

**ANALYSIS OF THE USE OF ELECTRONIC SURVEILLANCE TO INVESTIGATE  
CARTEL CONDUCTS: A CASE STUDY OF THE COMPETITION COMMISSION  
OF SOUTH AFRICA IN PRETORIA**

by

**KGASHANE RAYMOND KGOMO**

submitted in accordance with the requirements for  
the degree of

**MASTER OF ARTS IN CRIMINAL JUSTICE**

in the subject

**CRIMINAL JUSTICE**

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF W MALULEKE

CO-SUPERVISOR: PROF DQ MABUNDA

26 JANUARY 2024

## DECLARATION

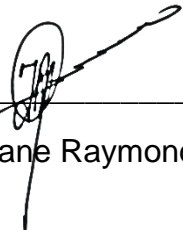
Name: KGASHANE RAYMOND KGOMO  
Student number: 18030513  
Degree: MASTER OF ARTS IN CRIMINAL JUSTICE

ANALYSIS OF THE USE OF ELECTRONIC SURVEILLANCE TO INVESTIGATE CARTEL CONDUCTS: A CASE STUDY OF THE COMPETITION COMMISSION OF SOUTH AFRICA IN PRETORIA.

I declare that the above dissertation is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the dissertation to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

  
\_\_\_\_\_  
Kgashane Raymond Kgomo

19/01/2024

## **DEDICATION**

I dedicate this dissertation to my parents for being inspirational to my life.

## **ACKNOWLEDGEMENTS**

I would like to thank the following individuals who extensively helped me to complete this study:

- To my esteemed supervisor, Professor W Maluleke and co-supervisor; Professor DQ Mabunda for their invaluable supervision and support systems during this academic journey.
- To the Commissioner of the Competition Commission of South Africa for granting permission to collect data.
- To all participants who were willing to be interviewed for this study.
- Special thanks is directed to my family for always supporting and believing in me.

## **ABSTRACT**

This study explored the value that electronic surveillance adds to cartel investigations by adopting a qualitative research approach, utilising a case study research design, and guided by the exploratory research objective. The non-probability: purposive sampling was employed to target ten (10) participants, distributed as follows: Five (05) investigators and other 05 legal counsels, attached to the Competition Commission of South Africa. Participants were chosen based on rank seniority, division roles and work experience. For data collection methods, the semi-structured face-to-face interviews, documentary studies and structured observations methods were conducted. The collected data was analysed using the inductive Thematic Content Analysis (TCA).

The findings of this study revealed that the application of electronic surveillance can facilitate the detection of cartel activities by monitoring suspicious communications and transactions among competitors. It is also established that the secretive nature of cartel conducts poses challenges for competition authorities around the world to effectively detect it. Individuals involved try to conceal their cartel activities and evidence thereof. Moreover, the consulted literature studies confirmed that use of electronic surveillance is a common practice among competition authorities in the developed countries to detect and investigate cartels.

For recommendations, it is provided that the investigation model on implementation of electronic surveillance as an investigation tool to assist the Competition Commission to easily detect and prosecute cartel activities, which may assist competition authorities to adopt a proactive stance to easily identify firms, which are potentially involved in cartels conduct.

**Keywords:** Case study, Cartel conducts, Competition Commission, Electronic surveillance, Investigate, Pretoria, South Africa

## ABBREVIATIONS AND DESCRIPTIONS

<b>CADE</b>	:	Administrative Council for Economic Defence
<b>ACLU</b>	:	American Civil Liberties Union
<b>AI</b>	:	Artificial intelligence
<b>ACCC IPCC</b>	:	Australian Competition and Consumer Commission Immunity Policy for Cartel Conduct
<b>APD</b>	:	American Psychological Association
<b>LGPD</b>	:	Brazilian General Data Protection Law
<b>CCPA</b>	:	California's Consumer Privacy Act
<b>CCTV</b>	:	Close-Circuit Television
<b>COMESA</b>	:	Common Market for Eastern and Southern Africa
<b>CDPP</b>	:	Commonwealth Director of Public Prosecutions
<b>CMA</b>	:	Competition and Market Authority
<b>CPI</b>	:	Competition Policy International
<b>CRC</b>	:	Convention of the Rights of the Child
<b>CLP</b>	:	Corporate Leniency Policy
<b>DPA</b>	:	Data Protection Act
<b>DCAF</b>	:	Democratic Control of Armed Forces
<b>DoJ</b>	:	Department of Justice
<b>EAC</b>	:	East African Community
<b>CEMAC</b>	:	Economic and Monetary Community of Central Africa
<b>ECOWAS</b>	:	Economic Community of West African States
<b>ECPA</b>	:	Electronic Communications Privacy Act
<b>EU</b>	:	European Union
<b>GDPR</b>	:	European Union's General Data Protection Regulations
<b>FBI</b>	:	Federal Bureau of Investigation
<b>FTC</b>	:	Federal Trade Commission
<b>FICA</b>	:	Financial Intelligence Centre Act
<b>GDPR</b>	:	General Data Protection Regulation

<b>GPS</b>	:	Global Positioning System
<b>ICN</b>	:	International Competition Network
<b>ICCPR</b>	:	International Covenant on Civil and Political Rights
<b>IPA</b>	:	Investigatory Powers Act
<b>ICA</b>	:	Israel Competition Authority
<b>LEAs</b>	:	Law Enforcement Agencies
<b>LAC</b>	:	Legal Advice Centre
<b>MLAC</b>	:	Money Laundering Advisory Council
<b>NCC</b>	:	National Communications Centre
<b>NDPP</b>	:	National Director of Public Prosecutor
<b>NIA</b>	:	National Intelligence Agency
<b>NICOC</b>	:	National Intelligence Co-ordinating Committee
<b>NITA</b>	:	National Investigative Training Academy
<b>NPA</b>	:	National Prosecuting Authority
<b>NSL</b>	:	National Security Letter
<b>NSIA</b>	:	National Strategic Intelligence Act
<b>OECD</b>	:	Organisation for Economic Cooperation and Development
<b>PPA</b>	:	Privacy Protection Authority
<b>RFID</b>	:	Radio Frequency Identification
<b>RICA</b>	:	Regulation of Interception of Communications and Provision of Communication-related Information Act
<b>SANDF DIC</b>	:	South African National Defence Force: Defence Intelligence Centre
<b>SAPS CID</b>	:	South African Police Service: Crime Intelligence Division
<b>SARS</b>	:	South African Revenue Services
<b>SASS</b>	:	South African Secret Service
<b>SSA</b>	:	State Security Agency
<b>SDA</b>	:	Surveillance Devices Act
<b>TIA</b>	:	Telecommunications Interception and Access

<b>UK</b>	:	United Kingdom
<b>UN</b>	:	United Nations
<b>UNODC</b>	:	United Nations Office on Drugs and Crime
<b>USDJ</b>	:	United States Department of Justice
<b>USA</b>	:	United States of America
<b>UDHR</b>	:	Universal Declaration of Human Rights
<b>UNISA</b>	:	University of South Africa
<b>WAEMU</b>	:	West African Economic Monetary Union



## TABLE OF CONTENTS

DECLARATION .....	i
DEDICATION.....	ii
ACKNOWLEDGEMENTS .....	iii
ABSTRACT.....	iv
ABBREVIATIONS AND DESCRIPTIONS.....	v
CHAPTER ONE: GENERAL ORIENTATION .....	1
1.1 INTRODUCTION AND BACKGROUND.....	1
1.2 PROBLEM STATEMENT .....	3
1.3 STUDY PURPOSE .....	5
1.4 STUDY AIM.....	5
1.5 STUDY OBJECTIVES.....	6
1.6 RESEARCH QUESTIONS.....	6
1.7 STUDY SIGNIFICANCE .....	7
1.8 DEFINITIONS OF KEY CONCEPTS .....	9
1.8.1 Cartel conducts .....	9
1.8.2 Electronic surveillance .....	9
1.8.3 Intelligence.....	10
1.8.4 Investigation.....	10
1.9 SCOPE OF THE STUDY .....	10
1.10 SUMMARY.....	11
CHAPTER TWO: LITERATURE REVIEW ON THE USE OF ELECTRONIC SURVEILLANCE TO INVESTIGATE CARTEL CONDUCTS .....	12
2.1 INTRODUCTION.....	12
2.2 THE IMPORTANCE OF USING ELECTRONIC SURVEILLANCE IN THE INVESTIGATION OF CARTEL CONDUCTS.....	13
2.2.1 The conceptualisation of the term ‘surveillance’ .....	14
2.2.2 The use of electronic surveillance during investigations of cartel conducts	16
2.2.3 The importance of electronic surveillance during investigations of other criminal conducts .....	18
2.3 THE ROLES OF ELECTRONIC SURVEILLANCE IN THE INVESTIGATION OF CARTEL CONDUCTS.....	21
2.3.1 The roles of electronic surveillance.....	22
2.3.2 The adoption of surveillance cameras for criminal investigations .....	25
2.3.3 The use of electronic surveillance to investigate online [Internet] crimes ....	26

<b>2.4 CIRCUMSTANCES LEADING TO AUTHORISED USAGE OF ELECTRONIC SURVEILLANCE FOR CARTEL CONDUCTS INVESTIGATIONS .....</b>	<b>28</b>
<b>2.5 THE CUSTODIANS OF ELECTRONIC SURVEILLANCE USAGE .....</b>	<b>29</b>
<b>2.5.1 State Security Agency .....</b>	<b>30</b>
<b>2.5.2 South African Police Service Crime Intelligence Division .....</b>	<b>30</b>
<b>2.5.3 Defence Intelligence Centre/Division: South African National Defence Force</b>	
31	
<b>2.5.4 Office for Interception Centre .....</b>	<b>31</b>
<b>2.5.5 National Communications Centre.....</b>	<b>32</b>
<b>2.5.6 South African Revenue Services .....</b>	<b>32</b>
<b>2.6 LEGAL REGULATIONS FOR THE USE OF ELECTRONIC SURVEILLANCE DURING INVESTIGATIONS OF CRIMINAL ACTIVITIES.....</b>	<b>33</b>
<b>2.7 SURVEILLANCE LAW IN VARIOUS JURISDICTIONS: THE INTERNATIONAL FOCUS .....</b>	<b>34</b>
<b>2.7.1 The United States of America laws on the use of surveillance for criminal investigations.....</b>	<b>35</b>
<b>2.7.2 United Kingdom laws on the adoption of surveillance for criminal investigations.....</b>	<b>36</b>
<b>2.7.3 Australian laws on surveillance .....</b>	<b>37</b>
<b>2.7.4 Brazilian laws on surveillance .....</b>	<b>38</b>
<b>2.7.5 Israel laws on surveillance .....</b>	<b>38</b>
<b>2.8 SURVEILLANCE LAWS IN AFRICAN COUNTRIES .....</b>	<b>39</b>
<b>2.9 THE SOUTH AFRICAN LEGISLATIVE FRAMEWORKS ON SURVEILLANCE ...</b>	<b>40</b>
<b>2.9.1 Regulation of Interception of Communications and Provision of Communications Related Information Act (No. 70 of 2002).....</b>	<b>40</b>
<b>2.9.2 National Strategic Intelligence Amendment Act (No. 67 of 2002) .....</b>	<b>40</b>
<b>2.9.3 Financial Intelligence Centre Act (No. 38 of 2001) .....</b>	<b>41</b>
<b>2.10 LIMITATIONS OF THE USE OF ELECTRONIC SURVEILLANCE DURING INVESTIGATIONS OF CARTELS CONDUCT .....</b>	<b>41</b>
<b>2.10.1 Right to privacy .....</b>	<b>42</b>
<b>2.10.2 The use of warrant to use surveillance during criminal investigations [Cartel conducts].....</b>	<b>47</b>
<b>2.11 THE CHALLENGES OF INVESTIGATING CARTEL CONDUCTS .....</b>	<b>48</b>
<b>2.11.1 The United Kingdom challenges in the investigation of cartel conducts .....</b>	<b>50</b>
<b>2.11.2 United States of American challenges in the investigation of cartel conducts.....</b>	<b>50</b>
<b>2.12 AUSTRALIAN CHALLENGES IN THE INVESTIGATION OF CARTEL CONDUCTS.....</b>	<b>51</b>
<b>2.12.1 Criminal versus civil cartel enforcement.....</b>	<b>51</b>

2.12.2 Increase in levels of private enforcement .....	52
2.12.3 Settlement of cartel cases .....	52
2.12.4 Informant reward system .....	52
<b>2.14 THE ISRAELI CHALLENGES IN THE INVESTIGATION OF CARTEL CONDUCTS</b>	<b>53</b>
<b>2.15 CHALLENGES IN AFRICAN COUNTRIES TO INVESTIGATE CARTEL CONDUCT</b> .....	<b>54</b>
2.15.1 South African challenges on investigations of cartel conducts .....	54
<b>2.16 THE BEST PRACTICES FOR INVESTIGATING CARTELS: INTERNATIONAL, AFRICAN AND SOUTH AFRICAN APPROACHES</b> .....	<b>55</b>
2.16.1 United States Sherman Act, 1890 .....	55
2.16.2 United Kingdom Competition Act of 1998.....	56
2.16.3 Australia Competition and Consumer Act of 2010 .....	56
2.16.4 Brazil Competition law: No. 8884/1994.....	57
2.16.5 Refocus to cartel enforcement – The Leniency Statute of 2000.....	57
2.16.6 Israel Economic Competition Law of 5748-1988 .....	57
2.16.7 African Competition law.....	58
2.16.8 Constitution of the Republic of South Africa, 1996 .....	59
2.16.9 Criminal Procedure Act (No. 51 of 1977) .....	59
2.16.10 South Africa Competition Act (No. 89 of 1998).....	59
<b>2.17 OTHER NOTABLE STRATEGIES TO INVESTIGATE CARTEL CONDUCTS</b> .....	<b>60</b>
2.17.1 The use of search warrants in the investigation of cartel conducts.....	61
2.17.2 The use of summons in the investigation of cartel conducts.....	62
<b>2.18 THE USE OF CORPORATE LENIENCY POLICY IN THE INVESTIGATION OF CARTEL CONDUCTS</b> .....	<b>62</b>
2.18.1 The use of leniency programme in United Kingdom.....	64
2.18.2 The use of leniency programme in the United States of America .....	64
2.18.3 The use of leniency by Australian Competition and Consumer Commission	
65	
2.18.4 The use of leniency by Brazil, Administrative Council for Economic Defence	
66	
2.18.5 The use of leniency by Israel Competition Authority .....	66
<b>2.19 THE USE OF LENIENCY PROGRAMMES IN AFRICAN COUNTRIES</b> .....	<b>67</b>
2.19.1 The use of leniency programme in South Africa.....	67
<b>2.20 PROACTIVE CARTEL DETECTION TECHNIQUES FOR INVESTIGATION OF CARTEL CONDUCTS</b> .....	<b>68</b>
2.20.1 The United Kingdom Competition and Market Authority .....	70

2.20.2 The United States of America, Department of Justice Antitrust Division and Federal Trade commission .....	71
2.20.3 Australian Competition and Consumer Commission .....	71
2.20.4 Brazilian Administrative Council for Economic Defence .....	72
2.20.5 Israeli Antitrust Authority .....	72
2.20.6 African Competition law .....	73
2.20.7 South African Competition Commission .....	74
<b>2.21 PROACTIVE CARTEL DETECTION METHOD AND ALGORITHMS COLLUSION</b>	
74	
<b>2.22 SUMMARY</b> .....	78
<b>CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY</b> .....	80
<b>3.1 INTRODUCTION</b> .....	80
<b>3.2 RESEARCH DESIGN</b> .....	80
<b>3.3 RESEARCH APPROACHES</b> .....	82
3.3.1 Study location .....	83
3.3.2 Study population .....	83
3.3.3 Sampling procedures .....	84
<b>3.4 DATA COLLECTION METHODS</b> .....	84
3.4.1 Semi-structured face-to-face interviews .....	85
3.4.2 Documentary studies .....	86
3.4.3 Structured observation method .....	86
<b>3.5 DATA ANALYSIS METHODS</b> .....	87
3.5.1 Organising data .....	88
3.5.2 Reading and memoing .....	88
<b>3.6 METHODS TO ENSURE TRUSTWORTHINESS</b> .....	90
3.6.1 Credibility .....	91
3.6.2 Transferability .....	91
3.6.3 Dependability .....	92
3.6.4 Confirmability .....	92
<b>3.7 ETHICAL CONSIDERATIONS</b> .....	92
3.7.1 Permission to conduct this study .....	93
3.7.2 Harm to participants .....	93
3.7.3 Informed consent .....	93
3.7.4 Invasion of privacy .....	94
3.7.5 Confidentiality and anonymity .....	94
<b>3.8 SUMMARY</b> .....	94

<b>CHAPTER FOUR: DATA PRESENTATIONS, ANALYSIS AND DISCUSSIONS.....</b>	<b>95</b>
<b>4.1 INTRODUCTION.....</b>	<b>95</b>
<b>4.2 FINDINGS .....</b>	<b>95</b>
<b>4.2.1 The importance of electronic surveillance.....</b>	<b>95</b>
<b>4.2.2 What the concept “electronic surveillance” entails .....</b>	<b>98</b>
<b>4.2.3 The role of electronic surveillance.....</b>	<b>101</b>
<b>4.2.4 Circumstances under which “electronic surveillance” should be authorised</b>	
103	
<b>4.2.5 The limitations of the use of electronic surveillance .....</b>	<b>106</b>
<b>4.2.6 Challenges of investigating cartel conducts .....</b>	<b>110</b>
<b>4.2.7 The effectiveness of strategies employed to investigate cartel.....</b>	<b>112</b>
<b>4.4 SUMMARY.....</b>	<b>117</b>
<b>CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS.....</b>	<b>119</b>
<b>5.1 INTRODUCTION.....</b>	<b>119</b>
<b>5.2 OVERALL STUDY SUMMARY .....</b>	<b>119</b>
<b>5.3 STUDY OVERALL CONCLUSION.....</b>	<b>120</b>
<b>5.4 STUDY RECOMMENDATIONS TO IMPROVE THE STUDY AIM AND IDENTIFIED THEMES.....</b>	<b>122</b>
<b>5.4.1 Recommendations relating to the study aim and identified themes.....</b>	<b>122</b>
<b>5.4.2 Recommendations based on study objective 01 and identified themes .....</b>	<b>123</b>
<b>5.4.3 Recommendations based on study objective 02 and identified themes .....</b>	<b>124</b>
<b>5.4.4 Recommendations based on study objective 03 and study themes.....</b>	<b>124</b>
<b>5.4.5 Recommendations based on study objective 04 and identified themes .....</b>	<b>125</b>
<b>5.4.6 Recommendations based on study objective 05 and identified themes .....</b>	<b>126</b>
<b>5.4.7 Recommendations based on study objective 06 and identified themes .....</b>	<b>127</b>
<b>5.5 STUDY LIMITATIONS .....</b>	<b>128</b>
<b>5.6 FUTURE RESEARCH STUDIES .....</b>	<b>128</b>
<b>LIST OF REFERENCES.....</b>	<b>130</b>
<b>ANNEXURE A: INFORMED CONSENT FORM.....</b>	<b>164</b>
<b>ANNEXURE B: INTERVIEW SCHEDULE GUIDE.....</b>	<b>166</b>
<b>ANNEXURE C: UNIVERSITY OF SOUTH AFRICA ETHICAL APPROVAL LETTER.....</b>	<b>168</b>
<b>ANNEXURE D: LETTER TO ASK FOR PERMISSION TO CONDUCT RESEARCH FROM THE COMPETITION COMMISSION OF SOUTH AFRICA.....</b>	<b>169</b>
<b>ANNEXURE E: COMPETITION COMMISSION ETHICAL APPROVAL LETTER.....</b>	<b>170</b>
<b>ANNEXURE F: EDITOR’S LETTER.....</b>	<b>171</b>
<b>ANNEXURE G: TURNITIN REPORT .....</b>	<b>172</b>

## **CHAPTER ONE: GENERAL ORIENTATION**

### **1.1 INTRODUCTION AND BACKGROUND**

Jaspers (2017:319) states that 'cartelists' have been manipulating economies for centuries without any detection. Countries around the world established competition authorities to enforce competition law to detect and prevent cartel conducts or activities (Whish & Bailey, 2021:1-4). To curb these cartel activities, most of the competition authorities around the world applied a reactionary cartel detection method, such as leniency programme, Organisation for Economic Cooperation and Development [OECD] (2013:260). However, with time this method became less effective as the conduct become sophisticated (Levenstein & Suslow, 2006:43). Mirasdar and Gupta (2017:2604) concur that cartel activities are increasing daily, and it is difficult for many competition authorities to curb them.

As a result, some of competition authorities around the world such as the European Commission, Israel Antitrust Authority, United States of America (USA), United Kingdom (UK), and Canada Competition Bureau shifted towards the application of proactive detection methods and employing a variety of methods, including intelligence gathering method such as electronic surveillance (OECD, 2022:3).

The Canadian Competition Bureau applies the use of wiretapping to fight cartels (Gillis, 2021:112). US antitrust division and Israel antitrust authority are empowered to prosecute cartel conducts as criminal offences, and they use advanced intelligence gathering methods, computer forensic capabilities and wiretapping (Stigler & Friedland, 2020:58; OECD, 2020:8). Schinkel (2014:6) argues that authorities that are faced with sophisticated cartels, need to shift and give more attention to proactive cartel detection measures to stay ahead of the cartelists.

Consulted literature studies show that the reactive cartel detection method is less effective; hence, competition authorities in other jurisdictions have decided to implement proactive detection measures (Mirasdar & Gupta, 2017:2604). In South Africa, in terms of the Competition Act (No. 89 of 1998), the Competition Commission still relies on reactive cartel detection methods, which had been proven to be less effective according to the 2020/2021 and 2021/2022 statistics published in its annual

reports. This is the reason that the researcher decided to conduct this study pertaining to the use of electronic surveillance to investigate cartel conducts. Therefore, this study explored the importance of using electronic surveillance in the investigation of cartels, with the intention of giving plausible recommendations on how to implement them in line with the legislation.

The study, in terms of the literature focused on jurisdictions in developed countries, namely: UK, USA, Australia, Brazil, and Israel. The reason is that competition authorities in these countries have made significant progress in implementing and enforcing anticompetitive regulations. As a result, South African Competition Commission draws heavily on the experience and practices of these countries.

When it comes to African competition law, based on the literature sources and the researcher's extensive experience as an employee of the Competition Commission of South Africa in the Cartels division, other African countries are novice to the competition law environment hence they are learning from South Africa to strengthen their competition laws and enforcement powers (Ogundele, 2022:1; Ng'ethe & Gathii, 2019:35). This is because South Africa is well developed and very active in the competition law field compared to other jurisdictions in the continent (Steyn, 2019:45). Its laws and policies are in-line with the international best practices; hence it relies heavily on the experience and practices of the developed countries like USA and UK (Lewis, 2018:68).

For instance, the Competition Commission of South Africa had a workshop on Characterisation from 21 to 22 August 2023 and Professor Bill Kovacic, Global Competition Professor of Law and Policy at the Washington University, was invited to give his perspective on international jurisprudence on characterisation and also reflect on South African jurisprudence. This is because characterisation of cartel conduct is a new phenomenon in South Africa and most of the parties use it as a defence at the Tribunal/courts. The Competition Commission affirmed that it is faced with the "new generation" of cartel cases which are "characterised by a clear shift in the pendulum", being the cartel cases the Commission had been unsuccessful in prosecuting (Legal brief, 2022:1). South Africa is ahead of all African countries in the enforcement of competition policies. For example, there is a learning programme run by South African

Competition Commission in which other African competition authorities send their staff to learn more on competition laws and policies. At times, South African Commission staff members are sent to these agencies to assist with the implementation of their competition policies. Buthe and Kigwiri (2020:41) emphasise that the research on African national competition laws adoption is limited, and studies on their implementation and enforcement are even rarer. Sokol, Cheng and Lianos (2013:1) conclude that the academic literature on competition law focuses on developments in the USA and European Union (EU). Africa has been overlooked by competition law academia. In view of the above, experience drawn from African jurisdictions would not be sufficient for the purpose of this study.

The consulted literature studies confirmed that use of electronic surveillance is a common practice among competition authorities in the developed countries to detect and investigate cartels (Marinniello, Brismi & Regibeau, 2021:210). However, it is not the case in developing jurisdictions, and this can be attributed to several factors such as a lack of resources, inadequate legal framework, and/or limited technical expertise (Licetti, 2013:3). As result it is difficult to detect and investigate cartels (Werden, Hammond & Barnett, 2011:221). This is the gap the researcher has identified and intended to analyse the use of electronic surveillance in South Africa as one of the developing jurisdictions.

According to Lyons (2017:75) electronic surveillance is a useful tool for competition authorities to gather evidence of cartels, price fixing, market manipulation, abuse of dominance, and other violations of antitrust laws. However, it also raises concerns about the protection of privacy and human rights of the individuals and entities that are subject to surveillance (Bennett, 2011:486). As such, the reviewed literature further pointed out that electronic surveillance should be subjected to strict judicial oversight and safeguards to prevent violations and ensure accountability. As a result, this study analysed the use of electronic surveillance to investigate cartel conducts, while using the Competition Commission of South Africa in Pretoria, as a case study.

## **1.2 PROBLEM STATEMENT**

Problem statement is a statement that specifies exactly what is being studied or researched. Van Thiel (2014:12) provides that research problem lays the foundations



for the rest of the research, and it brings into focus what exactly will be studied and how. The researcher is a Senior Investigator at the Cartels division of Competition Commission of South Africa (Competition Commission) in Pretoria, from November 2011 to date (2024).

The Cartels division is responsible for investigating and prosecuting the cartel conducts, which include price fixing, market allocation and collusive tendering. The researcher also observed and experienced that the investigation techniques the Cartels division apply to resolve cartel conducts are interviews, interrogations, summons, dawn raids, corporate leniency policy and analysis of market conduct. These reactional cartel detection methods have proved not to be effective enough to curb cartels as attested by the 2020/2021 and 2021/2022 annual statistics nationally.

During 2020/2021 financial year Cartels division completed 28 cartel investigations and only six of these finalised cases were referred to the Tribunal for prosecution, while 22 were non-referred and closed. The 2021/2022 annual report indicates that Cartels division received and initiated 35 complaints. About 14 cases were referred to the Competition Tribunal for prosecution and 21 cases were non-referred and closed. This high number of non-referrals may suggest that the current investigation techniques and methods are not as effective as expected, in such that sophisticated and profitable cartels are not easily detected.

Van Heerden and Botha (2015:309) highlight that the secretive nature of cartel conducts poses challenges for competition authorities around the world to effectively detect them. Individuals involved try to conceal their illegal activities and evidence (Van Heerden & Botha, 2015:309). Competition Commission (2008:2) further showcased that cartel activities are conducted through a conspiracy among a group of firms, with the result that it becomes difficult to detect or prove without the assistance of a member who is part of it. Therefore, the study suggests that the Competition Commission should move from its reactional stance to devote significantly more attention to pro-active cartel detection measures. Pro-cartel detection measures include, electronic surveillance, which is an intelligence-gathering tool (OECD, 2024:2). The OECD (2013:9) further explains that cartels investigation can be

extremely challenging for competition authorities because they are reactionary most of the time, and they are more rarely taking proactive actions.

Additionally, in this study the researcher focused on the use of electronic surveillance as an intelligence gathering tool to investigate cartels conduct. Moreover, this study offers analysis of the use of electronic surveillance to investigate cartel conducts, while applying the case study on Competition Commission of South Africa in Pretoria. Electronic surveillance was seen as a useful investigative technique that may encourage the Competition Commission to adopt a proactive action to identify firms, which are potentially involved in a cartel conspiracy.

### **1.3 STUDY PURPOSE**

Van Thiel (2014:15) contends that it is important for the researcher to define the purpose of the study. The purpose of this study is to explore the importance of electronic surveillance in the investigation of cartels conducts at the Competition Commission in Pretoria. Exploratory research happens when a researcher examines a new interest or when the subject of the study itself is relatively new (Stebbins, 2001:2). Babbie (2020:91) highlights that the focus of the exploratory research is on the discovery of ideas and insights. Babbie (2020:91) further states that exploratory research studies have three main purposes, namely:

- To satisfy the researcher's curiosity and desire for better understanding.
- To test the feasibility of undertaking a more extensive study.
- To develop the methods to be employed in any subsequent study.

This study explored the value electronic surveillance adds in the investigation of cartels, which may assist competition authorities to adopt a proactive stance to easily identify firms, which are potentially involved in cartels conduct.

### **1.4 STUDY AIM**

De Vos, Strydom, Fouché and Delport (2011:107) share that the aim of the research is to establish facts and to determine whether there are interesting patterns in the existing data. Van Thiel (2014:15) argues that it is important for the researcher to give

a precise indication of what purpose the research is meant to serve. Therefore, the aim of this study was *'to explore the importance of electronic surveillance in the investigation of cartels conducts, focusing on the Competition Commission of Pretoria.'*

The researcher hopes the study would assist in arriving at constructive recommendations regarding the utilization of electronic surveillance for investigating cartel conduct, raise awareness of its importance and complexity, identify common challenges and best practices for its implementation in the Competition Commission of South Africa, and encourage individuals within the Commission to view electronic surveillance as an effective investigative tool.

## **1.5 STUDY OBJECTIVES**

To achieve the aim of this study, the following study objectives were designed:

- To determine what the concept “electronic surveillance” entails in investigations of cartel conducts at the Competition Commission in Pretoria.
- To analyse the role of electronic surveillance in the investigation of cartels at the Competition Commission in Pretoria.
- To highlight circumstances under which “electronic surveillance” should be authorised to be used during investigations of cartel conducts at the Competition Commission in Pretoria.
- To showcase limitations of the use of electronic surveillance during investigations of cartel conducts at the Competition Commission in Pretoria.
- To present the challenges of investigating cartel conducts in the Competition Commission in Pretoria.
- To determine the effectiveness of strategies employed to investigate cartel conducts at the Competition Commission in Pretoria.

## **1.6 RESEARCH QUESTIONS**

Creswell and Creswell (2018:133) emphasises that a research question is a single, overarching central question posed by the researcher to address the research problem. Fandino (2019:611) argues that a question is one of the first queries made when a researcher explores ideas. In addition, the findings of the study may be

relevant if they provide an accurate and unbiased answer to a question (Fandino, 2019:611). This implies that forming a question is identified as the initial step in research. From the purpose of this study, study aim and objectives, the central research question for this study was as follows:

- *What is the importance of using electronic surveillance in the investigation of the cartel conducts at the Competition Commission in Pretoria?*

The researcher presented several sub-questions to further refine the central question. Denscombe (2010:31) explains that research questions provide a clear picture of what exactly must be investigated and gives a full account of the nature of the work to be undertaken. Sub-questions are presented as a means of subdividing the central question into several parts (Creswell & Creswell, 2018:134). The following sub-questions were formulated to address the problem that was identified:

- What is electronic surveillance?
- What is the role of electronic surveillance in the investigation of cartel conducts?
- Under which circumstances should electronic surveillance be authorised to be used during the investigation of cartel conducts?
- What are the limitations of using electronic surveillance during the investigation of cartel conducts?
- What are the challenges encountered during the investigation of cartel conducts?
- How effective are the strategies applied to investigate cartel conducts?

## **1.7 STUDY SIGNIFICANCE**

Bryman (2021:5) emphasizes the significance of research that not only advances existing knowledge but also meets practical needs, and addresses contemporary societal issues. This research contributed to the body of knowledge regarding the importance of using electronic surveillance in the investigation of cartel conducts. It is mentioned under problem statement that competition authorities rarely take proactive actions to identify firms, which are potentially involved in a cartel conspiracy. Therefore, the researcher is of the view that the result of the research will add value to Competition Commission as it enhanced the process of detecting and investigating

cartel conducts. The outcome of this study helped to improve the knowledge and competence of the investigators regarding the application of electronic surveillance in the investigation of cartel conducts.

It is envisaged that the outcome of this study will also be available to students at the University of South Africa and the broader academic community. Healthy market conditions benefit society by fostering competition among firms, which can lead to lower prices, higher quality goods and services, greater variety, and increased innovation.

Furthermore, to satisfy the viewpoints of De Vos, Strydom, Fouche and Delport (2011:94), this study possibly benefited the following sectors:

- **Academic community:** The new knowledge will be available to UNISA libraries, and the greater academic community will have access to the information. The information can be used both in curriculum and learning programmes and as a referral source for students and researchers for further studies on this subject (Analysis of the use of electronic surveillance to investigate cartel conducts: A case study of Competition Commission in Pretoria).
- **Industry:** The South African Competition Commission will benefit from this research. It will provide the investigation model on how to implement electronic surveillance as an investigation tool to assist the Competition Commission to easily detect and prosecute cartel activities. The application of electronic surveillance can facilitate the detection of new cartels by monitoring suspicious communications and transactions among competitors. This research will benefit investigators as they will acquire more knowledge, improved skills, methods and techniques in terms of applying electronic surveillance to investigate cartels.
- **South African society:** The successful implementation of electronic surveillance as a result of this research recommendation to prevent cartel behaviour will lead to increased customer choices and reduced prices for goods and services, which can enhance the quality of life for consumers. It will encourage innovation by creating a level playing field for businesses to

compete on merit rather than on unfair advantages. Lastly, it will stimulate economic growth by creating a conducive environment for investment, job creation, and technological advancement.

## **1.8 DEFINITIONS OF KEY CONCEPTS**

### **1.8.1 Cartel conducts**

It is an illegal secret agreement concluded between competitors to fix prices, restrict supply, divide markets or rig tendering procedures (Jaspers, 2017:320). The agreement often relates to sales prices or increase in such prices, restriction on sales or production capacities, sharing out of product or geographic market or customers, and collusion on the other commercial conditions for the sale of products or services (Rodger & MacCullah, 2015:213). According to Crowe and Jedličková (2016:401), cartel conducts are widely considered immoral and economically inefficient because they undermine the role of an open and competitive market. In terms of the Competition Act (No. 89 of 1998), as amended, a cartel conduct exists when firms in the same line of business or who are competitors agree to act together to improve their profits and dominate the market, instead of competing. In terms of Section 4(1)(b) of the Competition Act, 1998 cartel conduct includes price fixing, market allocation and collusive tendering (Roberts, 2020:414).

### **1.8.2 Electronic surveillance**

Friedewald and Burgess (2022:45) define electronic surveillance as the collection or monitoring of information about a person or persons using technology, often in the context of security and crime investigation. Electronic surveillance has become popular due to technological advances, and it can significantly help in criminal investigations because it allows the government to observe and listen to people during their inattentive moments, when they may be talking about their criminal activities (Wilson, 2019:45). Heibutzki (2018:1) further mentioned that electronic surveillance refers to the surveillance of email, fax, internet, and telephone communications. Other examples of electronic monitoring include computer forensics and subpoena of data stored in the cloud.

### **1.8.3 Intelligence**

Intelligence is the continuous or prolonged observation of a target individual, group, or organisation by clandestine means to gather information relative to an open criminal investigation (Ratcliffe, 2022:54). Gill and Phythian (2018:22) define intelligence as a product created through the process of collecting, collating, and analysing data, for dissemination as usable information that typically assesses events, locations or adversaries, to allow the appropriate deployment of resources to reach a desired outcome. According to Cordner and Scarborough (2010:91), intelligence involves collecting and analysing information that relates to the existence, scope and impact of organised crime.

### **1.8.4 Investigation**

An investigation is evidence gathering and assessment process conducted by competition authorities for ascertaining whether specific undertakings have infringed competition law (Urmonaite, 2022:1). Hess and Orthman (2010:6) add that investigation is a systematic search for truth, mainly aimed at actively clarifying the criminal situation based on objectives and subjective traces. Investigation involves the identification of physical evidence, gathering of information, collecting and protecting evidence, interviewing witnesses and interrogating suspects in order to find truth about the alleged crime (Gehl & Plecas, 2018:62).

## **1.9 SCOPE OF THE STUDY**

This study was confined to the Competition Commission of South Africa, Pretoria, soliciting views of ten (10) participants overall. The Competition Commission is responsible for investigating and prosecuting anti-competitive behaviour, including cartel conducts. The investigators and legal counsels are major role players in the investigation and prosecution of cartel conducts in the institution.

The selection of the organisation and participants allowed the researcher to collect complete and rich data on the investigative measures used to combat cartel behaviour, and the possibility of using electronic surveillance in investigations of cartel behaviour. The time frame provided was sufficient for the purposes of the study, which was, to explore the importance of electronic surveillance in the investigation of cartels conducts at the Competition Commission in Pretoria.

## **1.10 SUMMARY**

In this chapter, the research was introduced by providing a short background, followed by an overview of the conceptual framework for the study. It identifies the research problem, that is, the low effectiveness of cartel reactional detection methods to curb cartel activities. As a result, the researcher decided to explore the importance of using electronic surveillance as an intelligence gathering tool to investigate cartel conducts. This chapter further outlined the research aim, research objectives, research questions, definition of key concepts, study significance and scope of the study. The purpose of this chapter was to ensure that the reader understood the topic under research.

The next chapter (Two) presents a literature review related on the use of electronic surveillance to investigate cartel conducts. The study aim, and objectives, guided this study. Sources consulted were drawn from international jurisdictions in developed countries because of sufficient literature available on the subject and significant progress made by these countries in implementing and enforcing anti-competitive regulations.



## CHAPTER TWO: LITERATURE REVIEW ON THE USE OF ELECTRONIC SURVEILLANCE TO INVESTIGATE CARTEL CONDUCTS

### 2.1 INTRODUCTION

This chapter presents a selected literature review related to the research topic. The primary objective was to offer research studies on what is already known on the use of electronic surveillance to investigate cartel conduct, to this end, the cartel conducts are also regarded as a criminal activity (Machi & McEvoy, 2009:2). This literature review intends to further orientate the reader on what earlier empirical studies found on this subject. It will also focus on available legislations, relating to the 'Local, National and Globally.' In the absence of literature addressing topics similar to the research topic, the researcher used the sub-headings to get reliable and relevant information on this research topic. The reviewed studies are guided by this study aim; *'What is the importance of using electronic surveillance in the investigation of the cartel conducts at the Competition Commission in Pretoria?'*

Moreover, stemming from the study aim, the following study objectives were formulated and acted as guidelines thereof:

- To determine what the concept 'electronic surveillance' entails in investigations of cartel conducts at the Competition Commission in Pretoria.
- To analyse the roles of electronic surveillance in the investigation of cartels at the Competition Commission in Pretoria.
- To highlight circumstances under which "electronic surveillance" should be authorised to be used during investigations of cartel conducts at the Competition Commission in Pretoria.
- To showcase limitations of the use of electronic surveillance during investigations of cartel conducts at the Competition Commission in Pretoria.
- To present the challenges of investigating cartel conducts in the Competition Commission in Pretoria.
- To determine the effectiveness of strategies employed to investigate cartel conducts at the Competition Commission in Pretoria.

The guiding study aim, and objectives were not restricted to the study location, the focus was based on available local and international studies on this subject. Seminal sources were consulted to respond to the study aim and objectives. Information outside this subject were not included in this chapter. Seminal sources consulted were drawn from international jurisdictions in the developed countries because of sufficient literature available on the subject and significant progress made by these countries in implementing and enforcing anti-competitive regulations.

Therefore, the literature on this study focused on jurisdictions in developed countries, namely United Kingdom, United States of America, Australia, Brazil, and Israel. The reason was that competition authorities in these countries have made significant progress in implementing and enforcing anti-competitive regulations. In these jurisdictions competition authorities have implemented proactive cartel detection measures, including electronic surveillance in the investigation of cartel activities. The objective of this study was easily achieved by drawing experience from these jurisdictions. Moreover, there was an ample amount of literature available on this subject. This was demonstrated during the discussion of the literature on cartel conduct investigations in this study. The researcher also highlighted the status of Competition law in Africa.

## **2.2 THE IMPORTANCE OF USING ELECTRONIC SURVEILLANCE IN THE INVESTIGATION OF CARTEL CONDUCTS**

This section of the literature review addresses the study aim *‘to explore the importance of electronic surveillance in the investigation of cartels conducts, focusing on the Competition Commission of Pretoria.’* The aim of this study was mapped with objective 1 of this study, namely: *‘To determine what the concept “electronic surveillance” entails in investigations of cartel conducts at the Competition Commission in Pretoria.’*

According to Watney (2008:1), electronic surveillance is one of the investigation tools used by Law Enforcement Agencies (LEAs) and government agencies around the world to detect, prevent, investigate and prosecute criminal activity. Watney (2008:1) further mentions that it is an intrusive method used to gather information or evidence of suspected criminal activities in a secret manner and without the knowledge of the

suspect or targeted person. Heibutzki (2018:1) states that there are different types of surveillance, which include electronic surveillance. In addition, it is important to firstly understand the meaning of surveillance and its origin, before focusing on electronic surveillance and its importance in the investigation of criminal activities.

### **2.2.1 The conceptualisation of the term ‘surveillance’**

Zhang, Peterson Jr and Sun (2017:98) highlight that surveillance is widely used around the world and is defined as the act of monitoring behaviour or activities for the purpose of influencing, controlling, guiding or protecting people. Heibutzki (2018:1) defines surveillance as the covert observation technique used by law enforcement and government agencies, and private sectors to investigate allegations of illegal behaviour. This implies that surveillance can be used for several reasons, such as protecting people and properties, gaining information on a certain objective or finding evidence on a person or organisation (Watney, 2010:525; and Turanjanin, 2020:292).

Petersen (2012:3) indicates that surveillance’s origins can be traced back to a time when humanity learned to craft metal and glass to observe more distant objects, when it meant nothing more than spying from behind bushes. Surveillance then evolved into the realm of technology, moving from human eyes and security forces to sensors and software. This shows that surveillance is an investigation tool that kept on evolving (Watney, 2010:525).

Voitovych (2020:191) reveals that surveillance is one of the oldest ways to obtain information about crime, and it is still used today by LEAs around the globe to detect, prevent and investigate crime. Therefore, surveillance is a common investigation method used by LEAs around the globe for criminal activities. Van Brakel and De Hert (2011:168) state that ‘surveillance’ refers to the ‘monitoring, observing, or listening to people, their movements, conversations, or other activities or communications; recording anything monitored, observed, or listened to during surveillance; and surveillance by or with the assistance of a surveillance device. Hulnick (2022:39) asserts that surveillance has traditionally been performed primarily by a single spy or a small group of spies. It consisted mainly of spying agents who were engaged in both criminal and political investigations. Michael (2021:45) adds that historically, surveillance gathered and collected information, monitored the actions of other people (Usually enemies), and used that information to help gain a better understanding of

the party being spied on. Coleman and McCahill (2011:3) emphasize that surveillance and criminal investigation go hand in hand as they make police more effective and efficient in combating complex and covert criminal activities. Haggerty, Wilson and Smith (2011:231) agree that surveillance has always been associated with policing and fighting crime.

Strauss, Wright and Kreissl (2015:53) point out that as technology developed, so did surveillance and thus became part and parcel of modern societies. LEAs are now using advanced technology for surveillance, including high-technological cameras, audio equipment and computer hacking. Van Brakel and De Hert (2011:170) confirm that surveillance has always been an integral part of the LEAs, and in recent decades surveillance technology has become digitalised and proliferated, taking on more and more police roles, thereby changing the responsibilities of the LEAs around the globe. Van Brakel and De Hert (2011:170) further add that digital systems are becoming increasingly important for usage by LEAs to combat serious organised crime.

Geldenhuis (2021:16) also agrees that surveillance technology is playing an increasingly important role in law enforcement, as it is primarily introduced to combat criminal activity where traditional police methods seem to fail. Geldenhuis (2021:16) further states that the use of surveillance allows law enforcement a chance to gather extensive information either covertly or overtly. Covert surveillance is carried out without the knowledge of subject under investigation whereas overt surveillance is performed using devices that are visible and recognisable such as a Close-Circuit Television (CCTV) system. Moreover, there are different types of surveillance, from electronic surveillance equipment to complex methods and systems.

Furthermore, the system and equipment used depend on the type of case under investigation. Heibutzi (2018:1) outlines selected examples of surveillance in criminal investigation:

- **Electronic surveillance:** With the advancement of electronic devices in becoming smaller, more powerful and more connected electronic surveillance has changed immeasurably and it is a most commonly used tool during investigations. This relates to monitoring electronic-[e]-mail, fax, internet and telephone communications.

- **Fixed surveillance:** It is also known as stakeout. It requires officers to covertly monitor people and places from a distance.
- **Technical surveillance:** The investigator installs a hidden camera and recording equipment in a parked car.
- **Undercover operations:** This type of surveillance has long been a tool for conducting serious and complex investigations. It is mostly a covert type of surveillance which happens when investigators infiltrate criminal network and pose as offenders to uncover organised crime activity.

These bulleted surveillance examples recommended for criminal investigations illustrate the evolution of technology, showcasing how surveillance tools have become increasingly sophisticated, capable of capturing more information than ever before. Vervaele (2013:116) contends that surveillance is increasingly used as an investigative technique and involves different *modus operandi*, namely behavioural surveillance, communication surveillance, data surveillance, location and tracing, body surveillance, attitude surveillance or a combination of these. The continuous innovation of technical devices and the digitalisation of society result in constantly new *Modus Operandi (MO)*.

### **2.2.2 The use of electronic surveillance during investigations of cartel conducts**

Based on this study, the reviewed literature studies focus on the use of electronic surveillance as an intelligent or evidence gathering tool in the investigation of cartel conducts. The literature covers what the concept electronic surveillance entails and its importance in the investigation of criminal activities. The electronic surveillance is a broad term that refers to the use of one or more electronic devices to monitor the actions and conversations of others without their knowledge or consent (DCAF, 2022:1). The purpose of electronic surveillance is significantly different, however, in law enforcement is to collect evidence of a crime or to collect information about suspected criminal activity (DCAF, 2022:3). Jepsen (2018:97) proves that electronic surveillance emerged as early as the telegraph. After the invention of the telegraph in 1844, techniques for intercepting communications were developed. Hochmann (2022:29) highlights that wiretapping, the first form of electronic surveillance, began in New York in 1895 when a former telephone worker who joined the city police

suggested that it might be a good idea to tap phone lines to intercept the communications of a criminal network. Hochmann (2022:29) adds that before the tap became a crime-fighting tool, ordinary people used it as a means of missions such as stealing trade secrets and eavesdropping on gamblers' bets. It is now widely adopted by governments and LEAs around the world as a critical tool in combating organized crime and addressing national security threats (Wills, 2017:76).

Moreover, the DCAF (2022:1) adds that electronic surveillance is an intrusive method employed by LEAs to covertly gather information and evidence of suspected criminal activity without the knowledge of the suspect or subject. The information or evidence collected is mainly used in a court of law to prove the commission of crime. Vervaele (2013:116) describes electronic surveillance as a form of surveillance to monitor the whereabouts, movements and specific actions of individuals within the framework of criminal proceedings. According to the UNODC (2009:1), electronic surveillance performs a similar function to covert operations but allows for more comprehensive evidence gathering. It is a preferred investigative method to investigate serious and organised criminal activities.

Ball and Haggerty (2020:82) explains that electronic surveillance can be done in a variety of ways, including tracking people on Closed-Circuit Television (CCTV), reading text messages, sifting through internet browsing history and social media and spying on people by covertly activating webcams and microphones. The UNODC (2018:1) supports that there are several ways to electronically monitor an individual's conversations, online activity, and movements during criminal or cartel investigations. To this course, the following are regarded as types of surveillance used in criminal investigation by the LEAs and other regulatory bodies around the world:

- **Audio surveillance:** Audio surveillance involves listening to third-party conversations and recording them. This technique is often used by LEAs. Most audio surveillance systems involve bugging rooms, carrying cables, tapping phones, or listening remotely. Eavesdropping is one of the most common and simple forms of audio surveillance. This is a favoured method due to its very discreet nature and allows both sides of the conversation to be clearly recorded (Weiss, 2018:132).

- **Visual surveillance:** It consists of hidden video surveillance devices, in-car video devices, body worn video devices, thermal imaging, forward-looking infrared and CCTV (Smith & McCusker, 2020:89).
- **Tracking surveillance:** Tracking surveillance is a technique that involves monitoring and recording the movements of individual or objects. Tracking surveillance can be conducted using various methods such as Global Positioning System (GPS) tracking, Radio Frequency Identification (RFID), and video surveillance (Cunningham & Hester, 2023:65).
- **Data surveillance:** Data surveillance is the practice of monitoring and collecting online data as well as metadata. It is concerned with the continuous monitoring of users' communications and actions across various platforms (Andrejevic, 2022:41).

The integration of video and audio monitoring provides a comprehensive overview of the events taking place at a specific place and moment. It is a means of monitoring behaviour, activity and information with the aim of protecting, managing, or influencing a certain location (Phadtare & Goud, 2018:1623). The utilisation of mobile phone surveillance is quickly emerging as an effective method for gathering personal information about an individual. Geographic location can be easily tracked and is useful in determining a person's location in the future (Watney, 2021:464).

### **2.2.3 The importance of electronic surveillance during investigations of other criminal conducts**

Countries around the world acquired and developed techniques or tools to disrupt and dismantle domestic and transnational organised crime groups (Fijnaut & Weenink, 2021:97). Electronic surveillance is one of the most important and a highly effective law enforcement tool in fighting organised crime. Such surveillance may occur live and in real-time or after the fact. It enables LEAs to learn about crimes before they occur through the surveillance of criminal activities, such as conspirators making plans to meet or deliver contrabands or disrupting activities where appropriate (Wheatley, 2018:14). Taylor and Evans (2021:145) agrees that surveillance is an important part of crime investigation. It is necessary for the simple reason that criminals go to great lengths to cover up their criminal activities. Watney (2010:525) states that electronic

surveillance is one of the central and most important tools of modern law enforcement. It facilitates the detection, investigation, prevention and deterrence of crime, the safety of society and police officers, the arrest and prosecution of criminals and the protection of innocent people.

Geldenhuys (2021:17) approves that electronic surveillance is an important tool for investigators when detecting or preventing crime and holding perpetrators to account. Geldenhuys (2021:17) further adds that the ever-increasing rate of crime and the use of cutting-edge technology to commit crime, especially organised crime makes it imperative that LEAs increase their use of crime-fighting technology. Orthman and Hess (2013:445) view surveillance as important in the investigation of crime because it assists the LEAs, amongst others, to accomplish the following factors:

- To gain information needed for building up a criminal complaint.
- To collect the information for search or warrant.
- To find out who the associates of the suspects are.
- To observe crimes while they are being committed, carry out lawful arrest.
- To catch criminals red-handed while busy committing crimes and arrest them.
- It helps the investigators to gather reliable and objective evidence of a crime.

The bulleted factors indicate the undeniable importance of utilising electronic surveillance in criminal investigation, as it enables the gathering of “impossible” evidence. It enables the LEAs to address the increasingly complex and sophisticated crimes committed by organised criminal gangs. Graham and Kitchin (2021:215) asserts that electronic surveillance is an infinite tool used for a variety of purposes, including finding valuable evidence for criminal suspects. Goold (2022:78) reiterates that surveillance plays an important role in the law enforcement fraternity as it helps police officers to monitor public places and private properties, collect vital evidence and track the movements of suspects. Miller and Sweeney (2023:112) further emphasises that this technology has revolutionised the way law enforcement works and has become an integral part of modern law enforcement. Some of the reasons for LEAs, including the National government to initiate the need for surveillance cameras, including CCTVs for crime combating, prevention and investigations, as the following section refers:



- **Crime prevention:** According to Welsh, Farrington and Taheri (2011:111), video surveillance or the CCTV is a very popular and widely used means of preventing crime and improving safety in public spaces in many countries. Coleman and McCahill (2010:14) concur that surveillance has a long history in relation to fighting crime.
- **Real-time monitoring:** Sung and Park (2021:1) state that surveillance cameras can actively monitor in real-time monitoring to detect crime and other incidents without human input.
- **Investigation:** Coleman and McCahill (2010:4) indicate that surveillance footage provides valuable evidence in criminal investigations, including identifying suspects and providing a timeline of events leading up to the crime. The camera footage can help investigators to build a compelling case against suspects and increase the chances of a successful prosecution.
- **Public safety:** Capers (2012:959) highlight cities and towns around the world are increasingly using CCTV public video surveillance as a law enforcement tool to monitor public areas, schools, business and residential areas. This can help improve community relations with law enforcement and create a safer environment for everyone.
- **Cost-effective:** Matczak, Wójtowicz and Dabrowski (2022:557) state that surveillance cameras are a cost-effective way to improve public safety. They are relatively inexpensive compared to other forms of law enforcement technology, and their installation and maintenance costs are minimal.

In summary, CCTV video surveillance is a tool that is successfully used to reduce and prevent crimes. It provides valuable visual evidence that can help identify suspects and provide a clear record of what happened. Therefore, LEAs should take advantage of the benefits of surveillance technology to resolve complex and sophisticated cases. According to Welsh and Farrington (2009:716) the primary purpose of the CCTV camera is to create awareness among members of the public, especially potential offenders, that they are under surveillance and there is a heightened risk of being apprehended by the authorities if a crime is committed. The above bulletins continue to highlight that the CCTV camera can be a cost-effective way to deter, document, and

reduce crime. Bulletins demonstrate that the introduction of the CCTV cameras have contributed to reductions in various crimes (Welsh & Farrington, 2021:33).

### **2.3 THE ROLES OF ELECTRONIC SURVEILLANCE IN THE INVESTIGATION OF CARTEL CONDUCTS**

Ran (2016:7) states that surveillance, among other things, helps governments collect more information and exert greater control over modern society. Haggerty, Wilson and Smith (2011:231) concurs that surveillance as a technology of governance, has been viewed as an integral feature of social control, disciplinary power and modern subjectivity. It is a technological tool often associated with policing and crime control. Hendrix, Taniguchi, Strom, Barrick and Johnson (2018:55) add that surveillance has always been a central part of law enforcement work but, over time, its form has changed significantly, giving law enforcement more authority in combating criminal activity. Holmes (2014:1) concurs that surveillance technology helps LEAs to stay one step ahead of criminals.

Murphy and Wakeman (2022:245) emphasises that the future of crime fighting is being defined by the usage of technology, which includes the use of electronic surveillance. Murphy and Wakeman (2022:245) further states that electronic surveillance is becoming more popular among LEAs as it gives them unprecedented powers to crack down on serious and complex criminal activity. Vervaele (2013:116) agrees that evolving technology is helping law enforcement to combat new forms of crime as criminals become more sophisticated in their use of technology and data.

The United States Department of Justice [USDJ] (2013:3) shares that electronic surveillance is an important crime-fighting tool because it plays a key role in combating serious organised crime, including cartel activity around the world. This implies that it is an important tool used by LEAs, including competition authorities to detect, prevent, investigate and prosecute the guilty.

According to Clark (2016:3), the main purpose of electronic surveillance is to protect society by preventing illegal and dangerous activities. Neyroud and Beckley (2022:162) claims that surveillance technology benefits community and LEAs in many

ways. For instance, a mere presence of electronic surveillance device, such a video camera can deter a criminal from committing a crime. This confirms that electronic surveillance serves as a crime deterrence mechanism.

McStay (2021:145) adds that surveillance generates a proper chain of evidence that can easily be admissible in a court of law. It, therefore, assists LEAs to obtain evidence needed to carry out investigations for successful prosecution of a crime. The digitalisation of the global economy is forcing competition authorities around the world to modernise their cartel investigation methods and adapt to new technologies used by companies to do business (OECD, 2020:2). As a result, competition authorities have begun to turn their attention to the use of proactive cartel detection methods (Hüschelrath, 2010:1). Foremny and Dorabialski (2018:950) state that proactive detection methods, amongst other, include electronic surveillance.

Furthermore, Baker and Gunter (2005:1) suggest that the role of electronic surveillance is to collect information for the furtherance of an investigation. The investigator may require the information for search warrant, to gather intelligence for a dawn raid or to locate a suspect, contraband, or the site of illegal activities. Ashby (2017: 441) adds that the deployment of surveillance equipment may vary depending on the type of information required. The intention could be to prevent crime, to obtain evidence, to obtain information for interrogation purposes or to obtain information for court proceedings. To sum it up as McCulloch and Wilson (2021:112) indicates that the surveillance allows investigators to uncover the evidence necessary to convict criminals or justify further legal action, such as issuing search warrants; to track suspects' actions and their whereabouts using surveillance methods, looking for their involvement into criminal activities and to identify and map criminal networks, including relationships between suspects and their allies, providing valuable insight into how criminal organisations are structured and operated.

### **2.3.1 The roles of electronic surveillance**

There are several ways to electronically monitor an individual's conversations, online activity and movements during the investigation of criminal activities. The role of each type of electronic surveillance is discussed in the following section:

- **Audio Surveillance:** According to Gulzar, Abbasi, Wu, Ozbal and Yan (2013:83) audio surveillance is one of the oldest methods of surveillance technology. It is mainly used by LEAs, private investigators and government intelligent services to track phone conversations, track location and monitoring the data. Gulzar *et al.*, (2013: 83) further states that wiretapping is one of the most common and simple forms of audio surveillance. Most audio surveillance consists of either bugging a room, wearing a wire, tapping a phone or distance listening (Gill & Phythian, 2018:112).
- **Wiretapping:** Wiretapping is the interception of the contents of communication through a secret connection to the telephone line of one whose conversations are to be monitored usually for the purpose of criminal investigation by law enforcement Nunn (2018:28). Nunn (2018:28) went on to mention that wiretappings are primarily tool used by law enforcement to investigate criminal activities, especially organised crime and counterintelligence.
- During the investigation the investigators can define the scope of criminal conspiracy or organisation, the nature of its activities, and the identities of its participants. It also makes it possible to covertly obtain evidence of a particular conversation, series of conversations or meetings that investigators use in prosecuting suspects of crimes. Dressler, Thomas III, and Medwed (2017:783) assert that Wiretapping is strictly regulated by state law and is carried out when there is reasonable suspicion that a crime has been committed or attempted to be committed.
- **Room microphone:** This is another audio surveillance technique which involves planting a wireless microphone in a room to pick up conversations. Room microphone works in a similar fashion to wiretapping. The microphone sends a signal to a receiver, just like a wiretap does, and the signal can be directly recorded (Weiss, 2018:92).
- **Video surveillance:** Gulzar *et al.*, (2013:85) state that video surveillance uses video cameras to view a wide range of areas for detection and prevention of criminal activities. Alexandrie (2017:210) contends that the CCTV surveillance has become widely used to investigate different criminal activities from common robberies to serious organised crimes. Priks (2015:289) concurs that surveillance cameras have become a common method to investigate crime. Morales, Salazar-

Reque, Telles and Diaz (2019:1) emphasise that it is a method which enable the LEAs to investigate variety of criminal activities, and it helps LEAs to identify and arrest the perpetrators of crime.

Surveillance can play a crucial role in investigating cartel conduct as it helps the competition authorities to gather evidence and monitor the activities of suspected cartels. By using surveillance techniques, authorities can identify cartel members, their communication channels, and the nature of their illegal activities. According to International Competition Network [ICN] (2021:18), some of the ways surveillance can assist in investigating cartels conduct include the following categories:

- **Monitoring communication:** Surveillance allows authorities to monitor phone calls, emails, and other forms of communication to gather evidence of cartel activities. It helps LEAs to corroborate other evidence, such as linking suspects to a crime through their communications.
- **Gathering evidence:** Surveillance can provide valuable evidence such as recordings, documents, and other materials that can be used to prove the existence of a cartel and its illegal activities.
- **Identify cartel members:** Surveillance can help identify individuals involved in cartel conduct by tracking their movements, interactions, and communication patterns.
- **Uncovering hidden agreement:** Surveillance can reveal hidden agreements or arrangements between cartel members that are not publicly known.
- **Detecting collusive behaviour:** Surveillance can help to detect collusive behaviour by monitoring price-fixing activities, bid-rigging schemes, market allocation agreements, and other anti-competitive practices.

The bulleted points show that electronic surveillance is a practical investigative tool if the cartel under investigation is ongoing, and the agency has sufficient information about the details of the cartel's activities. Electronic surveillance can provide valuable and effective evidence of cartel activities and may be an appropriate option when an agency has secured internal cooperation to support the use of covert recording devices (Buccirossi, 2023:315). However, it should be noted that in many countries, national laws impose strict restrictions on the use of electronic surveillance as an

investigative tool, often limiting its use to criminal investigations only. It may be better to use this tool for serious and complex cartel cases, ICN (2021:18).

### **2.3.2 The adoption of surveillance cameras for criminal investigations**

As claimed by Ratcliffe (2020:1) that surveillance camera are valuable tools that help criminal investigations in several ways. The footage captured by video cameras provide a wealth of information that can be used to identify suspects, track their movements, and piece together the sequence of events leading up to a crime scene. According to Norris and Armstrong (2019:287), limited key roles of surveillance cameras during investigation of criminal activities include the following:

- **Capturing key evidence:** Surveillance cameras often capture images and footage that can be used to identify suspects, their vehicles and other important details that can help to solve a crime.
- **Providing multiple perspectives:** Surveillance cameras can be placed in multiple locations and thus providing different perspectives on a crime scene. This can help investigators to get a complete picture of what happened and can help in reconstructing the sequence of events.
- **Real-time monitoring:** Surveillance camera capture real-time footage of various locations, helping LEAs to gather valuable evidence. The footage obtained from the surveillance camera can be used to identify suspects, establish timeless, corroborate witness statements, and provide visual evidence in court. Surveillance camera can provide real-time monitoring of public spaces, allowing law enforcement to respond quickly to incidents and potentially arrest suspects in the act. This can be helpful in cases where time is of the essence, such as in cases of violent crimes or terrorism.
- **Helping with investigations:** Surveillance footage can help investigators identify witnesses, track suspects' movements and build a timeline of events. It can also be used to corroborate witness statements and help to rule out potential suspects.
- **Reducing reliance on eyewitness testimony:** Eyewitness testimony can be unreliable. Therefore, surveillance footage can provide objective evidence that can help corroborate or disprove eyewitness testimony.

The bulleted points' shows that surveillance cameras play a crucial role in providing necessary detail to assist in criminal investigation. When an investigator sees a surveillance camera at a crime scene, what comes to mind is to review the recording

to identify the suspect and potential witness. Therefore, it is important to have quality footage as it allows investigators to watch the entire crime incident in detail, providing information about the course of the incident, the methods used and to identify eyewitnesses (Ashby, 2017:444).

### **2.3.3 The use of electronic surveillance to investigate online [Internet] crimes**

Watney (2010:8) states that internet surveillance is a general term that refers to the collection of different types of information from the Internet through monitoring methods. The purpose of electronic surveillance conducted over the internet is to collect electronic surveillance information to investigate serious crimes. Trottier (2014:609) adds that internet surveillance is needed to reduce crime, it allows government and other agencies to maintain control, recognise and monitor threats, suspicious or anomalous activity, and prevent and investigate criminal activity. Watney (2010:1) asserts that cybercrime undoubtedly threatens the global growth and future of the internet. Many government agencies have decided to use electronic surveillance as an investigative method to prevent, detect, investigate and prosecute crimes on electronic media such as the Internet.

Stratton, Powell and Cameron (2016:25) mention that digital technology provides opportunities for law enforcement and government agencies to explore and investigate criminal activity both online and offline. For instance, data stored or transmitted on digital devices may be used to prove some criminal elements such as how a crime happened or to assist in providing an alibi or proof of intent. Stratton, Powell & Cameron (2016:26) argue that digital technologies enhance opportunities for state-sanctioned surveillance to occur. The use of surveillance technology by LEAs has expanded significantly, and plays an important role in policing, because new policing models are geared towards predicting what will happen in the future (Van Brakel & De Hert, 2011:163). Graef (2017:1) states that in the business arena, prices are increasingly set by computers instead of human actors. Chen, Mislove and Wilson (2016:1339) submit that the rise of e-commerce has unlocked practical applications for algorithmic pricing, where sellers set prices using computer algorithms.

Chen, Mislove and Wilson (2016:1339) further reveal that travel websites and other well-known e-retailers, have already applied algorithms pricing strategy to determine

what price best matches the demand and the offers of competitors. Algorithms can monitor prices more efficiently than human beings and are able to respond to market changes more quickly and accurately (Graef, 2017:1). However, Capobiano and Nyeso (2018:19) indicate that there is concern that businesses also use algorithms to engage in collusive conduct in the absence of any formal agreement or human interaction.

According to a report by Davenport and Ronanki (2022:108), companies are increasingly using algorithms to support the development of business strategy and prices. These algorithms are designed to predict an answer based on the available data. The more data is available the more accurate and useful the algorithm becomes. A market where all firms unilaterally adopt their own pricing algorithm, accessing their competitors' real-time pricing and adjusting to each other's prices within seconds or even in real time can constitute a breeding ground for tacit collusion.

This is the reason competition authorities are concerned whether the use of algorithms enable a new form of 'algorithmic collusion. Ong (2021:189) provides that competition authorities have become wary of potential anti-competitive outcomes that may result from the use of these computer-based tools by market participants, particularly those who compete directly against each other in digital markets. Calvano, Calzolari, Denicolo and Pastorello (2020:3267) add that there have been concerns that pricing algorithms could raise their prices above the competition level in a coordinated manner, even if they are not specifically instructed to do so and even if they do not communicate with each other. Calvano *et al.*, (2019:155) further state that Price decisions are increasingly in the hands of artificial algorithms, so algorithms can support collusive outcomes more effectively than human decision makers. Hansen, Misra and Pai (2021:3) highlight that competition authorities use machine learning algorithms to monitor price fixing by business such as e-retailers. In fact, machine learning algorithms are used to detect price fixing in many industries. For example, the European Union uses machine learning algorithms to detect price fixing in the financial sector. Hansen, Misra and Pai (2021:3) further state that researchers have developed machine learning algorithms that can detect price fixing in the airline industry. Larsson (2019:42) reveals that the machine learning algorithms can be used to monitor algorithmic trading by detecting deviating behaviour. Competition laws in the USA, EU



and UK have long forbidden competitors from colluding or conspiring to fix prices. Prior to the induction of Artificial Intelligence (AI) practices and the advent of pricing algorithms, price fixing was typically the result of wink-and-nod agreements reached in back rooms. Now, price fixing often depends on an entirely new character, that is, price algorithms.

## **2.4 CIRCUMSTANCES LEADING TO AUTHORISED USAGE OF ELECTRONIC SURVEILLANCE FOR CARTEL CONDUCTS INVESTIGATIONS**

This section focuses on the circumstances, legislations, policies and theoretical framework regulating the application of the electronic surveillance in the investigation of cartel conducts in South Africa and other international jurisdictions. The DCAF (2022:2) states that the widespread use of electronic surveillance by law enforcement has led to public scrutiny in recent years. This has been caused by prevalent violations of the laws regarding the conduct of electronic surveillance, even in the most democratic countries (Ioannou & Tussyadiah, 2021:101774). For instance, wiretapping abuses have been detected in most countries (Hildebrandt & Ekatarina, 2013:150).

Muñoz Muñoz, Urueña Pascual, Aparicio Morenilla and Rodríguez de los Santos López (2015:2) state that to prevent this, governments in various countries have put measures to highlight circumstances under which electronic surveillance can be used and the limitations in using electronic surveillance for investigation. This can be accomplished by providing for the oversight of law enforcement surveillance, accountability for abuses and errors and limits against common forms of surveillance (Solove, 2004:1708).

The reviewed literature studies in this section highlight that electronic surveillance is used throughout the world to fight serious and complex crimes, terrorism and to avert danger to state security. The electronic surveillance has been defined as a covert and intrusive method of gathering information that is done secretly without the target's knowledge (DCAF, 2022:1). Loftus and Goid (2012:275) state that traditionally, covert and intrusive tactics have been used by LEAs to obtain evidence against a subject who is suspected of having committed or while committing a crime. It is no

longer LEAs that are empowered with technology, but all consumers who can afford the systems and technologies that can be used to observe and to watch “without ceasing” (Abbas, Michael & Aloudat, 2011:32). It is for the reason, amongst others, that there are blends of legislation governing surveillance practices to avoid abuse and infringing citizens’ right to privacy.

## **2.5 THE CUSTODIANS OF ELECTRONIC SURVEILLANCE USAGE**

Baker and Gunter (2005:1) state that electronic surveillance is a critical investigative tool in the fight against crime and is used by government agencies and the private sector. Baker and Gunter (2005:1) argue that surveillance is one of the investigation techniques used by LEAs for criminal activities, but it is more common in the private sector because LEAs are, in most cases, reactive to a situation with the intention to arrest and prosecute criminals whilst private security provides protection through proactive and preventive measures.

In this study, the focus was on LEAs and intelligence services as these are government bodies that use electronic surveillance given their dealings with serious and organised crimes. The LEAs and other intelligence agencies use electronic surveillance to gather information for the purpose of detecting and preventing criminal activity or terrorist intent (Kolaszyński, 2019:128). LEAs have the task of gathering information in relation to a specific crime for prosecution purposes. The roles of law enforcement are confined within the criminal justice system, and intelligence agencies collect information for national security purposes (Herman, 2022:55). According to (Cocq & Galli, 2015:24), the information obtained by LEAs during the investigation is open to scrutiny during prosecution in a court of law and the information collected for intelligence purposes is deemed classified. In summary, the role of LEAs is to maintain law and order, protect citizens, and prevent, detect, and investigate criminal activity (Akhgar, Bayerl & Sampson, 2017:3).

There are other legal authorities which may be permitted to use electronic surveillance in the execution of their duties, namely: The State Security Agency (SSA), South African Police Service: Crime Intelligence Division (SAPS CID), South African National Defence Force: Defence Intelligence Centre (SANDF DIC), National Communications

Centre (NCC), and South African Revenue Services (SARS). However, not all these agencies might possess technical capacities for electronic surveillance, therefore; the implementation may be outsourced to relevant agencies who have the capacity (DCAF, 2022:3).

### **2.5.1 State Security Agency**

The SSA is the civilian intelligence agency of the South African government, falling under the Ministry of State Security. The SSA was formed in 2009 as an amalgamation of the National Intelligence Agency (NIA), which was responsible for domestic intelligence gathering, and the South African Secret Service (SASS), which was responsible for foreign intelligence gathering. The mandate of the SSA is to provide the government with intelligence on domestic and foreign threat or potential threats to national stability, the constitutional order, and the safety and well-being of these people. This allows government to implement policies to deal with potential threats and better understand existing threats, and thus, improve their policies.

The SSA focuses on national interest areas, including terrorism, which involves deliberate acts to create terror through force, aiming to influence targets politically or materially; Sabotage refers to intentional actions or omissions that endanger the safety, security, or defence of vital public or private properties, including installations, structures, equipment, or systems; Subversion refers to covert unlawful acts or violent efforts intending to undermine or destroy the constitutional systems of government in South Africa; Espionage, which refers to unlawfully acquisition of sensitive information or assets in South Africa (National Government, 2023:1).

### **2.5.2 South African Police Service Crime Intelligence Division**

According to Scheepers and Schultz (2019:361), the SAPS CID, which belongs to the South Africa Police Service, is responsible for gathering intelligence and monitoring criminal activities in the Republic of South Africa. Its responsibility involves collecting information about illegal behaviour, supporting police investigations, and enhancing the efficacy of crime prevention endeavours. The SAPS CID's main objective is to gather, analyse, and distribute information with the aim of foreseeing, deterring, and observing unlawful acts. This suggests that it helps combat crime by collecting, organising, and evaluating intelligence data that can be used for effective law enforcement operations. There are two ways in which this occurs. Firstly, through the

SAPS CID operations, which provide for crime investigations based on intelligence. Secondly, the Intelligence and Information Management which involves analysing patterns of crime intelligence to assist in crime detection. This is done to support both crime prevention and crime investigation efforts (SAPS, 2009:1).

### **2.5.3 Defence Intelligence Centre/Division: South African National Defence Force**

According to Hurley (2012:12), the SANDF DIC/Division is the primary military intelligence agency responsible for cyberwarfare intelligence, surveillance, target acquisition, and reconnaissance. Engelbrecht (2007:1) adds that the SANDF DIC/Division is a military intelligence organisation that reports directly to the SANDF. Intelligence agencies contributing to the effective implementation of military operations and helps to ensure the success of these operations. Intelligence is therefore closely tied to leadership and operations. The Command and control is about making and carrying out decisions. The main purpose of intelligence is to support this process. Intelligence strives to achieve two goals. First, it provides accurate, timely, and relevant information about the enemy (Or potential enemy) and the environment. In other words, the primary purpose of intelligence is to support decision-making by reducing uncertainty about the enemy's situation to an appropriate level, Engelbrecht (2007:1). Counter-intelligence operations are supported by intelligence targets to protect friendly forces. Counter-intelligence includes both active and passive measures aimed at depriving the enemy of valuable information about the situation of allies. Counter-intelligence activities also include activities related to combating hostile espionage, sabotage, and terrorism. Counter-intelligence directly supports force protection efforts by helping commanders withhold information from the enemy and plan appropriate security measures (Engelbrecht, 2007:2).

### **2.5.4 Office for Interception Centre**

According to Fonseca and Van Wyk (2021:591), the Office for Interception Centre (OIC) was established in 2002 in terms of the Regulation of Interception of Communications and Provision of Communication-related Information Act [RICA] (No. 70 of 2002) and falls under the SSA. It provides centralised interception services to South African LEAs mandated with national security. It administers the 'hand over' of data from internet service providers and network operators to LEAs. In the past, LEAs used to carry out interception efforts separately, possibly leading to unnecessary

repetition of tasks and utilisation of resources. The establishment of the Interception Centre consolidates interception operations and lays the groundwork for enhanced interception management, aiming to enhance efficiency, reduce resource and cost duplication, as well as regulate and govern the interception landscape (Watney, 2015:1).

### **2.5.5 National Communications Centre**

The National Communications Centre (NCC) is a national facility for intercepting and collecting electronic signals and falls under the South Africa SSA. It is responsible for bulk electronic surveillance and eavesdropping of foreign communications. Sutherland (2017:83) reveals that the NCC has mass surveillance capabilities unregulated by law, which would necessarily be unconstitutional. On two occasions the Ministry has introduced legislation that sought to recognise the NCC in law. Firstly, the National Strategic Intelligence Amendment Bill No. B51-2002 was withdrawn, secondly the relevant provisions were removed during parliamentary debate. Sutherland (2017:83) further highlights that another concern is the unregulated use by Financial Intelligence Centre Act [FICA] (No. 38 of 2001), the SSA and SAPS. There were, however, claims by the UN Human Right Committee that the South African government is unlawfully conducting surveillance, intercepting and monitoring private communications (Like electronic e-mails (e-mails), Short Message Services (SMSs), and phone calls of its citizens on a mass scale (Giles, 2016).

### **2.5.6 South African Revenue Services**

The SARS utilises intelligence gathering techniques to identify instances of tax evasion and recover concealed revenues. It has implemented a new high-tech system that uses computer algorithms, machine learning, and other advanced technologies to ensure taxpayer compliance (Ferreira, 2021:13). The SARS gathers, examines, and shares financial intelligence data with appropriate authorities to combat illicit financial activities associated with money laundering. The SARS employs advanced data analytics and artificial intelligence to enhance its auditing processes and identify taxpayers for further scrutiny or investigations (Meyer and Verhoef (2023:25).

The SARS could use AI to identify false submissions. In the case of tax, an AI system can develop a model for recognising false submissions based on its analysis of ones belonging to known tax offenders. Overall, SARS is using intelligence to improve its

collection efforts and combat money laundering activities (Smit & Nel, 2023:155). The use of technology has made it easier for SARS to detect tax evasion and recover hidden revenues, making it more difficult for taxpayers to lie regarding their returns (Tshabalala & Jacobs, 2024:88).

## **2.6 LEGAL REGULATIONS FOR THE USE OF ELECTRONIC SURVEILLANCE DURING INVESTIGATIONS OF CRIMINAL ACTIVITIES**

The use of surveillance by LEAs around the world has caused controversy in recent years (Moore, 2011:114). As such there are circumstances under which a surveillance device can be used guided by measures put in place by government to avoid misuse and abuse.

- Due to its intrusive nature, electronic surveillance is subject to strict judicial controls and legal guarantees to prevent abuse and limit invasion of privacy (McIntyre, 2016:1).
- Electronic surveillance should be used as a last resort to investigate cartel activities. This implies that it should only be considered after other investigative methods and techniques have been shown to be ineffective in solving a case or in gathering information important to solving a case (Zhang & Mitchell, 2023:56).
- Any invasion of privacy must be proportionate to the severity of the alleged crime and the evidence expected (UK Government, 2018:30). There must be respect for human rights, and at the same time, recognise the dangers posed by suspected crime (DCAF, 2022:4).
- The law stipulates the specific requirements that must be met for electronic surveillance to be undertaken (Mutung'u, 2021:175):
  - Strong suspicion that a specific crime has been committed,
  - Seriousness of the offence justifies surveillance, investigative activities,
  - Investigative activities thus far have been unsuccessful and further enquiries would have no prospect for success.
- The law further stipulates who may be monitored, the type of surveillance allowed, the type of authorisations required and the subsequent procedural conclusions and

steps that must be taken for every piece of surveillance intelligence gathered (Mutung'u, 2021:175).

- A warrant of arrest is required as a control mechanism, to create balance between law enforcement's need for secrecy, individual privacy, and transparency (Bloch-Wehba, 2018:145). According to Desai (2014:579), warrants limit LEAs on how and when surveillance can be used. The LEAs can monitor individuals and intercept private communications, but there are rules about when and how they can do this. The police are required to apply to court of a law for a warrant before they can begin surveillance or a wiretapping operation. (Desai, 2014:579) concur that surveillance often require a warrant, involving review by a neutral judge. A warrant places limits on what information can be collected, how it can be collected and how it can be used.

The researcher submits that the indicated conditions reflect that it is the responsibility of government to put measures in place to define guidelines under which surveillance could be carried out. Such guidelines help to ensure that the use of surveillance technologies is lawful and responsible, and that there are measures in place that apply to collection, handling, and disclosure of material obtained using these technologies in order to protect individual privacy, personal data, human rights and fundamental freedom while effectively and appropriately pursuing legitimate law enforcement objectives. Therefore, other legal regulations guiding the use of electronic surveillance as an investigatory method exists and they differ per country, as discussed in the following sections.

## **2.7 SURVEILLANCE LAW IN VARIOUS JURISDICTIONS: THE INTERNATIONAL FOCUS**

Ran (2016:2) states that surveillance and privacy law are driven by social and technological change. The rise of the internet has complicated privacy laws, and many believe that the law has fallen behind. Hence legislators keep on enacting new laws, as technology evolves. The right to privacy is enshrined in article 12 of the Universal Declaration of Human Rights (UDHR), article 17 in the legally binding International Covenant on Civil and Political Rights (ICCPR) and in article 16 of the Convention of the Rights of the Child (CRC). As a result, many national constitutions and human

rights documents mention the right to privacy (Khan & Edwards, 2022:405). Roberts, Farahat, Oloyede and Mutung'u (2021:7) state that surveillance law provides a means to ensure that surveillance is narrowly targeted, while protecting citizens' rights by defining in law privacy and due process safeguards, transparency and independent oversight mechanisms.

## **2.7.1 The United States of America laws on the use of surveillance for criminal investigations**

### **2.7.1.1 Electronic Communications Privacy Act of 1986**

Kerr (2014:373) states that in 1986, Congress enacted the Electronic Communications Privacy Act (ECPA), 1986 to regulate government access to Internet communications and records. The ECPA, 1986 is widely regarded as outdated. The Bureau of Justice Assistance [BJA] (2023:1) indicates that the ECPA, 1986 updated the Federal Wiretap Act of 1968, which addressed interception of conversation using "hard" telephone lines but did not apply to interception of computer and other digital and electronic communications. Several subsequent pieces of legislation, including The USA Patriot Act of 2001 clarify and update the ECPA, 1986 to keep pace with the evolution of new communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases.

### **2.7.1.2 The National Security Letter**

Richards (2013:1942) states that the National Security Letter (NSL) of USA is the provision of the Patriot Act which authorises the Federal Bureau of Investigation (FBI) to obtain information about people from their telephone companies, internet service providers, bank and credit agencies without prior court approval. The American Civil Liberties Union [ACLU] (2023:1) mentions that the NSLs are covert and come with a gag order that prohibits the recipient of the letter from disclosing its existence, even to the person whose secrets have been told to the government. The NSLs can currently be obtained under four federal statutes:

- The Right to Financial Privacy Act of 1978.
- The Electronic Communications Privacy Act of 1986.
- The Fair Credit Reporting Act of 1971.
- National Security Act of 1947.

The mentioned Acts together allow the Federal Bureau of Investigation (FBI) to access a wide variety of information about people, including historical and transactional



information about people, including historical and transactional information relating to telephone calls and emails, financial information, and consumer credit information (Whitehead & Whithead, 2023:45). The letters, in accordance with the USA Patriotic Act, 2001 had a provision stating that the recipients were not allowed to discuss the letter's contents or instructions with anyone except a lawyer. These letters did not need approval from a judge and were only subject to a restricted assessment by the judiciary (Cole, 2021:112).

### **2.7.2 United Kingdom laws on the adoption of surveillance for criminal investigations**

The current legislator around surveillance law derives mostly from the Investigatory Powers Act (IPA), 2016 of the UK. The IPA, 2016 makes provisions on the interception of communications, equipment interferences, the acquisition and retention of communications data and bulk personal datasets. This Act sets out the investigatory powers which may be used. It also outlines powers suggesting interference of data, imposing duties and protection for privacy. Other legislation covering surveillance is the Data Protection Act (DPA), 2018, which was developed to protect peoples' personal data. The General Data Protection Regulation (GDPR), thus, the EU law, sets out the procedure organisations have to adhere to, when collecting personal data. Given that the UK has left the EU, GDPR laws will be retained into UK law as the UK GDPR. The Act provides for the power by granting a warrant to gather data, through tapping directly into communication channels from mobiles and computers. The government can demand that a public telecommunications service intercepts an individual's communications, allowing for the monitoring of activities without the knowledge of the individual (Lodder & Wright, 2022:223). According to Vallance & Mullen (2021:152), to protect the human rights of individuals, IPA, 2016 includes the following provisions:

- It places strict limits on the organisations and people which are allowed to use covert surveillance techniques.
- It sets the purpose for and conditions under which the techniques can be used.
- It specifies the way the information obtained covertly can be handled.
- It paces limitations on the way authorised bodies are allowed to carry out surveillance (i.e. the way the police can assess communications data, listen into phone calls, follow individuals, take photographs and intercept emails).

- A warrant must be in place before phone calls and emails can be intercepted.

The outlined bulleted provisions clearly show IPA, 2016 is now the main legislation governing the acquisition of communications data by authorities such as law enforcement agencies, and intelligence agencies. Therefore, this Act provides tools for law enforcement to investigate and disrupt the most dangerous criminals. It also put in place strict measures to ensure they are used in a way that is both necessary and proportionate. The IPA, 2016 governs the way in which law enforcement and intelligence agencies should use their investigatory powers.

### **2.7.3 Australian laws on surveillance**

Kendall and Frost (2022:249) states that the Australian government reformed the law in relation to electronic surveillance network and introduced the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021. Prior the amendment, the Attorney General's Department administered the Telecommunications Interception and Access (TIA) Act, 1979 and the Surveillance Devices Act (SDA), 2004. The TIA Act, 1979 protects the privacy of Australians by prohibiting interception of communications and access to stored communications. The privacy of Australians is also protected by the Telecommunications Act, 1997, which prohibits telecommunications service providers from disclosing information about their customers' use of telecommunications services.

Zalnieriute (2022:332) states that the Australian government decided to reform the Act due to technological advancement in relation to the internet and digital communication. They stated that the act was based on outdated technological assumptions and definitions. Therefore, the reform was needed to ensure that the law should be able to accommodate advances in technology. McCord, Birch and Bizo (2022:298) mention that the Surveillance Legislation Amendment (Identify and disrupt) Act 2021 introduced three new powers for Australia Federal Police and Australian Criminal Intelligence Commission to identify and disrupt serious online criminal activity, namely the power to collect intelligence, conduct investigations disrupt and prosecute serious criminal online activity. Mann and Murray (2021:44) add that the powers help the agencies to deal with cyber-enabled crime in the digital era.

#### **2.7.4 Brazilian laws on surveillance**

De Castro, Silva and Canedo (2022:1228) states that the Brazilian General Data Protection Law (LGPD), Federal Law No. 13,709/2018 has been enforced since September 18, 2020. Similar to the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA) 2020. Moreover, the LGPD is intended to regulate the processing of personal data (Isaza & Katshir, 2020). The Brazil's legal framework for data protection has evolved gradually over the past decade (Ramiro & Cruz, 2023:3). The implementation of the LGPD has been successful in enforcing a long-awaited regulation for both private and public organisations regarding the handling of personal data. However, certain important aspects like law enforcement investigations and public safety were not included in its scope. According to data protection experts in Brazil, the installation of surveillance systems without appropriate regulations for safeguarding data could potentially lead to a violation of the fundamental principle of innocence, which is crucial for maintaining a just legal system (Ramiro & Cruz, 2023:3).

#### **2.7.5 Israel laws on surveillance**

Golumbic and Golumbic (2008:107) states that data Protection in Israel is governed primarily by the Protection of Privacy Law, 5741-1981 ('the Privacy Law') and enforced by the Privacy Protection Authority (PPA). The Privacy Law covers collection and use of personal data and sensitive data, sets the rights and obligations of the parties collecting and using the data, including security requirements with respect thereto, and sets the rights afforded to individuals whose data is collected and used.

According to Halabi (2010:223), the Private law forbids any "invasion of privacy," which include, *inter alia*, close observation of a person that might harm him/her, intercepting and wiretapping private conversations, photographing a person in a private place, and a statutory secrecy obligation regarding person's private matters. Golumbic and Golumbic (2008:107) mention that this law does not cover the subject of data collection in computer centres, how this is regulated by the Computer Law, 1995. According to Nuruddin-Khan (2023:782), the Computer Law, 1995 forbids the illegal access to computer material, data and system interference and misuse of devices alongside other offences. The Computer Law, 1995 forbids the illegal interception of

communication between computers. Despite these laws, lawmakers in Israel have acknowledged the need to address apparent gaps between existing surveillance oversight and current technological capacity. This was triggered by explosive claims that police have been using the cell phone surveillance software called Pegasus to gain access to Israel citizens' phones (Keller-Lynn, 2022:1).

## **2.8 SURVEILLANCE LAWS IN AFRICAN COUNTRIES**

The use of electronic surveillance technology in African countries has been a concern for many years. One such issue is the impact of the unregulated use of electronic surveillance on the rule of law (Abdulrauf, 2018:365). Most African countries are gradually evolving into becoming a surveillance society because of the extent and sophistication of the current practices. According to Adebajo and Aning (2023:45), the political diversity of African governments ranges from the feudal monarchies of Morocco and Swaziland to the authoritarian and highly modernised democracies of Ethiopia and Rwanda, to the sometimes-unstable democracies of Botswana and South Africa. Many African governments are constantly striving to obtain state-of-the-art software that will allow them to monitor the activities of their citizens (Munoriyarwa & Chiumbu, 2019:26). Moreover, most countries keep their surveillance capabilities confidential. Since the rule of law concerns doing things accordingly to laid-down laws and procedure, it is important to identify the law and policy on electronic surveillance. Abdulrauf (2018:365) in Africa, the law and policy on electronic surveillance may be said to be contained in a combination of legal instruments. Abdulrauf (2018:365) further states that electronic surveillance is regulated by the provisions on the right to privacy in the constitutions of the countries since, in many cases, it is an unwarranted interference in the privacy of a person. The constitutions provide for respect for the right to privacy in their Bill of Rights, which protects unlawful and unnecessary surveillance against citizens. In some countries, such as Nigeria and South Africa, there is well developed jurisprudence on the protection of privacy through private law (Jimoh, 2023:1). Electronic surveillance may also be regulated through the interception of communications legislation. Such legislation basically gives the government or security agencies powers to intercept individuals' communications under certain explicitly stated circumstances, in most cases for the purposes of law enforcement. It covers various aspects such as the making of applications for, and

issuing of, directions authorising the interception of communications and the provision of communication-related information under certain circumstances (South African Government, 2003:4). Examples are the South Africa regulation of Interception of Communications Act of 2002 and the Regulation of Interception of Communications Act of 2010 in Uganda. Nigeria currently does not have legislation on the interception of communication. However, a draft regulation of the Nigerian Communications Commission has that effect. These laws are useful in that they provide for the permissible limit of surveillance (Abdulrauf, 2018:365).

## **2.9 THE SOUTH AFRICAN LEGISLATIVE FRAMEWORKS ON SURVEILLANCE**

### **2.9.1 Regulation of Interception of Communications and Provision of Communications Related Information Act (No. 70 of 2002)**

In South Africa, the primary legislation, which, inter alia, regulates the interception of communications and communication-related information is the RICA, 2002. The RICA, 2022 states that the interception of domestic communications can only be done with the authorisation of a designated judge. An interception direction may be granted when there are reasonable grounds to believe that a serious criminal offence has been, is being or probably will be committed. The law applies to internet service providers and telecommunications network operators, who are obliged to comply with any such warrant, called an 'interception direction.' This Act provides an emergency provision in which law enforcement agencies can track the location of a person's phone without getting pre-authorisation from a judge, provided that post-fact authorisation is sought.

### **2.9.2 National Strategic Intelligence Amendment Act (No. 67 of 2002)**

The National Strategic Intelligence Act [NSIA] (No. 67 of 2002) is an amendment to the National Strategic Intelligence Act, 1994 in South Africa. The amendment aims to exclude the Minister as a member of the National Intelligence Co-ordinating Committee (NICOC), redefine counter-intelligence, provide for security screening by the relevant members of the national intelligence structure, further define the functions of the Minister pertaining to co-ordination of intelligence, regulate the functions of the National Intelligence Structures, and provide for matters connected therewith. It

creates a range of intelligence structures and provides general guidelines for their function, including stipulating that covert intelligence gathering may only legally be conducted by these agencies (South Africa Government, 2003:2).

### **2.9.3 Financial Intelligence Centre Act (No. 38 of 2001)**

The FICA, 2001 is one of the laws forming the basis of surveillance in South Africa. The FICA, 2001 was enacted to identify the proceeds of unlawful activities as well as to combat money-laundering activities it establishes a financial reporting centre to collect data that may be useful in achieving its goal. The act established the FICA, 2001 and the Money Laundering Advisory Council (MLAC) to oversee and regulate financial institutions and other persons who might be used for money laundering purposes (South African Government, 2001:14). The FIC is responsible for collecting, analysing, and disseminating financial intelligence information to relevant authorities to combat money laundering activities.

The MLAC, on the other hand, provides advice to the FIC on matters related to money laundering and terrorist financing. Financial institutions in terms of the act are therefore required to collect and keep records of their clients and transactions, and to report suspicious transactions as well as transactions above certain limits (Roberts, Farahat, Oloyede & Mutung'u, 2021:169).

## **2.10 LIMITATIONS OF THE USE OF ELECTRONIC SURVEILLANCE DURING INVESTIGATIONS OF CARTELS CONDUCT**

While electronic surveillance will undoubtedly improve governments' ability to solve crimes, the inherent nature of these technologies can seriously compromise an individual's privacy (Newell, Timan & Koops, 2018:1). Electronic surveillance has long posed a classic confrontation between privacy interests and the need for effective law enforcement (Solove, 2023:53). Van Heek, Aming & Ziefle (2016:1) agrees that surveillance is an important law enforcement tool that is highly effective in detecting and preventing crime, but it is also a dangerous tool with serious consequences for people's freedom and democracy. Bennett (2011:486) supports that a major concern with electronic surveillance is that it can compromise privacy. These powers that the government possess in monitoring individuals have raised difficult issues about

individuals' liberty and democracy hence (Khan, 2021:102) is of the view that governments need to ensure that surveillance is tightly controlled, does not intrude on people's privacy, and focuses solely on crime prevention. It is proven that electronic surveillance is a widely used investigation tool, however there are limitations placed on the use of it, such as the right to privacy and the use of warrant.

### **2.10.1 Right to privacy**

The right to privacy is the right to be free from undue surveillance by government or anyone else. Surveillance by the government should only occur if necessary and authorised by an independent judicial officer (Browne, 2022:78). Ran (2016:11) mentions that the right to privacy is an important individual right that is often referred to in everyday life, and the use of surveillance by government carries a great risk of infringing upon an individual's privacy and other democratic values when it is not regulated properly. Mitsilegas and Vavoula (2021:1) add that the evolution and expanded use of surveillance in these digital times has profound implications for fundamental rights, including the right to privacy.

Humble (2021:1) provides that the right to privacy is a fundamental human right and part of various legal traditions at the international level are aimed at restricting governmental and private actions that threaten an individual's privacy. Moore (2011:114) shares the same sentiment that concerns about protecting individual privacy are heightened around the world due to technological advances in the use of electronic surveillance. Baker and Gunter (2005:15) add that surveillance should in no way interfere with the subject's reasonable expectation of privacy. Macnish (2018: 40) emphasises that one of the main arguments against surveillance is that it threatens an individual's privacy. Cohen (2023:10) concur that there is growing concern around the world about the increasing potential threats posed by technology and governments to individual privacy. Solove (2008:3) argues that privacy is an issue of fundamental importance all over the world. For instance, wiretapping invades the privacy interests of people who speak on the telephone. Government agents and informants can easily gain access into people's properties to overhear and record conversations, and as such, this act may reveal information that is extremely private in nature. As a result, covert electronic surveillance can destroy the individual's privacy if left to the full discretion of law enforcement officers. Wiretapping and eavesdropping, due to threats

to privacy, have been subject to numerous constitutional challenges by the affected society around the world (Abdulrauf, 2018:366).

For instance, in January 2018, the Court of Appeal in UK ruled that the Data Retention and Investigatory Power Act of 2014 (A previous law covering state surveillance which has been expanded on in the Investigatory Power Act of 2016 was unlawful. The court ruled that the legislation breached British people`s right by collecting internet activity and phone records and letting public bodies grant themselves access to these personal details with no suspicion of “serious crime” and no independent sign-off, Khan (2018:78). To protect privacy as a fundamental human right, Solove (2008:3) opines that countries around the world must adhere to laws, constitutional rights and court decisions. Privacy has been enshrined in constitutions around the world as a fundamental human right, following the Universal Declaration of Human Rights at the United Nations General Assembly in 1948 (Kayaalp, 2018:8). For instance, in South Africa the right to privacy is constitutionally protected by virtue of Section 14 of the Constitution. Brazil proclaims that “the privacy, private life, honour and image of people are inviolable”; South Korea announces that “no privacy of citizens shall be infringed”. When privacy is not directly mentioned in constitutions, the courts of many countries have recognised implicit constitutional rights to privacy such as Canada, France, Germany, Japan and India. It is, therefore, important to balance privacy against surveillance (Bygrave, 2021: 102).

Nandy (2023:14) states that a balance needs to be struck between the effective use of electronic evidence and the protection of citizens’ rights. The main reason is to prevent surveillance from being abused against citizens. Therefore, there should be a degree of control over law enforcement agencies on how to conduct surveillance for people to feel free. The goal of surveillance law is to allow law enforcement agencies to effectively execute their duties without any violation of human rights. Solove (2004:1708) explains that surveillance abuse can be avoided by providing oversight of law enforcement surveillance projects, accountability for exploitation and failure, and limiting common forms of surveillance.

Roberts, Farahat, Oloyede and Mutung’u (2021:10) agree that to avoid surveillance abuse, an independent oversight body should supervise the activities of the



investigating authorities. Roberts, Farahat, Oloyede and Mutung'u (2021:10) add that these oversight mechanisms are missing in some in the world. Roberts, Farahat, Oloyede and Mutung'u (2021:10) also mention that South Africa is exceptional as it has strong civil organisations, independent media and independent courts to challenge government actions. Subsequently, the South African legal principles governing the use of electronic surveillance by LEAs and other agencies to protect citizens' privacy rights are as follows:

- **The right to privacy:** In South Africa is a fundamental right, protected in the Bill of Rights (Section 14 of the Constitution of the Republic of South Africa, 1996). However, there are limitations, which provides by the RICA, Act 70 of 2002. In terms of this Act, private communications can be intercepted for the purposes of investigating and prosecuting serious criminal offences. Therefore, the legal authority is required to conduct surveillance.
- **Protection of Personal Information Act (No. 4 of 2013):** The purpose of this law is to ensure that all South African institutions act responsibly when collecting, processing, storing and disclosing personal data of another entity in any way. It protects personal information, strikes a balance between the right to privacy and the need for the free flow of, and access to information, and to regulate how personal information is processed (Naude & Papadopoulos, 2016:51).

The bulleted points affirm that there should be a balance between the use of surveillance and the rule of law considering that surveillance system is widely used as an investigation tool. This means that there should be an adequate oversight to protect constitutional rights and ensure that surveillance operators remain accountable. Therefore, taking into consideration the rule of law, law enforcement agencies must ensure that electronic surveillance is only applied when other "less intrusive means have proven ineffective or when there is no reasonable alternative to obtain crucial information or evidence to minimise the risks of infringing on citizen's rights to privacy.

Roberts (2021:1) emphasises that South Africa has strong oversight mechanisms to monitor law enforcement actions in relation to the use of surveillance. The Right2know (2016:10) agree that in South Africa there is a parliamentary committee that oversees

all security services to ensure transparency and accountability. This means that the parliamentary committee ensures that surveillance activities are carried out only when necessary and with the least possible violation of the right to privacy. However, Right2know (2016:8) argues that despite the mechanisms in place, there is ample evidence that surveillance has taken place outside the legal framework in ways that violate privacy rights. For instance, an international transparency report by Vodafone, indicated that government agencies accessed Vodacom customers' voice and data without any formal request made. This means that authorities ignored Section 42 of RICA, 2002, which regulate the interception of communications and associated processes such as applications for and authorisation of interception of communications. The Right2know (2018:4) advances that it is easy for law enforcement to illegally obtain metadata (Extremely large collections of electronically stored data) from telecommunications operators without a warrant or provide fictional details for judicial authorisation. For instance, SAPS crime intelligence division made an application to tap the communications of two Sunday Times investigative journalists granted under suspicious circumstances. The SAPS intelligence division got an approval to intercept mobile phones by providing fictional names and suggesting such interception was needed to investigate a criminal syndicate. Subsequently, the *Amabhungane* Centre for Investigative Journalism challenged the government on the constitutionality of the RICA, 2002 in the Northern High Court in Pretoria.

The North Gauteng High Court declared the bulk interception of communications an unjustifiable limitation to the right to privacy and found various aspects of surveillance legislation unconstitutional, Right2know (2018:2). The Right2know (2016:17) further states that many other studies confirmed that the National Communication Centre can intercept communications without the knowledge of either telecommunication service providers or RICA, 2002 judge. The reality in South Africa is that there is an increasingly widespread and deliberate abuse and violation of the right to privacy occurring within a vacuum of specific legal control, oversight, enforcement and political will and accountability (Right2know, 2016:5).

Duncan (2022:2) agrees that scandals about intelligence agencies spying on journalists, academics, civil society and opposition political parties have become a frequent occurrence. Munoriyarwa and Mare (2023:53) indicate that issues of abuse

and violation of right to privacy became more prevalent when former president Jacob Zuma turned the country into a surveillance and intelligence driven state. To this date, there is generally a lack of political and societal will to confront these increasing abuses and violations of the right to privacy.

Kendall and Frost (2022:249) mentions that in Australia, the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 impacts on the journalists, sources and media organisations. The warrants undermine media freedom and worse than previous warrants by giving law enforcement the power to access data on a journalist's computer to specifically reveal the identity of a confidential source; to access the online accounts of journalists and source without their knowledge to collect evidence; and to modify or delete information held by a journalist and sources. Roberts (2021:1) states that monitoring surveillance practice against privacy rights protections requires well defined transparency and independent oversight mechanisms. However, it is hard to monitor the legality of surveillance in some countries due to the following barriers:

- Legal provisions enabling surveillance are found in different laws. This makes it difficult to tell which law applies.
- Independent oversight bodies to monitor the activities of law enforcement authorities are absent.
- Investigating authorities do not publicly report on their activities.
- There are several surveillance provisions that are not subject to the supervision of a judge. For instance, access to a database of subscribers by security agencies only requires the approval of a government agency, such as the Nigeria Communication Commission) which is granted under the registration of Telephone Subscribers Regulations.

Therefore, to remove the bulleted barriers, it is important to improve legislation and public awareness of privacy and surveillance rights. This would allow citizens to hold the government accountable and protect citizens' privacy. The use of surveillance technology must be carried out in accordance with local laws and international obligations and commitments. It is important to ensure that systemic oversight and accountability mechanisms have sufficient authority and resources to identify and remedy possible abuses.

## **2.10.2 The use of warrant to use surveillance during criminal investigations [Cartel conducts]**

According to the UNODC (2009:13), the use of electronic surveillance by law enforcement is typically governed by warrant-based systems, especially if the person being monitored has reasonable expectations of privacy. The courts have a regulatory role in issuing warrants to conduct surveillance. In a democratic system such as South Africa, judges act as arbiters of law enforcement agencies between secrecy operations and individual freedoms in a very powerful way. It is for this reason that law enforcement agencies obtain judicial warrants before using electronic surveillance to obtain information that is deemed to be violating the right to privacy. According to UNODC (2009:13), a warrant applies in situations where the monitored person has a reasonable expectation of privacy. The judges in South Africa are guided by the RICA, 2002 to authorise a warrant to conduct surveillance (Davies, 2021:215). It is an important piece of a legislature as it regulates the interception of communications and associated processes such as applications for and authorisation of interception of communications. According to the Parliamentary Monitoring Group (2014:1), the interception of communication can only be done after judicial authorisation, and the judge must be convinced there are reasonable grounds to believe that a criminal offence has been or is being or probably will be committed. The Parliamentary Monitoring Group [PMG] (2014:1) indicates that an application should meet the following conditions before the judge can authorise a warrant:

- A serious offence has been or is being or will be committed or public health or safety is threatened.
- The interception should clearly provide information regarding the offence.
- The facilities from which the communications will be intercepted are usually used by the person.
- Other investigative methods have been unsuccessful to detect or investigate the offence.

The bullet points indicate that a person issuing a warrant for surveillance operations must believe that the activities carried out are fit for purpose (UK Government (2018:31)). This happens to avoid surreptitious electronic surveillance, as it is important for law enforcement agencies to ensure that electronic surveillance is considered

when less intrusive means have been exhausted, or when it is not possible to suggest any reasonable alternative to the collection of evidence, taking into account the circumstances of the case. The bullet points also show that electronic surveillance is only possible when certain thresholds are met, and these thresholds include a level of suspicion. In other words, the threshold at which law enforcement can enter private spaces depends on the jurisdiction and can include probable cause, reasonable suspicion, reasonable grounds, and it often requires prior judicial authorisation Vervaele (2013:117). Therefore, it is very important that surveillance of individuals or organisations does not exceed the given scope defined in the approved surveillance application.

## **2.11 THE CHALLENGES OF INVESTIGATING CARTEL CONDUCTS**

Competition Policy International [CPI] (2023:1) provides that cartel activities show signs of widespread increase and that leniency applications have declined. The OECD (2022:3) concurs that between 2015 and 2020, the number of leniency applications declined worldwide. In Latin America and the Caribbean, the number of leniency applications were 68,6 per cent lower in 2020 than in 2015. There are, however, challenges which weakens the effectiveness of the leniency policy, and these vary by jurisdiction and depend on a range of specific circumstances and factors.

Klein (2011:10) argues that widely analysed literature shows that leniency program can be an effective tool to destabilise, detect and deter cartels, however; negative effects are possible as well. According to Klein (2011:10), an increase in the number of cartels may occur due to lower expected value of fines, which is a threat to the efficiency of the leniency programme. According to the OECD (2023:5), many agencies around the world report that their programmes have not yet reached their full potential. Such agencies mentioned some of the challenges, including a lower-than-hoped for number of leniency applications, low awareness of competition requirements and leniency options and procedures, opaque procedural steps to apply for and be granted leniency, and low incentives to co-operate with competition authorities.

Shekhar and Chauhaan (2022:400) suggest that due to these challenges the leniency programme may soon become redundant as international trends indicate that the

programme has started to weaken. Shekhar and Chauhaan (2022:412) state that the situation may get worse with the application of emerging technologies such as blockchain (an advanced database mechanism that allows transparent information sharing within business networks), which enables competitors to build trust capacity amongst themselves. This technology has great repercussions for the leniency programme all over the world. Schinkel (2014:257) concurs that competition authorities today are faced with sophisticated cartels, and they need to get over leniency and look seriously at supplementing it with proactive methods to stay ahead of the cartelists. Stephan (2014:334) states that another challenge that has a significant impact on the corporate leniency programme is the criminalisation of cartel conduct. The law requires that directors or managers of companies that engage in cartel conduct can be prosecuted for anti-competitive behaviour. Van Heerden and Botha (2015:327) mention that enforcing the criminalisation of cartel conduct could undermine the effectiveness of the corporate leniency policy. It is the risk of incarceration which poses a great threat to the policy because it is the directors or managers of the firms that decide whether to apply for leniency on behalf of such firms (Van Heerden & Botha, 2015:325). In other words, the directors or manager of the applicant firm may face a further risk of being criminally prosecuted for the cartel offences. These directors bear the risk of being imprisoned for a long time, and criminal proceedings will have to be paid out of their own pockets. This is because the granting of the immunity to a leniency applicant, in countries like South Africa, does not translate into automatic absolution from criminal prosecution by the National Prosecuting Authority (NPA).

Criminalisation might not only prevent companies from applying for leniency, but it also makes the suspected individuals within the companies not to cooperate with the ongoing leniency investigation (OECD, 2022:4). Barlund (2020:17) states that the legal uncertainty as to whether current and former directors, managers, and other members of staff applicants for immunity are shielded from individual sanctions such as fines, disqualification, or imprisonment, could prevent potential applicants from applying for leniency.

Barlund (2020:20) suggests that firms participating in cartels may abuse leniency when they find it fit. For instance, firms may seek leniency if they see that the cartel is

failing and want to put their competitors at a disadvantage. In June 2018, the Organisation for Economic Co-operation and Development held a roundtable with different jurisdictions to discuss the challenges in relation to the leniency programme. The challenges encountered by these different jurisdictions are discussed in detail below.

### **2.11.1 The United Kingdom challenges in the investigation of cartel conducts**

The OECD (2018:2) states that one of the significant challenges faced by the authority, like other authorities globally is that a cartel operates secretly and uses sophisticated methods to avoid detection and making it difficult for the authority discover it. Another key challenge experienced by the Competition and Market Authority, which is common to other competition authorities is to raise awareness of competition law to businesses and individuals to the damaging effect of cartel conduct. Again, this is to know how cartels contravene competition law and the benefits of leniency (OECD, 2018:3).

The OECD (2018:5) further reports that developing a strong intelligence function running alongside leniency, avoids having to rely exclusively on the leniency regime as a means of detecting cartel activity. The OECD (2018:6) raised the importance of building relationships with other stakeholders to manage the interplay of co-enforcement, co-ordination, and co-operation (i.e., which in the UK includes sectoral regulators and other enforcement agencies, as well as competition authorities in other jurisdictions).

### **2.11.2 United States of American challenges in the investigation of cartel conducts**

According to Bell and Millay (2019:14), the USA implemented its initial leniency policy in 1978, which underwent revision in 1993. The purpose of the revision was to enhance transparency and bolster the incentives for individuals involved in cartels to come forward and self-report. Hammond (2008:4) states that the positive outcomes were achieved due to the alterations made, as the leniency programme resulted in the identification and dismantling of the most significant international cartels ever pursued, which consequently led to record-setting fines in the USA.

OECD (2018:3) also mentions that the authority experienced a challenge by giving up prosecution of the first corporation to turn on its conspirators and this was initially unsettling to many prosecutors. The granting of leniency without criminal conviction, fines or prison sentences for anti-competitive behaviour was necessary to encourage cartel participants to turn on each other and self-report. Ultimately, the Antitrust Division won support from prosecutors by convincing them that leniency policies would reveal highly secretive corporate conduct that would otherwise go undetected and unabated (OECD, 2018:3).

## **2.12 AUSTRALIAN CHALLENGES IN THE INVESTIGATION OF CARTEL CONDUCTS**

The 'Australian Competition and Consumer Commission Immunity Policy for Cartel Conduct' (ACCC IPCC) is widely considered to be the most important tool at its disposal for enforcing the law against cartel conduct. However, Beaton-Wells (2008:71) highlighted that the policy effectiveness experienced four major challenges arising from important national and international developments in the anti-cartel enforcement arena.

### **2.12.1 Criminal versus civil cartel enforcement**

According to Hay and Perry (2020:214), since the introduction of criminal liability for cartel-related activities in 2000, Australia has adopted a two-pronged enforcement approach, in which cartel cases can be prosecuted based on criminal or civil penalties. Most cases are still being pursued by the ACCC through civil proceedings. However, for cases deemed 'serious,' the ACCC will refer them to the Commonwealth Director of Public Prosecutions (CDPP) for potential criminal prosecution.

The CDPP's office is responsible for making final decisions on criminal immunity and their approach to immunity differs greatly from that of the ACCC. The DPP's approach lacks the necessary transparency, certainty, and predictability that are crucial for an effective immunity policy in this area. The issue of bifurcation in relation to immunity poses challenges for both the ACCC as a regulatory authority and the CDPP as a prosecuting institution (Beaton-Wells, 2008:77).



### **2.12.2 Increase in levels of private enforcement**

The rise in private enforcement and damage claims for cartel conduct in Australia worsened the tension between private claimants' access to information disclosed by immunity applicants and the immunity applicants' need to maintain confidentiality (Beaton-Wells, 2008:103). Lythgo-Marshall (2016:222) adds that private enforcement aims to compensate those impacted by cartel conduct through private actions for damages against the cartels. To pursue damages, third party claimants face evidentiary challenges equivalent to competition regulators when proving the cartel's existence. In contrast to the regulators, third party claimants lack access to immunity documents.

### **2.12.3 Settlement of cartel cases**

Settling cases with implicated parties is challenging. The competition authorities globally use an immunity policy that grants full immunity to the first-in applicant. This policy remains the most effective way to spot and prosecute cartel activity. The competition authorities want to find the best way to get information and cooperation from conspirators who do not win first place. This system is valuable to law enforcement as it helps them achieve timely results, allocate resources efficiently, and enhance overall law enforcement activities, thereby achieving greater deterrence (Beaton-Wells, 2009:246).

### **2.12.4 Informant reward system**

Lythgo-Marshall (2016:222) states that the concept of implementing financial incentives for informants is controversial. A challenge is whether policies can be developed to recruit and reward informants who provide inside information about cartel activity, independent of immunity or leniency programmes. It concerns the rationale and justification of such policies, their design and parameters (Beaton-Wells, 2009:265).

## **2.13 THE BRAZILIAN CHALLENGES IN THE INVESTIGATION OF CARTEL CONDUCTS**

According to Martinez (2015:261), leniency programme in Brazil was launched in 2000, and like other jurisdictions, it was inspired by the US leniency programme. Despite the success of the leniency programme, Brazil has major challenges in relation to the implementation of the leniency. Brazil mostly received its leniency

applications from large companies. This could be that small and medium-sized companies do not have compliance departments, as such are not well informed about the competition issues. As a result, the Brazil competition authority would need to find more effective ways of promoting its leniency programme among these companies.

Another challenge raised by the Brazilian competition authority was market diversification in leniency applications. The application received were mostly concentrated on construction services, automotive and electronic components markets. Collusion exists in most markets, therefore, the authority needed to enhance its detecting capability in diverse markets through screening and other intelligence tools. There was concern about the balance between public and private enforcement of cartel conducts. Leniency applicants were concerned about the repercussions of signing an agreement with the authority, as they were likely to be the first (and easier) target for follow-on civil damages actions. Moreover, there was a challenge raised in relation to the criminalisation of the cartels. Some individuals or companies may have had an interest in applying for the leniency, however, hesitated to do so as prosecution of criminal conduct was not subject to immunity.

## **2.14 THE ISRAELI CHALLENGES IN THE INVESTIGATION OF CARTEL CONDUCTS**

The 'Israel Antitrust Authority' considers their leniency programme ineffective. It was indicated that since the inception of the leniency programme in 2005, only few applications have been made. Few of those applications led to conviction, meaning that the programme has not led to the discovery of many cartels (OECD, 2018:2). Calvani and Calvani (2011:187) state that one of the challenges in deterring cartel activities is low fines imposed by the authority. Therefore, these insufficient fines need to be augmented to adequately deter cartel behaviour (Calvani & Calvani, 2011:193). Gal and Dahan (2019:133) concur that effective deterrence requires that the anticipated fines should outweigh the benefits of anti-competitive violations.

Certain terms of the programme may create legal uncertainties regarding the outcome of any application for immunity. For example, a condition that denies immunity to a cartel leader may discourage potential applicants who are unsure whether they will be

classified as a cartel leader (OECD, 2018:4). Some attribute the inefficiency to broader socio-economic factors. Israel is a small country, and potential applicants fear that if the cartelists are exposed, they will face retaliation, loss of livelihoods, and the inability to find work (OECD, 2018:5).

## **2.15 CHALLENGES IN AFRICAN COUNTRIES TO INVESTIGATE CARTEL CONDUCT**

Buthe and Kigwiru (2020:44) highlight that Africa is sometimes referred to as the “last frontier” of competition law because many African countries have only recently introduced modern competition laws (South Africa was the first to do so in 1999). Connor (2016:1) states that, except for South Africa, African and West Asian countries have failed to make the important leap into dealing with cartel activities. In almost all countries in Africa, the introduction of competition laws (Antitrust laws) and institutions is a new phenomenon, however, a country like South Africa has relatively comprehensive laws (Buthe & Kigwiru, 2020:42). Most of the competition authorities in Africa are relatively young authorities with limited resources and capacity constraints. Gordon and Mweemba (2022:35) concurs that African agencies are younger entrants to the competition law playfield. According to Ng'ethe and Gathii (2019:35), African competition authorities learn from South Africa's competition law to strengthen their competition laws and expand the powers of LEAs.

### **2.15.1 South African challenges on investigations of cartel conducts**

In line with various other international jurisdiction, the South African Competition Commission adopted the Corporate Leniency Policy (CLP) in 2004 which was revised in 2008. The CLP has had its successes, and despite this, there are challenges that can affect its effectiveness. On 1 May 2016 South Africa joined an array of other jurisdictions criminalising cartel conduct such the US, UK, Canada, Australia and some European countries, such as the UK and Germany (Morphet & Hlatswayo, 2017:36).

Morphet and Hlatswayo (2017:36) further point out that there are some concerns that it may have a negative impact on the CLP, which has been used very effectively by the Competition Commission in uncovering cartel conduct. In terms of Section 73A of the Competition Act of 1998, which introduce the South Africa cartel offence, provides for directors or persons in a position of management authority, causing its firm to

participate in cartel activity, or knowingly acquiescing to such conduct, to be liable to a fine of up to R500 000 or imprisonment not exceeding 10 years, or both. Thus, Section 73A of the Act may pose a serious challenge in that willing individuals may hesitate to apply for leniency to avoid criminal sanctions on leniency policy (Rowan, 2020:68). The second challenge is the different decision-making roles and responsibilities of the Competition Commission and the office of National Director of Public Prosecutor (NDPP). The office of the NDPP, with which final decisions as to criminal immunity rest, has a very different approach to immunity to that of the Competition Commission and it is an approach that lacks the hallmarks of transparency, certainty and predictability considered essential to an effective immunity policy in this field Beaton-Wells (2008:71). This means that a framework for the coordination between the Competition Commission and NPA should be developed. The two institutions should establish a memorandum of understanding (Rowan, 2020: 25).

## **2.16 THE BEST PRACTICES FOR INVESTIGATING CARTELS: INTERNATIONAL, AFRICAN AND SOUTH AFRICAN APPROACHES**

According to Albaek (2013:67), competition authorities were established around the world to benefits consumers by giving them a choice in terms of lower prices, higher quality goods and services and greater innovation. Roy (2016:1) adds that it ensures that business and companies compete fairly with each other and create a wider choice for the consumers and helps to reduce prices and improve quality of products or services. It was therefore important for competition authorities, in different jurisdictions, to develop various legislative frameworks and investigative techniques to effectively investigate cartel activities. Below are some best practices from South African Acts and international approaches that contribute to successful cartel investigations:

### **2.16.1 United States Sherman Act, 1890**

According to Hovenkamp (2010:874), the Sherman Act sought to preserve competition in the market by forbidding monopolies and other business practices that restrain trade. Some of restraints are blatantly anti-competitive, such as price fixing and market allocation. These are considered 'per se' violations of the Sherman Act of 1890, other alleged restraints are analysed under the "rule of reason" to determine whether they

unreasonably restrict trade. DePamphilis (2011:54) stresses that the Sherman Antitrust Act remains the most important source of antitrust law today.

According to Kovacic and Winerman (2010:929), the congress, in 1914, passed the Federal Trade Commission Act of 1914, to ban anti-competitive behaviour. Hovenkamp (2010:871) adds that Federal Trade Commission was established to identify and prosecute 'unfair methods of competition and unfair or deception acts or practices.' Any conduct that violates the Sherman Act, 1890 violates the Federal Trade Commission Act as well (Federal Trade Commission, 2023:1). Although most enforcement actions are civil, the Sherman Act is also a criminal law. Criminal prosecutions are typically limited to intentional and clear violations such as when competitors fix prices or rig bids. The Sherman Act imposes criminal penalties of up to \$100 million (R 1 898 040 000.00) by the time of drafting this section or a corporation and \$1 million (R18 980 400.00) by the time of drafting this section, for an individual, along with up to 10 years in prison.

### **2.16.2 United Kingdom Competition Act of 1998**

Rodger and MacCulloch (2008:1) contend that Competition law in the European Commission (EC) and UK plays an important and ever-increasing role in regulating the conduct of business. The law prevents businesses from entering into anti-competitive agreements and from abusing their dominant market position. The UK introduced the competition Act in 1998 to align competition law as closely as possible with the EC law (Article 81 and 82), to prohibit anti-competitive agreements and abuse of a dominant position respectively (Colino, 2011:18). The anti-competitive behaviour is prohibited under Chapter I and II of the Competition Act of 1998. Parties found to have contravened these provisions can be subjected to an administrative penalty of up to 10 per cent of the firm's annual turnover generated in its preceding financial year.

### **2.16.3 Australia Competition and Consumer Act of 2010**

According to Groshinski and Davies (2015:1), Australia has a mature and high-quality competition law system. This is a federal law contained in the Competition and Consumer Act 2010 (formerly known as the Trade Practices Act of 1974 prior to January 1, 2011). The purpose of the Act is to prohibit anti-competitive conduct under Part IV and to promote competition and efficiency in the Australian economy by eliminating anti-competitive rules and regulations. It helps to ensure consumer

protection in the marketplace and promotes competition among businesses to benefit all consumers (ACCC, 2003:1). Violations of the Competition and Consumer Act of 2010 results in fines and penalties. The maximum penalty for violating the Competition and Consumer Act of 2010 is \$50 000 000 (R 949 020 000.00) at the time of compiling this section or 30 per cent of the corporation's adjusted turnover during the breach turnover period for the offence.

#### **2.16.4 Brazil Competition law: No. 8884/1994**

According to Todorov and Filho (2012:234) on June 11, 1994, Brazil introduced a new competition law: law No. 8884/94 (as amended). The first law to repeal previous competition legislation, law No. 8884 has important implications for the substance and enforcement of Brazilian competition law. The most significant change brought about by the new law was the desire to strengthen competition law and policy. The other significant change was the adoption of an effective mandatory merger control system.

#### **2.16.5 Refocus to cartel enforcement – The Leniency Statute of 2000**

According to Calliari (2010:68), in 2000 Brazil started to use more aggressive means of investigating cartels that were, until then, not used. Todorov and Fihho (2012:234) states that there were two important changes introduced to antitrust law. The first change concerned the possibility for companies to apply for leniency in relation to cartel activities. The second change relates to new powers granted to the *Conselho Administrativo de Defesa Economica* (CADE), the Brazil competition authority called the Administrative Council for Economic Defence, in conducting antitrust investigations with the possibility of asking the court for permission to conduct unannounced dawn raids in the premises of the parties under investigation. Calliari (2010:68) adds that introducing new tools like dawn raids to a system that was not used to them was far from straightforward. Certainly, leniency agreements are not the only tool for exposing illegal activities. Dawns raids have also been a key part of the authorities' work since 2003 and are often used as part of investigations prompted by leniency agreements. In short, the leniency programme and dawn raids have combined to improve the detection of cartels in Brazil (Todorov & Filho, 2012:234).

#### **2.16.6 Israel Economic Competition Law of 5748-1988**

Economic Competition Law of 5748-1988 is the primary law dealing with competition and antitrust issues in Israel (Bendor & Heller, 2018:103). The law aims to prevent

harm to competition or the public by prohibiting various restrictive trade practises such as restrictive arrangements, mergers, monopolies, and concerted groups. It strengthens the enforcement against anti-competitive conduct (Eyal-Boger, Schwartz & Brown, 2021:1).

According to OECD (2022:2), the Israel Competition Authority (ICA) has a policy of mainly criminal enforcement against cartels and bid-rigging violations. Cartel activities constitute criminal offences under Israel competition law. The ICA's Investigations Department has initiated dozens of criminal investigations of cartels and bid-rigging cases in a broad array of sectors, and it has indicted over 50 cartels and bid-rigging cases. The ICA uses various techniques to investigate cartel conduct, including dawn raids, whistleblowers, leniency programme and settlements (Arbel & Keren, 2021:654).

### **2.16.7 African Competition law**

Buthe and Kigwiru (2020:47) share that most African countries have enacted competition laws, but their effective implementation and enforcement requires the presence of competition authorities. As such, few African competition agencies have adopted more investigative tools, such as leniency and dawn raids, in cartel investigations. The Namibia, Kenyan, South African, Mauritanian, and Zambia agencies have also adopted leniency programs to supplement the agency-initiated enforcement efforts. By all indications, however, only South Africa has operated an effective and successful leniency program so far (Kaira, 2017:73).

Kaira (2017:73) further states that reasons for cartel enforcement in neighbouring countries not to be successful range from capacity to lack of sufficient understanding of competition law by enforcers as much as by adjudicators/courts. Ncube and Nkuembe (2020:82) add that in South Africa, the leniency policy has been fundamental to the Competition Commission's fight against cartels, and this is in sharp contrast to other African jurisdictions where leniency programmes have seemingly made little impression.

According to Mubangizi and Masuku (2021:183), all effective strategies such as leniency programmes, utilising whistle-blowers, informants, and raids, are under-utilised by other African countries. Morphet and Hlatswayo (2017:10) add that several African countries have leniency policies in place, although not all of them are actively

used. Ginsburg (2022:45) concur that a handful of developing countries, worldwide, actively fight cartels, including using leniency programmes and the vast majority appear not to.

#### **2.16.8 Constitution of the Republic of South Africa, 1996**

The Constitution of the Republic of South Africa, 1996 is the supreme law of the country and provides the legal framework for criminality in South Africa. The constitution was adopted on May 8, 1996, and amended on October 11, 1996, by the Constitutional Assembly. The constitution provides for the rights of arrested, detained, and accused people, including the right to silence, protection against self-incrimination, the right to counsel and legal aid, the right to a fair trial, the presumption of innocence, and the prohibition of double jeopardy and *ex post facto* crimes (South Africa Government, 1996:125).

#### **2.16.9 Criminal Procedure Act (No. 51 of 1977)**

The Criminal Procedure Act [CPA] (No. 51 of 1977) is a South African law that provides procedures and related matters in criminal proceedings. The act is divided into several chapters, including general provisions, arrest, search and seizure, bail, indictment and plea, trial and sentence, appeals, and special proceedings. It has its basis mainly in English law (Department of Justice and Constitutional Development [DoJ & CD] (2015:1).

#### **2.16.10 South Africa Competition Act (No. 89 of 1998)**

Ramburuth (2012:207) highlights that the Competition Act (No. 89 of 1998) is the primary legislation governing competition law in South Africa. The purpose of this Act is to promote and maintain competition and it provides for the prosecution of anti-competitive conduct, merger control and the granting of exemptions. It establishes the Competition Commission, which is responsible for investigating, controlling, and evaluating restrictive practices, abuse of dominant position, and mergers. Unterhalter (2012:219) asserts that cartel conduct is one of the key areas addressed by competition law in South Africa. According to Mabizela (2021:221), the effectiveness of competition law in South Africa to investigate cartels has been enhanced through various measures. Labuschagne and Lotter (2015:1) further state that in terms of Section 4 of the Act prohibits certain conduct by firms or associations of firms in a horizontal relationship, including price fixing, market division, and collusive tendering.



This Act allows for an application of 'rule of reason' analysis in the assessment of horizontal anti-competitive conduct.

The South African competition commission has implemented policy reforms to better detect, prosecute, and deter cartel behaviour and these reforms include the introduction of Corporate Leniency Policy [CLP] (Kaira, 2015:10). According to Nkosi and Boshoff (2022:348), the introduction of the CLP in 2004 was a key innovation in South African anti-cartel policy. Nkosi and Boshoff (2022:348) further add that the policy was introduced as a measure to intensify the detection activities of the competition authorities and in the long run to serve as a deterrent measure. Mahlangu (2014:4) asserts that the Competition Commission through its CLP has been successful in detecting a number of cartels that would not have otherwise been detected without the policy. Kaira (2015:10) states that the initial fine of R196 million, following the first leniency application showed the implicated parties that the Competition Commission was not bluffing. The CLP has been successful in uncovering cartel conduct in South Africa and has contributed to the prosecution of about 30 per cent of the cartels prosecuted in the country (Labuschagne & Lotter, 2015).

## **2.17 OTHER NOTABLE STRATEGIES TO INVESTIGATE CARTEL CONDUCTS**

Investigating cartels requires a multifaceted approach that combines legal frameworks, investigative techniques, and international cooperation. HüscheIraTh (2010:3) states that competition authorities around the world use various methods of cartel detection, namely reactive methods and proactive methods. According to Vadasz, Benczur and Munk (2016:255), reactive cartel detection methods are an approach based on an external event, such as receipt of complaint (From competitor, a customer, an agency, or an employee), possession of external information (From whistle-blowers or informants), or Information obtained from leniency applicant.

Vadász, Benczur and Munk (2016:255) further state that the proactive cartel detection method is the detection method characterised by initiatives taken by the authorities. Vadász, Benczur and Munk (2016:255) explain that these initiatives include analysing past antitrust and competition law cases; monitoring the market, industry, press and internet reporting; working with competition and other national and international investigative authorities; including, but not limited to, quantitative tools for screening.

Foremny and Dorabialski (2018:949) point out that the proactive method includes surveillance aspects such as infiltration and other operational methods, as well as screening and econometric studies.

Vadász, Benczur and Munk (2016:255) confirm that competition authorities mainly rely on the reactive detection method to enforce competition law and it is mainly characterised by passive waiting for the evidence. For the success of this reactive detection method competition authorities require specific powers of investigation (Jerez, 2015:114). Neuhoff, Govender, Versfeld and Dingley (2006:251) state that competition authorities have the power to investigate companies and seek information or evidence if they believe that cartel activity has been committed or is happening. The most common powers of Investigation the competition authorities have include powers to search business premises, to summons information and individuals for interrogations. The OECD (2011:53) adds that in other jurisdictions such as the Israel Competition Authority, in addition, have powers to detain and arrest suspects. Common investigation powers found in various jurisdictions will be discussed in detail below:

### **2.17.1 The use of search warrants in the investigation of cartel conducts**

The OECD (2020:5) states that one of the investigation tools that is widely used by competition authorities around the globe for the detection and prosecution of cartel activities is the dawn raid. The ICN (2010:1) adds that competition authorities consider dawn raids as one of the most effective investigative tools in the detection and investigation of cartels. Insights (2016:1) agrees that most competition authorities use searches and seizures as part of a cartel investigation, as searches are an effective tool for gathering evidence of possible competition law violations. Searches are conducted when competition authorities suspect that evidence could be altered, hidden, removed or destroyed. Furthermore, Andrews, Gorecki and McFadden (2015:115) highlight that searches that are unannounced, have an element of surprise which is important for securing the evidence. Camatsos and Foer (2007:5) concur that competition authorities do not give any advance notice to the suspected firms prior to search and seize operations. Jerez (2015:125) states that search and seizure operations require a search warrant that are issued by a judge based upon reasonable

grounds to believe that a particular firm(s) committed a crime to justify making a search. It is not always that these dawn raids yield positive results.

### **2.17.2 The use of summons in the investigation of cartel conducts**

In terms of the South African Competition Act (No. 89 of 1998), the competition authority can issue a formal request for documents, information and interviews either in conjunction with searches or after the search at a later stage of their investigation. Written requests for information or documents are sent to firms that are not suspected of having played a role in the cartel. Sometimes, usually towards the end of the investigation, the competition authority may send written requests to suspected firms for information if there are no grounds to believe it would be destroyed or concealed.

Camatsos and Foer (2007:5) indicate that the summons serves two purposes when investigating cartel conduct. Firstly, the commission authority may summons the implicated firm(s) to furnish any information or evidence which may help with the investigation. Secondly, it may summon a person who is believed to have knowledge that his or her firm is participating in cartel behaviour with other firms, to appear before the Commissioner or a person authorised by the Commissioner to be interrogated. The challenge is that, unless, the investigator knows exactly what information is required to prove the case, firms are reluctant to volunteer the information or evidence which will implicate them in a cartel behaviour. The same happens during the interrogations, where most of the directors or managers choose not to volunteer the information to implicate their firms and/or themselves.

## **2.18 THE USE OF CORPORATE LENIENCY POLICY IN THE INVESTIGATION OF CARTEL CONDUCTS**

Chen and Harrington (2007:59) state that the leniency policy has been widely used as one of the most effective tools to fight against cartels. The USA Department of Justice first introduced the leniency programme in 1978 and revised it in 1993. Since then, it has resulted in a significant success cartel detection, spurring the adoption of similar programmes in many countries not only in America and Europe but also in Asia and Africa (Choi & Hahn, 2014:883). The leniency policy is designed to give incentives to cartel members to take the initiative to approach the competition authorities and admit

their participation in a cartel activity and assist the competition authorities to prosecute other implicated companies (Siddique, 2016:16).

Van Heerden and Botha (2015:310) mention that due to the secretive and collusive nature of cartels, some other investigative mechanisms were not sufficient to combat them. Competition authorities in various jurisdictions have therefore sought to address the problem of detection and prosecution of cartels by introducing leniency programmes. Aubert, Rey and Kovaic (2006:1) add that competition authorities around the world introduced leniency programmes for cartel members that denounce their collusive conducts. This policy was established to encourage firm(s) participating in cartel conduct to disclose the information in return for immunity from prosecution. According to Yilmaz (2009:142), introducing a leniency programme is one of the tools competition authorities use to gather evidence and increase their likelihood of prosecuting cartels.

Yilmaz (2009:142) further presents that leniency programmes can fight against collusion in four ways in that, the applicant can easily provide evidence which may lead to successful prosecution; it can assist with the detection and investigation of cartels; it can make them less profitable and thus deter cartel formation; and it can make cartels more unstable and thus make them more likely to break down by themselves.

Neuhoff, Govender, Versfeld and Dingley (2006:367) agree that the competition authorities around the world introduced corporate leniency programmes to improve the detection and prevention of cartel conducts. Van Heerden and Botha (2015:313) further state that various other prominent competition jurisdictions, such as the UK, Australia, Canada and Korea, also make use of leniency programmes to supplement the powers of their competition authorities in the prevention and detection of cartels.

The Competition Commission of South Africa adopted the corporate leniency policy in line with other various international jurisdictions. Since the introduction of the leniency programme, competition authorities have had considerable success in prosecuting cartels. Hammond (2004:25) concur that leniency programmes have led to the detection and dismantling of the largest global cartels ever prosecuted and resulted in

record-breaking fines in the United States, the UK, Canada, the EU and other jurisdictions.

### **2.18.1 The use of leniency programme in United Kingdom**

According to Merdian (2013:34) before 1998, it was not a crime per se to engage in cartel activities in UK, until the introduction of the Competition Act of 1998. Section 2, Chapter I prohibition, stipulates a wide prohibition on anti-competitive arrangement. The leniency programme was first introduced into European Union Competition law (EU Competition law) in 1996. The policy was subsequently revised in 2002 and 2006 to increase incentives for firms to self-report, leading to numerous cartel prosecutions. The EU encouraged its member states to independently adopt leniency programmes (Dong, Massa & Zaldokas, 2019:887). As a result, UK also adopted its own leniency policy, in line with the EU regulations. The Competition and Market Authority (CMA) operates a leniency programme that provides full or partial exemption from fines under certain conditions to companies and individuals who provide evidence of cartel activity and cooperate with CMA investigations.

The OECD (2023:2) provides that the CMA's leniency policy continues to play a vital role in the detection and investigation of cartels in the UK, and in the deterrence of cartel activity. However, the CMA decided to add cartel proactive detection measures by established programmes for detecting cartels independently of any leniency application (Beth & Gannon, 2022:77).

Approximately half of the CMA's cartel cases are intelligence-led rather than resulting from a leniency application. The focus is on an intelligence development toolkit, with about half of the CMA cartel cases discovered through CMA's initiatives and are intelligence-led. The OECD (2023:4) further states once CMA receive intelligence suggesting the existence of a cartel, the authority deploys investigative tools to make follow ups on such intelligence. The investigative tools include surveillance, access to communication and the use of covert human intelligence sources.

### **2.18.2 The use of leniency programme in the United States of America**

Hinloopen (2003:415) indicates that the USA has the longest history of antitrust law enforcement in the world and was the first to implement a leniency programme in 1978. The programme was amended in 1993 because few amnesty applications were filed

prior to amendment. Hinloopen (2003:415) further shares that the programme then became more effective in detecting and cracked an increased number of cartel activities compared to other reactional methods, such as search warrants and interrogations. Chen and Rey (2013:917) reveals that the revised leniency programme resulted in high number of amnesty applications. The number moved from one per month to three per month.

Hammond (2004:22) adds that in the USA, firms have been fined more than US\$3.8 billion (R107.072 trillion) for anti-competitive behaviour since 1997, with over 90 per cent of the total tied to investigations assisted by leniency applicants. Griffin (2003:7) confirms that the extraordinary success of the leniency programme has generated widespread interest around the world, as such, the USA advised several other countries globally in drafting and implementing effective leniency programmes in their jurisdictions. Leslie (2011:175) concurs that in the USA, the programme has been the most effective generator of cartel cases and is believed to be the most successful programme in the USA history for detecting large commercial crimes.

Hammond (2004:22) emphasises that the leniency programme has changed the way competition authorities around the world detect, investigate, and deter cartels conducts. This has led companies to stop cartel activity and turn to competition authorities to provide evidence against other cartel members. The OECD (2018:7) mentions that the USA leniency programme transformed the investigation methodology of cartel enforcement authorities, led to the successful prosecution of amnesty of longstanding and serious international cartels, and subsequently served as a model for leniency programmes deployed in dozens of jurisdictions around the world.

### **2.18.3 The use of leniency by Australian Competition and Consumer Commission**

In 2003 the ACCC adopted an IPCC to expose and deter secret company cartels operating in Australia. Australia has implemented this policy following success reported by international jurisdictions such as the UK, USA, Canada and the European Commission in disrupting the cartel (ACCC, 2003:1). The policy was revised in 2005 to include conditions such as full cooperation, cessation of the cartel. The figures show

that between 2000 and 2013, the ACC granted nine final immunities out of 46 conditional immunities. The figures show that the leniency programme has not generated a significant increase in cartel detections and prosecutions. As such these casted doubt on the effectiveness of the in aiding prosecutions (Beaton-Wells, 2014:315). Consequently, the ACCC has developed an intelligence methodology for identifying and examining industries and sub-sector domestically for susceptibility to collusion, under what is known as the Cartel Intelligence Project.

#### **2.18.4 The use of leniency by Brazil, Administrative Council for Economic Defence**

The 'leniency programme' in Brazil was first introduced in 2000, with the aim of intensifying the fight against cartel activities. The responsibility of the implementation of the leniency programme in Brazil lies with the Administrative Council for Economic Defence [CADE] (Athayde, 2016:2). According to Martinez (2015:260), the leniency programme in Brazil was first launched in 2000, and it was inspired by the USA leniency programme. It underwent a major review in 2011 (Pinha & Braga, 2019:1860).

The first leniency application led to the uncovering of a bid-rigging cartel involving private security companies with activities in the Brazilian southern region (Todorov & Filho, 2012:234). Pinha and Braga (2019:1860) further indicate that since its adoption in 2000 until 2017, more than eighty leniency agreements were signed in Brazil, but the number of agreements *per se* does not mean success or failure. According to Athayde (2016:2), leniency programme has been one of the most important investigative tools for detecting collusive conduct among competitors in Brazil.

As a result, Brazil has an increasing number of cartel investigations, record fines for cartel offences, individuals being held criminally accountable, and increasing cooperation among criminal and administrative enforcers, with the change in perception by criminal prosecutors and judges as to the seriousness of cartels (Martinez, 2015:260).

#### **2.18.5 The use of leniency by Israel Competition Authority**

The Israel Competition Authority has a formal leniency programme since 2005. According to Eyal-Boger, Schwatz and Zackay (2022:1), the leniency programme is not considered to be successful in Israel as it has only been applied a few times since

its initiation. OECD (2018:4) adds that after more than 10 years, the existing leniency programme has not been successful, because relatively few applications were made and even fewer have led to investigation. Although during the same period of the ineffectiveness of leniency programme, many cartels were investigated, indictment were filed and the participants in the cartels convicted, all without any leniency application. The competition authority is reviewing the leniency programme, with a view to increase its effectiveness (OECD, 2018:5).

## **2.19 THE USE OF LENIENCY PROGRAMMES IN AFRICAN COUNTRIES**

A few African competition agencies have adopted more investigative tools, such as leniency and dawn raids, in cartel investigations. The Namibia, Kenyan, South African, Mauritanian, and Zambia agencies have also adopted leniency programmes to supplement the agency-initiated enforcement efforts. By all indications, however, only South Africa has operated an effective and successful leniency programme so far (Kaira, 2017:73). Kaira (2017:73) further states that the reasons for cartel enforcement in neighbouring countries not to be successful range from capacity to lack of sufficient understanding of competition law by enforcers as much as by adjudicators/courts.

### **2.19.1 The use of leniency programme in South Africa**

In South Africa, a leniency programme in terms of the South African Competition Act, 1998 is termed the Corporate Leniency Policy (CLP). The first version of the CLP was published in May 2008. A revised version was published in March 2012. Since its initial adoption, the CLP has arguably been the most successful enforcement tool in uncovering and prosecuting cartels (Shabalala, 2022:107). Hagerman and McIntosh (2023:345) further state that Corporate Leniency Policy has been successfully applied in a high number of cartel investigations across a range of industries, including high- and low-profile investigations. Industries that have seen notable high-profile investigations and prosecutions involving the successful application of the Corporate Leniency Policy include pre-cast concrete, bread manufacturing, construction, wheat and maize milling and cement.

Lavoie (2010:141) argue that the CLP proved to be an important tool in assisting the Competition Commission of South Africa with the detection and investigation of cartels. Lavoie (2010:141) add that since the adoption of the corporate leniency, the



Competition Commission received increasing number of applications for immunity, and as result, major cartels were dismantled and prosecuted under the Competition Act, 1998. According to Lavoie (2010:141), Five (05) years after the adoption of the leniency, the Competition Commission of South Africa received fifty-four applications from different industries and the trend continued in 2008 (Received Nineteen-19 applications) and 2009.

## **2.20 PROACTIVE CARTEL DETECTION TECHNIQUES FOR INVESTIGATION OF CARTEL CONDUCTS**

Foremny and Dorabialski, (2018:951) states that identifying anti-competitive agreements is complex and requires considerable interdisciplinary knowledge, experience, appropriate choice of tools, availability of selected data and sometimes even long-term market observation. In order to successfully fight cartels, it is necessary to constantly improve the detection methods, monitor technical progress and develop new tools using previously unavailable techniques and resources.

The already reviewed studies present that the reaction cartel detection methods are based on information provided to competition authorities by third parties, whilst proactive methods refer to the situations when the competition authority engaged in the detection activity on its own initiatives (Zlatcu & Suciu, 2017:15). According to Hüsichelrath (2010:1), despite that reactive cartel detection method still plays a role in cartel detection, there are signs that proactive cartel detection methods are gaining traction as a tool to increase the likelihood of cartel detection. Hüsichelrath (2010:3) further highlights that proactive methods offer a variety of tools to actively detect cartels and that include, constant monitoring of industries through infiltration, career tracking of industry managers, press and internet monitoring. These are good examples of surveillance techniques used to gathering information/evidence about cartel activities.

Foremny and Dorabialski (2018:950) agree that proactive methods may include the use of surveillance, cooperation among competition agencies and other authorities, and the use of economics based on available data to perform screening tests. Foremny and Dorabialski (2018:950) also points out that one of the proactive methods

is the surveillance of a publicly available data source, which includes the public media, the information supplied by economic intelligence or the news on interventions carried out by competition authorities in other jurisdictions.

Schinkel (2013:5) argues that some competition LEAs in different jurisdictions are now faced with sophisticated cartels, as such they need to supplement their reaction methods with proactive measures. According to Harrison and Patterson (2021:58), competition authorities choose to use proactive cartel detection methods for different reasons. Firstly, the competition authority may want to demonstrate the existence of a credible threat of being detected and sanctioned (Especially in the absence of an application for leniency).

Secondly, the Competition authority can end a series of simultaneous investigations in the same field and pursue new cases, and lastly, the competition authority may have acquired new enforcement powers and tools and is looking to put them into practice to emphasise the deterrent effect of its activities. Gelles, Mirkow and Mariani (2019:4) share that law enforcement agencies, including competition authorities, are currently facing a rapidly changing environment that is challenging on all fronts. As law enforcement agencies around the world are working to absorb new technology, criminals are constantly piloting, iterating, and expanding their criminal tactics.

Gelles, Mirkow and Mariani (2019:4) believe that criminals are often among the earliest adopters of new technology. Van Brakel and De Hert (2011:220) concur that professional criminals are taking full advantage of new opportunities presented by technology. They are more aware of the risks of being detected by authorities and increasingly make use of counter-surveillance techniques and tactics. Vervaele (2013:123) reveals that in most countries, the organised crime paradigm is used not only to redefine investigative tools, but also to introduce new specialised investigative techniques such as wiretapping and eavesdropping, infiltration and surveillance that can only be used to solve serious and complex crimes. These investigative techniques are used in a proactive way to investigate the existence and behaviour of potentially suspicious persons and organisations to prevent serious crimes. It is for this reason that competition authorities in some jurisdictions where reactionary cartel detection methods proved to be less effective have shifted their attention towards the application of pro-active cartel detection methods and employ a variety of methods, such as the

monitoring of firms' activities for detection (Mirasdar & Gupta, 2017:2607). These include European Commission, Israel Antitrust authority, USA, UK and Canada Competition Bureau.

### **2.20.1 The United Kingdom Competition and Market Authority**

The UK has taken steps to follow a more proactive, intelligence-led approach. It has established cartels intelligent function as one of the key areas to enhance intelligence, investigation, and enforcement capacity (OECD, 2018:5). The OECD (2018:6) further states that the UK uses the full range of its investigatory powers, including covert investigation powers under the Regulation of Investigatory Powers Act (RIPA) of 2000, under which it can require the production of communications data, carry out surveillance (Directed and Intrusive) and uses covert human intelligence sources. The UK is increasingly taking a proactive approach to cartel detection. Most of their cases do not originate from the leniency application. Their proactive approach also reflected in their reliance on material gathered using covert surveillance powers, for example in 2016 galvanised steel tanks decisions, where a meeting of competitors was recorded and relied on as evidence of unlawful information sharing (OECD, 2018:6).

The proactive approach was a success to the UK, as half of new cases opened were intelligence-led. This means those cases were uncovered by the authority through its own investigative capabilities. Like in the USA, cartel has been criminalised in the UK. The authority is working together with the police and other law enforcement agencies which enables the authority to make use of the full range of its investigative tools (OECD, 2014:208). The UK also explored the opportunities offered by new technology and developed a cartel screening tool to focus on the use of algorithms to spot unusual bidder behaviour and pricing patterns which may indicate that bid-rigging has taken place (OECD, 2018:6). Whish and Bailey (2021:2) add that in 2020 the UK Competition and Market Authority reported on the state of competition in the UK economy and the findings were that powerful platforms such as Google, Amazon and Facebook have added to these concerns. As such it has been whether the existing competition tools are adequate to deal with such platforms, or whether new tools are needed.

### **2.20.2 The United States of America, Department of Justice Antitrust Division and Federal Trade Commission**

The USA has two (02) primary competition authorities, namely, the Department of Justice (DoJ) and Federal Trade Commission (FTC). According to Federal Trade Commission (2023), both the FTC and DoJ Antitrust Division enforce the federal antitrust laws. In some respects, their authorities overlap, but in practice the two agencies complement each other. The DoJ is a federal executive department responsible for the administration of justice and enforcement of law, including competition law through its Antitrust Division. The FTC is a federal agency whose tasks include consumer protection and enforcement of competition law. The FTC's Bureau of Competition enforces the nation's antitrust laws, which form the foundation of the country's free-market economy (Ohlhausen, 2014:1). In the USA, hard core cartels are prosecuted as criminal offences. The USA Department of Justice's antitrust division is empowered to prosecute criminal violations. The department investigates and prosecutes cartel cases and use the tools of the USA Federal criminal investigation to detect cartels. Therefore, cartels investigation is supported by the FBI and other USA government agencies. The investigations are not done in silos in the USA. Hence, the department is well equipped to fight any type of crime with all the necessary resources (OECD, 2014:209). The USA is already making use of informants, consensual monitoring/wiretap authority, and hidden microphones and video cameras and other sophisticated technological tools.

### **2.20.3 Australian Competition and Consumer Commission**

In 2003 the ACCC adopted IPCC, and it was revised in 2005 to include conditions such as full cooperation, cessation of the cartel. According to Beaton-Wells, (2014:315), the ACCC granted number of final leniencies to the applicant firms were very low and casted doubt on the effectiveness of leniency policy in assisting the investigation and prosecution. The OECD (2023:2) showcases that it considered shifting to the implementation of effective proactive detection programme to reinforce the leniency policy. These, amongst other, included the use of intelligence sources as a pipeline for new investigations, using a sophisticated cartel screening tool to analyse large datasets, and using an anonymous whistle-blower tool. The intelligence methodology developed by the ACCC is used to identify and screen sectors and sub-sectors at the national level for vulnerability to collusion (OECD, 2013:81). The OECD

(2013:81) further adds that the methodology produces potentially valuable results in cartel detection without any dependence at all on an immunity applicant. This indicates that the shift from reactionary detection methods to proactive detection approach benefits the Commission in tackling the cartel activities.

#### **2.20.4 Brazilian Administrative Council for Economic Defence**

According to Pinha and Braga (2019:1860), fighting cartels in Brazil is a major concern like in other jurisdictions around the world. The Brazilian leniency programme was adopted in 2000 and reviewed in 2011. Brazil signed the first leniency agreement in 2003 (Calliari, 2010:68). Since the 83 agreements have been signed (i.e., 64 per cent national cartels, 18 per cent international cartels with global dynamics, 18 per cent cartels with national and international effects). Despite the increasing intelligence efforts and independent proceedings, the leniency programme is still the main tool for detecting cartels in the country and between 2003 and 2011, 70 per cent of leniency agreements were signed in relation to international cartel cases.

Consequently, the prosecution of bid rigging improved, and the number of nation cases grew significantly (OECD, 2018:2). Pinha and Braga (2019:1865) confirms that the leniency programme was effective in tackling cartel activities. Calliari (2010:68) concludes in addition to leniency programme, Brazil introduced more aggressive means of investigating cartels that were not used such as dawn raids, wiretapping (Electronic surveillance) and the use of quantitative and econometric analytical techniques.

#### **2.20.5 Israeli Antitrust Authority**

The Israeli Authority never considered the leniency programme effective because it has not led to the discovery of many cartels. Many cartel cases which were investigated and prosecuted, were initiated by the authority without any assistance from the leniency programme (OECD, 2018:4). As a result, Israeli Authority treats cartel conducts like any other white-collar crime or organised crime syndicates that warrants infiltration. With advanced intelligence gathering methods, computer forensic capabilities, wiretapping (i.e., electronic surveillance) and sophisticated questioning techniques, Israeli Authority has been able to uncover cartels (OECD, 2014:123).

### **2.20.6 African Competition law**

Competition law enforcement has developed significantly in several African countries, but with a greater focus on merger review transactions. Efforts to detect and prosecute cartels have largely been left to more established authorities, such as the South African Competition Commission, which has been in operation since 1999. Some countries in the southern region, such as Zambia, Botswana, Namibia and Tanzania, are also pursuing cartels and are stepping up investigations based on South Africa's experience. The success of leniency prosecutions in South Africa has led some of these countries to introduce their own leniency policies (Irvine, 2016:3).

Naidu and Tzarevski (2019:1) contend that the Africa's competition regulators are improving merger analysis and understanding prohibited practices. Opong and Klaaren (2020:50) concur that the African continent is seeing a steady growth in competition legislation and regulators turn their attention from a narrow focus on merger control to a wider focus on enforcement. In addition to country regulations, Africa has several regional competition regulators, such as the West African Economic Monetary Union (WAEMU), the East African community (EAC), the Common Market for Eastern and Southern Africa (COMESA), the Economic Community of West African States (ECOWAS) and the Economic and Monetary Community of Central Africa (CEMAC), Naidu and Tzarevski (2019:1). These regional competition regulators have different mandates and responsibilities, but they generally ensure fair business practices, market participation, and consumer protection. These authorities ensure that there is a level playing field for business across their respective regions (Buthe & Kigwiri, 2020:58). Baker (2022:122) provides that all effective strategies such as leniency programmes, utilising whistleblowers, informants, and raids, are under-utilised by other African countries. Morphet and Hlatswayo (2017:1) add that several Africa countries have leniency policies in place, although not all of them are actively used. Cseres (2021:30) concur that a handful of developing countries, worldwide, actively fight cartels, including using leniency programme and the vast majority appear not to be doing the same.

### **2.20.7 South African Competition Commission**

The South African Competition Commission uses market inquiry as a proactive technique to detect anti-competitive behaviour in the market (Burke, 2018:261). According to Motta, Peitz & Schweitzer, (2021:1), market inquiry is a new competition tool which allows authorities to intervene in markets which do not function as they should. The provision of the Competition Amendment Act of 2009 gives the Competition Commission the power to conduct a market inquiry. Section 43A of the Competition Act defines a market inquiry as “a formal inquiry in respect of the general state of competition in a market for particular goods or services, without necessarily referring to the conduct or activities of a particular firm” (Sutherland, 2018:8).

Moreover, the market inquiry is a tool used by regulatory authorities to accurately assess the overall state of competition in the market for certain goods or services, to determine whether a market feature or combination of features impedes competition in the internal market. The objective is to determine whether the process of competition is operating effectively in all markets (Chetty, Njisane, Mbikiwa & Martin, 2014:4). The South African Competition Commission has previously conducted several market inquiries, including inquiries into the health care sector, the grocery retail sector, the data services sector and inquiry into online intermediation platform services in South Africa. Therefore, the researcher submits that while these measures such as market inquiry and leniency policy have contributed to effectiveness of competition law in South Africa to investigate cartels, it is important to continuously evaluate and adopt new strategies to address emerging challenges and ensure robust enforcement of cartel conducts.

### **2.21 PROACTIVE CARTEL DETECTION METHOD AND ALGORITHMS COLLUSION**

Cartel conduct and algorithms have become topics of interest in the field of competition law. Algorithms, which are sets of instructions or rules followed by computers, can potentially be used as a vehicle for collusion among competitors. While traditional cartels involve agreements between rivals, the use of algorithms can enable parallel pricing and other forms of coordination without direct communication between competitors, ICN (2020:2). Advances in technology have made cartel activities more

sophisticated, and law enforcement has long been seen as lagging behind technological innovations (Feiglin, 2020:1139).

Recently, markets have adopted algorithm-based pricing models for economic gain, which has caused serious concerns in the recent competition law community. Deng (2020:965) states that the threat of algorithmic collusion is real and poses far greater challenges to competition authorities than human coordination and collusion. It is important to understand the concept 'algorithm' and how can it sustain anti-competitive behaviour in the market. According to Hutchinson, Ruchkina and Pavlikov (2021:951), algorithms can be broadly defined as "a sequence of simple and/or well-defined operations that should be performed in an exact order to carry out a certain task or class of tasks or to solve a certain problem or class of problems."

In the competition law context, Feiglin (2020:1139) define pricing algorithm, as the use of software algorithms to determine the price of goods or services and it may possibly be programmed to collude. The European Commission conducted an enquiry between June 2015 and March 2016 and found out that 53 per cent of the respondent retailers track the online prices of competitors, out of which 67 per cent use automatic software programs for that purpose. Data collected by such algorithms, combined with the use of pricing programmes that allow the automatic establishment of agreed prices among competitors, can raise competition concerns (Hutchinson, Ruchkina & Pavlikov, 2021:951).

Consequently, Schrepel (2020:1) points out that algorithmic collusion is the subject of a growing body of literature, but no empirical studies have yet been produced that document the frequency of the phenomenon in the real world. Schrepel (2020:1) argues that algorithms have not yet been quantified, and even if they were, they would not pose fundamental problems for antitrust and competition law. However, there are already different views contrary to Schrepel's assertion. The OECD (2017:7) argues that algorithms are changing the competitive landscape by allowing companies to achieve complicit outcomes in novel ways that do not necessarily require consensus or perhaps human interaction in the traditional antitrust sense. Calvano, Denicolo and Pastorello (2019:155) concur that academics and competition regulators have expressed concern that algorithms can more effectively sustain collusive outcomes



than human decision makers. This implies that algorithms may help competing firms to avoid detection for their anti-competitive behaviour such as price-fixing. Fzrachi and Stucke (2019:220) suggest that firms may agree to collude by fixing the price for their competing products and use algorithms to facilitate their collusion. The OECD (2017:19) agrees that some companies in the market may use algorithms to achieve profits that violate competition laws. Fzrachi and Stucke (2019:220) further add that pricing algorithms can lead to more frequent pricing attempts, which may potentially be more difficult to detect. It is for this reason that algorithm poses a concern to competition authorities as they view it to be helping competitors to avoid cartel detection. As a result, competition authorities around the world need to understand how algorithms work in the digital markets. The OECD (2017:25) further explains that competition authorities need to be aware of the risks that collusion might become easier to sustain due to algorithms. Competition authorities should have the capability to establish how companies might collude and still put in place the necessary structures to coordinate strategies, allocate gains and enforce the agreement. The reviewed literature studies showed that a major challenge for competition authorities is that the use of algorithms widens the grey area between illegal explicit collusion and legal implicit collusion (Yuanyuan-Xiong, 2022:91).

In other words, algorithms may enable firms to replace explicit collusion with tacit coordination. Therefore, it is important for competition authorities to understand how digital technology works and how algorithms can facilitate or support anti-competitive behaviour. The ICN (2020:2) adds that the impact of algorithms on cartel conduct is an area of ongoing research and debate. Competition authorities and scholars are studying the challenges raised by big data and algorithms in cartel enforcement. The use of algorithms as monitoring tools for cartel enforcement is also being explored.

Lee (2018:41) provides that the current cartel investigation tools are limited in effectively deterring algorithmic tacit collusion. As such, competition authorities need to shift towards using proactive measures and invest in digital products or electronic tools to survey such conducts. Gal (2022:22) states that competition authorities around the world have begun experimenting with different ways to limit algorithmic coordination. Lee (2018:44) mentions that it is only through a proactive enforcement tool that competition authorities may detect if firms are colluding. Traditional

investigation techniques are being supplemented and increasingly replaced, by digital technologies and techniques to keep up with the cartelists who apply advanced technologies to collude. The OECD (2017:13) observes that the growing usage of algorithms in the business world has caused government agencies to have increased interest towards the use of algorithm, especially in the detection of anti-competitive behaviour. The United State has already made some initiation towards a more data-driven approach to detect patterns of criminal behaviour by designing a machine-learning algorithm. Lorenzoni (2022:37) add that some competition authorities are beginning to consider developing their own internal digital investigation tools. The OECD (2023:2) showcases that it relies on proactive detection policy to strengthen cartel deterrence and encourage self-reporting by companies. Following a decline in leniency applications the Italian Competition Authority adopted a set of comprehensive and complementary measures and initiatives to strengthen its cartel detection tools.

The OECD (2023:3) further indicates that New Zealand (NZ) Commerce Commission still considers leniency a valuable and effective tool, however it is looking to increase intelligence gathering capabilities to be proactive in dealing with cartel activities. It is therefore clear that some authorities, after realising that the leniency programme is becoming less and less effective, have decided to develop their own methods of data filtering to identify cartel activities, hence moving from analogy cartel detection methods to more digital ones.

According to Beth and Gannon (2022:77), it is not surprising that competition authorities and international bodies such as the OECD or the ICN are increasingly encouraging the use of screens to detect cartels. Therefore, it is evident that competition authorities need to shift to proactive cartel detection (i.e., Which includes electronic surveillance) methods to keep pace with the fast evolution of the digital technology. Competition authorities should strive for more innovative and alternative advanced means to boost their reactional detection methods. Summarily, the researcher shares that cartel activities are sophisticated and secretive, making them challenging to detect by competition authorities. To detect and deter cartel conducts, competition authorities employ various tools and techniques to uncover evidence of cartel behaviour. One of the primary tools used by competition authorities is leniency programmes. Leniency programmes provide incentives for cartel members to come

forward and cooperate with authorities in exchange for reduced penalties or immunity from prosecution. By encouraging cartel members to expose their illegal activities, leniency programmes can be a powerful tool in detecting cartels and supporting cartel enforcement. In addition to leniency programmes, competition authorities, especially in the developed jurisdictions use other tools such market analysis, whistleblowing programmes and electronic surveillance. Some competition authorities use electronic surveillance as a supplementary tool to leniency programmes in the investigation of cartel activities, as part of proactive cartel detection measures. The main aim of electronic surveillance in the context of anti-competitive practice is to gather evidence that can be used to prosecute individuals involved in cartel behaviour.

By monitoring communications, tracking movements, and gathering other types of information, competition authorities can build a stronger case against those engaged in cartel behaviour. However, it is important to note that electronic surveillance must be conducted within the confines of the law and is subject to legal restrictions. The use of electronic surveillance should be carefully regulated to ensure that privacy rights are protected and that the evidence obtained is admissible in court.

Cartels are becoming more sophisticated, and parties are increasingly using online platforms to engage in cartel activities, such as algorithms. Cartel conducts and algorithms have become topics of interest in the field of competition law because algorithms can potentially be used to facilitate cartel behaviour. Competition authorities are actively studying algorithms and its effect to develop strategies and tools to detect and deter cartel activities. Through a combination of electronic surveillance, leniency programmes, customer education and market inquiry competition authorities can protect competition and ensure a level playing field for businesses and consumers.

## **2.22 SUMMARY**

In this chapter (Two), the researcher conceptualised the concepts of electronic surveillance. The roles of electronic surveillance in the investigation of cartel conducts were analysed. The researcher focused on the circumstances, legislations, policies and theoretical framework regulating the application of the electronic surveillance in

the investigation of cartel conducts in South Africa and other international jurisdictions. Challenges of the investigation of cartel conducts worldwide were presented. The effectiveness of investigating cartels, which include the best practices in both developed and developing jurisdictions were explored. Proactive measures where competition authorities engaged in the detection activity on its own initiatives were highlighted. The consulted literature also highlighted the evolving of algorithm-based pricing models which has caused serious concerns in the law community recently. The next chapter (Three) presents the adopted research design and methodology.

## **CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY**

### **3.1 INTRODUCTION**

Dantzker, Hunter and Quinn (2018:44) explain that methodology section provides details of procedures used in the study. It should provide enough information for the reader to understand, evaluate, and critique. Daniel and Sam (2011:41) state that research methodology is a way to systematically solve the research problem. It may be understood as a science of studying how research is done scientifically and study various steps that are generally adopted by a researcher in analysing his research problem along with the logic behind them.

According to Eriksson and Kovalainen (2015:68), “methodology refers to the ways used to gain a better understanding of the world from a strategy-as-practice perspective”. Carey (2012:83) emphasises that research methodology helps researchers to gain comprehensive understanding of the process itself extensively instead of only looking at the results of a scientific study.

This means the methodology of the study is about drawing up the research to guide a researcher in search of answers to solve the research problem in a systematic manner. This section outlines the research approach and design. It describes the methods of data gathering, population, sampling, ethical considerations, and trustworthiness of the study.

### **3.2 RESEARCH DESIGN**

There are several qualitative research designs, that the researcher may adopt for the study, which include case study, ethnography, phenomenological study, grounded theory study, narrative inquiry, and content analysis (Leedy & Ormrod, 2019:260). In this study, the researcher adopted a case study design to explore the use of electronic surveillance in an investigation of cartel activities. Yin (2018:15) explains that case study research involves the study of a case within a real life, contemporary context or setting. Denscombe (2010:52) mentions that case studies focus on one (or just few)

instances of a particular phenomenon with a view to providing an in-depth account of events, relationships, experiences, or processes occurring in that instance.

This research design was aided by the exploratory research objective, defined as the methodology approach that investigates research questions that have not previously been studied in-depth. It is often used when the issue you are studying is new, or the data collection process is challenging in some way (George, 2022:1). For the purpose of this study, the researcher adopted the exploratory research objective to find out if the utilisation of electronic surveillance would enable the Competition Commission to successfully curb the cartels conduct amongst firms.

According to Thomas and Lawal (2020:79), exploratory research design is a type of research that is conducted when the researcher has little or no knowledge about the subject matter. Mbaka and Isiramem (2021:29) concur that exploratory research is conducted when enough is not known about a phenomenon and a problem that has not been clearly defined. The main objective of exploratory research is to improve a researcher's knowledge of a topic, and it is often used to clarify research questions that guide the whole research project (Singh, 2021:2).

Haile (2023:579) states that one main advantage of exploratory research objective is that it is flexible and adaptable, as there are no specific set rules about conducting it. Haile (2023:583) further adds that in exploratory research, the sample size tends to be small. Small samples save time and resources. According to Mbaka and Isiramem (2021:29), this research objective can add quality and insightful information to a study and is vital to a study. This research objective allows the researcher to be creative in order to gain the greatest amount of insight on a subject.

One disadvantage of the exploratory research objective is that it often fails to provide adequate answers to research questions, as the sample size and methods may not be representative of the larger population of interest (Dudovskiy, 2018:19). The other disadvantage of this research objective is that it provides qualitative data, and interpretation of qualitative data information can be judgemental and biased. It lacks statistical strength and inability to draw definite conclusions (Jebb, Parrington & Woo, 2017:267).

### 3.3 RESEARCH APPROACHES

There are three (03) methods that can be adopted when conducting research, namely quantitative, qualitative and the mixed-method approach. However, this study adopted a qualitative research approach for data collection and documentary analysis as part of the research method. Mohajan (2018:23) states that “qualitative research is a form of social action that stresses the way people interpret and make sense of their experiences to understand the social reality of individuals.”

Mohajan (2018:23) further reveals that a qualitative research approach tries to help researchers to understand the social world in which they live, and why things are the way they are. Creswell and Poth (2018:45) concurs that qualitative research is applied when the researcher needs to explore and have a detailed understanding of the issues, which can only be established by talking directly with the people.

Traditionally researchers apply either a quantitative or qualitative research approach in a single project. However, some researchers adopt the combination of quantitative and qualitative approach, which is a mixed-method approach (Seale, 2012:480). Therefore, the qualitative research approach was employed in this study, as the researcher explored the views, experiences, and beliefs of individual participants.

According to Etikan, Musa and Alkassim (2016:2), qualitative research approach is intended to acquire an in-depth understanding of the study undertaken. Qualitative approach will be used to get the perception of cartel investigators in relation to the use of electronic surveillance to investigate cartel conducts. As such the researcher will obtain practical answers to address the research problem since the participants are expected to give answers based on their personal experience. According to (Bachman & Schutt, 2013:135), a qualitative approach allows the researcher to obtain richer data.

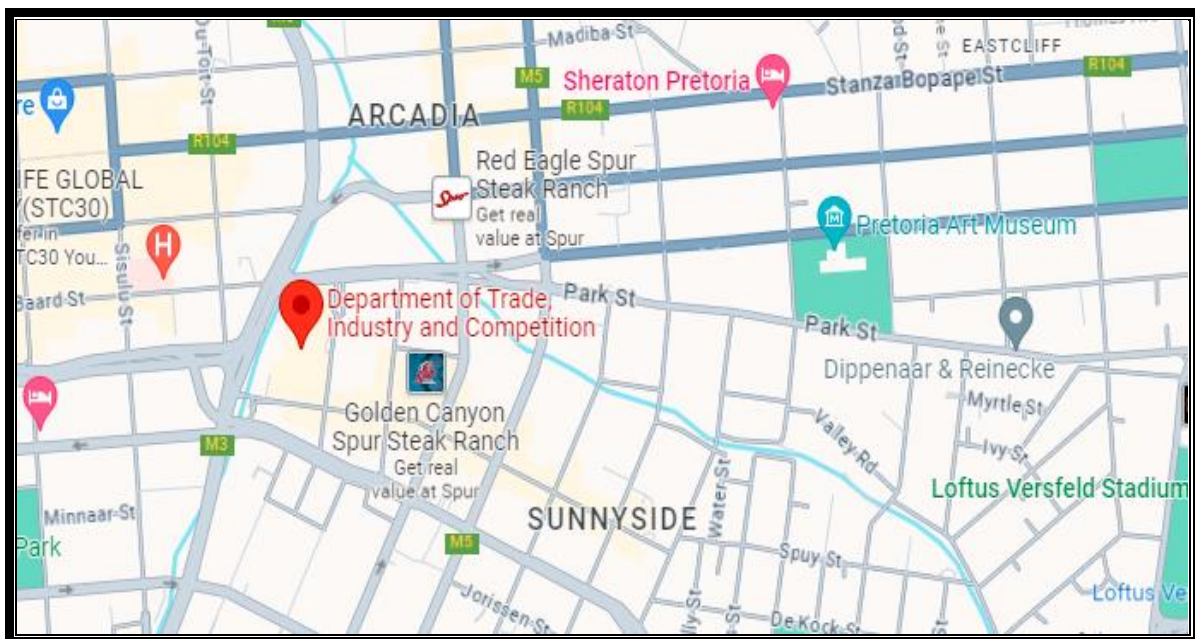
However, this could also disadvantage the outcome of the study if the quality of the data gathered is subjective. This will be because of the perceptions of participants being influenced by personal biases and experiences (Creswell & Poth, 2018:49). Another disadvantage is that the influence of the researcher can have a negative effect on the collected data, in that, if a researcher has a biased point of view, then their

perspective will be included and affect the outcome (Creswell & Poth, 2018:49). The advantage of qualitative research is that it uses individual choices as workable data (Creswell & Poth, 2018:135). The other advantage is that the researcher is able to interact with participants face-to-face and create a positive rapport (Rahman, 2020:104).

### 3.3.1 Study location

The study was conducted in the office of the Competition Commission of South Africa, situated at The Department of Trade Industry and Competition (DTIC) Campus, Mulayo (Block C), 77 Meintjies Street, Sunnyside, Pretoria. The Competition Commission is a statutory body, established in terms of the Competition Act, of 1998, constituted by the Government of South Africa to investigate, control, and evaluate restrictive business practices, abuse of dominant positions, and mergers to achieve equity and efficiency in the South African economy.

**Figure 1:** Map of the Competition Commission of South Africa



Source: AfriGIS (2024)

### 3.3.2 Study population

Dantzker, Hunter and Quinn (2018: 68) highlight that population is the complete group or class from which information is to be gathered. Defining the target population is an important and often difficult part of the study because the choice of the target population will profoundly affect the statistics that result (Sharon, 2019:3). In this study,



the target population was the Competition Commission with the staff compliment of 249 (Two hundred and forty-nine) members. The ideal study population was the Cartels Division, which consists of 30 (Thirty) members and Legal division with 24 (Twenty-four) members.

### **3.3.3 Sampling procedures**

To answer the study aim, objectives and research questions, the researcher needed to collect data. It was practically burdensome for the researcher to collect data from the whole population. As such, there was a need to select a sample from the overall population. In qualitative research, an effective sample selection process is very important because inappropriate procedure may seriously affect the findings and outcomes of a study (Whitehead, 2016:124). The method of sampling that was followed in this study was purposive sampling. This type of sampling enables the researcher to select individuals who can purposefully inform an understanding of the research problem and central phenomenon of the study (Creswell & Poth, 2018:148). The criteria used to select the participants was based on their ability to provide information that could be used to answer the study aim, objectives, and research questions. In this study, the researcher targeted (05) five investigators from the Cartels division and other 05 (five) Legal counsels from the Legal services.

The investigators and Legal counsels were selected based on the following criteria: Rank seniority, divisional roles and work experience. The Principal and Senior investigators in these two divisions have the experience and knowledge necessary to investigate cartels conduct. They conduct factual and legal analysis of the alleged contraventions and manage the teams responsible for cartel investigation cases. Overall, about ten (10) participants formed part of this study. The Cartels division and Legal services are parts of the divisions, which constitute the Competition Commission of South Africa. The Cartels division is responsible for the investigation and prosecution of cartels conduct. The Legal services division is responsible for providing the cartels division with legal support and managing litigation before the Tribunal.

## **3.4 DATA COLLECTION METHODS**

Qualitative data collection is about the types of data to be collected and the procedures for gathering such data. According to Blaxter, Hughes and Tight (2010:156), there are

two issues, which may confront the researcher when considering collecting data for the study namely, access and ethics. These issues have to do with what data the researcher can collect, how to get it and how to use it. According to (Creswell & Creswell, 2018:147), it means gaining permission, conducting a good qualitative sampling strategy, developing means for recording information both digitally and on paper, storing the data, and anticipating ethical issues that may arise. Denscombe (2010:153) explains that there are four main methods that the researcher can use to collect data, namely, questionnaires; interviews; observations and documents. In this study, data was collected by using the following:

#### **3.4.1 Semi-structured face-to-face interviews**

The face-to face interview refers to a data collection method involving the researcher and participant meeting in person (Saunders, Lewis & Thornhill, 2016:391). It is often used in qualitative research, where the researcher asks open-ended questions to gather detailed information about the participant's experiences, opinions, and attitudes. Face-to-face interviews can be conducted as structured, semi-structured and unstructured interviews. In a semi-structured interview, the researcher uses a set of pre-determined questions, and the participants answer in their own words (Ritchie, Lewis, Nicholls & Ormston, 2014:141). Al Balushi (2016:726) states that semi-structured interviews can be an effective tool in interpretive research because they help the researcher gain in-depth data of participants' perspectives and make sense of their experiences as told by them.

According to Brinkmann and Kvale (2018:123), in the application of semi-structured face-to-face interviews, researchers have a set of certain questions, but they can change their order and can give explanations and examples whenever needed. The researcher can also use open-ended questions related to the context of the interview. The semi-structured face-to-face interviews with reference to the 'Interview Schedule Guide' channelled this process to define the topic under research and provide opportunities for both researcher and participant to discuss some topics in more detail.

Semi-structured interviews allow the researcher to prompt or encourage the participants to provide more information related to the topic. The researcher had semi-structured face-to-face interviews with ten (10) officials attached to the Competition

Commission to share their views, experience and knowledge about the use of electronic surveillance in the investigation of cartel conducts.

### **3.4.2 Documentary studies**

Documentary studies are a form of qualitative research in which documents are interpreted by the researcher to give voice and meaning (Patton, 2015:519). O’Leary (2017:297) describes documentary analysis as a procedure which encompasses the identification, verification and consideration of documents which are related to the subject under investigation.

According to O’Leary (2017:268) documents can be in the form of written, visual, or audio materials, such as books, articles, photographs, videos, and audio recordings. The researcher conducted documentary analysis of intelligence operation policies, rules, and regulations, as well as related legislative framework. The literature review on previous studies on this subject was consulted, including books, journal articles, internet sources, newspaper and other relevant sources related to this subject, with the following databases visited:

- **Kluwer Competition Law** – it allows the researcher to make informed decisions in all aspects of international competition law, including cartels conduct, merger control, and offers the researcher constant access to practical tools and research materials.
- **Google Scholar** – it provides a simple way to broadly search for scholarly literature.
- **Unisa Library database** – it contains bibliographic references to academic, peer-reviewed journal articles, theses, books, chapters in books and conference papers. Database visited includes Unisa Institutional Repository, Sabinet, ProQuest, eBook and Oracle.

### **3.4.3 Structured observation method**

This study employed the structured observation method. According to Cohen, Manion and Morrison (2017:566), this method is structured in the sense that pre-determined categories are used to guide the recording process. According to Byrne (2021:4), structured observation is a systematic method of collecting behavioural data within a controlled environment. It uses a structured schedule to document activities, clearly outlining which activities are to be recorded and the method of recording. This form of

observation attempts to minimize bias by using a repeatable and verifiable approach, ensuring that the observations can be reliably used as an accurate reflection of what is being observed.

Jibril (2018:232) further states that in structural observation, the researcher (a) selects which behaviours are of interest and which are not, (b) clearly defines the characteristics of each behaviour so that observers all agree on the classifications, and (c) notes the occurrence and frequency of these targeted behaviours in the situation under analysis. Silverman (2016:76) shares the same view that structured observation is a data collecting method in which researchers gather data without direct involvement with the participants (the researcher watches from afar) and the collection technique is structured in a well-defined and procedural manner.

According to Bryman (2012:272), it is used extensively in the study field of psychology. It allows researchers to collect data that could not be collected using typical research methods like surveys and interviews. Jamshed (2014:87) states that observation is a type of qualitative research method which not only included participant's observation, but also covered ethnography and research work in the field. Jamshed (2014:87) further concludes that observational methods are, sometimes, supplemental means for corroborating research findings.

### **3.5 DATA ANALYSIS METHODS**

De Vos et al., (2011:397) state that qualitative analysis transforms data into findings. This involves reducing the volume of raw information, sifting significance from trivia, identifying significant patterns, and constructing a framework for communicating the essence of what the data reveals. According to Nowell, Norris, White and Moules (2017:2), data analysis in a qualitative research approach consists of preparing and organising the data for analysis, then reducing the data into themes through a process of coding and condensing the codes, and finally representing the data in figures, tables, or a discussion. Flick (2022:232) and De Vos et al., (2011:416) state that interpretation involves making sense of the data, the "lessons learned". Interpretation in qualitative research involves abstracting out beyond the codes, and then relating themes to the larger meaning of the data. It is a process that begins with the

development of the codes, the formation of themes from codes, and then organisation of themes into larger units of abstraction to make sense of the data. The process of data collection, data analysis, and report writing are inter-related and often go on simultaneously in a research project (Creswell & Poth, 2018:180). Leedy and Ormrod (2019:380) concur that in the qualitative designs data collection, data analysis and data interpretation are largely three (03) separate steps, but they are closely intertwined. Therefore, the following stages of thematic content analysis were applied in this study as follows:

### **3.5.1 Organising data**

Data management begins the process. This step is very important, and it is about organising and preparing the data that was collected. This is to be sorted depending on the information from source. Typing notes, transcribing interviews, and scanning materials are all part of this step (Creswell & Poth, 2016:185). This means that organising data effectively helps the researcher to identify, locate and use research data files efficiently and effectively. Therefore, the researcher organised the data in a way that was easy to locate as the analysis proceeds.

### **3.5.2 Reading and memoing**

At this stage the researcher read the collected data through and understood every detail of it before breaking it into parts. The researcher wrote notes or memos in the margins of transcripts or field notes. The memos as explained by Mohajan and Mohajan (2022:6) are short phrases, ideas, reflections, insights or key concepts that occur to the reader. Mohajan and Mohajan (2022:8) further state that memos should be exploratory and open-ended; they don't need to provide definitive conclusions.

### **3.5.3 Describing, classifying and interpreting data into codes and themes**

The researcher identified a list of potentially helpful ways of classifying and coding the data. This comprises of highlighting and grouping the concise statements, which form the main idea of the text which emerged from the participants' responses and field notes describing the expressions which could be defined to interpret the hidden meaning. Creswell and Poth (2018:195) encourages the researchers to look for code segments that can be used to describe information and develop themes. These codes can represent the following aspects:

- Information that researchers expect to find before the study.

- Surprising information that the researcher did not expect to find.
- Information that is conceptually interesting or unusual to researchers, as well as potential participants and audiences.

At this stage the researcher accurately described and formulated comprehensible themes. Themes in qualitative research are broad units of information that consist of several codes aggregated to form a common idea (Braun & Clarke, 2022:78). The researcher interpreted the data considering the research problem and questions.

The researcher used the inductive TCA method to analyse the obtained data. The choice of thematic analysis is encouraged by the views of Braun and Clarke (2022:2) that it is a powerful method for analysing data that allows researchers to summarise, highlight key features of, and interpret a wide range of data sets. Clarke and Braun (2013:120) further state that the inductive TCA offers researchers great flexibility with respect to the following aspects:

- The type of research questions it can address, from personal accounts of people's experiences and understanding to broader constructs in various social contexts,
- The type of data and documents examined,
- The volume of data analysed,
- The ability to analyse data with an inductive, data-driven approach or a deductive, theory-driven approach.

According to Vaismoradi, Turunen and Bondas (2013:398), thematic analysis is best suited for exploratory studies. It was, therefore, useful for finding out about people's experiences, views, and opinions. Moreover, the adopted inductive TCA, enabled the researcher to elicit themes from the analysed data, as obtained from the selected participants. According to Dawadi (2020:62), thematic analysis is a good approach to research where the researcher is trying to find out something about people's views, opinions, knowledge, experience or values from a set of qualitative data. The researcher closely examined the data to identify common themes, that is, topics, ideas, and patterns of meaning that came up repeatedly. To this course, the researcher followed the following Six (6) steps of the inductive TCA as highlighted by Dawadi (2020:64):

**1. Familiarisation:** The researcher transcribed the audio records and familiarised himself with the collected data by repeatedly reading it and making notes of the

reviewed literature studies and conducted interviews, supported by the adopted structured observation schedules to later foster development of study themes.

- 2. Coding:** Codes were then developed to capture key analytical ideas within the data related to the study aim, objectives and research questions, as well as the reviewed literature studies and empirical findings.
- 3. Generating themes:** Themes were generated by grouping codes which relate to a concept, guided by the study aim, objectives and research questions; based on the interviewed participants, reviewed documents and conducted observation schedule. Then the researcher constructed an analytic narrative to explain what is happening within the data, how this relates to the research question.
- 4. Reviewing themes:** To ensure that the identified study themes are presented accurately, solely based on the study aim, objectives and research questions, aided by the reviewed studies or documents and observations were made to enhance the presented data. The researcher focused on the data set, theoretical (Literature studies) and empirical data to compare the identified themes against such aspects.
- 5. Defining and naming themes:** Defining themes involves formulating exactly what each study theme means and how it helps to understand the data, based on the study aim, objectives and research questions, supported by the literature studies and observation schedule. Naming of the study themes involved coming up with an easily understandable conceptualisation.
- 6. Writing-up:** Lastly, the researcher presented analysis within the dissertation entirely in report form.

### **3.6 METHODS TO ENSURE TRUSTWORTHINESS**

Connelly (2016:435) describes trustworthiness of a study as the degree of confidence in data, interpretation, and methods used to ensure the quality of a study. In each study, the researcher should establish the protocols and procedures necessary for a study to be considered worthy of consideration by readers (Amankwaa, 2016:121). A study is trustworthy only if the reader of the research report judges it to be so (Gunawan, 2015:10). According to Connelly (2016:435), the following criteria adopted by Guba & Lincoln in 1985 are accepted by many qualitative researchers, and they were applied in this study:

### **3.6.1 Credibility**

Korstjens and Moser (2018: 121) indicates that credibility in research is an assessment of whether or the research findings represent a credible conceptual interpretation of the data drawn from the participants' original data. Connelly (2016:435) concurs that credibility of the study or the confidence in the truth of the study and therefore the findings, is the most important standard by which the study may be judged. These descriptions of credibility in a research study imply that research is only credible when its findings mirror the views of the participants about the reality of the situation under study.

To ensure credibility in this study, the researcher conducted a literature review to be familiar with the contents of the topic under study, the use of electronic surveillance in the investigation of cartels conduct. The researcher conducted interviews with the participants to get in-depth information through their perceptions and experiences. The in-depth information obtained through literature study and interviews helped the researcher to express the actual situations which have been researched and the context around it.

### **3.6.2 Transferability**

Transferability involves the extent to which the study results could be applied in other circumstances, locations, and groups (Korstjen & Moser, 2018:121). According to Connelly (2016:435), the nature of transferability, the extent to which findings are useful to person in other settings, is different from other aspects of research in that readers determine how applicable the findings are to their situation. To allow transferability, the researcher provided sufficient detail of the context of the fieldwork for a reader to be able to decide whether the situation is similar to the problem under research. Therefore, the researcher provided the reader with evidence that the findings of the research could be applicable to other contexts, situations, times, and populations. The researcher also indicated the following aspects to achieve this element:

- The name and the location of organisation where the participants were selected.
- Any constraints in the type of individuals who provided the information.
- The volume of the individuals active in the fieldwork.



- The data collection techniques which were used.
- The number and length of the data collections.
- The period over which the data was accumulated.

### **3.6.3 Dependability**

Connelly (2016:435) explains that dependability refers to the consistency and reliability of the research findings and the degree to which research procedures are documented. This is to ensure that the findings, interpretation, and recommendations of the study are all supported by the data as received from the participants. In this study the researcher conducted semi-structured interviews for data collection, and this ensured a coherent linkage between the data and the findings. The researcher ensured that the information that contributed towards this study is available and accessible. A consensus discussion was held between a researcher and the supervisor to corroborate identified themes and inferences.

### **3.6.4 Confirmability**

Confirmability refers to the degree to which the result could be confirmed or corroborated by other researchers (Korstenjens & Moser, 2018:121). To ensure confirmability, the researcher kept detailed record of all literature consulted. As a result, the researcher was able to prove that the findings and interpretation of the findings did not derive from the researcher's imagination or fabrication but are clearly linked to the data. The researcher kept detailed notes of all the decisions and analysis as the research progressed. The notes may be reviewed or discussed by colleagues. This is to prevent biases from only one person's perspective on the research. The researcher ensured that all material and sources used were acknowledged and secured to prove that the findings were not subjected to the researcher's views.

## **3.7 ETHICAL CONSIDERATIONS**

Leedy and Ormrod (2019:135) state that "in certain disciplines the use of human beings in research is, of course, quite common" and therefore should be approached with great careful. According to Dantzker, Hunter and Quinn (2018:21), ethics refers to doing what is morally and legally right in conducting research. The researcher must look closely at the ethical implications of what they are proposing to do. A due consideration should be given to the rights and feelings of those affected by the

research. The University of South Africa (UNISA) has introduced a Policy on Research Ethics, which requires that research be conducted in a responsible and moral way (UNISA, 2016). As such, this study was based on honesty, trust, fairness, respect, and responsibility. The following ethical issues played an important role in ensuring that this research adhered to all ethical principles:

### **3.7.1 Permission to conduct this study**

The researcher obtained permission from UNISA in terms of the UNISA Policy on Research Ethics (2016:5), which states that “it is the responsibility of the researcher to ensure that he or she does not undertake research without ethical clearance. Researchers may only undertake research that has been approved by an appropriate Ethics Review Committee”. The researcher also obtained permission from the Commissioner of the Competition Commission to conduct the research. The researcher made use of informed consent forms to obtain permission from the participants who took part in the study. The researcher adhered to the code of ethics for employees of the Competition Commission (2013:1), where employees commit to the following aspects:

- To execute my duties efficiently and without fear or favour.
- To treat all people with dignity and respect, as I want to be treated.
- To uphold the principle of equality, fairness and basic human rights.
- To not to take improper advantage of my position.
- In all my action, uphold the values and the spirit of the Competition Act.

### **3.7.2 Harm to participants**

Dantzker, Hunter and Quinn (2018:25) explain that when the research involves direct human contact, ethics play an important role. Individuals participating in research should not be exposed to unnecessary physical or psychological harm (Leedy & Ormrod, 2019:135). Leedy and Ormrod (2019:135) further explain that the researcher should treat all participants in a courteous and respectful manner. This implies that the researcher needs to be sensitive to those who will be involved in the research.

### **3.7.3 Informed consent**

Participants of this research were informed of the nature of the study to be conducted and were given the opportunity to choose to be part of the study or not. Dantzker, Hunter and Quinn (2018:26) state that the researcher should not only seek to obtain

consent but should also inform the prospective participants that participation is voluntary. The participants were also informed of their rights to withdraw from the study at any given time.

#### **3.7.4 Invasion of privacy**

In terms of the Section 14 of the South African Constitution of 1996, every individual has the right to privacy. This means that the privacy of every individual participating in this study will be respected. The researcher, therefore, kept the details and views of the participants strictly confidential.

#### **3.7.5 Confidentiality and anonymity**

Dantzker, Hunter and Quinn (2018:28) explain that in some research fieldwork the researcher is required to go under cover, however, such research cannot be conducted if the subjects become aware that they are being studied because subjects may change their behaviour. In this study, the researcher was honest and open about the nature of the study and did not rely on misrepresentation or deception as a means of getting the necessary information. The findings of the study reflected what transpired without any distortion. The researcher fully acknowledged the use of others' ideas and words. Confidentiality and anonymity refer to an agreement between persons that limits others' access to private information (Denzin, & Lincoln, 2018:77). The information received was stored (Password protected) by the researcher. The findings of the research were documented in the form of an academic thesis.

### **3.8 SUMMARY**

This chapter (Three) highlighted the adopted research design and methodology. It describes the employed research approach, study location, study population and sampling procedures, as well as data collection and analysis methods. The methods to ensure trustworthiness of this study and ethical considerations also formed part of this chapter. The following chapter (Four) focuses on data presentations, analysis and discussions.

## CHAPTER FOUR: DATA PRESENTATIONS, ANALYSIS AND DISCUSSIONS

### 4.1 INTRODUCTION

This chapter consists of the data that was collected and analysed for this study. It highlights the responses based on the questions asked and themes generated from the verbatim expression of the selected participants. These responses were guided by the study aim, objectives and research questions. The researcher discussed the findings in reference to the already presented literature studies for triangulation purposes to provide real life interpretations of the responses by the participants. The responses of the selected 10 participants were tested regarding the subject under research, while considering the problem statement of this study.

Therefore, the findings of this study are categorised under the study aim, objectives and research questions, in reference to the reviewed literature studies and the gathered empirical data, with the identification of study themes. To conceal the true identities of the interviewed participants, the referencing method for the conducted interviews in this study comprised a numerical sequence of 'participant 1-10.'

### 4.2 FINDINGS

#### 4.2.1 The importance of electronic surveillance

This question was asked to the selected participants: *Why should electronic surveillance be used to investigate the cartel conducts?*

The following are the participants responses in relation to the above-mentioned question:

**Participant 2** *“Cartel conduct is secretive in nature. Those involved in such behaviour are aware that their actions are prohibited by the law. Consequently, when engaging in cartel conduct, they strive to maintain a high level of secrecy.”*

**Participant 3** *“Cartel is the conduct that takes place in secret, and it is not easy to detect. Surveillance becomes relevant in the fight against a cartel conduct given the secretive nature.”*

**Participants 5** *“Cartel conducts it is very secretive, and most of the time we do not get enough information to prosecute. Even when there is a leniency applicant you might not get full information and then you can use electronic surveillance to then investigate cartel conduct”.*

**Participants 7** *“it is a very secretive conduct and most often there are no evidential material”. It might be necessary to use surveillance in order to gather evidence”.*

The themes that emerged when analysing the responses of the participants is that cartel is secretive in nature. The participants were of the view that cartel conduct is secretive in nature, as such it is difficult to detect and obtain crucial evidence. Electronic surveillance will be a valuable tool because it will be used to gather information that is unattainable through other means. Some of the participants were of the view that the evolution of technology has made cartel conduct more sophisticated and difficult to detect. Therefore, it is important to introduce advanced detection measures, such as electronic surveillance to be able to crack it.

Another view was that the current investigation tools are still helpful, however, they should be strengthened with advanced cartel detection measures to easily deal with complex and sophisticated cartel conduct. These expressed views by the participants read with section 1.2 of Chapter One of this study, when Van Heerden and Botha (2015:309) highlighted that the secretive nature of cartel conducts poses challenges for competition authorities around the world to effectively detect it.

In section 1.1, Mirasdar and Gupta, (2017:2604) shared the same view with Van Heerden and Botha that cartel activities are increasing daily, and it is difficult for many competition authorities to curb them. In the same section 1.1, Schinkel (2014:6) confirmed the finding when mentioning that authorities are faced with sophisticated cartels, and as such, there is a need to shift and give more attention to proactive cartel detection measures to stay ahead of the cartelists. Another question was asked to the selected participants, as follows: *What value would electronic surveillance add in the investigation of cartel conducts?*

The participants responded as follow:

**Participant 3** *“I believe that incorporating electronic surveillance could indeed improve our approach investigating cartels. In situations where traditional methods have proven ineffective, surveillance useful in obtaining evidence”.*

**Participant 4** *“Surveillance is a tool that will add value to crack cartels. Cartel members have up their game and the level of sophistication is high, so we also need to up our game considering tools such as the electronic surveillance tool”.*

**Participant 5** *“I think it will add the much value in that it will provide us with indisputable evidence like if you have video recording of firms, discussing how they going to engage in cartel conduct”.*

**Participant 7** *“It will add more value to obtain crucial evidence”.*

**Participant 9** *“It will add value in getting real time data. I think it would certainly assist the authorities to be able to gather genuine evidence of potential collusion between firms”.*

**Participant 10** *“The fact that it would expedite the investigations that is one of the biggest values. If you look at it, we will gather evidence in real time, as and when these criminals are discussing issues that are anti-competitive”.*

The theme emerged from the responses of the participants is gathering of indisputable evidence. The participants shared that electronic surveillance is a powerful investigative tool that can assist in obtaining real-time evidence in the investigation of cartel conduct, and this will expedite the investigation. It will provide the Competition Commission with indisputable evidence obtained from recorded communications between individuals suspected of engaging in cartel conduct. This can be especially useful in cases where individuals are actively engaged in illegal activities and are difficult to catch through other traditional methods.

Some of the participants indicated that electronic surveillance should be utilised in conjunction with other traditional methods to crack sophisticated and complex cartel cases, however, it should be used as a last resort. In section 2.3.2, Ratcliffe (2020:1) confirmed the study findings by indicating that electronic surveillance can capture real time information of various activities to assist the authorities to gather valuable evidence. In section 2.2.3 Orthman and Hess (2013:445) echoed the same views as participants by stating the undeniable importance of utilising electronic surveillance in the criminal investigation, as it enables the gathering of “impossible” evidence. It

enables the law enforcement agencies to address the increasingly complex and sophisticated crimes committed by organised criminal gangs. In the same section 2.2.3, Graham and Kitchin (2021:215) asserted that electronic surveillance is an infinite tool used for a variety of purposes, including finding valuable evidence on criminal suspects. The view is also supported by Geldenhuys (2021:16) in section 2.2.1 who stated that the use of surveillance allows law enforcement a chance to gather extensive information either covertly or overtly.

#### **4.2.2 What the concept “electronic surveillance” entails**

To achieve the study objective 01, the following question was posed to the selected participant, *‘what do you understand by electronic surveillance?’*

The following are some of the responses to the question asked:

**Participant 2** *“My understanding of electronic surveillance involves the use of electronic surveillance equipment. It includes bugs that will transmit information, or monitoring people’s activities on computers without their consent”.*

**Participant 3** *“My understanding of electronic surveillance is limited because it is not an area that I have been exposed to. But based on general knowledge, electronic surveillance seems to involve the utilisation of various devices to acquire information or evidence”.*

**Participant 4** *“Electronic surveillance is one of the tools used to gather information or evidence. This tool is not commonly used due to its intrusive nature”.*

**Participant 5** *“My general understanding is that electronic surveillance involve practices such as wiretapping and secret recordings”.*

**Participant 7** *“My understanding of electronic surveillance involves gathering of confidential material or information using electronic devices like bugs, wiretaps, CCTV and GPS tracker. This is mostly done surreptitiously, without the knowledge or consent of the individuals targeted by these devices”.*

The identified theme is evidence gathering tool. The selected participants in their responses mentioned that electronic surveillance is an investigative tool used to gather crucial information or evidence by monitoring cartel activities. The participants understand that it is about tapping communication and monitoring internet activities by

means of various surveillance devices. The participants further mentioned that targeted individuals are monitored without their knowledge. Some participants, however, presented a general understanding of what is electronic surveillance. The responses shared by the participants reads well with section 1.8.2 of the literature, when Heibutzki (2018:1) confirmed that electronic surveillance refers to the surveillance of email, fax, internet, and telephone communications. In section 2.2.1 Van Brakel and De Hert (2011:168) presented the expressed views that 'surveillance' refers to the 'monitoring, observing, or listening to people, their movements, conversations, or other activities or communications; recording anything monitored, observed, or listened to during surveillance; and surveillance by or with the assistance of a surveillance device.

Subsequently, this question '*what are different types of surveillance?*' was asked to the selected participant and their verbatim expressions read as follows:

**Participant 2** "*I know bugs can be used to get information, as well as the gathering of information through computers by monitoring activities of individuals on platforms like Facebook. Bugs work as listening devices that can be installed in places where people reside or work to monitor their conversations*".

**Participant 4** "*I think there are different types of electronic surveillance such as phone tapping, the use of video or audio recording equipment and the placement of recording devices in place like boardrooms. It could also be tools that are used to monitor data, including activities on social media platforms*".

**Participant 6** "*It involves tapping of the phones where conversations and WhatsApp messages are monitored. Another method is the use of CCTV, where a camera is placed to observe activities and identify individuals*".

**Participant 7** "*I know about audio surveillance, such as wiretapping where communications between parties are intercepted and room bugging, where meetings can be monitored if informed in advance. Visual surveillance methods which installing car cameras, using body-worn devices for image capture, and setting up CCTV cameras to monitor suspects movement and activities*".

**Participant 8** "*The use of video cameras to monitor and record activities in specific locations is one aspect. Other methods include phone and communication interception, internet surveillance, and implementation of GPS tracking*".



**Participant 9** *“I know of drone technology that is used for physical monitoring, and the use of spyware or malware within computers”.*

This study offered that in their responses, the participants mentioned that surveillance refers to phone tapping, video and audio monitoring bugging devices and GPS tracking. In section 2.2.2, different sources (Weiss, 2018:132; Smith & McCusker, 2020:89; Cunningham & Hester, 2023:65; Andrejevic, 2022:41) supported the study findings by indicating different types of surveillance as audio surveillance, visual surveillance, tracking surveillance and data.

Ball and Haggerty (2020:82) in section 2.2.2 also confirmed the responses shared by the selected participants by providing that electronic surveillance can be done in a variety of ways, including tracking people on CCTV, reading text messages, sifting through internet browsing history and social media and spying on people by covertly activating webcams and microphones.

This study further posed this question *‘Which types of surveillance can effectively be used to investigate cartel conducts?’* to achieve objective 01 of this study.

**Participant 2** *“I believe computer software can be used to track the activities of people on internet. Bugging devices can be installed to listen to individuals’ conversations”.*

**Participant 3** *“Data surveillance can be used for online data analysis. This includes the use of algorithms. Video surveillance and bugging devices can be used to monitor interactions between cartelists”.*

**Participant 4** *“Electronic surveillance such as phone tapping, video and audio recording can be used to investigate cartel”.*

**Participant 7** *“The investigator should recommend the appropriate device depending on the nature of the case. Audio and visual devices can be used to gather information related to the under investigation”.*

The theme that emerged is the use of audio and visual surveillance. As a result, the majority of the participants in their responses mentioned audio surveillance, visual surveillance and their views are supported by different sources in section 2.2.2 of the literature conducted. Weiss (2018:132) mentioned that audio surveillance is often used by law enforcement agencies and this technique involves bugging rooms, carrying

cables, tapping phones, or listening remotely. The most common and favoured method due to its very discreet in nature is eavesdropping.

Andrejevic (2022:41) in the same section shares the same views with some of the participants about data surveillance. Andrejevic (2022:41) highlighted that data surveillance is the practice of monitoring and collecting online data as well as metadata. It is concerned with the continuous monitoring of users' communications and actions across various platforms, as section 2.2.2 affirmed.

The selected participants were also subjected to this question '*which act regulate the usage of electronic surveillance as an investigation tool?*' For the accomplishment of objective 01. In response, the selected participants hinted on the following aspects in verbatim:

**Participant 4** "*I think it is the electronic communications act. I think that is the primary legislation. I think there are also regulations, but those regulations are meant to compliment this act.*"

**Participant 6** "*One of them is the electronic communications act*".

**Participant 8** "*In South Africa we have the regulation of interception of communication and provision of communication related information act*".

Most of the selected participants have a basic understanding of the act that regulates the usage of electronic surveillance as an investigation tool. At least one participant mentioned RICA, Act 70 of 2002. Section 2.4.3.7 presented that the South African legislative frameworks on surveillance, and it confirm the findings of the one participant on RICA, Act of 2002.

#### **4.2.3 The role of electronic surveillance**

In an attempt to accomplish objective 02 of this study, this question '*what is the role of electronic surveillance in the investigation of crime?*' was asked to the selected participants. These are some of their verbatim responses:

**Participant 3** "*The use of electronic surveillance in crime plays a big role especially insofar as organised crime is concern. It is not easy to gather evidence in organise*

*and sophisticated crimes, so the use of electronic surveillance can play that role to assist in gathering the evidence that is required to crack that criminal activity under investigation”.*

**Participant 4** *“Electronic surveillance helps to collect information or evidence which can then be used in a court of law to fight or to prosecute criminals. It also provides leads to the investigation”.*

**Participant 5** *“The role of electronic surveillance is to gather evidence that can used to proof the commission of a crime. This kind of evidence is usually indisputable when presented to prove the case”.*

**Participant 9** *“I think that electronic surveillance mainly serves the purpose of collecting evidence”.*

Upon analysing the collected data, two themes emerged, namely, evidence gathering tool and creates investigation leads. For discussion purposes, the common response from the selected participants is that the role of the electronic surveillance is to gather evidence to prosecute cartelists. These expressed views of the participants read with section 2.3, when Baker and Gunter (2005) agreed that the role of electronic surveillance is to collect information for the furtherance of an investigation. The investigator may require the information for search warrant, to gather intelligence for a dawn raid or to locate a suspect, contraband, or the site of illegal activities.

In the same section 2.3 McCulloch and Wilson (2021:112) indicated that the surveillance allows investigators to uncover the evidence necessary to convict criminals or justify further legal action, such as issuing search warrants; to track suspects’ actions and their whereabouts using surveillance methods, looking for their involvement in criminal activities and to identify and map criminal networks, including relationships between suspects and their allies, providing valuable insight into how criminal organisations are structured and operated.

In section 2.3 Holmes (2014:1) affirmed the study findings by confirming that surveillance technology helps law enforcement agencies to stay one step ahead of criminals. The cited authors in this section also support the views of the participants that the role of the electronic surveillance is to provide the LEAs with the leads to

further their investigations or leads to uncover hidden evidence necessary for the prosecution and conviction of perpetrators of cartel activities. In section 2.3.2, Ratcliffe (2020:1) supported these views by revealing that footage captured by video cameras can be used to piece together the sequence of events that can lead to a crime scene.

#### **4.2.4 Circumstances under which “electronic surveillance” should be authorised**

To achieve objective three (03) of this study, the researcher combined the responses of the following two questions because the selected participants provided similar answers to the following posed two (02) questions:

- *What circumstances should allow the Competition Commission to apply for a warrant to conduct electronic surveillance operations?*
- *When should the electronic surveillance be used as an investigation tool to investigate cartel conducts?*

The selected participants shared the following verbatim responses to provide answers to the indicated 02 questions.

**Participant 1** *“Electronic surveillance should only be used when other investigation methods failed to uncover evidence”.*

**Participant 3** *“I think that the application of electronic surveillance should be considered a last resort, only when all other investigative tools prove ineffective in gathering evidence. The test for using electronic surveillance should be reasonableness and proportionality to ensure that it is not applied unnecessary”.*

**Participant 5** *“It should be applied in a situation where there is a reasonable basis to suspect ongoing cartel activities, and all other investigative tools failed to uncover evidence”.*

**Participant 7** *“Electronic surveillance should only be used when the other traditional investigative methods have proven to be ineffective or when there is no viable alternative means of gathering information”.*

The identified theme is that use electronic surveillance as last resort. For analysis, the participants are of the view that electronic surveillance should be used when there are strong suspicions and only when the normal investigation methods have proven to be

ineffective. One participant mentioned that the test is reasonableness and proportionality to ensure that it is not applied unnecessarily. It must be used as a last resort to obtain crucial information. Section 2.6 confirmed the findings when Mutung'u (2021:175) mentioned that the law stipulates the specific requirements that must be met for electronic surveillance to be undertaken; (1) strong suspicion that a specific crime has been committed, (2) seriousness of the offence justifies surveillance, and (3) investigative activities thus far have been unsuccessful and further enquiries would have no prospect for success.

The findings are also supported by section 2.6 of the literature when Zhang and Mitchell (2023:56) highlighted that electronic surveillance should be used as a last resort to investigate cartel activities. This implies that it should only be considered after other investigative methods and techniques have been deemed unsuccessful in solving the case or in gathering information important to solving the case.

Another question '*who should be authorised to apply for a warrant to conduct electronic surveillance operations during the investigation of cartel conducts?*' was asked to solicit thoughts of the selected participants in this regard.

**Participant 2** "*The investigators responsible for the under investigation should be authorised to apply for a warrant*".

**Participant 3** "*I believe the Commissioner should take the lead as the accounting officer. The Commissioner can delegate these powers, allowing for a more effective distribution of responsibilities down to the investigation team, the foot soldiers who ultimately need to execute the tasks*".

**Participant 4** "*Certainly, the use of this tool raises complex legal issues, so I would suggest that only legal practitioners, preferably practicing advocates, should be authorised to apply for a warrant to conduct surveillance*".

**Participant 7** "*The Commissioner normally applies for the warrant and then delegates that authority by granting power of attorney to the manager of the relevant division responsible for the investigation*". Furthermore, another question '*who should be allowed to conduct electronic surveillance operations during the investigation of cartel*

conducts?’ was posed to gather views of the selected participants and these are their responses:

**Participant 4** *“It should not be anyone within the organisation who is appointed as an investigator, or inspector, but it must be inspectors or investigators with accreditation”.*

**Participant 5** *“I am thinking senior investigators and experienced investigators should be allowed to conduct electronic surveillance operations”.*

**Participant 6** *“The divisional manager, principal investigators and investigators should work closely in conducting surveillance operations. Individuals appointed at this level must possess the capability to keep sensitive information confidential”.*

**Participant 7** *“The institution should have a relevant dedicated unit with people who specialises in surveillance, who will only focus on surveillance operations”.*

**Participant 8** *““The operations obviously must be implemented by the investigator who is investigating the case”.*

**Participant 10** *“The ultimate responsibility and accountability for proving a case rest on the lead investigator. Therefore, I would say the lead investigator assigned to that particular case should conduct the operation”.*

For discussions, the views of the participants highlighted three different but related aspects, lead investigator, trained dedicated team and ability to keep a secret. Some of the participants indicated that the lead investigator, including seniors involved in the investigation should be allowed to conduct surveillance operations. Others are of the view that the commission should have a dedicated trained team/unit that should be responsible for the surveillance operation. Members of the team should be allocated to investigation which requires surveillance operations and hand over the evidence to the lead investigator when done with the operation. The literature in this study did not cover this part of the findings. Paragraph 2.20 Foremny and Dorabialski (2018:949) confirms the findings that identifying anti-competitive agreements is complex and requires considerable interdisciplinary knowledge, experience, appropriate choice of tools, availability of selected data and sometimes even long-term market observation. Moreover, the researcher also asked this question *‘for how long should the warrant to conduct electronic surveillance operations be effective? Elaborate’*, to the selected participants and they shared the following verbatim responses.

**Participant 5** *“Certainly, it cannot be indefinite, and I am considering a duration based on the nature of the investigation. I propose that a timeframe of one year, or twelve months, should suffice for the warrant to be active”.*

**Participant 7** *“I think the duration of each warrant should be guided by the nature of the case under investigation”.*

**Participant 8** *“The severity or the seriousness of the suspected offence should determine the duration of that warrant”.*

In discussion, there is a strong view from the participants that the period of the surveillance warrant should be guided by the circumstances of each case, however it should not be in perpetuity. The participants believed the period of the warrant should be aligned with the duration of the investigation, meaning that once the required information or evidence is obtained the warrant should cease with immediate effect. In section 2.6, Mutung’u (2021:175) validated the findings by indicating that the law stipulates who may be monitored, the type of surveillance allowed, the type of authorisations required and the subsequent procedural conclusions and steps that must be taken for every piece of surveillance intelligence gathered.

#### **4.2.5 The limitations of the use of electronic surveillance**

This question *‘what limitations should be considered when conducting electronic surveillance operations?’* was posed to the selected participants and their responses are recorded as follows.

**Participant 5** *“Certainly, when implementing electronic surveillance operations, it is important to ensure that it does not carelessly involve parties unrelated to the investigation”.*

**Participant 6** *“The limitation, of course, is the potential infringement on individuals’ right to privacy”.*

**Participant 7** *“The financial aspect is an important consideration because these tools and technologies can be quite expensive. In addition, one needs to account for the need for expertise and training. A team of well-trained specialist is essential to navigate the complexities involved in electronic surveillance operations”.*

**Participant 8** *“Surveillance operations should adhere to ethical standard and stay within the boundary of privacy regulations”.*

The identified theme is right to privacy. For analysis, most of the selected participants, in their response emphasised more on the right to privacy. They mentioned that the scope of the surveillance operations should only be limited to the subject(s) under investigation. Two of the participants mentioned the resources as one of the limitations in terms of costs in acquiring the necessary equipment, training the human resource and the time spent during the operation.

Section 2.10.1 aligned with the findings when Ran (2016:11) mentioned that the right to privacy is an important individual right that is often referred to in everyday life, and the use of surveillance by government carries a great risk of infringing upon an individual’s privacy and other democratic values when it is not regulated properly. In the same section, Baker and Gunter (2005:15) added that surveillance should in no way interfere with the subject’s reasonable expectation of privacy.

Another question *‘what do you understand by the fundamental rights to privacy?’* was directed to the selected participants and they hinted on the following in response.

**Participant 4** *“The right to privacy it is one of the fundamental rights, entrenched in the constitution and I would describe it as one of the inherent human rights, or one of the inherent rights that human beings have. The right to privacy is considered as a fundamental right that must be always protected. The Constitutional court has taken measures to ensure that this inherent right is fully protected and could only be interfered with under reasonable conditions and circumstances”.*

**Participant 5** *“I know that privacy rights are enshrined in the constitution, both on a personal and business level”.*

**Participant 8** *“The fundamental right to privacy is rooted in the concept that individuals possess a fundamental entitlement to a private sphere in their personal lives, free from unwarranted intrusion or interference by others including the government. It is a corner stone of the constitutional frameworks in many countries. Ours is enshrined in the bill of rights”.*

This study presents that the selected participants know and understand the fundamental right to privacy. They are aware that it is a right that protects individuals



for arbitrary interference with privacy, family, home or correspondence. In their responses the participants displayed an understanding that the right to privacy can be compromised through surveillance operations without the individual being aware.

The participants further exhibited knowledge and understanding that the right to privacy is a fundamental right, however it is not an absolute right and may be limited in certain circumstances. For example, the right may be limited if it is necessary to conduct a surveillance operation to crack cartel conduct cases. These views are supported by section 2.10.1 of the literature when Kayaalp (2018:8) revealed that privacy has been enshrined in constitutions around the world as a fundamental human right, following the Universal Declaration of Human Rights at the United Nations General Assembly in 1948. Humble (2021:1) provided that the right to privacy is a fundamental human right and part of various legal traditions at the international level aimed at restricting governmental and private actions that threaten an individual's privacy. Ran (2016:11), in the same section stated that the right to privacy is an important individual right that is often referred to in everyday life, and the use of surveillance by government carries a great risk of infringing upon an individual's privacy and other democratic values when it is not regulated properly. The first bulletin under section 2.10.1 indicates that there are limitations, which are provided by the RICA, 2002. In terms of this Act, private communications can be intercepted for the purposes of investigating and prosecuting serious criminal offences.

Moreover, this additional question *'what regulations should be put in place internally to govern the usage of electronic surveillance?'* was subjected to the selected participants and they shared the following verbatim responses in this regard.

**Participant 2** *"Electronic surveillance must be applied with the authorisation of the courts. Following the approval from the court, strict regulations should indicate who has the authority to run the surveillance operations. This authority should be confined to a limited number of individuals".*

**Participant 5** *"It is important to introduce internal policies or guidelines that can be disseminated among employees. These regulations should be updated from time to*

*time. In developing such policies, the Commission should benchmark with other experiences institutions like Special Investigation Unit.*

**Participant 6** *“The investigators in cartels division need to be well-informed about the procedures and processes associated with use of electronic surveillance. Investigators must receive a training on how to conduct surveillance”.*

*‘How should the organisation guard against the misuse of electronic surveillance operations?’* was another question posed to the selected participants and their verbatim responses read as follows.

**Participant 2** *“Serious disciplinary measures should be implemented against an individual in a position of authority who misuses a device intended for specific purpose by using it for unauthorised activities.*

**Participant 5** *“The use of electronic surveillance within the organisation must be strictly limited to situations where a warrant has been legally granted”.*

**Participant 6** *“There should be a structured bureaucratic process, including specific levels of approval, wherein a designated individuals is responsible for signing off on any surveillance operations. There should also be strict disciplinary measures to deter unauthorised surveillance operations”.*

Themes that emerged when analysing interview data in relation to the above questions are development of internal policies and consequences management or serious disciplinary measures. As a result, this study provides that the views of the selected participants are that the Commissioner should put measures in place to define guidelines under which surveillance could be carried out. There should be measures to ensure that the use of surveillance operations are lawful and responsible. These measures should also include consequence management for those who would misuse the surveillance equipment for reasons other than an approved investigation. The participants are of the view that there should be independent oversight mechanisms to monitor all the activities related to surveillance operations.

In section 2.6, McIntyre (2016:1) supports the views of the participants by indicating that due to its intrusive nature, electronic surveillance is subject to strict judicial controls and legal guarantees to prevent abuse and limit invasion of privacy. In the

same section 2.6 Bloch-Wehba, (2018:145) mentions that a warrant of arrest is required as a control mechanism, to create a balance between law enforcement's need for secrecy, individual privacy, and transparency. Therefore, such guidelines help to ensure that the use of surveillance technologies is lawful and responsible, and that there are measures in place that apply to collection, handling, and disclosure of material obtained using these technologies in order to protect individual privacy, personal data, human rights and fundamental freedom while effectively and appropriately pursuing legitimate law enforcement objectives.

In section 2.10.1, Roberts, *et al.*, (2021:10) aligned with the findings when mentioning that to avoid surveillance abuse, an independent oversight body should supervise the activities of the investigating authorities. In the same section [2.10.1], Roberts, (2021:10) emphasised that South Africa has strong oversight mechanisms to monitor law enforcement actions in relation to the use of surveillance.

Roberts (2021:10), in the same section [2.10.1] further stated that monitoring surveillance practice against privacy rights protections requires well defined transparency and independent oversight mechanisms. In section 2.10.1, Solove (2004:1708) showcased that to guard against the abuse of electronic surveillance can be accomplished by providing for the oversight of law enforcement surveillance, accountability for abuses and errors and limits against common forms of surveillance.

#### **4.2.6 Challenges of investigating cartel conducts**

This question '*what challenges are there in terms of investigation techniques the Competition Commission is faced with in the investigation of cartel conducts?*' was posed to the selected participants to meet objective 05 of this study and these are some of their verbatim responses.

**Participant 2** "*The challenge with other investigative tools such as dawn raids is that we access historical information rather than real-time data. As a result, the effectiveness of dawn raids may diminish over time for obtaining up to date information*".

**Participant 4** *“Criminalisation of the cartel conduct lessen the chances of directors of companies to approach the authority to report their illegal activities. Leniency policy proven to be an effective tool to dismantle cartels, however, the current limitations stemming from criminalisation provisions have reduced its efficacy”.*

**Participant 5** *“The introduction of criminal provisions for directors’ possesses a serious challenge. Many directors of firms engaged in cartel conduct are reluctant to come forward, recognising the potential criminal implications of their actions. Without a leniency applicant, the difficulty arises in gathering sufficient evidence to pursue prosecutions for cartel conduct”.*

**Participant 8** *“The leniency program has been significantly impacted by the introduction of criminalisation of cartel conduct”.*

**Participant 9** *“The Competition Commission is faced with a growing need for electronic surveillance methods to collect data, given the prevalent shift away from traditional paper trails in many companies and industries. This challenge is heightened by the use of algorithms pricing model. So, the Competition Commission should recruit highly skilled IT and software development experts to set up algorithms to monitor pricing data.*

Two themes were identified during the analysis of the responses of the participants, namely, criminalisation of cartel conduct and evolution of technology in the market. For analysis, views expressed by participants are that firms are moving away from the paper trail, as such competition authorities find themselves faced with sophisticated cartel conducts and difficult to detect cartel activities. Firms invest much of their resources around the use of technology. Firms employ IT experts to set up algorithm programmes and use that as a platform to collude.

The literature expressed the same sentiments in section 2.11, when Schinkel (2014:257) mentioned that competition authorities today are faced with sophisticated cartels, and they need to get over leniency and look seriously at supplementing it with proactive methods to stay ahead of the cartelists. In section 2.3.3, Chen, Mislove and Wilson (2016) submitted that the rise of e-commerce has unlocked practical applications for algorithmic pricing, where sellers set prices using computer algorithms. The participants further mentioned that another challenge is the

introduction of criminalisation of cartel conduct, which discourages firms or directors to come forth and report their activities to the authorities as they fear to be criminally prosecuted. This reads well with section 2.11 of the literature when Stephan (2014:334) highlighted that another challenge that has a significant impact on corporate leniency programme is the criminalisation of cartel conduct.

The law requires that directors or managers of companies that engage in cartel conduct be prosecuted for anticompetitive behaviour. In the same section, Van Heerden and Botha (2015:327) indicated that enforcing the criminalisation of cartel conduct could undermine the effectiveness of the corporate leniency policy. These directors bear the risk of being imprisoned for a long time, and criminal proceedings will have to be paid out of their own pockets. This is because the granting of the immunity to a leniency applicant, in countries like South Africa, does not translate into automatic absolution from criminal prosecution by the NPA.

Some participants mentioned characterisation as another challenge competition authorities are faced with in the investigation of cartel activities. This is highlighted in section 1.1 of the literature, when Legal brief (2022:1) revealed that the Competition Commission affirmed that it is faced with the “new generation” of cartel cases which are “characterised by a clear shift in the pendulum,” being the cartel cases the Commission has been unsuccessful in prosecuting.

#### **4.2.7 The effectiveness of strategies employed to investigate cartel**

The researcher asked this question *‘Do you think the reactional cartel detection method is still effective in the fight against cartel conducts?’* The selected participants shared the following insights in verbatim responses.

**Participant 3** *“Various methods employed previously have proven to be effective over the past decade, resulting in significant progress in cracking down cartels. However, acknowledging the evolving nature of the market and also the fact that cartelists are finding new ways to manipulate market it is important for the Commission to adopt new investigative strategies to effectively respond to evolving cartel activities”.*

**Participant 4** *“Reactional cartel detection methods undoubtedly contributed significantly. However, these methods are challenged by evolving technologies and*

*societal change. So, the utilisation of both traditional and proactive cartel detection methods is important for effective and adaptive investigative practices.*

**Participant 5** *“Traditional investigation techniques are still to a certain extent retain a degree of effectiveness. However, with the introduction of artificial intelligence algorithms, it is necessary for the Commission to update investigative tools to be more proactive and responsive”.*

**Participant 7** *“We need to be more proactive than relying solely on reactive methods such as people submitting complaints and leniency applications. There is a need to invest proactive tool because it will be easy to uncover potential issues before they are reported”.*

The identified study theme is reactional versus proactive cartel detection measures. In responding to the question posed and the verbatim responses provided, the selected participants are of the opinion that with time the reactional cartel detection method becomes less effective as the conduct becomes more sophisticated. They are also of the opinion that the traditional investigation tools need to be supplemented with proactive cartel detection measures to keep up with the changes as the technology evolves.

They further suggest that the Competition Commission needs to be more innovative to cope with the evolving nature of the market to be able to deal with intelligent programs such as algorithms. Section 1.1 confirmed these findings as stated by Levenstein and Suslow (2006:43) that most of the Competition Commission authorities around the world applied a reactional cartel detection method and with time this method became less effective as the conduct becomes more sophisticated. In the same section, Mirasdar and Gupta, (2017:2604) shared the same sentiment that cartel activities are increasing daily, and it is difficult for many competition authorities to curb them. In section 1.1, Schinkel (2014:6) agreed with the views of the participants that authorities are faced with sophisticated cartels, need to shift and give more attention to proactive cartel detection measures to stay ahead of the cartelists. Schinkel (2014:257), in section 2.11 sided with the participants that competition authorities today are faced with sophisticated cartels, and they need to get over leniency and look seriously at supplementing it with proactive methods to stay ahead of the cartelists.

Another question *‘What investigation technique(s) do you think work(s) better to resolve cartel cases currently?’* was also asked to the selected participants and their verbatim responses are confined to the following aspects.

**Participant 2** *“There are two effective tools that have been applied to tackle cartel conduct. The first one is corporate leniency policy which encourages firms to come forward and report cartel activities in exchange for leniency. However, there are signs that it is becoming less effective, possibly due to the increased stability and secrecy of existing cartel. The second one is dawn raid, which involve surprising entities in their offices without prior warning, have proven to be more effective”.*

**Participant 3** *“The Corporate Leniency Policy has played a significant role in addressing cartel conduct, but it is important to acknowledge the evolving era and the need for more proactive measures. In this new era, relying solely on existing tools may not be sufficient.*

**Participant 6** *“The Competition Commission has Corporate Leniency Policy encouraging individuals to involved in cartel activities to approach the Commission and disclose their activities for leniency. This policy has some limitations. It is reactive as individuals may participate in cartel activities for several years before deciding to approach the Commission out of fear of being caught. By then, the potential damage caused by the cartel may already be significant”.*

In the discussions, selected participants mostly mentioned the leniency programme that used to be a powerful tool for Competition Commission to detect cartel cases, however, the number of leniency applications has significantly declined. The participants further responded that the decline in leniency application may require the Competition Commission to invest in other detection tools, proactive cartel detection tools such as electronic surveillance, to supplement reactionary detection methods. The participants believe that firms are increasingly developing more sophisticated ways of colluding and such practices involve not only agreements on traditional competition parameters, but also aspects such as technological innovations.

These findings are confirmed in section 2.16.10 where Mahlangu (2014:4) pointed out that the Competition Commission through its CLP has been successful in detecting several cartels that would not have otherwise been detected without the policy. In the same section, Labuschagne & Lotter (2015:1) mentioned that The CLP has been

successful in uncovering cartel conduct in South Africa and has contributed to the prosecution of about 30 per cent of the cartels prosecuted in the country. In section 2.20 Hüschelrath (2010:1) supported the views of the participants that even though the reactive cartel detection method still plays a role in cartel detection, there are signs that proactive cartel detection methods are gaining traction as a tool to increase the likelihood of cartel detection.

*‘What pro-active detection measures should the Commission apply in order to get ahead of the cartelists?’* was another question posed to the selected participants to respond to objective 06 of this study and their verbatim responses are recorded as follows.

**Participant 2** *“The use of electronic surveillance via software, particularly in the context of monitoring prices, can be proactive. This approach involves collecting pricing data, inputting it into a system, and analysing how prices evolve over time. This less invasive form of electronic surveillance can be applied selectively in industries chosen for market inquiries”.*

**Participant 3** *“I have indicated the importance of adopting various tools for cartel detection and with the advent of digitalisation and big data, we need to move towards the detection of cartel via the use of algorithms. Cartels should be detected through algorithmic analysis and combining it with different investigative methods”.*

**Participant 5** *“The Commission has a division known as the Policy and Research division, which specialises in extensive market research. Using this division, we can proactively monitor market patterns, including price movements. This proactive approach allows us to stay abreast of market dynamics and swiftly identify potential cartel patterns”.*

**Participant 6** *“We are moving into fourth industrial revolution, so relying on traditional methods becomes increasingly challenging. Times of finding physical paper with incriminating evidence are gone. Individuals engaged in cartel activities often resort to digital communication. To counter this evolving trend and effectively combat cartels, electronic surveillance emerges as a crucial tool”.*

Alternatively selected participants responded that when investigating the Competition Commission should use a variety of tools, including a market inquiry, to gather



information and evidence. A market inquiry will enable the Competition Commission to understand a particular market better. Some participants believe that electronic surveillance should be introduced to supplement current investigation tools to get real-time information. These participants are of the view that technology has taken over most of business activities, and conventional methods would not assist much in detecting cartel behaviour.

Therefore, the introduction of electronic surveillance will match the current trends of committing anti-competitive behaviour. One participant mentioned the use of algorithms as a detection tool because various markets have adopted algorithms for pricing purposes which could either be pro-competitive or anti-competitive. Section 2.20.7 of this study confirmed this finding as stated by Burke (2018:261) by indicating that the South African Competition Commission uses market inquiry as a proactive technique to detect anti-competitive behaviour in the market. The expressed views of the participants also read with section 2.20.7, when Motta, Peitz and Schweitzer (2021:1) stated that market inquiry is a new competition tool which allows authorities to intervene in markets which do not function as they should. In section 2.21 ICN (2020:2) mentioned that while traditional cartels involve agreements between rivals, the use of algorithms can enable parallel pricing and other forms of coordination without direct communication between competitors. Deng (2020:965) in section 2.21 agrees with the views of one participant about algorithms by indicating that the threat of algorithmic collusion is real and poses far greater challenges to competition authorities than human coordination and collusion.

*'Do you think the act should be amended to incorporate the use of electronic surveillance in the investigation of cartel conducts?'* was another question asked to the selected participants and their verbatim responses showcase the following:

**Participant 2** *"It is necessary to amend the Act to empower the Commission to conduct surveillance operations. If the South African Police Service Act contain specific provisions related to surveillance, it could serve as a reference point for incorporating similar provisions into the Competition Act. Participant 3* *"Certainly, the Act needs to be amended to legally empower the Commission to use electronic surveillance. The amendments should explicitly outline the conditions, procedures, and limitations under which such surveillance operations can be conducted".*

**Participant 6** *“Amending the Act to include the use of electronic surveillance as an investigative tool aligns with the dynamic nature of today’s business and technology environments”.*

**Participant 10** *“To stay ahead of cartelists, incorporating electronic surveillance into the Act could be a strategic move”.*

The emerged theme is that the Competition Act of 1998 be amended to add a provision on electronic surveillance. This study provided that the participants are of the view that the use of technology in cartel activities has become more sophisticated and complex over the years, as such the Act needs to be amended to accommodate provisions in relation to electronic surveillance. The provision should align with the Constitution of the Republic of South Africa, 1996 and the entire regulatory framework that governs electronic surveillance.

It is also mentioned that some lessons can be drawn from other jurisdictions or agencies where electronic surveillance was successfully utilised. One of the participants gave an example that the South African Police Service has a provision in their Act related to the use of electronic surveillance and lessons can be drawn from them. Some participants mention that it is necessary to amend the Act to be up to date with the use of the latest technological advancements.

Section 2.5 captured the custodian of electronic surveillance usage in South Africa, where Baker and Gunter (2005:1) supported the findings of this study by highlighting that electronic surveillance is a critical investigative tool in the fight against crime and is used by government agencies and the private sector. The same section in the literature, lists other legal authorities that are permitted by the surveillance Act to use electronic surveillance in the execution of their duties. Those institutions are some of essential organisations in this regard; SSA, SAPS CID, SANDF DIC, NCC and SARS.

#### **4.4 SUMMARY**

This chapter (Four) highlighted an analysis of presentation of the data that was collected based on the study aim and objectives, mapped with the research questions to easily find the identified study themes. The researcher presented the questions asked to the participants and the participants’ verbatim expressions. The researcher

provided the linkage between the questions posed to the selected participants against the reviewed literature studies to achieve triangulation. The following chapter (Five) focuses on the summary, conclusion and recommendations.

## CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

### 5.1 INTRODUCTION

This chapter highlights an overall summary and conclusion of this study. It includes recommendations to the study aim, researcher questions and identified themes, study limitations and future research studies.

### 5.2 OVERALL STUDY SUMMARY

- **Chapter (One)** outlined the research aim, research objectives, research questions, definition of key concepts, study significance and scope of the study. The purpose of this chapter was to ensure that the reader understood the topic under research. The progression of the next chapters of the study was highlighted in this chapter.
- **Chapter (Two)** presented a literature review related to the use of electronic surveillance to investigate cartel conducts. The researcher conceptualised the concepts of electronic surveillance and analysed the its roles in the investigation of cartel conducts. The researcher focused on the circumstances, legislations, policies and theoretical framework regulating the application of the electronic surveillance in the investigation of cartel conducts in South Africa and other international jurisdictions. Challenges of the investigation of cartel conducts worldwide were identified and addressed. The effectiveness of investigating cartels, which include the best practices in both developed and developing jurisdictions were explored. Proactive measures where competition authorities engaged in the detection activity on its own initiatives were highlighted. The consulted literature also highlighted the evolving of algorithm-based pricing models which has caused serious concerns in the law community recently.
- **Chapter (Three)** highlighted the adopted research design and methodology. It describes the employed research approach, study location, study population and sampling procedures, as well as data collection and analysis methods. The methods to ensure trustworthiness of this study and ethical considerations also formed part of this chapter.
- **Chapter (Four)** highlighted an analysis of presentation of the data that was collected. The researcher presented the questions posed to the participants and the participants' verbatim expressions. The researcher provided the linkage

between the questions posed to the participants, versus the reviewed literature studies to achieve triangulations. The following chapter (Five) focuses on the summary, conclusion and recommendations.

- **Chapter (Five)** This chapter highlights an overall summary and conclusion of this study, including the study recommendations aligned to the study aim, posed questions and identified study themes. The study's limitations and future research also formed part of this chapter.

### **5.3 STUDY OVERALL CONCLUSION**

The aim of this study was to explore the importance of electronic surveillance in the investigation of cartel conducts, focusing on the Competition Commission of South Africa in Pretoria. The outcome of the study confirms that electronic surveillance plays an important role in the investigation of cartel conduct. This is supported by the majority views of the participants when responding to question related to the study aim.

It was evident that electronic surveillance will assist the Competition Commission to detect and identify cartelists. Considering that cartel activities are hidden or secretive, the authority will be able to uncover “impossible’ evidence necessary to prosecute and convict cartel members. This conclusion is supported by the literature study which stated that other authorities in developed jurisdictions are effectively applying electronic surveillance as one of their investigative tools to investigate cartel conduct. In achieving the study Objective 01, the selected participants in their responses to questions posed to them, mentioned that electronic surveillance is an investigative tool used to gather crucial information or evidence by secretly monitoring cartel activities. Their responses further indicated that the use of this technique involves bugging rooms, tapping or listening to communications of the targeted individuals remotely. The obtained literature studies attest to this finding, in section 2.2, when Watney (2008:1) mentions that electronic surveillance is an intrusive method used to gather information or evidence of suspected criminal activities in a secret manner and without the knowledge of the suspect or targeted person. To accomplish Objective 02 of the study, participants expressed the same views that the role of the electronic surveillance is to gather information or evidence to prosecute cartelists and provide

leads to identify patterns of behaviour and connections between cartel members to build a strong case. In section 2.3, Baker and Gunter (2005:1) support the findings by mentioning that the role of electronic surveillance is to collect information for the furtherance of an investigation. In section 2.3.2, Ratcliffe (2020:1) supported these views by revealing that footage captured by video cameras can be used to piece together the sequence of events that can lead to a crime scene.

Objective 03 of the study focused on the circumstances under which electronic surveillance should be authorised to be used during the investigation of cartel conducts at the Competition Commission South Africa in Pretoria. It was evident from the participants' responses that electronic surveillance should be used when there are strong suspicions and only when the normal investigation methods have proven to be ineffective.

There was a strong sentiment amongst the participants that the use of electronic surveillance should be guided by a warrant aligned with the scope of the investigation. These findings are supported by section 2.6 of the reviewed literature studies. Another finding was in relation to the person responsible for conducting surveillance operations, in which participants preferred that a dedicated intelligence team should be appointed to run the operations and should work closely with the lead investigator. This aspect is not covered under Chapter Two of this study.

Objective 4 of the study covered the limitations, fundamental right to privacy, internal measures to govern the usage of electronic surveillance. The findings emphasised more on the right to privacy as the fundamental right enshrined in the Constitution. Therefore, it is important to ensure that surveillance operations do not infringe upon people's right to privacy, and as a result the Commissioner should put in place internal measures to guide the usage of the surveillance equipment. The internal measures must be guided by the legal framework. These findings are supported by section 2.10.1 of the reviewed literature studies.

The study Objective 5 presented challenges of investigating cartel conducts in the Competition Commission. The findings revealed three challenges namely the evolution of technology, criminalisation and characterisation of cartel conduct. In terms

of the evolution of technology, companies are now investing more of their resources towards advanced technology to set up programmes such algorithms to create platforms for collusion.

Criminalisation of the conduct discourages firms and directors from approaching the authority relating to cartel behaviour for fear of being criminally prosecuted. Lastly, characterisation changes the definition of cartel conduct as some of the activities are considered procompetitive. The highlighted study findings are confirmed in sections 1.1, 2.3.3 and 2.11 of this study.

Objective 06 of this study determined the effectiveness of strategies employed to investigate cartel conduct at the Competition Commission in Pretoria. The main view from the participants is that new measures need to be adopted to supplement the current investigation measures to ensure that the authority has more powers to be able to keep up with new trends of collusion. Therefore, the Competition Act of 1998 needs to be amended to include a provision regarding electronic surveillance. This is confirmed by several sections of the study, namely sections 1.1, 2.5, 2.11, 2.16.10, 2.20, 2.20.7, and 2.21.

## **5.4 STUDY RECOMMENDATIONS TO IMPROVE THE STUDY AIM AND IDENTIFIED THEMES**

### **5.4.1 Recommendations relating to the study aim and identified themes**

Section 4.2.1 of the study's findings outlined two aspects, firstly, that cartel conduct is secretive in nature, as such it is difficult to detect and obtain crucial evidence. Secondly, evolution of technology has made cartel conduct more sophisticated and difficult to detect. It was suggested that electronic surveillance will be a valuable tool that could be used to keep up with the new trend of collusion because it will be used to gather information that is unattainable through other means.

Subsequent to the revealed study findings, it is recommended that electronic surveillance should be used by the Competition Commission to investigate complex and sophisticated cartel conduct because it is a powerful investigative tool that can assist in obtaining real-time evidence. Fighting cartels remains a priority for the

Competition Commission but cartels are secretive in nature and the cartelists are good in concealing their anti-competitive behaviour. Therefore, electronic surveillance will allow the Competition Commission to collect information that would be otherwise unattainable through other available means. By monitoring communications, online transactions other illegal activities the Competition Commission can uncover hidden patterns, identify key players in the market and understand the inner workings of cartels. The application of electronic surveillance will act as a deterrent because the cartelists will think twice before engaging in cartel activities knowing that the Competition Commission has the power to gather evidence covertly.

#### **5.4.2 Recommendations based on study objective 01 and identified themes**

Section 4.3.1 of the study findings mentioned that electronic surveillance is an investigative tool used to gather crucial information or evidence by monitoring cartel activities. There are different types of surveillance used to investigate criminal activities, namely, audio surveillance, visual surveillance, tracking surveillance and data surveillance. These types of electronic surveillance include techniques such as room bugging, wiretapping and video tapping.

Therefore, it is recommended that the choice of an electronic surveillance tool to be used to investigate cartel conduct should depend on the nature of the investigation, the type of the information being sought and the legal framework. The commonly used electronic surveillance tools include wiretaps, GPS tracking devices, and covert cameras. However, it will be important for the Competition Commission to utilise equipment that involves the analysis of observable economic data, tracking of firms and individuals to detect behaviour that is inconsistent with a healthy competitive process.

Due to the evolution of technology and other digital tools (Such as algorithms) are being explored to detect cartel activities by authorities in other jurisdictions. It is therefore recommended that the Competition Commission needs to explore and understand how algorithms work in digital markets. The use of algorithms as monitoring tools for cartel enforcement in the digital market also needs to be explored.



Moreover, it is important for the Competition Commission to understand the algorithms and how can it sustain anti-competitive behaviour in the market.

#### **5.4.3 Recommendations based on study objective 02 and identified themes**

In terms of section 4.3.2 of the study findings, the role of the electronic surveillance is very important in an investigation because it helps to gather crucial evidence through warrants to prosecute members of cartels. The researcher recommends that electronic surveillance should be used because it will play a pivotal role in addressing cartel conduct. Surveillance will help the Competition Commission to gather information about cartel activities, including meetings, agreements and coordination.

This information will assist in building a strong case against the involved parties. Surveillance will provide real time insights into cartel behaviour. Investigators can track movement, observe interactions and identify patterns that reveal collusion. Recently, the Competition Act of 1998, was amended to introduce criminal liability for directors and individuals involved in cartel conduct, therefore, electronic surveillance evidence can be crucial in prosecuting these cases.

As far as recommendations are concerned, the introduction of the use of electronic surveillance will mean that firms accused of engaging in cartel conduct will have to think more carefully before admitting to a contravention to settle a case for commercial reasons. One of the participants mentioned that companies often allocate funds for potential settlements with the Competition Commission in case they are found to be in violation of competition law. Such companies would not be deterred to contravene competition law with the intention to settle the case. Therefore, the introduction of electronic surveillance will work as a deterrent factor to companies that intentionally violate competition law with the intention to settle with the Competition Commission.

#### **5.4.4 Recommendations based on study objective 03 and study themes**

As outlined in section 4.3.3 of the study findings, it was evident that electronic surveillance should be used when there are strong suspicions and only when the normal investigation methods have been proven to not yield the desired outcome. There was a strong view that the use of electronic surveillance should be guided by a

warrant and aligned with the scope of the investigation. As such, it is recommended that the usage of electronic surveillance should be a last resort when investigating cartel conduct due to its sensitivity in that it is an intrusive method that can infringe on the privacy of individuals.

It should only be considered when other less intrusive means have failed or when there is no reasonable alternative to obtain crucial information. It should be justified by the seriousness of the crime being investigated and the necessity of the information being sought. To ensure that a surveillance warrant application adheres to these conditions, the Commissioner of the Competition Commission should delegate the Head of Legal to review all the applications and oversee the whole process from the outset.

It is recommended that the Commissioner of the Competition Commission should establish a Surveillance Unit and appoint skilled individuals who will be responsible for surveillance operations. Individuals appointed must be subject to a solid vetting process to determine their security competency. The surveillance team should have a close working relationship with the investigators to understand cases under investigation, however, under no circumstances should the investigators be allowed to conduct surveillance operations.

It is also recommended that the duration of the warrant should be proportionate to the seriousness of the crime being investigated and the nature of the information being sought. The warrant must specify the duration of the surveillance, which should be limited to the time necessary to achieve the objective of the investigation. These facts will assist the judge to determine whether the proposed duration is reasonable and necessary.

#### **5.4.5 Recommendations based on study objective 04 and identified themes**

The study findings in terms of section 4.3.4 emphasised more on the right to privacy that during surveillance operations, it must be ensured that individuals' rights to privacy are protected. There should be internal measures in place to guide the application of electronic surveillance and these measures should be within and guided by the legal

framework. It is recommended that electronic surveillance should be used as an additional tool to gather evidence, however, it is important for the authority to note that there are limitations associated to using such tool during the investigation. It involves monitoring private communications, which raises ethical and legal questions about privacy rights. Therefore, striking a balance between effective investigation and individual privacy is essential. It is important for the authority to develop internal policies and procedures guided by the legal framework to guard against abuse and misuse of the equipment.

The other limitation that was mentioned by the participants is the cost of acquiring the equipment, training investigators, and undertaking surveillance operations. To mitigate against these costs, the authority should limit surveillance operation to complex and sophisticated investigations. The investigation team, including legal counsel and economists should be given the responsibility to assess the magnitude and complexity of the case and thereafter recommend the necessity of applying for the use of electronic surveillance.

It is also recommended that the Competition Commission should employ individuals with technical skills to operate and maintain surveillance equipment and having the knowledge of relevant computer software. It is also recommended that the employed members must undergo a vetting process to ensure that they are trustworthy and would not compromise the integrity of the investigation.

#### **5.4.6 Recommendations based on study objective 05 and identified themes**

In section 4.3.5, the study findings highlighted that the introduction of criminalisation of cartel conduct may discourage firms or directors to come forth and report their activities to the authorities as they fear to be criminally prosecuted. It is recommended that the Competition Commission should look seriously at supplementing the traditional methods with pro-active cartel detection measures to stay ahead of the cartelists. For instance, algorithms have become a topic of interest in the field of competition law because it helps competitors to avoid cartel detection. Thus, it is by means of a proactive enforcement tool that the Competition Commission can detect if firms are colluding. Digital technology can assist the authority to keep up with cartel

members who apply advanced technology to collude. Criminalisation of cartels would no longer be a problem as the authority would have the capacity to detect cartels themselves rather than relying on leniency applications. In the same section 4.3.5 of this study, some participants mentioned characterisation as another challenge the competition authorities are faced with in the investigation of cartel activities. Characterisation changes the definition of cartel conduct as some of the activities are considered procompetitive.

It is recommended that the investigation team should conduct an impact analysis of the alleged conduct to ascertain if the conduct is anti-competitive or if it is meant to achieve pro-competitive outcome before concluding the matter. This will help the investigators to understand the competitive landscape and the impact of the alleged conduct in the market.

#### **5.4.7 Recommendations based on study objective 06 and identified themes**

In section 4.3.6 of this study, the selected participants believe that the traditional investigation tools need to be supplemented with a cartel detection measure to keep up with changes as technology evolves. In the same section 4.3.6, the findings suggested that the Competition Commission needs to be more innovative to cope with the evolving nature of the market to be able to deal with intelligent programs such as algorithms. Following these findings, it is recommended that the Competition Commission should introduce a new investigation strategy to bring new specialised investigative tools such as wiretapping and eavesdropping, infiltration and other forms of surveillance to solve complex and sophisticated cartel cases. In section 4.3.6 of this study, the selected participants are of the view that technology has taken over most business activities, and conventional methods would not assist much in detecting cartel behaviour. The findings also highlighted that the use of algorithms as a detection tool because various markets have adopted the algorithm pricing model. It is therefore recommended that the Competition Commission needs to explore and understand how algorithms work in digital markets. The use of algorithms as monitoring tools for cartel enforcement in the digital market also needs to be explored. It is important for the Competition Commission to understand algorithms and how they could sustain anti-competitive behaviour in the market. There is a suggestion, in section 4.3.6 of the

findings, that the Competition Act of 1998 should be amended to include provisions on electronic surveillance to be able to cope with the latest advanced trends of competitive behaviour in different markets. Following these findings, the study recommends that the Competition Act of 1998 needs to be amended to add provisions on the use electronic surveillance when investigating cartel activities.

The changes in the Competition Act, 1998 will allow the Competition Commission to have a multi-disciplinary approach when dealing with cartel conduct. When the need arises during the assessment and investigation of complex and sophisticated cases, the Competition Commission will be able to apply this proactive cartel detection tool, namely electronic surveillance.

## **5.5 STUDY LIMITATIONS**

The only limitation encountered during the study is in relation to the targeted participants. The researcher initially targeted the 'Principal investigators and Senior investigators' for data collection. However, some of them were not available due to work commitments. As a result, the researcher interviewed four (4) Principal investigators, three (3) Senior investigators and another three (3) Investigators. The investigators interviewed have extensive experience and in-depth knowledge of investigating cartels. Each of them has more than ten years of experience working for the Competition Commission as the 'Cartel Investigators.'

## **5.6 FUTURE RESEARCH STUDIES**

The researcher proposes the following future research studies:

- The effect of criminalisation on leniency programmes.

There is a debate or concern regarding the criminalisation provisions in the Competition Act of 1998 that it could have a negative implication for South Africa's cartel leniency programme. The cause for concern is that the NPA is not obliged to consider the Competition Commission's submissions regarding leniency when prosecuting cartelists. This creates disincentive for employees to report cartels to the Competition Commission or to co-operate during a cartel investigation. In section 2.6

of the literature of this study, Van Heerden and Botha (2015) supported this view by mentioning that enforcing the criminalisation of cartel conduct could undermine the effectiveness of the corporate leniency policy. In the same section 2.6, Barlund (2020) stated that the legal uncertainty as to whether current and former directors, managers, and other members of staff/applicants for immunity are shielded from individual sanctions such as fines, disqualification, or imprisonment, could prevent potential applicants from applying for leniency. Therefore, this could be a topic of interest to explore to clear the uncertainty brought by criminalisation of cartel conduct.

- How does characterisation of cartel redefine the cartel behaviour?

In section 4.3.5 of Chapter Four, some participants mentioned characterisation as another challenge that the competition authorities are faced with in the investigation of cartel activities. This is also highlighted in section 1.1 of the literature studies, when Legal brief (2022:1) revealed that the Competition Commission affirmed that it is faced with the “new generation” of cartel cases which are “characterised by a clear shift in the pendulum”, being the cartel cases the Commission has been unsuccessful in prosecuting. In terms of characterisation, some cartel behaviour may achieve efficiency as opposed to other anti-competitive behaviour. Therefore, characterisation brings a new dimension in defining cartel activities, and it is also a topic worth to be explored by the researchers.

## LIST OF REFERENCES

- Abbas, R., Michael, K., Michael, M.G. & Aloudat, A. 2011. Emerging forms of covert surveillance using GPS-enabled devices. *Journal of Cases on Information Technology*, 13(2):19-33.
- Abdulrauf, L.A. 2018. The challenges for the rule of law posed by the increasing use of electronic surveillance in sub-Saharan Africa. *African Human Rights Law Journal*, 18(1):365-391.
- Adebajo, A. & Aning, K. 2023. African Political Systems: A Comparative Analysis of Monarchy, Authoritarianism, and Democracy. *African Affairs*, 122(489):45-68.
- Africa, S. 2009. The South African Intelligence Services: A Historical Perspective. *Changing Intelligence Dynamics in Africa*, 67:61-94.
- Akhgar, B., Bayerl, P.S. & Sampson, F. 2017. *Open-source intelligence investigation: from strategy to implementation*. California: Springer.
- Al Balushi, K. 2016. The use of online semi-structured interviews in interpretive research. *International Journal of Science and Research (IJSR)*, 57(4):2319-7064.
- Albæk, S. 2013. Consumer welfare in EU competition policy. *Aims and Values in Competition Law*, 67-88.
- Alexandrie, G. 2017. Surveillance cameras and crime: A review of randomized and natural experiments. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 18(2):210-222.
- Amankwaa, L. 2016. Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity*, 23(3):121-127.
- American Civil Liberties Union [ACLU]. 2023. *National Security Letters*. Available at: <https://www.aclu.org/other/national-security-letters> (accessed on: 13 May 2023).
- Andrejevic, M. 2022. *The Big Data Divide: How Data Surveillance Impacts Society*. London: Routledge.

- Andrews, P., Gorecki, P., McFadden, D. & Webber, J. 2015. Modern Irish Competition Law. *Common Law World Review*, 45(1):115.
- Arbel, A. & Keren, M. 2021. Cartel Investigations and Enforcement in Israel: Techniques and Practices. *Journal of Competition Law & Economics*, 17(4):654-673.
- Ashby, M.P. 2017. Surveillance cameras and crime: A review of randomised natural experiments. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 18(2):210-222.
- Athayde, A. 2016. *Nearly 16 years of the leniency program in Brazil: Breakthroughs and challenges in cartel prosecution*. Available at: <https://ssrn.com/abstract=2796133> (accessed on: 11 September 2023).
- Aubert, C., Rey, P. & Kovacic, W.E. 2006. The impact of leniency and whistle-blowing programs on cartels. *International Journal of Industrial Organisation*, 24(6):1241-1266.
- Australian Competition & Consumer Commission. 2003. *ACCC launches leniency policy to expose hard core cartels in Australia*. Available at: <https://www.accc.gov.au/media-release/accc-launches-lenieny-policy-to-expose-hard-core-cartels-in-australia> (accessed on: 10 August 2023).
- Babbie, E. 2020. *The practice of social research*. Australia: Cengage.
- Bachman, R & Schult, R.K. 2014. *The practice of research in criminology and criminal justice*. London: Sage.
- Bachman, R & Schutt, R.K. 2013. *The practice of research in criminology and criminal justice*. London: Sage.
- Baker, B.D. & Gunter, W.D. 2005. Surveillance: concepts and practices for fraud, security and crime investigation. *International Foundation for Protection Officers*, 2:1-17.
- Baker, R. 2022. Cartel Enforcement in Africa: Comparative Analysis of Strategies and Effectiveness. *African Competition Journal*, 10(2):122-143.
- Ball, K. & Haggerty, K. D. 2020. *The Surveillance Studies Reader*. London: Routledge.



- Barlund I M H B. 2020. *Leniency and Criminalisation of Cartels: Suggestions for giving the Commission's Leniency Offer more leverage*. Rapport. Available at: <https://konkurransetilsynet.no/wp-content/uploads/2020/07/Rapport-6-2020-Leniency-and-Criminalisation-of-Cartels.pdf> (accessed on: 8 April 2023).
- Beaton-Wells, C. 2008. Forks in the Road: Challenges Facing the ACCC's Immunity Policy for Cartel Conduct (Part 1). *Competition and Consumer Law Journal*, 16:71-113.
- Beaton-Wells, C. 2009. Forks in the Road: Challenges Facing the ACCC's Immunity Policy for Cartel Conduct (Part 2). *Competition and Consumer Law Journal*, 16:246-278.
- Beaton-Wells, C. 2014. Leniency Policies: Testing for Effectiveness. *An Antitrust Tribute*, 2:303-317.
- Bell, R.B. & Millay, K. 2019. The Antitrust Division's Corporate Leniency Program: Learn from the past or be condemned to repeat it. *Criminal Justice*, 34:14.
- Bendor, A. & Heller, M. 2018. The Economic Competition Law of Israel: An Overview of Antitrust Legislation and Enforcement. *Israeli Journal of Law and Economics*, 6(2):103-121.
- Bennett, C.J. 2011. In defence of privacy: The concept and the regime. *Surveillance & Society*, 8(4):485-496.
- Beth, H. and Gannon, O. 2022. Cartel screening—can competition authorities and corporations afford not to use big data to detect cartels? *Competition Law and Policy Debate*, 7(2):77-88.
- Blaxter, L., Hughes, C. & Tight, M. 2010. *How to research*. (11<sup>th</sup> edition). New York: Open University Press.
- Bloch-Wehba, H. 2018. Exposing secret searches: A First Amendment Right of Access to Electronic Surveillance Orders. *George Washington Law Review*, 93:145.
- Braun, V. & Clarke, V. 2022. *Thematic Analysis: A Practical Guide*. Los Angeles: Sage Publications.

- Brinkmann, S. & Kvale, S. 2018. *Interviews: learning the craft of qualitative research interviewing*. Thousand Oaks: SAGE.
- Browne, C. 2022. *Regulating Surveillance: Balancing Privacy and Security*. Cambridge: Cambridge University Press.
- Bryman, A. 2012. *Social research methods*. Oxford: Oxford University Press.
- Bryman, A. 2021. *Social Research Methods*. Oxford: Oxford University Press.
- Bureau of Justice Assistance. 2023. *Electronic Communications Privacy Act of 1986 (ECPA)*. Available at <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285> (accessed on 30 March 2023).
- Buccirosi, P. 2023. *Handbook of antitrust economics*. Cambridge: MIT Press.
- Burke, M. 2018. Prioritization in practice: insights from the Competition Commission South Africa. *Journal of Antitrust Enforcement*, 6(2):261-280.
- Buthe, T. & Kigwiru, V.K. 2020. The spread of competition law and policy in Africa: A research agenda. *African Journal of International Economic Law*, 1(1):41-83.
- Bygrave, L. E. 2021. *Balancing privacy and security: an international comparative analysis*. Oxford: Oxford University Press.
- Byrne, J.A. 2021. Observation for data collection in urban studies and urban analysis. In *Methods in Urban Analysis*.127-149.
- Calliari, M. & Guimaraes, D.A. 2010. Brazilian cartel enforcement: from revolution to the challenges of consolidation. *Antitrust*, 25:67.
- Calvani, T. & Calvani, T.H. 2011. Cartel sanctions and deterrence. *The Antitrust Bulletin*, 56(2):185-206.
- Calvano, E., Calzolari, G., Denicolò, V. and Pastorello, S. 2019. Algorithmic pricing what implications for competition policy? *Review of industrial organization*, 55:155-171.
- Calvano, E., Calzolari, G., Denicolo, V. and Pastorello, S. 2020. Artificial intelligence, algorithmic pricing, and collusion. *American Economic Review*, 110(10):3267-3297.

- Camatsos, S.G. & Foer, A.A. 2007. *Cartel Investigation in the USA*. American Antitrust Institute. Available at: <https://ssrn.com/abstract=1103624> (accessed on: 11 April 2023).
- Capers, I.B. 2012. Crime, surveillance, and communities. *Fordham Urban Law Journal*, 40:959.
- Capobianco, A. & Nyeso, A. 2018. Challenges for competition law enforcement and policy in the digital economy. *Journal of European Competition Law & Practice*, 9(1):19-27.
- Carey, M. 2012. *Qualitative research skills. Theory and practice*. University of Manchester, UK: Ashgate.
- Chan, S. & Camp, L.J. 2002. Law enforcement surveillance in the network society. *IEEE Technology and Society Magazine*, 21(2):22-30.
- Chen, J. & Harrington Jr, J.E. 2007. The impact of the corporate leniency program on cartel formation and the cartel price path. *Contributions to Economic Analysis*, 282:59-80.
- Chen, L., Mislove, A. & Wilson, C. 2016. An empirical analysis of algorithmic pricing on amazon marketplace. *In Proceedings of the 25<sup>th</sup> international conference on World Wide Web*, 1339-1349.
- Chen, Z. & Rey, P. 2013. On the design of leniency programs. *The Journal of Law and Economics*, 56(4):917-957.
- Chetty, D., Njisan, Y., Mbikiwa, M. and Martin, C. 2014. *The role of market inquiries in assessing the state of competition and facilitating ex ante regulation of markets*. Paper presented to the 8<sup>th</sup> Annual Competition and Economic and Policy Conference, Johannesburg, South Africa. 4-5 September.
- Choi, Y.J. & Hahn, K.S. 2014. How does a corporate leniency program affect cartel stability? Empirical evidence from Korea. *Journal of Competition Law and Economics*, 10(4):883-907.
- Clark, I. 2016. The digital divide in the post-Snowden era. *Journal of Radical Librarianship*, 2:1-32.

- Clarke, V. & Braun, V. 2013. Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The psychologist*, 26(2):120-123.
- Cocq, C. & Galli, F. 2015. *The use of surveillance technologies for the prevention, investigation and prosecution of serious crime*. EUI Department of Law Research Paper. Available at: [https://cadmus.eui.eu/bitstream/handle/1814/37885/LAW\\_2015\\_41%20.pdf?sequence=1&isAllowed=y](https://cadmus.eui.eu/bitstream/handle/1814/37885/LAW_2015_41%20.pdf?sequence=1&isAllowed=y) (accessed on: 5 April 2023).
- Cohen, J. E. 2023. *Privacy in the age of surveillance: new challenges and new solutions*. Oxford: Oxford University Press.
- Cohen, L., Manion, L. & Morrison, K. 2017. *Research methods in education*. New York: Routledge.
- Cole, D. 2021. *The USA Patriot Act: a legal analysis*. New York: The New Press.
- Coleman, R. & McCahill, M. 2011. *Surveillance and crime*. London: Sage.
- Colino, S.M. 2011. *Competition Law of the EU and UK*. USA: Oxford University Press.
- Competition Commission. 2008. *Corporate Leniency policy*. Available at: <https://www.compcom.co.za/corporate-leniency/> (accessed on: 14 October 2022).
- Competition Commission. 2009. *Ten years of enforcement by the South African competition authorities: unleashing rivalry*. Available at: <https://www.compcom.co.za/wp-content/uploads/2017/11/10year.pdf> (accessed on 31 July 2024).
- Competition Policy International. 2023. *Development in cartel screening*. Available at: <https://www.competitionpolicyinternational.com/developments-in-cartel-screening/> (accessed on: 7 April 2023).
- Connelly, L. M. 2016. Trustworthiness in qualitative research. *MEDSURG Nursing*, 25(6):435-436.
- Connor, J.M. 2016. *The rise of anti-cartel enforcement*. Available at: [https://www.zbw.eu/econis-archiv/bitstream/11159/278376/1/EBP075042827\\_0](https://www.zbw.eu/econis-archiv/bitstream/11159/278376/1/EBP075042827_0) (accessed on: 12 September 2023).

- Cordner, G.W. & Scarborough, K.E. 2010. *Police administration*. (7<sup>th</sup> edition). Cincinnati, OH: Anderson.
- Creswell, J. W. & Poth, C. N. 2016. *Qualitative inquiry and research design: Choosing among five approaches*. Los Angeles: Sage.
- Creswell, J. W. & Poth, C. N. 2018. *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Los Angeles: Sage Publications
- Creswell, J. W., & Creswell, J. D. 2018. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Los Angeles: Sage Publications.
- Crowe, J. & Jedličková, B. 2016. What's wrong with cartels? *Federal Law Review*, 44(3):401-418.
- Cseres, K. 2021. Cartel Enforcement in Developing Countries: Challenges and Opportunities. *Global Competition Review*, 24(3):30-45.
- Cunningham, A. C. & Hester, T. R. 2023. *Surveillance Technologies: Advances and Applications*. Switzerland : Springer.
- Daniel, P. S. & Sam, A. G. 2011. *Research methodology*. Delhi: Kalpaz.
- Dantzker, M. L., Hunter, R. D. & Quinn, S. T. 2018. *Research method for criminology and criminal justice*. Burlington: Jones & Bartlett.
- Davenport, T. H. & Ronanki, R. 2022. Artificial Intelligence for the Real World: How Smart Companies Use AI to Achieve Results. *Harvard Business Review*, 100(1):108-117.
- Davies, S. 2021. Surveillance and Privacy: The Impact of RICA on South African Law. *South African Journal of Human Rights*, 37(2):215-234
- Dawadi, S. 2020. Thematic analysis approach: A step by step guide for ELT Research Practitioners. *Journal of Nepal English Language Teachers' Association*, 25(2):62-71.
- De Castro, E.T.V., Silva, G.R. and Canedo, E.D. 2022. Ensuring privacy in the application of the Brazilian general data protection law (Pp.1228-1235). *In Proceedings of the 37<sup>th</sup> ACM/SIGAPP Symposium on Applied Computing*.

- De Vos, A. S., Strydom, H., Fouché, C. B. & Delport, C. S. L. 2011. *Research at grassroots for the social sciences and human service professions*. (4<sup>th</sup> edition). Pretoria: Van Schaik.
- Democratic Control of Armed Forces. 2022. *Safeguards in electronic surveillance*. Available at: <https://www.dcaf.ch/sites/default/files/publications/documents/Safeguards%20in%20Electronic%20Surveillance.pdf> (accessed on: 9 November 2022).
- Deng, A. 2020. Algorithmic collusion and algorithmic compliance: Risks and Opportunities. *The Global Antitrust Institute Report on the Digital Economy*, 27:965-1023.
- Denscombe, M. 2010. *The good research guide for small-scale social research projects*. England: Open University Press.
- Denzin, M. K. & Lincoln, Y. 2018. *The SAGE Handbook of Qualitative Research*. Thousand Oaks: SAGE.
- DePamphilis, D. 2011. *Mergers and acquisitions basics: All you need to know*. Amsterdam: Elsevier
- Department of Justice and Constitutional Development. 2015. *Criminal Procedure Act 51 of 1977*. Available at: <https://www.justice.gov.za/legislation/acts/1977-051.pdf> (accessed on: 20 October 2023).
- Desai, D.R. 2014. Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding. *Notre Dame Law Review*, 90:579.
- Dong, A. Massa, M. & Zaldokas, A. 2019. The effects of global leniency programs on margins and mergers. *The RAND Journal of Economics*, 50(4):883-915.
- Dressler, J., George C. Thomas III, G. C. & Medwed, D. S. 2017. *Criminal procedure: principles, policies, and perspectives*. St. Paul: West Academic.
- Dudovskiy, J. 2018. *The ultimate guide to writing a dissertation in business studies: a step by step assistance*. New York: Sage Publishers.
- Duncan, J. 2022. *National security surveillance in Southern Africa: An anti-capitalist perspective*. New York: Bloomsbury Publishing.

- Easwaramoorthy, M. & Zarinpoush, F. 2006. Interviewing for research. *Imagine Canada*, 425:1-2.
- Engelbrecht, L. 2007. *A guide to the SANDF*. Unpublished Manuscript, Johannesburg.
- Eriksson, P. & Kovalainen, A. 2015. *Qualitative methods in business research: a practical guide to social research*. Los Angeles: Sage.
- Etikan, I, Musa, S.A. & Alkassim, R. 2016. Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics* 5(1): 1-4.
- Eya-Boger, T., Schwartz, Z. and Brown, S. 2021. Israel: *Competition Law Regime*. Available at: <https://globalcompetitionreview.com/review/the-european-middle-east-and-african-antitrust-review/2022/article/israel-competition-law-regime> (accessed on: 11 September 2023).
- Eyal-Boger, Schwartz and Zackay.-2022. *Israel: national competition law regime and how it affects multinationals*. Available at: <https://globalcompetitionreview.com/review/the-european-middle-east-and-african-antitrust-review/2023/article/israel-national-competition-law-regime-and-how-it-affects-multinationals> (accessed on: 13 September 2023).
- Fandino, W. 2019. Formulating a good research question: Pearl and Pitfall. *Indian Journal of Anaesthesia*, 63 (8): 611.
- Federal Trade Commission. 2023. *The Antitrust Laws*. Available at: <https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/antitrust-laws> (accessed on: 1 August 2023)
- Federal Trade Commission. 2023. *The enforcers*. Available at: <https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/enforcers> (accessed on: 13 September 2023).
- Feiglin, N. 2020. Algorithmic collusion and scrutiny: Examining the role of the ACCC's information gathering powers in the digital era. *The University of New South Wales Law Journal*, 43(4):1137-1166.

- Ferreira, C. 2021. *Software Robot Process Automation at the South African Revenue Service (SARS)*. Unpublished MA Dissertation, University of Nelson Mandela, Port Elizabeth.
- Fijnaut, C. & Weenink, W. 2021. *Transnational Organized Crime: Law Enforcement, Intelligence, and Policy*. London: Routledge.
- Flick, U. (2022). *An Introduction to Qualitative Research*. London: Sage Publications.
- Fonseca, R.S. & van Wyk, J.A. 2021. Cybersecurity in South Africa: Status, governance, and prospects. *In Routledge Companion to Global Cyber-Security Strategy*, 591-607.
- Foremny, A. & Dorabialski, W. 2018. Review of collusion and bid rigging detection methods in the construction industry (Pp.946-953). *In Creative Construction Conference 2018*.
- Friedewald, M. & Burgess, J. P. 2022. *Surveillance, Privacy and Security: Citizens' Perspectives*. London: Routledge
- Fzrachi, A. & Stucke, M.E. 2019. Sustainable and unchallenged algorithmic tacit collusion. *Northwestern Journal of Technology & Intellectual Property*, 17:217.
- Gal, M. 2022. Limiting Algorithmic Cartels. *Berkeley Technology Law Journal*, 38(1):22.
- Gal, M.S. and Dahan, R. 2019. Legal obstacles to private enforcement of competition law. *Market & Competition Law Review*, 3:133.
- Gehl, R. and Plecas, D. 2018. *Criminal investigation: Processes, practices and thinking*. Abbotsford, BC: University of Fraser Valley.
- Geldenhuys, K. 2021. Surveillance as an investigative tool. *Servamus Community-based Safety and Security Magazine*, 114(11):16-18.
- Gelles, M., Mirkow, A. & Mariani, J. 2019. *The future of law enforcement: Policing strategies to meet the challenges of evolving technology and a changing world*. Deloitte: Insight. Available at: [file:///C:/Users/KgashaneK/Downloads/DI\\_Future-of-law-enforcement.pdf](file:///C:/Users/KgashaneK/Downloads/DI_Future-of-law-enforcement.pdf) (accessed on: 30 March 2023).



- George, T. 2022. Exploratory research: definition, guide and examples. *Scribbr*. Available at: <https://www.scribbr.com/methodology/exploratory-research/> (accessed on: 26 October 2022).
- Giles, J. 2016. *UN concerned about privacy and interception in South Africa*. Available at: <https://www.michalsons.com/blog/un-human-rights-committee-concerned-about-privacy-and-interception-in-south-africa/19226> (accessed on: 13 September 2023).
- Gill, P. & Phythian, M. (2018). *Intelligence in an Insecure World*. Cambridge: Polity Press.
- Gillis, D. 2021. *The Use of Wiretapping and Electronic Surveillance in Canadian Competition Law Enforcement*. *Canadian Competition Law Review*, 15(2):112-129.
- Ginsburg, D. 2022. Cartel Enforcement in Developing Countries: A Comparative Analysis of Effective Strategies and Implementation Challenges. *Journal of Antitrust Enforcement*, 10(1):45-68.
- Golumbic, M.C. & Golumbic, M.C. 2008. *The legal framework in Israel. Fighting terror online: The convergence of security, technology, and the Law*. New York: Springer.
- Goold, B. J. 2022. CCTV and the Law: Surveillance and Policing. *Journal of Law and Public Policy*, 28(1):78-95.
- Gordon, W. & Mweemba, D. 2022. The Evolution of Competition Law in Africa: Challenges and Opportunities. *African Competition Law Journal*, 10(1):35-52.
- Gorham-Oscilowski, U. & Jaeger, P.T. 2008. National Security Letters, the USA PATRIOT Act, and the Constitution: The tensions between national security and civil rights. *Government Information Quarterly*, 25(4):625-644.
- Graef, I. 2017. Algorithms and fairness: What role for competition law in targeting price discrimination towards ends consumers? *Columbia Journal of European Law*, 24:541.

- Graham, M. & Kitchin, R. 2021. Digital Surveillance: Methods, Applications, and Challenges. *International Journal of Surveillance, Security, and Privacy*, 12(3):215-230.
- Griffin, J. M. 2003. *The modern leniency program after ten years: a summary overview of the antitrust division's criminal enforcement program. The United States Department of Justice.* Available at: <https://www.justice.gov/atr/speech/modern-lenieny-program-after-ten-years-summary-overview-antitrust-divisions-criminal> (accessed on: 15 May 2023).
- Groshinski, K & Caitlin, D. 2015. Competition law in Asia Pacific: A practical guide. *International Law*, 1-92.
- Gulzar, N., Abbasi, B., Wu, E., Ozbal, A. & Yan, W. 2013. Surveillance privacy protection. *Intelligent multimedia surveillance: Current trends and research*, 83-105.
- Gunawan, J. 2015. Ensuring trustworthiness in qualitative research. *Belitung Nursing Journal*, 1(1):10-11.
- Hagerman, L. & McIntosh, B. 2023. The Impact of Corporate Leniency Policy on Cartel Investigations in South Africa. *Antitrust Bulletin*, 68(2):345-370.
- Haggerty, K.D., Wilson, D. & Smith, G.J. 2011. Theorizing surveillance in crime control. *Theoretical criminology*, 15(3):231-237.
- Haile, Z.T. 2023. Power Analysis and Exploratory Research. *Journal of Human Lactation*, 579-583.
- Halabi, U. 2010. Legal analysis and critique of some surveillance methods used by Israel (Pp, 223-242). In E. Zureik, D. Lyon, Y. Abu-Laban (Eds). *Surveillance and control in Israel/Palestine: Population, territory, and power*. London: Routledge.
- Hammond, S.D. 2004. *Cornerstones of an effective leniency program*. Paper presented In ICN Workshop on Leniency Programs, Sydney.
- Hammond, S.D. 2008. Cornerstones of an effective cartel leniency programme. *International Competition Law*, 4:4.

- Hansen, K.T., Misra, K. & Pai, M.M. 2021. Frontiers: Algorithmic collusion: Supra-competitive prices via independent algorithms. *Marketing Science*, 40(1):1-12.
- Harrington, J. & Chang, M. 2015. When can we expect a corporate leniency program to result in fewer cartels? *The Journal of Law & Economics*, 58(2):417-449.
- Harrison, R. & K. Patterson. 2021. Proactive Detection of Cartels: Strategies and Motivations. *Journal of Antitrust Enforcement*, 9(1):58-76.
- Hay, J. & Perry, M. 2020. Cartel Enforcement and Criminal Liability in Australia: A Two-Pronged Approach. *Australian Business Law Review*, 48(3):214-235.
- Heibutzki, R. 2018. Types of Surveillance in criminal investigations. *Hearst*, 01 July. Available at: <https://work.chron.com/types-surveillance-criminal-investigations-9434.html> (accessed on: 24 October 2022).
- Hendrix, Josh, A., Travis A. Taniguchi, Kevin J. Strom, Kelle Barrick, & Nicole J. Johnson. 2018. The Eyes of the law enforcement in the New Panoptican: Police-community racial asymmetry and the use of surveillance technology. *Surveillance & Society*, 16(1): 53-68.
- Hess, K. & Orthmann, M.H. 2010. *Criminal investigation*. (9<sup>th</sup> edition). New York: Delmar Cengage Learning.
- Herman, M. 2022. National security and intelligence: a comparative analysis. London: Routledge.
- Hildebrandt, M. & de Vries, E. 2013. *Privacy, due process and the computational turn: the philosophy of law meets the philosophy of technology*. London: Routledge.
- Hinloopen, J. 2003. An economic analysis of leniency programs in antitrust law. *De Economist*, 151(4):415-432.
- Hochmann, B. 2022. *The listeners: A history of wiretapping in the United States*. Cambridge: Harvard University Press.
- Holmes, D. 2014. *5 ways technology boosts crime-fighting*. Available at: <https://pcjc.blogs.pace.edu/2014/07/22/5-ways-technology-boosts-crime-fighting/comment-page-1/> (accessed on: 25 March 2023).

- Hovenkamp, H. 2010. The federal trade commission and the Sherman act. *Florida Law Review*, 62:871.
- Hulnick, A. S. 2022. *The New Craft of Intelligence: An Introduction to the Intelligence Process* (3rd ed.). London: Routledge.
- Humble, K.P. 2021. International law, surveillance and the protection of privacy. *The International Journal of Human Rights*, 25(1):1-25.
- Hurley, M.M. 2012. For and from cyberspace: Conceptualizing cyber intelligence, surveillance, and reconnaissance. *Air & Space Power Journal*, 26(6):12-33.
- Hüschelrath, K. 2010. How are cartels detected? The increasing use of proactive methods to establish antitrust infringements. *Journal of European Competition Law & Practice*, 1(6):522-528.
- Hutchinson, C.S., Ruchkina, G.F. and Pavlikov, S.G. 2021. Tacit collusion on steroids: The potential risks for competition resulting from the use of algorithm technology by companies. *Sustainability*, 13(2):951.
- Insights. 2016. How to survive dawn raids and searches warrants in antitrust/competition investigations. Available at: <https://www.jonesday.com/en/insights/2016/09/how-to-survive-dawn-raids-and-search-warrants-in-antitrustcompetition-investigations> (accessed on: 10 April 2023).
- International Competition Network. 2021. *Chapter 5 Investigative strategy and interviewing*. Anti-cartel enforcement manual. Available at: [https://www.internationalcompetitionnetwork.org/wp-content/uploads/2022/01/CWG\\_ACEM\\_Investigative\\_Strategy\\_CH5-2021.pdf](https://www.internationalcompetitionnetwork.org/wp-content/uploads/2022/01/CWG_ACEM_Investigative_Strategy_CH5-2021.pdf) (accessed on: 19 September 2023).
- Ioannou, A. & Tussyadiah, I. 2021. Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. *Technology in Society*, 67:101774.
- Irvine, H. 2016. *African competition law enforcement – 18 months in perspective*. Competition World at: <https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/imported/competition-world-q1->

[2016.pdf?revision=9de54f61-4474-4824-a14a-1e1bd17ec36b&revision=5247642455617387904](#) (accessed on: 20 September 2023).

Isaza, J.J. & Katshir, H. 2020. *Brazil passes landmark privacy law: The general law for the protection of privacy*. Available at: [https://www.americanbar.org/groups/business\\_law/resources/business-law-today/2020-may/brazil-passes-landmark-privacy-law/#:~:text=Brazil%20has%20enacted%20its%20own,enforcement%20is%20paramount%20for%20compliance](https://www.americanbar.org/groups/business_law/resources/business-law-today/2020-may/brazil-passes-landmark-privacy-law/#:~:text=Brazil%20has%20enacted%20its%20own,enforcement%20is%20paramount%20for%20compliance) (accessed on: 13 September 2023).

Jamshed, S. 2014. Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy*, 5(4):87-88.

Jaspers, J. D. 2017. Managing cartels: how cartel participants create stability in the absence of law. *European Journal on Criminal Policy Research*, 23: 319-335.

Jebb, A.T., Parrigon, S. and Woo, S.E. 2017. Exploratory data analysis as a foundation of inductive research. *Human Resource Management Review*, 27(2):265-276.

Jepsen, T. 2018. " A new business in the world": The telegraph, privacy, and the US Constitution in the nineteenth century. *Technology and Culture*, 59(1):95-125.

Jerez, H. V. 2015. Competition law enforcement and compliance across the world: a comparative review. *International Competition Law Series*, 61:73-234.

Jibril, A. 2018. Observational research in the social sciences: A neglected qualitative research technique. *Sokoto Journal of the Social Sciences*, 8(3):231.

Jimoh, M. 2023. The Place of Digital Surveillance under the African Charter on Human and Peoples' Rights and the African Human Rights System in the Era of Technology. *African Journal of Legal Issues in Technology*, 1:1-30.

Kaira, T. 2015. *A cartel in South Africa is a cartel in a neighbouring country: Why has the successful cartel leniency policy in South Africa not resulted into automatic cartel confessions in economically interdependent neighbouring countries?*. Paper presented to the 1<sup>st</sup> Annual Competition and Economic Regulation (ACER) Conference, Victoria Falls, Zimbabwe. 20-21 March.

- Kaira, T. 2017. 3 Cartel enforcement in the southern African neighbourhood (Pp.71-96). In J. Klaaren, S. Roberts, I. Valodia (Eds). *Competition Law and Economic Regulation: Addressing Market Power in Southern Africa*, 71.
- Kayaalp, M. 2018. Patient privacy in the era of big data. *Balkan medical Journal*, 35(1):8-17.
- Keller-Lynn, C. 2022. *Legislators examine gaps in surveillance laws: No one foresaw' NSO spyware tech*. Available at: <https://www.timesofisrael.com/legislators-examine-gaps-in-surveillance-laws-no-one-foresaw-nso-spyware-tech/> (accessed on: 13 September 2023).
- Kendall, S. & Frost, D. 2022. Network activity, account takeover and data disruption warrants: how novel law enforcement powers impact media freedom. *Australian Journal of Human Rights*, 28(2-3):249-265.
- Kerr, O.S. 2014. The next generation communications privacy act. *University of Pennsylvania law review*, 373-419.
- Khan, F. A. & Edwards, K. 2022. International Human Rights Law and Privacy: An Overview. *Human Rights Review*, 23(4):405-421.
- Khan, M. 2018. The Court of Appeal's Decision on DRIPA and Its Impact on Surveillance Law. *Journal of Law and Technology*, 34(1):78-92.
- Khan, M. 2021. *Privacy and Surveillance: Balancing Security and Civil Liberties*. London: Oxford University Press.
- Klein, G. 2011. Cartel destabilization and leniency programs—Empirical evidence. *ZEW-Centre for European Economic Research Discussion Paper*, 10-107.
- Kolaszyński, M. 2019. Surveillance powers of law enforcement and intelligence services in Poland. *Security Outlook*, 127-141.
- Korstjens, I. & Moser, A. 2018. “Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing”. *European Journal of General Practice*, 24(1):120-124.

- Kovacic, W.E. & Winerman, M. 2010. Competition Policy and the Application of Section 5 of the Federal Trade Commission Act. *Antitrust Law Journal*, 76(3):929-950.
- Labuschagne, R. & Lotter, D. 2015. *Chambers legal practice guides – cartels 2015 South Africa Chapter*. Bowmans. Available at: <https://bowmanslaw.com/insights/competition/2015-chambers-legal-practice-guides-cartel-enforcement-south-africa/> (accessed on: 15 August 2023).
- Larsson, F. 2019. *Algorithmic trading surveillance: Identifying deviating behaviour with unsupervised anomaly detection*. Unpublished MA Dissertation, Uppsala University, Sweden.
- Lavoie, C. 2010. South Africa's Corporate leniency policy: A five-year review. *World Competition*, 33(1):141-162.
- Lee, K. 2018. *Algorithmic collusion & its implications for competition law and policy*. Available at: <https://ssrn.com/abstract=3213296> (accessed on: 5 April 2023).
- Leedy, P. D. & Ormrod, J. E. 2019. *Practical research: Planning and design*. Essex: Pearson.
- Legal Brief. 2022. *Characterisation: Much ado about nothing*. Werksmans. Available at: <https://www.werksmans.com/legal-updates-and-opinions/characterisation-much-ado-about-nothing/> (accessed on: 24 September 2023).
- Leslie, C. 2011. Editorial: antitrust leniency programmes. *Competition Law Review*, 7: 175-179.
- Levenstein, M. C. & Suslow, V. Y. 2006. What determines cartel success? *Journal of Economic Literature*, 44(1):43-95.
- Lewis, D. 2018. *Competition law and policy in South Africa*. Cape Town: Juta & Company Ltd.
- Licetti, M.M. 2013. Combating cartels in developing countries: implementation challenges on the ground. *Competition Policy International*, 12.



- Lodder, A. & Wright, D. 2022. Surveillance Law and Policy: Understanding the UK's Investigatory Powers Act and Its Impact. *Journal of Data Protection & Privacy*, 15(3):223-240.
- Loftus, B. & Goold, B. 2012. Covert surveillance and the invisibilities of policing. *Criminology & Criminal Justice*, 12(3):275-288.
- Lorenzoni, I. 2022. Why do competition authorities need Artificial Intelligence? *Yearbook of Antitrust and Regulatory Studies*, 15(26):33-55.
- Lyons, Bruce. 2017. *Surveillance and the Detection of Cartels: Legal and Practical Considerations*. London: Cambridge University Press.
- Lythgo-Marshall, P. 2016. *The Australian Competition and Consumer Commission Immunity Policy for Cartel Conduct: A Critical Legal Analysis*. Unpublished PhD Thesis, University of Wollongong. Australia.
- Mabizela, K. 2021. Enhancing Cartel Investigations: The Evolution and Effectiveness of Competition Law in South Africa. *South African Law Journal*, 138(2):221-245.
- Machi, L. A. & McEvoy, B. T. 2009. *The literature review: Six steps to success*. California: Corwin.
- Macnish, K. 2018. *The ethics of surveillance: An introduction*. New York: Routledge.
- Mahlangu, P. L. 2014. *Enforcement against cartels in South Africa competition law: advantage and challenges*. Unpublished MA Dissertation, University of Pretoria, Pretoria.
- Mann, M. & Murray, A. 2021. Striking a balance: Legislative expansions for electronic communications surveillance. *Precedent*, (166):44-51.
- Martinez, A.P. 2015. Challenges ahead of leniency programmes: the Brazilian experience. *Journal of European Competition Law & Practice*, 6(4):260-267.
- Matczak, Wójtowicz & Dabrowski. 2022. Cost-effectiveness of CCTV surveillance systems: evidence from a Polish city. *European Journal on Criminal Policy and Research*. Available at: <https://link.springer.com/article/10.1007/s10610-022-09527-5#citeas> (accessed on: 20 August 2023).



- Mariniello, M., Brisimi, V. & Regibeau, P. 2021. Digital competition law in Europe: a practical guide. Oxford: Oxford University Press.
- Mbaka, N. & Isiramen, O.M., 2021. The Changing Role of An Exploratory Research In Modern Organisation. *GPH-International Journal of Business Management*, 4(12):27-36.
- McCord, A., Birch, P. & Bizo, L.A. 2022. Digital displacement of youth offending: addressing the issue. *The Journal of Forensic Practice*, 24(3):298-311.
- McCulloh, J. & Wilson, D. 2021. *Pre-Crime: pre-emption, precaution, and the future*. New York: Routledge.
- McIntyre, T.J. 2016. Judicial oversight of surveillance: the case of Ireland in comparative perspective. *Judges as guardians of constitutionalism and human rights*.136-162.
- McStay, A. 2021. *Privacy and the Media*. London: SAGE Publications.
- Merdian, M., 2013. *The criminalisation of cartel conducts in South Africa and the United Kingdom*. Unpublished MA Dissertation. University of Cape Town.
- Meyer, S. & Verhoef, G. 2023. Artificial Intelligence and Data Analytics in Tax Administration: The Case of SARS. *Journal of Tax Administration and Technology*, 9(1):25-41.
- Michael, J. 2021. *The History and Evolution of Surveillance: From Ancient Times to the Digital Age*. London: Cambridge University Press.
- Miller, J. D. & Sweeney, D. 2023. Surveillance and Modern Policing: Innovations and Challenges. *Journal of Contemporary Law Enforcement*, 40(2):112-129
- Mirasdar, U. U. & Gupta, S. L. 2017. Importance of electronic surveillance in criminal investigation. *International Research Journal of Engineering and Technology*, 4(6):2604-2606.
- Mitsilegas, V & Vavoula N. 2021. *Surveillance and privacy in the digital age: European, transatlantic and global perspective*. Oxford: Hart Publishing.
- Mohajan, D. & Mohajan, H. 2022. Memo writing procedures in grounded theory research methodology. *The Munich Personal RePEc Archive (MPRA)*, 115246.

- Mohajan, H. K. 2018. Qualitative research methodology in social science and related subjects. *Journal of Economic Development, Environment and People*, 7(1): 23-48.
- Moore, A.D. 2011. Privacy, security, and government surveillance: Wikileaks and the new accountability. *Public Affairs Quarterly*, 25(2):141-156.
- Morales, G., Salazar-Reque, I., Telles, J. & Díaz, D. 2019. May. Detecting violent robberies in CCTV videos using deep learning. *In IFIP International Conference on Artificial Intelligence Applications and Innovations*, 282-291.
- Morphet, L & Hlatswayo, N. 2017. *Trends in competition law enforcement across Africa*. HoganLovells. Available at: <https://www.hoganlovells.com/en/publications/trends-in-competition-law-enforcement-across-africa> (accessed on: 8 September 2023).
- Morphet, L. & Hlatswayo, N. 2017. South Africa: criminalisation of cartel conduct. *Journal of European Competition Law & Practice*, 8(1):36-40.
- Motta, M., Peitz, M. and Schweitzer. 2021. *Market Investigations: A new competition tool for Europe?* London: Cambridge.
- Mubangizi, J. C. & Masuku, T. 2021. Challenges in Antitrust Enforcement in Africa: A Review of Strategies and Practices. *African Journal of International and Comparative Law*, 29(2):183-204.
- Munoriyarwa, A. & Chiumbu, S.H. 2019. Big brother is watching: Surveillance regulation and its effects on journalistic practices in Zimbabwe. *African Journalism Studies*, 40(3):26-41.
- Munoriyarwa, A. & Mare, A. 2023. *Digital surveillance in southern Africa: Policies, politics and practices*. Johannesburg: Springer Nature.
- Muñoz Muñoz, A., Urueña Pascual, M., Aparicio Morenilla, R. & Rodríguez de los Santos López, G. 2015. Digital Wiretap Warrant: Improving the security of ETSI Lawful Interception. *Digital Investigation*, 14:1-16.
- Murphy, C. & Wakeman, S. 2022. *Digital Policing: The Future of Law Enforcement in a Technological Age*. *Journal of Policing and Society*, 32(3):245-260.

- Mutung'u, G. 2021. *Surveillance law in Africa: a review of six countries: South Africa country report*. UK: Institute of development Studies.
- Naidu, L. and Tzarevski, A. 2019. The growth of competition laws and enforcement in Africa. SA Financial Regulation Journal. Available at: <https://financialregulationjournal.co.za/2019/10/29/the-growth-of-competition-laws-and-enforcement-in-africa/> (accessed on: 19 September 2023).
- Nandy, D. 2023. Human rights in the era of surveillance: balancing security and privacy concerns. *Journal of Current Social and Political Issues*, 1(1):13-17.
- National Government. 2023. *State Security Agency*. Available at: <https://nationalgovernment.co.za/units/view/42/state-security-agency-ssa> (accessed on: 13 September 2023).
- Naude, A. & Papadopoulos, S. 2016. Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments. *Journal of Contemporary Roman Dutch Law*, 79:51.
- Ncube, M. & Nkuembe, M. 2020. The Role of Leniency Policies in Cartel Enforcement: A Comparative Analysis of South Africa and Other African Jurisdictions. *African Competition Law Journal*, 8(1):82-101.
- Neuhoff, M. N., Govender, M., Versfeld, M. & Dingley, D. 2006. *A practical guide to the South African Competition Act*. Durban: LexisNexis.
- Newell, B.C., Timan, T. and Koops, B.J. 2018. *Surveillance, Privacy and Public Space*. London: Routledge.
- Neyroud, P. & Beckley, A. 2022. *Policing, Ethics and Human Rights*. London: Routledge.
- Ng'ethe, N. & Gathii, J. T. 2019. *Competition Law and Policy in Africa: The Influence of South Africa*. In *African Competition Law and Policy*, 35-58
- Nieland, A.E. 2006. National security letters and the amended PATRIOT Act. *Cornell Law Review*, 92:1201.
- Nkosi, W.W. and Boshoff, W.H. 2022. Characteristics of Prosecuted Cartels and Cartel Enforcement in South Africa. *Review of Industrial Organization*, 60(3): 327-360.

- Norris, C. & Armstrong, G. 2019. The Politics of Surveillance: CCTV and Social Control in the Post-Industrial City. *Journal of Criminology and Public Policy*, 18(2):287-305.
- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. 2017. Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, 16(1):1-13.
- Nunn, P. 2018. *Surveillance, privacy and security*. London: Routledge.
- Nuruddin-Khan, D.S.G. 2023. International legislative framework of cybercrimes-A Comparative Study of India, Israel, And USA. *Journal of Positive School Psychology*, 782-800.
- Ogundele, O. 2022. *An Africa-Focused Competition performance index*. Competition Policy International. March 29. Available at: [https://www.pymnts.com/cpi\\_posts/an-africa-focused-competition-performance-index/](https://www.pymnts.com/cpi_posts/an-africa-focused-competition-performance-index/) (accessed on: 10 September 2023)
- Ohlhausen, M.K. 2014. Privacy challenges and opportunities: The role of the Federal Trade Commission. *Journal of Public Policy & Marketing*, 33(1):4-9.
- O'Leary, Z. 2017. *The Essential Guide to Doing Your Research Project* (3rd ed.). London: Sage Publications.
- Ong, B. 2021. The Applicability of Art. 101 TFEU to Horizontal Algorithmic Pricing Practices: Two Conceptual Frontiers. *IIC-International Review of Intellectual Property and Competition Law*, 52(2):189-211.
- Oppong, R. F. & Klaaren, J. B. 2020. *Competition law in Africa: maximising competitor welfare and economic development*. Netherland: Wolters Kluwer.
- Organisation for Economic Cooperation and Development. 2001. *Policy brief: Using leniency to fight hard core cartels*. Available at [http://www.oecd.org/daf/clp/CLP\\_reports/Leniency-e.pdf](http://www.oecd.org/daf/clp/CLP_reports/Leniency-e.pdf) (accessed on: 15 June 2022).
- Organisation for Economic Cooperation and Development. 2011. *Competition Law and Policy Reviews: Competition Law and Policy in Israel 2011*. Available at: [www.oecd.org/publishing/corrigena/](http://www.oecd.org/publishing/corrigena/) (accessed on: 17 August 2023).

Organisation for Economic Cooperation and Development. 2013. *Ex officio cartel investigations and the use of screens to detect cartels*. Available at [https://one.oecd.org/document/DAF/COMP\(2013\)27/en/pdf](https://one.oecd.org/document/DAF/COMP(2013)27/en/pdf) (accessed on 31 July 2024).

Organisation for Economic Cooperation and Development. 2013. *Policy roundtable: ex officio cartel investigations and the use of screens to detect cartels*. Available at: <https://www.fne.gob.cl/wp-content/uploads/2014/07/2013-Ex-officio-cartels-investigation-3569-KB1.pdf> (accessed on: 23 July 2024).

Organisation for Economic Cooperation and Development. 2017. *Algorithms and collusion: competition policy in the digital age*. Available at: <https://www.oecd.org/daf/competition/Algorithms-and-collusion-competition-policy-in-the-digital-age.pdf> (accessed on: 10 April 2023).

Organisation for Economic Co-operation and Development. 2018. *Roundtable on challenges and co-ordination of leniency programmes: note by Australia*. Available at: [https://one.oecd.org/document/DAF/COMP/WP3/WD\(2018\)22/en/pdf](https://one.oecd.org/document/DAF/COMP/WP3/WD(2018)22/en/pdf) (accessed on: 15 May 2023).

Organisation for Economic Co-operation and Development. 2018. *Roundtable on challenges and co-ordination of leniency programmes: note by BIAC*. Available at: [https://one.oecd.org/document/DAF/COMP/WP3/WD\(2018\)34/en/pdf](https://one.oecd.org/document/DAF/COMP/WP3/WD(2018)34/en/pdf) (accessed on: 16 May 2023).

Organisation for Economic Co-operation and Development. 2018. *Roundtable on challenges and co-ordination of leniency programmes: note by Brazil*. Available at: [https://one.oecd.org/document/DAF/COMP/WP3/WD\(2018\)13/en/pdf](https://one.oecd.org/document/DAF/COMP/WP3/WD(2018)13/en/pdf) (accessed on: 16 May 2023).

Organisation for Economic Co-operation and Development. 2018. *Roundtable on challenges and co-ordination of leniency programmes: note by Israel*. Available at: [https://one.oecd.org/document/DAF/COMP/WP3/WD\(2018\)5/en/pdf](https://one.oecd.org/document/DAF/COMP/WP3/WD(2018)5/en/pdf) (accessed on: 17 May 2023).

Organisation for Economic Co-operation and Development. 2018. *Roundtable on challenges and co-ordination of leniency programmes: note by the United*

Kingdom. Available at:  
[https://one.oecd.org/document/DAF/COMP/WP3/WD\(2018\)38/en/pdf](https://one.oecd.org/document/DAF/COMP/WP3/WD(2018)38/en/pdf)  
(accessed on: 16 May 2023).

Organisation for Economic Co-operation and Development. 2018. *Roundtable on challenges and co-ordination of leniency programmes: note by United State*. Available at:  
[https://one.oecd.org/document/DAF/COMP/WP3/WD\(2018\)33/en/pdf](https://one.oecd.org/document/DAF/COMP/WP3/WD(2018)33/en/pdf)  
(accesses on: 15 May 2023).

Organisation for Economic Cooperation and Development. 2020. *Criminalisation of cartels and bid rigging conspiracies – Note by Israel*. Available at:  
[https://one.oecd.org/document/DAF/COMP/WP3/WD\(2020\)7/en/pdf](https://one.oecd.org/document/DAF/COMP/WP3/WD(2020)7/en/pdf)  
(accessed on: 06 August 2020).

Organisation for Economic Co-operation and Development. 2020. *Digital evidence gathering in cartel investigations*. Available at:  
[https://one.oecd.org/document/DAF/COMP/LACF\(2020\)14/en/pdf](https://one.oecd.org/document/DAF/COMP/LACF(2020)14/en/pdf) (accessed on: 20 April 2023).

Organisation for Economic Cooperation and Development. 2022. *Interim Measures in Antitrust Investigations – Note by Israel*. Available at:  
[https://www.gov.il/BlobFolder/generalpage/interncooperation/he/interncooperation\\_Interim%20measures%20in%20antitrust%20investigations%20June%202022.pdf](https://www.gov.il/BlobFolder/generalpage/interncooperation/he/interncooperation_Interim%20measures%20in%20antitrust%20investigations%20June%202022.pdf) (accessed on: 12 September 2023).

Organisation for Economic Co-operation and Development. 2022. *Latin American and Caribbean competition forum: strengthening incentives for leniency agreements*. Available at:  
[https://one.oecd.org/document/DAF/COMP/LACF\(2022\)17/en/pdf](https://one.oecd.org/document/DAF/COMP/LACF(2022)17/en/pdf) (accessed on: 17 May 2023).

Organisation for Economic Cooperation and Development. 2022. *Legal instrument: Recommendation of the council concerning effective action against hardcore cartel*. Available at <http://www.legalinstruments.oecd.org/legal/0294>. (accessed on: 17 June 2022).

Organisation for Economic Cooperation and Development. 2023. *The future of effective leniency programmes – Note by United Kingdom*, Available at: [https://one.oecd.org/document/DAF/COMP/WP3/WD\(2023\)18/en/pdf](https://one.oecd.org/document/DAF/COMP/WP3/WD(2023)18/en/pdf) (accessed on: 14 August 2023).

Organisation for Economic Cooperation and Development. 2023. *The future of effective leniency programmes – Note by Italy*, 13 June 2023. Available at: [https://one.oecd.org/document/DAF/COMP/WP3/WD\(2023\)7/en/pdf](https://one.oecd.org/document/DAF/COMP/WP3/WD(2023)7/en/pdf) (accessed on: 14 August 2023).

Organisation for Economic Cooperation and Development. 2023. *The future of effective leniency programmes – Note by New Zealand*. 13 June 2023. Available at: [https://one.oecd.org/document/DAF/COMP/WP3/WD\(2023\)12/en/pdf](https://one.oecd.org/document/DAF/COMP/WP3/WD(2023)12/en/pdf) (accessed on: 14 August 2023).

Organisation for Economic Cooperation and Development. 2023. *The future of effective programme – Note by Australia*. Available at: [https://one.oecd.org/document/DAF/COMP/WP3/WD\(2023\)1/en/pdf](https://one.oecd.org/document/DAF/COMP/WP3/WD(2023)1/en/pdf) (accessed on: 15 August 2023).

Organisation for Economic Cooperation and Development. 2023. *The future of leniency programmes: Advancing Detection and Deterrence of Cartels – Background Note by the Secretariat*. Available at: [https://one.oecd.org/document/DAF/COMP/WP3\(2023\)1/en/pdf](https://one.oecd.org/document/DAF/COMP/WP3(2023)1/en/pdf) (accessed on 07 August 2024).

Organisation for Economic Cooperation and Development. 2024. Session III: ex officio investigations – calls for contributions. Available at: [https://one.oecd.org/document/DAF/COMP/LACCF\(2024\)3/en/pdf](https://one.oecd.org/document/DAF/COMP/LACCF(2024)3/en/pdf) (accessed on 31 July 2024).

Orthman, C. & Hess, K. M. 2013. *Criminal investigation*. New York: Cengage Learning

Parliamentary Monitoring Group. 2014. *Report on interception of private communications*. Available at: <https://static.pmg.org.za/160127report.pdf> (accessed on: 19 April 2023).

- Patton, M. Q. 2015. *Qualitative research & evaluation methods*. Thousand Oaks: SAGE.
- Petersen, J.K. 2012. *Introduction to surveillance studies*. Florida: CRC Press.
- Phadtare, G. & Goud, A. 2018. Electronic surveillance. *International Journal of Trend in Scientific Research and Development*, 2(4):1623-1625.
- Pinha, L.C. & Braga, M.J. 2019. Evaluating the effectiveness of the Brazilian leniency program. *Economics Bulletin*, 39(3):1860-1869.
- Priks, M. 2015. The effects of surveillance cameras on crime: Evidence from the Stockholm subway. *The Economic Journal*, 125(588):289-305.
- Rahman, M.S., 2020. The advantages and disadvantages of using qualitative and quantitative approaches and methods in language “testing and assessment” research: A literature review. *Journal of Education and Learning*, 6(1):102-112.
- Ramburuth, S. 2012. Chapter 5: South Africa, Part I: Regulator’s Introduction’. (Pp.207-217). In Vassily Rudomino, Jose Regazzini, et al. (Eds). *Competition Law in the BRICS countries*. International Bar Association Series, Volume 24.
- Ramiro, A. & Cruz, L. 2023. The grey-zones of public-private surveillance: Policy tendencies of facial recognition for public security in Brazilian cities. *Internet Policy Review*, 12(1),1-28.
- Ran, J. 2016. Striking the Balance between Privacy and Governance in the Age of Technology. *Penn Journal of Philosophy, Politics & Economics*, 11(1):2.
- Ratcliffe, J. 2022. *Intelligence-Led Policing*. London: Routledge.
- Ratcliffe, J. H. 2020. Video Surveillance of Public Places and Crime Prevention: Examining the Evidence. *Crime Science*, 9(1).
- Richards, N.M. 2013. The dangers of surveillance. *Harvard Law Review*, 126(7):1934-1965.
- Ritchie, J., Lewis, J., Nicholls, C. M & Ormston, R. 2014. *Qualitative research practice: a guide for social science students and researchers*. London: SAGE.
- Righ2know. 2016. The Surveillance State: *Communications surveillance and privacy in South Africa*. Right2know. Available at:



[https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa\\_surveillance-state-web.pdf](https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillance-state-web.pdf) (accessed on: 7 April 2023).

Right2know. 2018. *Surveillance of Journalists in SA*. Right2know. Available at: <https://www.r2k.org.za/wp-content/uploads/R2K-Surveillance-of-Journalists-Report-2018-web.pdf> (accessed on: 3 April 2023)

Roberts, S. 2020. Cartel enforcement: critical reflections from the South African experience. In *Research handbook on methods and models of competition law*, 414-435.

Roberts, T. 2021. *Surveillance laws are failing to protect privacy rights*. DailyMaverick. Available at: <https://www.dailymaverick.co.za/article/2021-11-08-surveillance-laws-are-failing-to-protect-privacy-rights-what-we-found-in-six-african-countries-including-south-africa/> (accessed on: 17 April 2023)

Roberts, T., Mohamed Ali, A., Farahat, M., Oloyede, R. & Mutung'u, G. 2021. *Surveillance Law in Africa: a review of six countries*. Brighton: Institute of Development Studies.

Rodger, B. S. & MacCullah, A. 2015. *Competition law and policy in the EU and UK*. London: Routledge.

Rodger, B.J. & MacCulloch, A. 2008. *Competition law and policy in the EC and UK*. Routledge-Cavendish.

Rowan, T. 2020. *The criminalisation of cartels in South Africa, United States and Australia and the effects of the Corporate Leniency Policy*. Unpublished MA Dissertation, University of Cape Town.

Roy, A. 2016. *Competition Law in India: A practical guide*. Netherlands: Kluwer Law International.

SAPS. 2009. *Annual report: crime intelligence*. Available at: [https://www.saps.gov.za/about/stratframework/annual\\_report/2008\\_2009/7\\_pr\\_g4\\_crime\\_intelligence.pdf](https://www.saps.gov.za/about/stratframework/annual_report/2008_2009/7_pr_g4_crime_intelligence.pdf) (accessed on: 14 September 2023).

Saunders, M., Lewis, P. & Thornhill, A. 2016. *Research methods for business students*. Harlow: Pearson Education,

- Scheepers, S.A. & Schultz, C.M. 2019. Organisational learning in Crime Intelligence: a qualitative review. *Journal of Contemporary Management*, 16(2):361-381.
- Schinkel, M. P. 2014. *Balancing proactive and reactive cartel detection tools: Some observations*. Available at: <http://www.oecd.org/daf/competition/exofficio-cartel-investigation-2013.pdf> (accessed on: 14 June 2022).
- Schinkel, M.P. 2013. *Balancing proactive and reactive cartel detection tools: some observations. OECD policy roundtables: ex officio cartel investigations and the use of screens to detect cartels*. Available at: <http://www.oecd.org/daf/competition/exofficio-cartel-investigation-2013.pdf> (accessed on: 15 April 2023).
- Schrepel, T. 2020. *The fundamental unimportance of algorithmic collusion for antitrust law*. Available at: <http://jolt.law.harvard.edu/digest/the-fundamental-unimportance-of-algorithmic-collusion-for-antitrust-law> (accessed on: 30 April 2023).
- Seale, C. 2012. *Researching society and culture*. London: Sage.
- Shabalala, K. 2022. The Success of the Leniency Policy in South Africa's Fight Against Cartels. *Journal of Competition Law & Economics*, 18(1):107-134.
- Sharon, L. L. 2019. *Sampling: Design and analysis*. New York: Chapman and Hall.
- Shekhar, A. & Chauhaan, A. 2022. The death of leniency? An analysis of the impact of blockchain on the Indian leniency program. *University of Illinois Journal of Law, Technology and Policy*.
- Siddique, B. 2016. Rationale and Benefits of Leniency Programs Under EU Competition Law and US Federal Anti-Trust Law. Available at: <https://ssrn.com/abstract=2954961> (accessed on: 25 April 2023).
- Silverman, D. 2016. *Qualitative Research*. London: Sage Publications
- Singh, A., 2021. An introduction to experimental and exploratory research. Available at SSRN 3789360.

- Smit, D. & Nel, R. 2023. The Role of Intelligence in Tax Collection and Anti-Money Laundering: Insights from SARS. *South African Journal of Economic and Management Sciences*, 26(2):155-171.
- Smith, R. G. & McCusker, R. 2020. *Surveillance and Crime Control: New Technologies in Criminal Justice*. London: Routledge.
- Sokol, D.D., Cheng, T.K. and Lianos, I. 2013. *Competition law and development*. Stanford: University Press.
- Solove, D. J. 2023. *Understanding Privacy*. Cambridge: Harvard University Press.
- Solove, D.J. 2004. Reconstructing electronic surveillance law. *George Washington Law School Review*, 72(6):1701-1747.
- Solove, D.J. 2008. *Understanding privacy*. Cambridge: Harvard University Press.
- South African Government. 2001. Financial Intelligence Centre Act 38 of 2001. *Government Gazette*, 438(22886). Pretoria: Government printers. 3 December.
- South African Government. 2003. National Strategic Intelligence Amendment Act 67 of 2002. *Government Gazette*, 237(24391). Pretoria: Government printers. 13 February.
- South African Government. 2003. Regulation of Interception of Communications and Provision of Communication-related information Act 70 of 2002. *Government Gazette*, 451(24286). Pretoria: Government printers. 22 January.
- South African Government. 1996. *Constitution of the Republic of South Africa*. Pretoria: Government Printer.
- Stebbins, R. A. 2001. *Exploratory research in the social science*. Thousand Oaks: Sage.
- Stephan, A. 2014. Four key challenges to the successful criminalization of cartel laws. *Journal of Antitrust Enforcement*, 2(2):333-362.
- Steyn, N. 2019. *Competition law in South African: the path ahead*. Cape Town: Juta & Company Ltd.
- Stigler, G. J. & Friedland, C. 2020. *The Chicago School of Economics: A Reader*. Routledge.

- Stratton, G., Powell, A. & Cameron, R. 2016. Crime and Justice in Digital Society: towards a 'digital criminology'? *International journal for Crime, Justice and Social Democracy*, 6(2):17-33.
- Strauss, S., Wright, D. & Kreissl, R. 2015. *Towards a taxonomy of social and economic costs: surveillance in Europe*. London: Routledge.
- Sung, C.S. & Park, J.Y. 2021. Design of an intelligent video surveillance system for crime prevention: applying deep learning technology. *Multimedia Tools and Applications*, 1-13.
- Sutherland, E. 2017. Governance of cybersecurity-the case of South Africa. *The African Journal of Information and Communication*, 20:83-112.
- Sutherland, P. 2018. *Inquiries about market inquiries*. Paper presented to the 4<sup>th</sup> Annual Competition and Economic Development (ACER) Conference Johannesburg, South Africa, 19-20 July.
- Taylor, J. & Evans, K. 2021. Surveillance and Crime: The Role of Monitoring Technologies in Modern Investigations. *Journal of Criminal Justice and Law*, 34(2):145-160.
- Thomas, O.O. & Lawal, O.R. 2020. Exploratory Research Design in Management Sciences: An X-Ray of Literature. *Annals of the University Dunarea de Jos of Galati: Fascicle: I, Economics & Applied Informatics*, 26(2):79-84.
- Todorov, F.R. & Filho, M.M.T. 2012. History of competition policy in Brazil: 1930–2010. *The Antitrust Bulletin*, 57(2):207-257.
- Trottier, D. 2014. Crowdsourcing CCTV surveillance on the Internet. *Information, Communication & Society*, 17(5):609-626.
- Tshabalala, M. & Jacobs, J. 2024. Technological Advances in Tax Administration: Enhancing Detection and Compliance at SARS. *Journal of South African Taxation*, 31(1):88-104.
- Turanjanin, V. 2020. Video surveillance of the employees between the right to privacy and right to property after Lopez Ribalda and others v. Spain. *University of Bologna Law Review*, (5):268.

- U. S. Department of Justice. 2013. *Electronic Surveillance Technologies for Criminal Justice Applications*. Available at: <https://nij.ojp.gov/sites/g/files/xyckuh171/files/media/document/NIJ-2011-2799.pdf> (accessed on: 10 November 2022).
- United Kingdom Government (2018) *Covert Surveillance and Property Interference: Revised Code of Practice*. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/742041/201800802\\_CSPI\\_code.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf) (accessed on: 8 April 2023).
- United Nations Office on Drugs and Crime. 2009. *Current practices in electronic surveillance in the investigation of serious and organised crime*. Available at: [https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic\\_surveillance.pdf](https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf) (accessed on: 23 October 2022).
- United Nations Office on Drugs and Crime. 2018. *Physical and electronic surveillance*. Available at: <https://www.unodc.org/e4j/zh/organized-crime/module-8/key-issues/special-investigative-techniques/physical-and-electronic-surveillance.html> (accessed on: 20 November 2022).
- United States Department of Justice. 2013. *Electronic surveillance technologies for criminal justice applications*. Available at: <https://nij.ojp.gov/sites/g/files/xyckuh171/files/media/document/NIJ-2011-2799.pdf> (accessed on: 13 April 2023).
- University of South Africa. 2016. *Policy on research ethics*. Available at: [https://www.unisa.ac.za/static/corporate\\_web/Content/Apply%20for%20admission/MD/Documents/Policy%20on%20Research%20Ethics%20-%20rev%20appr%20-%20Council%20-%202015.09.2016.pdf](https://www.unisa.ac.za/static/corporate_web/Content/Apply%20for%20admission/MD/Documents/Policy%20on%20Research%20Ethics%20-%20rev%20appr%20-%20Council%20-%202015.09.2016.pdf) (accessed on: 21 April 2022).
- Unterhalter, D. 2012. Chapter 5: South Africa, Part II: Cartels. (Pp.219-231). In Vassily Rudomino, Jose Regazzini, et al.(eds). *Competition Law in the BRICS countries*. International Bar Association Series, Volume 24.

- Urmonaite, I. 2022. *Investigations/inquiries*. Available at: <https://www.concurrences.com/en/dictionary/investigations#references> (accessed on: 24 October 2022).
- Vadász, P., Benczúr, A., Füzesi, G. & Munk, S. 2016. Identifying Illegal Cartel Activities from Open Sources. *Open-Source Intelligence Investigation: From Strategy to Implementation*, 251-273.
- Vaismoradi, M., Turunen, H. & Bondas, T. 2013. Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing and Health Science*, 15(3):398-405.
- Vallance, C. & Mullen, P. 2021. The Investigatory Powers Act 2016: A Comprehensive Review. *Journal of Privacy and Data Protection*, 11(2):152-171.
- Van Brakel, R. & De Hert, P. 2011. Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology-based strategies. *Technology- Led Policing*, 20:165-192.
- Van Heek, J., Aming, K. and Ziefle, M. 2016, April. "How fear of crime affects needs for privacy & safety": Acceptance of surveillance technologies in smart cities. *2016 5th international conference on smart cities and green ICT systems*. 1-12.
- Van Heerden, C. M & Botha, M. M. C. 2015. *Challenges to the corporate leniency policy in South African competition law*. Available at: <https://ssrn.com/abstract=2873073> (accessed on 21 October 2022).
- Van Heerden, C. M. & Botha, M. M. C. 2015. Challenges to the South African corporate leniency policy and cartel enforcement. *Journal of South African Law*, 2015(2):308-333.
- Van Thiel, S. 2014. *Research methods in public administration and public management: An introduction*. New York: Routledge.
- Vervaele, J.A. 2013. Surveillance and criminal investigation: blurring of thresholds and boundaries in the criminal justice system? (Pp.115-128). In S. Gutwirth, R. Leenes, P. De Hert (eds). *Reloading data protection: Multidisciplinary insights and contemporary challenges*, Netherland: Springer.

- Voitovych, N. 2020. Historical background and legal analysis of surveillance in crime prevention. *Interarm: History, Policy, Culture*, (8):189-209.
- Watney, M. 2008. *Understanding electronic surveillance as an investigatory method in conducting criminal investigations on the internet*. Available at: <http://www.isrcl.org/Papers/2008/Watney.pdf> (accessed on: 15 March 2023).
- Watney, M. 2010. The use of electronic surveillance in conducting criminal investigations on the internet. *Handbook of Electronic Security and Digital Forensic*, 525-551.
- Watney, M. 2015. August. State-on-nationals' electronic communication surveillance in South Africa: A murky legal landscape to navigate? *In 2015 Information Security for South Africa (ISSA)*,1-6.
- Watney, M., 2021, June. Mobile Phone Surveillance: An Overview of Privacy and Security Legal Risks. In *European Conference on Cyber Warfare and Security* (pp. 462-469). Academic Conferences International Limited.
- Weiss, A. 2018. *Surveillance and Intelligence Gathering: Techniques and Technologies*. New York: Palgrave Macmillan.
- Weiss, A. S. 2018. *Surveillance and Privacy in the Digital Age: Understanding the Complexities*. New York: Palgrave Macmillan.
- Welsh, B. C. & Farrington, D. P. (2021). *The Effectiveness of Public Area Surveillance for Crime Prevention: CCTV and Crime Prevention Revisited*. *Journal of Security Research*, 44(1):33-52.
- Welsh, B.C. & Farrington, D.P. 2009. Public area CCTV and crime prevention: an updated systematic review and meta-analysis. *Justice Quarterly*, 26(4):716-745.
- Welsh, Farrington & Taheri. 2011. Effectiveness and social costs of public area surveillance for crime prevention. *Annual Review of Law and Social Science*, 11:111-130.
- Werden, G.J., Hammond, S.D. & Barnett, B.A., 2011. Deterrence and detection of cartels: Using all the tools and sanctions. *The Antitrust Bulletin*, 56(2):207-234.

- Wheatley. 2018. *US Law enforcement techniques against organised crime groups*. Available at: [https://www.unafei.or.jp/publications/pdf/RS\\_No103/No103\\_6\\_1\\_VE\\_Wheatley.pdf](https://www.unafei.or.jp/publications/pdf/RS_No103/No103_6_1_VE_Wheatley.pdf) (accessed on: 10 April 2023).
- Whish, R. & Bailey, D. 2021. *Competition law*. London: Oxford University Press.
- Whitehead, D. 2016. *Nursing and midwifery research: Methods and appraisal for evidence-based practice*. Sydney: Elsevier.
- Whitehead, J. W. & Whitehead, N. 2023. *The federal surveillance law: a comprehensive guide to the U.S surveillance system*. New York: Routledge.
- Wilson, J. Q. 2019. *The Impact of Technological Advancements on Electronic Surveillance in Criminal Investigations*. New York: Routledge.
- Wills, A. 2017. *Surveillance and Privacy in the Digital Age*. Switzerland: Springer.
- Yilmaz, H. 2009. Leniency Programmes. *Competition Magazine*, 10(1):139-163.
- Yin, R. K. 2018. *Case Study Research and Applications: Design and Methods*. London: Sage Publications.
- Yuanyuan Xiong, B. & Crowe, J. 2022. Revisiting the notion of agreement in Australian cartel law in the algorithm-driven economy. *Competition and Consumer Law Journal*, 29(2):91-111.
- Zalnieriute, M. 2022. Reforming the Australian Framework for International Data Sharing. *International Data Privacy Law*, 12(4):332-345.
- Zhang, B., Peterson Jr, H.M. & Sun, W. 2017. Perception of digital surveillance: a comparative study of high school students in the US and China. *Issues in Information Systems*, 18(1):98-108.
- Zhang, Q. & Mitchell, A. 2023. Principles and Practices of Electronic Surveillance in Antitrust Investigations. *Journal of Antitrust Enforcement*, 11(1):56-74.
- Zlatcu, I. & Suciuc, M.C. 2017. The role of economics in cartel detection. A review of cartel screens. *Journal of Economic Development, Environment and People*, 6(3):15-26.



## **ANNEXURE A: INFORMED CONSENT FORM**

- **Affiliation:** Department of Criminal Justice
- **Researcher:** Kgashane Kgomo
- **Title of Study:** analysis of the use of electronic surveillance to investigate cartel conducts: Case study of Competition Commission in Pretoria

The purpose of this study is to explore the importance of electronic surveillance in the investigation of cartels conducts at the Competition Commission, Pretoria. The researcher wants to explore the value the electronic surveillance adds in the investigation of cartels, which may assist competition authorities to adopt pro-active stance to easily identify firms, which are potentially involved in cartels conduct.

- **Procedures:**

The researcher will use semi-structured interviews and systematic observation for collecting data. A tape recorder and observation notes will be used to record conversations. The researchers will be conducting the semi-structured one-on-one interviews with the help of an interview schedule and interviews will be not longer than one and half hours but may end sooner by natural process or on request of the participant or researcher, depending on the circumstances.

- **Risks and Discomfort:**

The researcher will ensure that the participants are protected from any unnecessary physical or psychological harm during the research study. To ensure non risk and discomforts, the researcher will adhere to the UNISA policy on research ethics and protect participants from any physical discomfort that may emerge from the research study. The participants have the rights when become tired or feel emotional discomfort at any time to request a break or the interview be postponed to a later date or terminated if so desired. The researcher will make every effort to ensure the risks and discomforts are avoided as far as possible for the participant.

- **Benefits:**

This study will benefit the research participants to understand better the importance of using electronic surveillance in the investigation of cartel conducts. It is envisaged that the outcome of this study will also be available to students at the University of South Africa and the whole academic community. Healthy market conditions will benefit the

society at large because the competition amongst firms will lead to lower prices, higher quality goods and services, greater variety, and more innovation.

- **Participant's rights:**

Participation in this study is voluntary and may be withdrawn at any time without negative consequences for the participant. All information is treated as confidential, and anonymity is assured by the researcher. The data shall be destroyed should the participant wish to withdraw. The researcher and the supervisor are the only individuals who will have access to raw data from interviews. Right of Access to Researcher: Participants are free to contact the researcher at the telephone number as stipulated on this form, at a reasonable hour, in connection with interview particulars, if they so wish.

I, the undersigned, agree to participate in this study voluntarily without duress.

Signed at.....on this.....day of.....20...

Name.....Signature.....

**THANK YOU FOR YOUR PARTICIPATION IN THIS STUDY**

## **ANNEXURE B: INTERVIEW SCHEDULE GUIDE**

1. What do you understand by electronic surveillance?
2. Why should electronic surveillance be used to investigation of cartel conduct?
3. What are different types of electronic surveillance?
4. Which type(s) of electronic surveillance can effectively be used to investigate cartel conducts?
5. What is the role of electronic surveillance in the investigation of crime?
6. When should electronic surveillance be used as an investigative tool to investigate cartel conducts?
7. Who should be authorised to apply for a warrant to conduct electronic surveillance operations during the investigation of cartel conducts?
8. Who should be allowed to conduct electronic surveillance operations during the investigation of cartel conducts?
9. What circumstances should allow the Competition Commission to apply for a warrant to conduct electronic surveillance operations?
10. For how long should the warrant to conduct electronic surveillance operations be effective? Elaborate.
11. What do you understand by the fundamental rights to privacy?
12. How can it be ensured that during the execution of electronic surveillance individuals' rights to privacy are protected?
13. What regulations should be put in place internally to govern the usage of electronic surveillance?
14. How should the organisation guard against the misuse of electronic surveillance operations?
15. Which Act regulates the usage of electronic surveillance as an investigation tool?
16. What limitations should be considered when conducting electronic surveillance operations?
17. What investigation technique(s) do you think work(s) better to resolve cartel cases currently?

18. What are the challenges in terms of the investigation techniques the Competition Commission is faced with in the investigation of cartel conducts?




19. Do you think the reactionary cartel detection method is still effective in the fight against cartel conducts?

20. What value would electronic surveillance add in the investigation of cartel conducts?

21. What proactive cartel detection measures should the Commission apply in order to be ahead of cartelists?

22. Do you think the Act should be amended to incorporate the use of electronic surveillance in the investigation of cartel conducts?

# ANNEXURE C: UNIVERSITY OF SOUTH AFRICA ETHICAL APPROVAL LETTER

 <b>UNISA</b> university of south africa College of Law_RERC		Ref #: 1857 Name: Mr Kgashane kgomo Student #: 18030513
Date: 10/10/2023 Dear: Mr Kgashane kgomo		
<b>Decision: Ethics Approval from 10/10/2023 to 10/10/2026</b>		
Researcher: Mr Kgashane kgomo The Competition Commission, DTI Campus, Block C, 77 Meintjies Street, Trevenna, Pretoria, 0002 kgashane.kgomo1@gmail.com 0633470121		
Supervisor: Professor Witness Moleleke <a href="mailto:witness.moleleke@unisa.ac.za">witness.moleleke@unisa.ac.za</a> Co-Supervisor: Dr Dumisani Quiet Mabunda <a href="mailto:mabunda@unisa.ac.za">mabunda@unisa.ac.za</a>		
<b>ANALYSIS OF THE USE OF ELECTRONIC SURVEILLANCE TO INVESTIGATE CARTEL CONDUCTS: A CASE STUDY OF COMPETITION COMMISSION IN PRETORIA</b>		
Qualification: MA (CRIMINAL JUSTICE)		
Thank you for the application for research ethics clearance by the College of Law_RERC for the above-mentioned research study Ethics approval is granted for three years.		
<p>The medium risk application was reviewed by College of Law_RERC on 10/10/2023 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.</p> <p>The proposed research may now commence with the provisions that:</p> <ol style="list-style-type: none"><li>1. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.</li><li>2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the College of Law_RERC.</li><li>3. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.</li><li>4. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.</li><li>5. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.</li><li>6. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.</li><li>7. No field work activities may continue after the expiry date 10/10/2026. Submission of a completed research ethics progress report will constitute an application for renewal, for Ethics Research Committee approval.</li></ol> <p><b>Additional Conditions</b></p> <ol style="list-style-type: none"><li>1. Disclosure of data to third parties is prohibited without explicit consent from Unisa.</li><li>2. De-identified data must be safely stored on password protected PCs.</li><li>3. Care should be taken by the researcher when publishing the results to protect the confidentiality and privacy of the university.</li><li>4. Adherence to the National Statement on Ethical Research and Publication practices, principle 7 referring to Social awareness, must be ensured: "Researchers and institutions must be sensitive to the potential impact of their research on society, marginal groups or individuals, and must consider these when weighing the benefits of the research against any harmful effects, with a view to minimising or avoiding the latter where possible." Unisa will not be liable for any failure to comply with this principle.</li></ol> <p><b>Note</b> The reference number 1857 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.</p>		
Kind regards,		
		
Prof Lincoln Fitz Chair of College of Law_RERC E-mail: <a href="mailto:lfitz@unisa.ac.za">lfitz@unisa.ac.za</a>	Executive Dean / By delegation from the Executive Dean of College of Law_RERC E-mail: <a href="mailto:fd@unisa.ac.za">fd@unisa.ac.za</a>	

## ANNEXURE D: LETTER TO ASK FOR PERMISSION TO CONDUCT RESEARCH FROM THE COMPETITION COMMISSION OF SOUTH AFRICA

93 Spaansriet Street  
5174/2 Arundo Estate  
The Reeds Ext. 45  
Centurion  
0157

16 October 2023

The Commissioner  
The Competition Commission  
DTI Campus, Mulayo (Block C)  
77 Meintjies Street, Sunnyside  
Pretoria

BY EMAIL: [DorteT@compcom.co.za](mailto:DorteT@compcom.co.za)

Dear Commissioner

### APPLICATION FOR PERMISSION TO CONDUCT RESEARCH IN THE COMPETITION COMMISSION: KGASHANE KGOMO

I am Kgashane Kgomo, Senior Investigator at Cartels Division. I am currently enrolled for Master of Arts in Criminal Justice at the University of South Africa.

My research proposal has been approved and I am now required to conduct a survey in the Commission to finalise my dissertation. The title of the study is: *Analysis of the use of Electronic Surveillance to Investigate Cartel Conducts: A Case Study of the Competition Commission of South Africa in Pretoria.*

The aim of the study is to explore the importance of using electronic surveillance in the investigation of cartel conducts. The study will explore the value that the electronic surveillance may add in the investigation of cartel activities. This research will contribute to the body of knowledge regarding the importance of using electronic surveillance in the investigation of cartel conducts.

I am requesting to conduct one-on-one semi-structured interviews with staff members from the Cartels Division and Legal Services. Each interview will last for approximately 45-60 minutes and will be recorded using an audio-recorder.

All responses will be kept confidential and will not be used in any way that may identify the participants.

I will abide by the rules of the organization while conducting the study.

Regards



KGASHANE KGOMO

## ANNEXURE E: COMPETITION COMMISSION ETHICAL APPROVAL LETTER

The screenshot displays an Outlook email window titled "RE: Permission to conduct research survey - Message (HT...". The interface includes a ribbon with various action buttons such as "Delete", "Archive", "Reply", "Forward", "Share to Teams", "Move", "Tags", "Editing", "Immersive", "Translate", "Zoom", "Find Time", "Report Message", "Viva Insights", and "Phish Alert Report".

The email content is as follows:

**RE: Permission to conduct research survey**

**Mduzuzi Msibi**  
To: Kgashane Kgomo  
Cc: Andile Gwabeni; Thozama Linganisa

You replied to this message on 2023/11/17 09:13.

Thu 2023/11/16 15:31

Dear Kgashane

The Commissioner approved yesterday requests, including yours, to conduct research at the Commission. You, and other applicants, are required to submit a research ethics clearance from your university before you commence with the research survey. Additionally, the Commission will issue a confidentiality/non-disclosure form which you will need to sign.

We wish that this process had taken much shorter to finalise than it has, however, this was not practicable given the various engagements that the Commissioner has been involved in recently.

Please contact me should you have any queries regarding this matter.

Regards  
Mduzuzi

---

**From:** Kgashane Kgomo <Kgashanek@compcom.co.za>  
**Sent:** Wednesday, November 15, 2023 10:52 AM  
**To:** Mduzuzi Msibi <MduzuziM@compcom.co.za>  
**Cc:** Andile Gwabeni <AndileG@compcom.co.za>; Thozama Linganisa <ThozamaL@compcom.co.za>  
**Subject:** FW: Permission to conduct research survey

Dear Mduzuzi

The Windows taskbar at the bottom shows the system tray with a temperature of 18°C, the time 17:09, and the date 2024/01/08.

## ANNEXURE F: EDITOR'S LETTER

JOAN HETTEMA - ENGLISH LANGUAGE EDITOR

250 Troye St., Muckleneuk, Pretoria, 0002

Date: 26 JANUARY 2024

TO WHOM IT MAY CONCERN

This is to certify that I have duly edited a dissertation in partial fulfilment of the requirements for a Master of Arts in Criminal Justice degree in the subject Criminal Justice at the University of South Africa (UNISA), with the title: *Analysis of the use of surveillance to investigate cartel conducts. A case study of the Competition Commission of South Africa, Pretoria* by Kgashane Raymond Kgomo.

I have a BA majoring in Latin and English (including isiZulu, Afrikaans and Anthropology among others) from the University of Pretoria, Honours in English Language and Literature from the University of South Africa (Unisa) and *Troisième Degré* in French from *l'Alliance Française*. (I also did some part-time studies in Mandarin and Russian).

Throughout my 37-year fulltime career and the more than twenty years since, I have been involved with the process of writing English, editing English or lecturing in the fields of Media Studies, English for Journalism and Business English at various tertiary institutions - for 11 years - (Tshwane University of Technology, Boston College, Damelin College, Rosebank College and College Campus) as well as editing documents and theses for students at universities throughout the country. I also served as judge for the annual competition of the Publications Forum of South Africa for nine years.

Yours sincerely,



J A Hettema

Joan Ann Hettema (née Thies) 072-126-5174

joanhettema9@gmail.com



## ANNEXURE G: TURNITIN REPORT



### Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author: Kgashane Raymond Kgomo  
Assignment title: Quick Submit  
Submission title: ANALYSIS OF THE USE OF ELECTRONIC SURVEILLANCE TO IN...  
File name: FINAL DISSERTATION\_KGOMO\_2024\_02\_18.docx  
File size: 916.29K  
Page count: 186  
Word count: 53,183  
Character count: 323,589  
Submission date: 18-Feb-2024 12:57PM (UTC+0200)  
Submission ID: 2297604474

THE UNIVERSITY OF BOTSWANA  
GABORONE CAMPUS  
DEPARTMENT OF EDUCATION

1.

UNIVERSITY OF BOTSWANA

1. NAME OF THE DEPARTMENT

2024

UNIVERSITY OF BOTSWANA

2024

UNIVERSITY OF BOTSWANA

2024

UNIVERSITY OF BOTSWANA

UNIVERSITY OF BOTSWANA

UNIVERSITY OF BOTSWANA

UNIVERSITY OF BOTSWANA

# ANALYSIS OF THE USE OF ELECTRONIC SURVEILLANCE TO INVESTIGATE CARTEL CONDUCTS: A CASE STUDY OF THE COMPETITION COMMISSION OF SOUTH AFRICA IN PRETORIA

## ORIGINALITY REPORT

<b>14%</b>	<b>10%</b>	<b>2%</b>	<b>7%</b>
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

## PRIMARY SOURCES

<b>1</b>	<b>stuff.co.za</b> Internet Source	<1 %
<b>2</b>	<b>centrocedec.files.wordpress.com</b> Internet Source	<1 %
<b>3</b>	<b>docplayer.fr</b> Internet Source	<1 %
<b>4</b>	<b>earf.meraka.org.za</b> Internet Source	<1 %
<b>5</b>	<b>www.law.wits.ac.za</b> Internet Source	<1 %
<b>6</b>	<b>www.werksmans.com</b> Internet Source	<1 %
<b>7</b>	<b>Submitted to South African National War College</b> Student Paper	<1 %
<b>8</b>	<b>www.mdpi.com</b> Internet Source	<1 %

## Turnitin Originality Report

Processed on: 18-Feb-2024 13:18 SAST  
ID: 2297604474  
Word Count: 53183  
Submitted: 1

Similarity Index	Similarity by Source
14%	Internet Sources: 10%
	Publications: 2%
	Student Papers: 7%

ANALYSIS OF THE USE OF ELECTRONIC  
SURVEILLANCE TO INVESTIGATE CARTEL  
CONDUCTS: A CASE STUDY OF THE  
COMPETITION COMMISSION OF SOUTH AFRICA  
IN PRETORIA By Kgashane Raymond Kgomo

< 1% match (Internet from 01-Mar-2023)

<https://stuff.co.za/2021/11/17/surveillance-laws-falling-to-protect-privacy-rights/>

[protect-privacy-rights/](https://stuff.co.za/2021/11/17/surveillance-laws-falling-to-protect-privacy-rights/)

< 1% match (Internet from 15-Dec-2022)

[https://centrocadec.files.wordpress.com/2015/07/chapter-5\\_investigative-strategy-2008.pdf](https://centrocadec.files.wordpress.com/2015/07/chapter-5_investigative-strategy-2008.pdf)

< 1% match (Internet from 17-Jan-2022)

<https://decolayer.fr/70476646-English-or-english-directorate-for-financial-and-enterprise-affairs-competition-committee.html>

< 1% match (Internet from 24-Feb-2015)

[http://saarf.marakka.org.za/Huifeesite/staff/the-huifee-group/paula-kotze-1/matse-tsoqang-phd/at\\_download/file](http://saarf.marakka.org.za/Huifeesite/staff/the-huifee-group/paula-kotze-1/matse-tsoqang-phd/at_download/file)

< 1% match ()

<http://www.law.wits.ac.za/saic/report/1to4.pdf>

< 1% match (Internet from 15-Sep-2023)

<https://www.worksmans.com/legal-updates-and-opinions/characterisation-much-ado-about-nothing/>

< 1% match (student papers from 16-May-2014)

[Submitted to South African National War College on 2014-05-16](#)

< 1% match (student papers from 26-Oct-2016)

[Submitted to South African National War College on 2016-10-26](#)

< 1% match (Internet from 26-Jan-2024)

<https://www.MDPT.COM/2021-1050/13/2/951>

< 1% match (Internet from 16-Dec-2022)

<https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=5058&context=std&httpsredir=1&of=emr->

< 1% match (Internet from 02-Feb-2024)

[https://oria.vub.be/ws/portafiles/porta/96388041/VANBRAKEL\\_DEHERT\\_Policing\\_surveillance\\_law.docx](https://oria.vub.be/ws/portafiles/porta/96388041/VANBRAKEL_DEHERT_Policing_surveillance_law.docx)

< 1% match (Internet from 06-Nov-2022)

[https://www.naac.com.na/cms\\_documents/206\\_franchising\\_report.pdf](https://www.naac.com.na/cms_documents/206_franchising_report.pdf)

< 1% match (Internet from 01-Dec-2021)

[https://etd.uam.edu.my/5785/1/1/993456\\_01.pdf](https://etd.uam.edu.my/5785/1/1/993456_01.pdf)

< 1% match (Internet from 17-Oct-2023)

[https://etd.uam.edu.my/10658/2/9903196\\_01.pdf](https://etd.uam.edu.my/10658/2/9903196_01.pdf)

< 1% match (Internet from 09-Jan-2023)

[https://www.legislation.gov.uk/eu/dir/2019/1/introduction/data\\_xhr?view=snippet&wrap=true](https://www.legislation.gov.uk/eu/dir/2019/1/introduction/data_xhr?view=snippet&wrap=true)

< 1% match (Internet from 17-Jul-2023)

<https://c.coak.info/pdf-statutory-and-regulatory-grc.html>

< 1% match (Internet from 27-Aug-2023)

[https://empe.usf.fi/dlstream/handle/123456789/30344/urn\\_nbn\\_fi\\_usf-20230991.pdf?isAllowed=y&sequence=1](https://empe.usf.fi/dlstream/handle/123456789/30344/urn_nbn_fi_usf-20230991.pdf?isAllowed=y&sequence=1)

< 1% match (Internet from 05-Apr-2022)

<https://www.oxfordlawtrava.com/view/10.1093/oxl/9780198836377.001.0001/oxl-9780198836377-chapter-1>

< 1% match (Internet from 06-Sep-2023)

<https://south.europeighbours.eu/wp-content/uploads/2022/07/Discussion-Paper-Facilitating-MSME-Access-to-Finance-Through-Fintech-The-Case-of-the-EU-PSD2-April2022-1.pdf>

< 1% match (Internet from 28-Oct-2010)

[http://www.europeanlawyer.co.uk/referencebooks\\_4\\_86.html](http://www.europeanlawyer.co.uk/referencebooks_4_86.html)

< 1% match (Internet from 06-Dec-2022)

[https://www.lexys.com/bnfiles/publicacao/anexo/20150203131310\\_challenges-ahead-of-lenency-programmes-the-brazilian-experience-journal-of-european-competition-law-e-practice-oxford-university-press-amp-fe.pdf](https://www.lexys.com/bnfiles/publicacao/anexo/20150203131310_challenges-ahead-of-lenency-programmes-the-brazilian-experience-journal-of-european-competition-law-e-practice-oxford-university-press-amp-fe.pdf)

< 1% match (Internet from 15-Jun-2023)

<https://9pdf.net/document/evl8xms-supplier-norwegian-electric-utility-business-behaviour-affects-competition.html>

< 1% match (Internet from 17-May-2023)

<https://9pdf.net/document/yd7xi3dl-control-systems-sustainability-exploring-patterns-norwegian-firm.html>

< 1% match (student papers from 21-Dec-2017)

[Submitted to University of Sussex on 2017-12-21](#)

< 1% match (Internet from 14-Mar-2023)