpretation. The SALRC made concessions regarding the *status quo* of electronic evidence and the CPA. It was found that the CPA was not enacted during a time where an object that was intangible was inconceivable.[463]

3.2 above included a discussion on the importance of differentiating between computer and cybercrime. This will allow legislative reform that addresses both aspects. The Cybercrimes Act, 2019 provides substantial and procedural aspects in terms of cybercrime. However, there needs to be procedural reform relating to both cybercrime and computer crime.

In 3.3 above it was highlighted that financial crime does not necessarily have a single definition. However the elements of misappropriation seems an apt start. Therefore, the electronic evidence collected needs to provide evidence of a financial crime. What was significantly highlighted was that financial crimes affects everyone and can be committed against anyone. Such crimes have a negative effect on the economy regardless of the victim.

The crux of this research is not merely to identify a gap in the procedural process of the fight against crime but includes the prosecution and conviction, which might lead to a deterrent of such further criminal activity. Thus, the law must be cognizant of this important component. There must be a welding and integration of process rather than a mere adoption as a means of removing an item off a checklist.

The SAPS needs to align itself with emerging techniques and skills set in investigations. When it comes to the investigation and subsequent search and seizure of electronic evidence in financial crimes there needs to be different skills set. Experts will therefore need to be utilised at every stage of the investigation including search and seizure. This is not sufficient, the sensitivity of electronic evidence and financial crime require that any and every one dealing with them be knowledgeable.

---

462 Cassim 2011 *CILSA* 137.

463 South African Law Reform Commission Discussion Paper 99 (Project 108) “Computer related crime: Preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects” (2001) 14.

5.3 Recommendations

The discussion in chapters 2 and 3 indicate that the investigation of financial crime for electronic evidence requires different layers. The SAPS must be established as the main investigative body in regards to all crimes including computer and cybercrime. This must be done by improving the legal framework in regards to the fight and combating of crime.[464] The legislative framework in the form of the CPA.

There is a need for a structural guideline regarding investigations. The best starting point would be to amend the Section 1 of the CPA and update the list of definitions to include terminology used in electronic evidence and technology.

The CPA must be amended to create two specific provisions, these include providing definitions and making provisions to have mandatory guidelines for the search and seizure of electronic evidence. This can be done by examining the guidelines from the international community, which as a whole is affected by cybercrime. The borderless nature of cybercrime is such that a victim can be far from a perpetrator.[465] The convention on cybercrime does not limit efforts to fight and combat cybercrime to legislation but indicates that there may be "other measures".

The Cybercrimes Act, 2019 is commendable in that it provides definition in both section 1 of the Act as well as the provision in section 25 dealing with powers to investigate. The CPA would benefit by providing definitions in regards to search and seizure.

These definitions would need to be aligned with the requirements of a valid search warrant. The courts discussed the requirements and summarised them as follows, a warrant must indicate the statutory provision in terms of which it is issued, who is conducting the search, and authority conferred on the search, identifies the person, container or premises searched and describes the article with sufficient particularity and specific offence.

For the CPA to be effective, substantive and procedural law must be aligned. Amending the CPA would require providing the following definitions:

---

464 The NCPF 11.

465 Interpol "Cybercrimes" https://www.interpol.int/en/crimes/cybercrimes (accessed on 20 June 2020).

- “Access”: includes without limitation to make use of data, a computer program, a computer data storage medium or a computer system or their accessories or components or any part thereof or any ancillary device or component to the extent necessary to search for and seize an article.
- “Article”: any data, computer devices, computer networks, databases, critical databases, electronic communication networks or national critical information infrastructures or any part thereof or any other information, instruments, devices or equipment.
- “Computer”: a functional programmable unit that consists of one of more associated processing units and peripheral equipment, that is controlled by internally stored programs, and that can perform substantial computations, including numerous arithmetic operations, or logic operations, without human intervention.[466]
- “Cybercrime”: illegal act, the commission of which involves the use of information and communication technology.[467]
- “Data” electronic representations of information in any form.

There needs to be cohesion in regards to particular provisions between the relevant legislative provisions.

The SAPS as a single unit would not be able to investigate computer and cybercrime. There is considerable effort made by the international community to ensure that there is mutual cooperation and mutual assistance relating to the fight and combating of cybercrime. The same co-operation and mutual assistance must be established between the different institutions within South Africa. The CPA would therefore provide for the co-operation as the central legislative framework for investigations. Chapter 6 of the Cybercrimes Act, 2019 makes provision for “point of contact”, this will assist in providing direction regarding how the three elements are merged for investigation. In terms of section 4 of the Cybercrimes Act, 2019

> (4) The Cabinet member responsible for policing may make regulations to further—
> *(a)* regulate any aspect provided for in subsection (3);

466 Mason *Electronic evidence* 1. “Computer is a programmable electronic machine for processing information”.

467 The NCPF 9. Illegal acts, the commission of which involves the use of information and communication technologies.

(b) impose additional duties on the designated Point of Contact; and
(c) regulate any aspect which is necessary or expedient for the proper implementation of this section.

There is a need for uniformity in the process of collecting evidence, especially electronic evidence relating to financial crimes. A central point of assistance within the SAPS needs to be established, in which everyone has access to it including individuals, private entities and public institutions. The central point will operate within the SAPS and investigate all financial crimes and not just a hand full that are deemed important. There needs to be a national instruction on the assignment of personal by the SAPS. An official document must be published, which lists all State investigating units and institutions. The document must include information relating to capacity, skill and relevant statute governing their powers to investigate. This will allow the Minister of Police to consolidate all the information and to determine how to establish a Unit that will fight and combat computer and cybercrime using resourcing and skill that is available.

- The Department of Police is tasked with primary investigations of crime. The department recognises the importance of cooperation between investigating units within the department, public-private partnerships, the private sector and the international community.
- The Department of Police in the form of the SAPS will establish a single “Computer and Cybercrime Unit”. This unit will dissolve and merge all cybercrime units within the department.
- This Unit will include experts in the field of computer and cybercrime. These include but not limited to;
    (a). Police officers with relevant qualification.
    (b). Forensic investigators who specialise in computer and cybercrime
    (c). Lawyers with specialisation in computer and cybercrime and relevant knowledge in policy drafting
- The Department of Police will release regulation relating to the investigation of computer and cybercrime. Including guidelines for cooperation relating to all relevant stakeholders.

In terms of the NCPF the DOJ&CD and the NPA are responsibility of prosecution of cybercrime.[468] It has tabled a line of responsibility within state institutions in the fight against cybercrime,

> The department of Police and the SAPS shall, in terms of the NCPF, be responsible for the prevention, investigation and combating of cybercrime in the Republic, which includes the development of cybercrime policies and strategies, and providing for specialised investigative capacity and interaction with national and international stakeholders.

There are significant recommendations that are made by the SALRC in regards to electronic evidence and this includes a single statute to regulate electronic evidence; interaction between relevant statutes and a less fragmented approach; handbook or guide on producing electronic evidence and the adoption of several definitions.[469]

The Unit will be established in terms of the procedural guidelines of the CPA. Its function and responsibilities will be as defined,[470]

> Functions and responsibilities may include all or a combination of:
> - investigations;
> - collection of data and forensic analysis;
> - intelligence collection, analysis and dissemination;
> - assessment and analysis of cybercrime phenomena;
> - contribution to drafting national legislation on cybercrime;
> - contribution to defining national cybercrime strategy;
> - coordination of regional/territorial units;
> - specialised support to other police units;
> - cooperation with the private sector;
> - international cooperation;
> - prevention;
> - defining internal procedures;
> - training programmes and
> - development of national reporting systems.

There needs to be penalties that will serve as a deterrent for those who want to commit such crimes. The forfeiture of assets that are ill-gotten must be pursued aggressively in order to take the profit out of crime. This would serve as a deterrent for criminals.[471]

---

468 The NCPF 26.

469 South African Law Reform Commission Issue Paper 27 (Project 126) "Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues" (2010) 77.

470 Council of Europe "Cybercrime@IPA specialised cybercrime unit - good practice study" www.coe.int/cybercrime (accessed on 01 July 2020).

471 *Mkhize v S* [2012] JOL 29750 (KZP) 8.

Therefore in this regard as part of the procedural guidelines for collecting evidence, the AFU needs to be part of the investigation of financial crime, this will be done in their capacity to trace proceeds of unlawfully obtained funds. The significance of heavy penalties is that they must deter criminals. In its report, the SALRC recommended that

> It has been noted that to have the greatest impact, legislation of this type must be future-proof and take into account the needs of society it serves.[472]

This is important in an emerging country such as South Africa. It is insufficient to have a criminal justice system that is constantly reacting. Most countries have or are in the process of building cyber capacity to come to terms with the sudden surge of cybercrime.[473]

There needs to be a move in which the prosecution of criminal activity is seen as a deterrent for any other possible criminal activity.[474] The motive behind financial crimes is the profits. One of the means of combating such crimes is to remove the profit from it. South Africa has made an attempt of eradicating the profit of criminal activating by establishing the AFU. However, this unit is an external body to the SAPS and it has to rely on the assistance of the SAPS to perform its functions fully.

> In today's environment, crimes generate huge profits, and one strategy that has been adopted to combat criminal activity is to eliminate the profits. However, to do that, investigators should be able to not only locate these profits, but also show that they are the possible proceeds of criminal activity.[475]

The world witnessed the detrimental effect of countries not legislating cybercrime, which meant that a perpetrator could not be extradited and subsequently prosecuted by for their crime.[476]

---

472 South African Law Reform Commission Issue Paper 27 (Project 126) "Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues" (2010) 10.

473 Memorandum on the objects of the Cybercrimes Bill 63.

474 Snyman *Criminal law* 15.

475 Jordaan *Analysis of bank account statements* 15.

476 Goodman 2002 *IJLIT* 142. One of the most famous cases is one referred to as the "Love Bug". In 2011, a Philippine national realised a virus that spread around the world causing havoc. The virus went as far as affecting the NASA and the CIA. However, the Philippine national could not be extradited to the USA for prosecution. This was because cybercrime was not legislated in the Philippines.

The Cybercrimes Act, 2019 imposes a maximum of 15 years with an option of a fine depending on the crime, important also is the aggravating circumstances with regard to sentencing:

> (5) A court which imposes any sentence in terms of this section must, without excluding other relevant factors, consider as aggravating factors—
>
> (a) the fact that the offence was committed by electronic means;
> (b) the extent of the prejudice and loss suffered by the complainant or other person as a result of the commission of such an offence;
> (c) the extent to which the person gained financially or received any favour, benefit, reward, compensation or any other advantage from the commission of the offence; or
> (d) the fact that the offence was committed in concert with one or more persons.

Therefore, the amendment of the CPA is part of a collective process. A change in the legal framework would be the initial step needed to properly regulate the collection of electronic evidence. Producing a procedural guide will ensure that law enforcement is well equipped and well prepared to reduce this form of crime.

BIBLIOGRAPHY

Books

Bellengere *Law of evidence*

Bellengere A *et al The law of evidence in South Africa* (Oxford 2013)

Britz C*omputer forensics and cybercrime*

Britz MT *Computer forensics and cybercrime: An introduction* 3rd ed (Pearson 2013)

Casey C*omputer crime*

Casey E *Digital evidence and computer crime: Forensic science, computers and the internet* 3rd ed (Elsevier 2010)

Joubert *Criminal procedure handbook*

Joubert JJ *Criminal procedure handbook* 12th ed (Juta 2017)

Mason *Electronic evidence*

Mason S *Electronic evidence disclosure, discovery and admission* (LexisNexis 2007)

Papadopoulos *Cyberlaw*

Papadopoulos S and Snail S *Cyberlaw @ SA III: The law of the internet in South Africa* 3rd ed (Van Schaik 2012)

Pasco *Criminal financial investigations*

Pasco GA *Criminal financial investigations: The use of forensics accounting techniques and indirect methods of proof* 2nd ed (CRC Press 2012)

Schwikkard *Principles of evidence*

Schwikkard PJ and Van der Merwe SE *Principles of evidence* 4th ed (Juta 2015)

Scott *Law of commerce*

Scott J *et al The law of commerce in South Africa* (Oxford 2009)

Snyman *Criminal law*

Snyman CR *Criminal law* 6th ed (LexisNexis 2016)

Tapper *Evidence*

Tapper C and Cross R on Evidence 12th ed (Oxford University Press 2010)

Wille *Financial law*

Wille C *et al Principles of financial law* (LexisNexis 2007)

Journals

Basdeo 2009 *PER*

Basdeo VM “The Constitutional validity of search and seizure powers in South African criminal procedure” 2009 *PER* 307 – 331

Basdeo 2017 *JLSD*

Basdeo VM, Montesh M and Lekubu BK “Search and seizure of evidence in cyber environments: A law enforcing the detection rate of commercial crime” 2017 *JLSD* 48 - 66

Bouwer 2014 *SACJ*

Bouwer GP “Search and seizure of electronic evidence: Division of traditional one-step process into a new two-step process in a South African context” 2014 *SACJ* 156 - 171

Budhram 2017 *crime quarterly*

Budhram T and Geldenhuys N “A losing battle? Assessing the detection rate of commercial crime” 2017 *SA crime quarterly* 7 - 16

Cassim 2011 *CILSA*

Cassim F “Addressing the spectra of cybercrime in Africa: Evaluating measures adopted by South Africa and other regional role players” 2011 *CILSA* 123 - 138

Cassim 2014 *CILSA*

Cassim F “Addressing the spectra of phishing: Are adequate measures in place to protect victims of phishing?” 2014 *CILSA* 401 - 428

Cassim 2015 *PER*

Cassim F “Protecting personal information in the Era of identity theft: Just how safe is our personal information from identity thieves?” 2015 *PER* 69 - 110

De Koker 2007 *IEA*

De Koker L “Financial crime in South Africa” 2007 *IEA* 34 - 38

Goodman 2002 *IJLIT*

Goodman MD and Brenner SW “The merging consensus on criminal conduct in cyberspace” 2002 *IJLIT* 139 - 223

Hofman 2006 *SACJ*

Hofman J “Electronic evidence in criminal cases” 2006 *SACJ* 257 - 274

Jackson 2015 *SAIPA*

Jackson D “Financial crime - driven by opportunity, technology and greed” 2015 *SAIPA* 8 - 19

Luehr 2005 *Crim. Just*

Luehr PH “Real evidence, virtual crimes - the role of computer forensic experts” 2005 *Crim. Just* 14 - 25

Montesh 2009 *Acta Criminologica*

Montesh M “An analysis of the role of the South African asset forfeiture unit and the special investigating unit” 2009 *Acta Criminologica* 31 - 40.

Mason 2013 *computer and security review*

Mason S “Electronic banking and how courts approach the evidence” 2013 *computer and security review* 144 – 151

Rautenbach 2014 *PER*

Rautenbach IM “Proportionality and the limitation clauses of the South African Bill of Rights” 2014 *PER* 2229 – 2267

Snail 2009 *JILT*

Snail S “Cybercrime in South Africa - Hacking, cracking and other unlawful online activities” 2009 *JILT* 1 – 13

Snail 2009 *JILT*

Snail S “Cybercrime in the context of the ECT Act” 2009 *JILT* 63 – 68

Watney 2009 *JILT*

Watney M “Admissibility of electronic evidence in criminal proceedings: An outline of the South African legal position” 2009 *JILT* 1 - 13

Research Papers and Theses

Basdeo *Constitutional Perspective of police powers of search and seizure*

Basdeo VM *A Constitutional perspective of police powers of search and seizure in the criminal justice system* (LLM University of South Africa 2009)

Jordaan *Analysis of bank account statements*

Jordaan J *Analysis of bank account statements to establish evidence of illicit financial activity (*M Tech University of South Africa 2007)

Montesh *Critical analysis of crime investigation system*

Montesh M *Critical analysis of crime investigation system within the South African criminal justice system: A comparative study* (PhD University of South Africa 2007)

Mudaly *Search and Seizure of documents*

Mudaly L *Search and seizure of documents in the investigation of tax-related cases (*M Tech University of South Africa 2011)

Myburgh *Developing a framework for the search and seizure of digital evidence*

Myburgh DC *Developing a framework for the search and seizure of digital evidence forensic investigators in South Africa* (MCom in Forensic Accountancy North - West University 2016)

Ndara *Computer seizure as technique in forensic investigation*

Ndara V *Computer seizure as technique in forensic investigation (*M Tech University of South Africa 2013)

South African Reform Law Commission Report (project 6) “Review of the law of Evidence” (1986)

South African Law Reform Commission Issue Paper 14 (Project 108) “Computer-related crime: options for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects” *(*1998*)*

South African Law Reform Commission Discussion Paper 99 (Project 108) “Computer related crime: Preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects” (2001)

South African Law Reform Commission Report (Project 101) “The Application of the Bill of right to the Criminal Procedure, Criminal Law and the Law of Evidence and Sentencing” (2001)

South African Law Reform Commission Report (Project 113) “The use of Electronic Equipment in Court Proceedings (postponement of criminal cases via audio-visual link)” (2003)

South African Law Reform Commission Issue Paper 27 (Project 126) “Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues” (2010)

South African Law Reform Commission Discussion paper 131 (Project 126) “The review of evidence” (2015)

Internet sources

Businesses Against Crime South Africa “About Us” https://www.bac.org.za/ (accessed on 20 February 2019)

Business Tech “South Africa crime Stats” https://businesstech.co.za/news/government/270689/south-africa-crime-stats-2018-everything-you-need-to-know/ (accessed on 20 February 2019)

Council of Europe “Cybercrime@IPA specialised cybercrime unit - good practice study” www.coe.int/cybercrime (accessed on 01 July 2020)

Definition “The Cloud” https://www.techopedia.com/definition/26514/cloud (accessed on 22 February 2019)

Department of Justice and Constitutional Development “Administration of Justice: Input for the SA yearbook 2003/2004” https://www.GCIS.co.za (accessed on the 19 January 2019)

Department of Justice and Constitutional Development “Cybercrimes and Cybersecurity Bill [B6 2017] http://www.justice.gov.za/legislation/bills/bills.htm (accessed on 3 August 2019).

Financial Action Task Force “An introduction to the FATF and its work“ https://www.fatf-gafi.org (accessed on 7 February 2019)

Financial Intelligence Centre “Combating Financial Crime in South Africa Typologies Report http://www.fic.gov.za (accessed on 16 February 2019)

Financial Intelligence Centre “Media Release Financial Intelligence Reports: FIC Role Clarified https://www.fic.gov.za/Documents/Media%20Release%20-%204%20Sept%202019%20(003).pdf (accessed on 16 September 2019)

Kempen A “Taking the profit out of crime - the Asset Forfeiture Unit” https://www.npa.gov.za/sites/files/files/FAQs%20on%20AFU.pdf (accessed on 26 October 2016).

Mason S “A convention on electronic evidence: helping to provide for certainty in international trade”

http://www.uncitral.org.pdf/english/congress/papers_for_Congress/38-MASON-A_Convention_on_Electronic_Evidence.pdf (accessed on 18 November 2018)

Mason S “Electronic evidence: A proposal to reform the presumption of reliability and hearsay”

https://www.sciencedirect.comscience/article/pii/S0267364913003057 (Date accessed 12 April 2019)

Mason S and Seng D “Electronic evidence” https://wwwjstor.org/stable/ (Date accessed on 1 April 2019)

Nortjé JGJ and Myburgh DC "The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa" *PER / PELJ* 2019(22) – DOI

http://dx.doi.org/10.17159/1727-3781/2019/v22i0a4886 (accessed on 25 June 2020)

Philippsohn S “The dangers of New Technology – Laundering on the Internet” 2001 JMLC 87 – 95 https://doi.org/10.1108/eb027295 (accessed on 12 February 2019)

President proclaims NDPP Investigating Directorate to strengthen fight against corruption http://www.thepresidency.gov.za/press-statements/President-proclaims-ndpp-investigating-directorate-strengthen-fight-against (accessed on 14 May 2019)

Public Service Commission South Africa August 2001 “A review of South Africa’s national anti-corruption agencies https://www.psc.gov/za/documents/reports/corruption/03.pdf (accessed on 19 February 2019).

South African Banking Risk Information Centre “Digital Banking Crime Statistics” https://www.sabric.co.za/media-and-news/press-release/digital-banking-crime-statistics/ (accessed on 20 February 2019)

South African Banking Risk Information Centre “SABRIC warms consumers to beware of phishing and malware https://www.sabric.co.za/media-and-news/press-release/sabric-warms-consumers-to-beware-of-phishing-and-malware (accessed on 20 February 2019)

South African Banking Risk Information Centre “SAPS and SABRIC Recommit to Intensify Fight against Bank Robberies https://www.sabric.co.za/media-and-news/press-release/saps-and-sabric-recommit-to-intensify-fight-against-bank-robberies/ (accessed on 20 February 2019)

South African Government “documents – Criminal Procedure Act 51 of 1977” www.gov.za/documents/criminal-procedure-act-1977-26-mar-2015-1224 (accessed on 29 September 2019)

South African Government Official website “How does the criminal justice system work” https://www.gov.za/faq/justice-and-crime-prevention/how-does-criminal-justice-system-work (accessed on 01 March 2019)

South African Police Service Official website “About Us” https://www.saps.gov.za/about/about.php (accessed on 31 July 2019)

South Africa Police Service “Commercial Branch”

https://www.gov.za/South-african-police-service-commercial-branch-success (accessed on the 19 February 2019).

South African Police service "Crim Statistics 2017/2018 https://www.saps.gov.za/services/crimestates.php (accessed on 18 December 2018)

South Africa Police Service "Directorate for priority crime investigation" https://www.saps.gov.za/dcpi/index.php (accessed on 02 February 2019)

Special Investigating Unit "Our Mandate" https://www.siu.org.za/our-mandate/ (accessed on 20 November 2018)

Statistics South Africa "While crime increases, fear rises and trust in criminal justice system drops" http://www.statssa.gov.za/?p=11627 (accessed on 15 March 2019)

Techopedia "The definition of the Cloud"

https://www.techopedia.com/definition/26514/cloud (accessed on 22 February 2019)

UNICEF "Ratification and Signatory " https://www.unicef.org/crc/index_30207.html (accessed on 7 February 2019)

Conventions and Protocols

Council of Europe Convention on Cybercrime Budapest 2001

Harmonization of ICT Policies in Sub-Saharan Africa "Computer Crime and Cybercrime: Southern African Development Community Model law" 2013

Harmonization of ICT Policies in Sub-Saharan Africa "Electronic Transactions and Electronic Commerce: Southern African Development Community Model" 2013

Table of statutes

Constitution of the Republic of South Africa, 1996

Computer Evidence Act 57 of 1983

Criminal Procedure Act 51 of 1977

Cybercrimes and Cybersecurity Bill, 2015

Cybercrimes and Cybersecurity Bill 2017

Cybercrimes and Cybersecurity Bill 2018

Cybercrimes Act, 2019

Electronic Communications and Transactions Act 25 of 2002

Financial Intelligence Centre Act 38 of 2001

Law of Evidence Amendment Act 45 of 1988

National Cybersecurity Policy Framework GG 39475 4 December 2015

National Prosecuting Authority Act 32 of 1998

Prevention of Organised Crime Act 121 of 1998

Protected disclosure Act 26 of 2002

Proclamation R123. GG 19599, 4 December 1998

Promotion of access to Information Act 2 of 2002

Protection of Personal Information Act 4 of 2013

Public Finance Management Act 1 of 1999

Regulation of Interception of Communication and Provision of Communication related Information Act 70 of 2002

South African Law Reform Commission Act 19 of 1973

South African Police Service Act 68 of 1995

South African Revenue Service Act 34 of 1997

Special Investigating Units and Special Tribunals Act 74 of 1996

Tax Administration Act 28 of 2011

Cases

Absa Bank Limited and others v Public Protector and others (48123/2017) [2018] ZAGPPHC 2

African Cash and Curry (Pty) Limited v Commissioner for the South African Revenue Service [2020] 1 All SA 1 (SCA)

Annex Distribution (Pty) Ltd and others v Bank of Baroda (52590/2017)

Beheermaatscappij Helling I NV v Magistrate, Cape Town and Others [2005] JOL 13758 (C)

Bernstein and others v Bester NO and others 1996 (4) BCLR 449

Bogoshi v Van Vuuren NO and others; Bogoshi and another v The Directorate: Office for Serious Economic Offences and others SCA 543/93

Cine Films (Pty) Ltd and Others v Commissioner of Police and Others [1972] 2 All SA 85 (A)

CSARS v Amawele joint venture CC (908/2017) [2018] ZASCA 115

CSARS v Volkswagen SA (Pty) Ltd (1028/2017) [2018] ZASCA 116

Ex parte Rosch [1998] 1 All SA 319

Feruccio Ferucci and Others v The Commissioner for The South African Revenue Service and Another 2002 (6) SA 219 (C)

Goqwana v Minister of Safety NO and others (20668/14) [2015] ZASCZ 186

Gumede v The State (800/2015) ZASCA 148 (2016)

Ismael v Durban City Council 1973 (2) SA 362 (N)

Jafta v Ezemuelo KZN wildlife [2008] BLLR 954 (LC)

Johncom Media Investment Limited v M and Others 2009 (4) SA 7 (CC)

Mdlongwa v The State (99/10) [2010] ZASCA 82 (21 May 2010)

Minister for Safety and Security and Van der Merwe and others CCT 90/10 [2011] ZACC 19

Minister of Police and Others v Kunjana [2016] ZACC 21

Minister of Safety and Security v Van der Merwe CCT 90/10 2011 ZACC 19

Mistry v Interim National Medical and Dental Council of South Africa [1998] ZACC 10

Mkhize v S [2012] JOL 29750 (KZP) 8

Mnyungula v Minister of Safety and security and others 2004 (1) SACR 219

Narlis v South Africa Bank of Athens 1976 (2) SA 573 (A)

National Director of Public Prosecutions v Mohamed [2007] SCA 138

National Union of South African Students v Divisional Commissioner, South African Police Service, Cape Western Division and others [1971] 2 All SA 620 (C)

Ndlovu v Minister of Correctional Services and another [2006] 4 All SA 165 (W)

Ntoyakhe v Minister of Safety and Security and Others 1999 (2) SACR 349 (E)

Powell and Others v Van der Merwe NO and Others 2005 (5) SA 62 (SCA)

S v Makwanyane (CCT3/94) [1995] ZACC 3; 1995 (6) BCLR 665

S v Ndiki and others [2007] 2 All SA 185 (ck)

S v Madiba 1998 (1) BCLR 38 (D)

S v Mashiyi and another [2002] JOL 9894 (Tk) 18

The Investigating Directorate: Serious Economic Offences v Hyundai Motors Distributors (Pty) Ltd v Smith 2000 BCLR 1079 (CC)

The Special Investigation Unit v Anthimoolan Nadason (5/2001)) [2001] ZASCA 117

Thint (Pty) Ltd v National Director of Public Prosecutions and Others; Zuma v National Director of Public Prosecutions and Others 2008 (2) SACR 421