AN EXPLORATION OF THE USE OF FINGERPRINTS IDENTIFICATION SYSTEMS ON LATENT PRINTS OF FIRST-TIME OFFENDERS IN SOUTH AFRICA

By

NTOMBENHLE CECILIA DUBE

Submitted in accordance with the requirements for the degree of

DOCTOR OF PHILOSOPHY

In the subject

CRIMINAL JUSTICE

At the

UNIVERSITY OF SOUTH AFRICA

PROMOTER: PROF. SA MABUDUSHA

February 2023

DEDICATIONS

I dedicate this research to my family and friends who inspired me to do this study. When I felt negative, your words of encouragement gave me strength and cheered me up (calling me *doctor* while I was still struggling).

To my parents: Mom and Dad, I know I have made you proud.

To my kids Phumla, Sibahle and Bonke for allowing me time away from home though we were in the same house. Thanks to my little one who would ask *"Mom, are you reading again? Oh no, not again!"* Thank you my boy I am, all yours now.

DECLARATION

I NTOMBENHLE CECILIA DUBE, Student number 32646275 declare that the thesis on "**AN EXPLORATION OF THE USE OF FINGERPRINTS IDENTIFICATION SYSTEMS ON LATENT PRINTS OF FIRST-TIME OFFENDERS IN SOUTH AFRICA"** is my own work and that I have acknowledged all the sources used and quotations included in this thesis by means of a complete reference.

____________________________SIGNATURE

NTOMBENHLE CECILIA DUBE

DATE: 10/02/2023

ACKNOWLEDGEMENTS

I would like to honour the Power of the Almighty God for giving me the opportunity, strength, and courage to pursue this study.

- To my supervisor, Professor SA Mabudusha: your exceptional guidance, patience and support during this research is appreciated. The level of understanding you portrayed during the country`s Covid-19 pandemic, when there was no access to libraries and no cooperation from the participants was exceptional. I really appreciate your continuous commitment and support.

- To my Master of Arts supervisor, Dr RJ Mokwena, Thank you for your assistance whenever I called for help, it is highly appreciated.

- My greatest appreciation goes to the University of South Africa (UNISA) Student Funding, Thank you for enabling me to complete my studies, without you I wouldn’t have made it. Thank you.

- To the South African Police Service (SAPS), Local Criminal Record Centre (LCRC), Department of Correctional Services (DCS), Department of Justice and Constitutional Development (DOJ & DC), Integrated Justice System Unit (IJSU) thank you for giving me permission to conduct this research.

- To the participants and their supervisors, thank you for your time and Patience. I value and appreciate your input and assistance.

ABSTRACT

The South African Police Service`s fingerprints system cannot identify latent prints of innocent people or first-time offenders, it can only identify persons who had previously been charged. Therefore, the purpose of this study was to explore the use of fingerprint systems to identify latent prints of first-time offenders. A literature review was conducted to provide a background to the topic and to highlight international standards when identifying offenders by means of fingerprints uplifted from the crime scene. The research approach used in this study is a qualitative approach with a case study research design to investigate the study topic through the experiences of officials who are working with the fingerprint system.

Nineteen interviews were conducted in this study. The sample used was small because of the shortage of fingerprint experts. The findings of this study revealed that the Local Criminal Record Centre (LCRC) cannot identify latent prints of first-time offenders and that many case dockets are still closed with positive fingerprints because of the lack of identification information. The implemented Person Identity Verification Application (PIVA) system which integrates the fingerprint systems from a few government departments cannot identify latent prints. The PIVA system is placed in police stations not in the LCRC as its aim is to assist the criminal justice system (mainly the courts) with case management and the movement of the offender.

The study therefore recommended the implementation of a system that will allow LCRC experts to identify first-time offenders who are not on LCRC database. It also recommended that the SAPS should have a database of fingerprints information from the citizens who are applying for security checks. This database can store information separately from that of the criminal records and will be accessed to search fingerprints information not found on the Automated Fingerprints Identification System (AFIS). To avoid poorly obtained fingerprints as it has been a concern of all participants, police stations should be issued with digital fingerprints scanners.

Key concepts: Crime scene, data integration, evidence, fingerprints, latent prints, offender.

NSOTHO

NYAKIŠIŠO YA TŠHOMIŠO YA DISESTEMO TŠA TLHAOLO YA DIKGATIŠO TŠA MENWANA GO DIKGATIŠO TŠEO DI UTILWEGO TŠA BASENYI BA LEKGA LA MATHOMO KA AFRIKA BORWA

KAKARETŠO

Sestemo ya dikgatišo tša menwana ya Tirelo ya Maphodisa ya Afrika Borwa ga e kgone go hlaola dikgatišo tše di utilwego tša batho bao ba se nago molato goba basenyi ba mathomo, e ka hlaola fela batho bao ba kilego ba latofatšwa peleng. Ka fao, morero wa nyakišišo ye e be e le go nyakišiša tšhomišo ya disestemo tša dikgatišo tša menwana go šupa dikgatišo tše di utilwego tša basenyi ba lekga la mathomo. Go dirilwe tshekatsheko ya dingwalo go fa setlogo sa hlogotaba le go gatelela maemo a boditšhabatšhaba ge go hlaolwa basenyi ka dikgatišo tša menwana tšeo di tšeerwego lefelong la bosenyi. Mokgwa wa nyakišišo wo o šomišitšwego mo nyakišišong ye ke mokgwa wa khwalithethifi wo o nago le tlhamo ya kheisisetati ya nyakišišo go nyakišiša hlogotaba ya nyakišišo ka maitemogelo a bahlankedi bao ba šomago ka sestemo ya dikgatišo tša menwana.

Dipoledišano tše lesomesenyane di dirilwe mo nyakišišong ye. Sampole yeo e šomišitšwego e be e le e nnyane ka baka la tlhaelelo ya ditsebi tša dikgatišo tša menwana. Dikutollo tša nyakišišo ye di utollotše gore Senthara ya Direkoto tša Bosenyi ya Selegae (LCRC) ga e kgone go hlaola dikgatišo tše di utilwego tša basenyi ba lekga la mathomo le gore ditokete tše ntši tša melato di sa tswalelwa ka dikgatišo tša menwana tše phosethifi ka lebaka la go hloka tshedimošo ya tlhaolo. Sestemo ye e phethagaditšwego ya Kgopelo ya Netefatšo ya Boitsebišo bja Motho (PIVA) yeo e kopanyago disestemo tša dikgatišo tša menwana go tšwa dikgorong tše mmalwa tša mmušo ga e kgone go hlaola dikgatišo tše di utilwego. Sestemo ya PIVA e bewa ka diteišeneng tša maphodisa e sego ka LCRC ka ge maikemišetšo a yona e le go thuša tshepedišo ya toka ya bosenyi (kudukudu dikgorotsheko) ka taolo ya melato le tshepetšo ya mosenyi.

Bjalo nyakišišo e šišinya phethagatšo ya sestemo yeo e tlago dumelela ditsebi tša LCRC go šupa basenyi ba lekga la mathomo bao ba sego tatapeising ya tshedimošo ya LCRC. E šišinya gape gore SAPS e swanetše go ba le tatapeisi ya tshedimošo ya dikgatišo tša menwana go tšwa go badudi bao ba dirago dikgopelo tša ditlhahlobo tša tšhireletšo. Tatapeisi ye e ka boloka tshedimošo ka thoko go ya direkoto tša bosenyi gomme e tla šomišwa go nyaka tshedimošo ya dikgatišo tša menwana tšeo di sa hwetšwego go Sestemo ya Boitsebišo ya Dikgatišo tša Menwana ya go Itiriša (AFIS). Go efoga dikgatišo tša menwana tšeo di sa hwetšwego gabotse ka ge e bile taba yeo e tshwenyago bakgathatema ka moka, diteišene tša maphodisa di swanetše go fiwa disekena tša dikgatišo tša menwana tša titšithale.

Dikgopolo tše bohlokwa: Lefelo la bosenyi, kopantšho ya datha, bohlatse, dikgatišo tša menwana, dikgatišo tše di utilwego, mosenyi.

ISIZULU

UKUHLOLWA KOKUSETSHENZISWA KWEZINHLELO ZOKUZAZISA ZEZIGXIVIZO ZEMINWE OKUCASHILE KWABEPHULA UMTHETHO OKOKUQALA NGQA ENINGIZIMU AFRIKA

ISIFINGQO

Uhlelo lwezigxivizo zeminwe loMbutho Wamaphoyisa aseNingizimu Afrika (eyaziwa ngokuthi yi-SAPS) alukwazi ukukhomba imibhalo-ecashile yabantu abangenacala noma abaphula umthetho okokuqala ngqa, lungakwazi kuphela ukukhomba abantu ababebekwe amacala ngaphambilini. Ngakho-ke, inhloso yalolu cwaningo bekuwukuhlola ukusetshenziswa kwezinhlelo zokugxivizwa kweminwe ukuze kutholakale imibhalo-ecashile yalabo abaqala ngqa ukuphula umthetho. Ukubuyekezwa kwemibhalo kwenziwa ukuze kuhlinzekwe isizinda esihlokweni kanye nokugqamisa izindinganiso zamazwe ngamazwe lapho kuhlonzwa izephula-mthetho ngokusebenzisa izigxivizo zeminwe ephakanyiswe endaweni yesigameko. Indlela yocwaningo esetshenziswe kulolu cwaningo iyindlela esezingeni eliphezulu enomklamo wocwaningo lwesihloko ukuze kuphenywe isihloko socwaningo ngokusebenzisa ulwazi lwezikhulu ezisebenza ngohlelo lweminwe.

Kulolu cwaningo kwenziwa izinhlolokhono eziyishumi nesishiyagalolunye. Isampula esetshenzisiwe ibincane ngenxa yokushoda kochwepheshe bezigxivizo zeminwe. Okutholwe kulolu cwaningo kuveze ukuthi i-Local Criminal Record Centre (LCRC) ayikwazi ukuhlonza imibhalo-ecashile yalabo abaqala ukuphula umthetho nokuthi amadokodo amaningi asavaliwe aneminwe emihle ngenxa yokushoda kweminininingwane yawo. Uhlelo olusetshenziswayo lwe-Person Identity Verification Application (PIVA) oluhlanganisa izinhlelo zezigxivizo zeminwe ezivela eminyangweni embalwa kahulumeni azikwazi ukuhlonza amaphrinti acashile. Uhlelo lwe-PIVA lubekwe eziteshini zamaphoyisa ezingekho kwi-LCRC njengoba inhloso yalo iwukusiza uhlelo lwezobulungiswa bobugebengu (ikakhulukazi izinkantolo) ngokuphathwa kwamacala kanye nokuhanjiswa kwabephuli mthetho.

Ngakho-ke lolu cwaningo luncome ukuqaliswa kohlelo oluzovumela ochwepheshe be-LCRC ukuthi bahlonze abaphula umthetho okokuqala ngqa abangekho kusizindalwazi se-LCRC. Iphinde yancoma ukuthi i-SAPS kufanele ibe nesizindalwazi solwazi lwezigxivizo zeminwe ezakhamuzini ezifaka izicelo zokuhlolwa ezokuphepha. Lesi sizindalwazi singagcina imininingwane ngokuhlukene naleyo yamarekhodi obugebengu futhi izofinyelelwa ukuze kuseshwe ulwazi lwezigxivizo zeminwe olungatholakali Ohlelweni Lokuhlonza Izigxivizo Zeminwe Ezizenzakalelayo (eyaziwa nge-AFIS). Ukuze kugwenywe izigxivizo zeminwe ezingatholakalanga kahle njengoba kube ukukhathazeka kwabo bonke ababambiqhaza, iziteshi zamaphoyisa kufanele zinikezwe izithwebuli zeminwe zedijithali.

Amagama abalulekile: Indawo yobugebengu, ukuhlanganiswa kweminingwane, ubufakazi, izigxivizo zeminwe, imibhalo-ecashile, isephula umthetho.

ACRONYMS AND DESCRIPTIONS

ABIS	Automated Biometric Identification System
AFIS	Automated Fingerprints Identification System
APB	Advisory Policy Board
BACS	Basic Access Control System
CJIS	Criminal Justice Information Services
CJS	Criminal Justice System
CPA	Criminal Procedure Act
CRC	Criminal Record Centre
DCS	Department of Correctional Service
DHA	Department of Home Affairs
DNA	Deoxyribonucleic Acid
DOJ & CD	Department of Justice & Constitutional Development
DOT	Department of Transport
DPP	Director of Public Prosecutions
DSD	Department
EPIC	Electronic Privacy Information Center
FBI	Federal Bureau of Investigation
HANIS	Home Affairs National Identification System
IAFIS	Integrated Automated Fingerprints Identification System
IJSB	Integrated Justice System Board
IJS	Integrated Justice System
IIMS	Integrated Inmate Management System
LCRC	Local Criminal Record Centre
NCPS	National Crime Prevention Strategy
NCIC	National Crime Information Centre
NGI	Next generation Identification
POPI Act	Protection of Personal Information Act
PIVA	Person Identity Verification Application
PMG	Parliamentary Monitoring Group
RICA	Regulation of Interception of Communications Act
SAPS	South African Police Service
USA	United State of America

LIST OF FIGURES

TABLE OF CONTENTS

CHAPTER ONE: GENERAL ORIENTATION

1.1. Introduction

Newburn, Williamson and Wright (2007: 320) are of the opinion that the transfer principle means that every time a person makes physical contact with anything it results in an exchange of physical materials such as fingerprints. It is therefore obvious that the access to and use of effective and efficient fingerprint identification systems by the police service is of vital importance.

The South African Police Service (SAPS) has a forensic unit which consists of qualified fingerprints experts responsible for the identification, comparison and verification of fingerprints. This forensic unit is called the Local Criminal Record Centre (LCRC). This centre verifies fingerprints obtained from suspects for a criminal record check which is necessary for court proceedings. These experts also compare and identify latent prints uplifted from the crime scene as evidence to detect the offender. Latent prints are found at residential places and business places during burglaries, and they are also found on recovered stolen properties including vehicles. The LCRC cannot identify latent prints of a first-time offender, as their database only keeps information of people who were arrested and charged before.

Section 15D (4) (b) of Criminal Law (Forensic Procedure) Act No. 6 of 2010 stated that the National Commissioner and the Director General of the Department of Transport (DOT), Department of Home Affairs (DHA) and the Department of Correctional Services (DCS), must under the chairpersonship of the National Police Commissioner develop standard operational procedures regarding access to the databases and implementation of safety measures to protect the integrity of information.

This implies that the SAPS and other government departments must develop a standard operating procedure that will assist the police in identifying latent prints of first-time offenders, that in turn will assist other departments in resolving their issues where sharing of information is concerned. The White Paper on Remand Detention Management in South Africa (2014: 14) pointed out the challenges faced by the

Department of Correctional Services because departments are using separate systems. Challenges mentioned include the use of multiple identities by remand detainees; redundant information; the slow process of verification of identity with the DHA; the lack of access to systems of other departments and an inadequate system for the identification of accused within the Criminal Justice System. In the light of the above discussion, the study intended to explore the use of fingerprints systems for the investigation of latent prints of first-time offenders.

1.2. Problem Description

Porte (2010:12) suggested that the problem statement is the section which helps the reader to situate himself or herself in the area in which the problem is found. Porte (2010:12) further mentioned that this section might aim to rationalise the problem and explain why that problem is in fact a problem. Gygi, DeCarlo and Williams (2005: 76) explained that the problem statement clarifies the situation by identifying what needs to be improved, the level of the problem and where it is occurring. The identified problem in this study is that the SAPS specifically the Local Criminal Record Centre (LCRC) does not have access to other departments` fingerprint systems, which are useful for a forensic investigative search. This is a problem because some cases where latent prints are involved remain unresolved because suspects are unknown, as they are not on the LCRC database.

As mentioned above that Section 15D (4) (b) of Criminal Law (Forensic Procedure) Act No 6 of 2010 suggested the sharing of databases between the Department of Transport (DOT), the Department of Home Affairs (DHA) and the Department of Correctional Services (DCS). Similarly, the White Paper on Remand Detention Management in South Africa (2014: 2) recommended the integration of systems between critical partners, namely the South African Police Service (SAPS), the Department of Social Development (DSD), the National Prosecuting Authority (NPA), the Department of Justice and Constitutional Development (DOJ & CD) and the Legal Aid South Africa. However, for the purpose of this study the researcher intended to consider the DHA and DCS because they work closely with SAPS.

Currently, a docket, with positive latent prints but with no information of the suspect is closed with a brought forward date for the docket to be reopened after five years.

In the fifth year, the case docket is reopened; and an attempt to find the suspect is made and if he/she cannot be traced the case docket is closed again. Such fingerprints are archived at the Local Criminal Record Centre (SAPS National Instruction 325, 2012). The SAPS National Instruction 325 (2012: 6) explained that if the same fingerprints or a suspect is involved in different cases, but the identity is still unknown the docket must be kept for ten years before it can be destroyed. Therefore, to fight the scourge of unresolved cases, the Criminal Law (Forensic Procedure) Amendment Act No. 6 of 2010 was enacted.

The Criminal Law (Forensic Procedure) Amendment Act No. 6 of 2010 was enacted to give the SAPS access to the fingerprint systems of other departments such as the DOT, DHA and DCS that will assist in identifying unidentified suspects. In support of this section of the legislation, the SAPS management, during the Strategic Management in 2010 (SAPS Strategic Plan, 2010/2014: 15) proposed to improve the collection of evidence at crime scenes. The SAPS Strategic Management added that the sharing of databases e.g., with the Department of Home Affairs, will strengthen the capacity of the SAPS in identifying individuals involved in crime.

Subsequent to this Act, the Integrated Justice System (IJS) implemented the PIVA system (Person Identification Verification Application) which integrates information from government departments. The Chairperson of IJSB explained to the police committee that PIVA solution entails instant verification of SA ID`s via the DHA HANIS/ABIS system using biometric devices (Leseba, 2015). However, this system also cannot identify latent prints of first-time offenders. The case dockets with fingerprints of first-time offenders are still closed with no lead to suspects because the suspects` information is not available on the LCRC database known as the Automated Fingerprints Identification System (AFIS).

1.3. Background of the Study

The former Justice Minister Hadebe, (as cited in News24, 2010) indicated that DHA fingerprint system previously known as the Home Affairs National Identification System (HANIS) now known as ABIS, contained fingerprints of over 41 million South African citizens and over 2.5 million foreigners. The SAPS Annual Report (2015/2016: 149) confirmed that the Department of Home Affairs assists the SAPS to identify fingerprints of circulated persons (including missing and wanted persons) and vehicles. The Department of Home Affairs system is indeed assisting the police with identification of circulated persons in cases where a warrant of arrest is issued, the person is missing, or an unknown person is found dead.

Regardless of the ABIS system in place, suspects who commit crime for the first time (first-time offenders) and who leave their fingerprints on crime scenes are still not identified through the DHA's ABIS system. This is because DHA assists with circulated persons (people who are recorded on SAPS system as wanted) who are wanted because a warrant of arrest had been issued by court or in the case of a missing person where the family provided information on such a missing person. SAPS Annual Report (2020/2021: 202) explained that SAPS circulates a wanted person where a warrant of arrest has been issued by the court on an offence that he/she is sought for and hiding from law enforcement. The Report further explained that a wanted person can also be a suspect who is sought, but not arrested and whose his/her particulars were known and used to circulate him/her as a wanted.

The police also send fingerprints of the unknown deceased to the National Criminal Record Centre for identification because the Local Criminal Record Centre does not have such information on their database (Evert, 2011: 58). They cannot identify an unknown deceased if he/she has never been arrested and charged as they do not have that function. Evert (2011: 58) confirmed that if a body has not been identified within seven days, the fingerprints taken are submitted to the Criminal Record Centre (CRC) and then to the DHA for identification.

- The DHA has upgraded the HANIS system to ABIS to enable multimodal biometrics and advance search capabilities for identification and verification.

> The ABIS will run on the new technology platform and enable fingerprint verification and identification for both citizens and known foreign nationals in the country (DHA Annual Report 2017/2018: 67). Its powerful search capabilities will increase the response rate and the ability to do latency searches/ partial fingerprints (DHA Annual Report 2017/2018: 67).

- This implies that the DHA is assisting SAPS with latent fingerprints search of any crime reported, however, some cases are still closed with positive fingerprints due to lack of suspects` information. Access to the DHA fingerprint information is still limited to all unidentified deceased and other priority or serious crimes. The LCRC does not have access to Home Affairs, nor do they have access to the PIVA system where information of all South African citizens is kept. It has been mentioned earlier that there is a system available with integrated fingerprint information namely the PIVA system as indicated by Leseba (2015), but it cannot identify latent prints, as it is not available in the LCRC.

According to Mofokeng and de Vries (2012: 28) many cases go undetected because of the poor criminal investigation capabilities of the police, especially in respect of forensic investigation. The community believes that when fingerprints are found on a crime scene; police will find the offender, but the community does not know that SAPS can only find criminals who are recorded on their database. They are not aware that SAPS does not have access to the DHA fingerprint system to identify someone who has committed a crime for the first time.

The former Justice Minister, Jeff Hadebe (as cited in News24, 2010), mentioned that the Criminal Law (Forensic Procedure) Amendment Act No. 6 of 2010 was intended to deal with two pivotal aspects of forensic crime fighting, namely the fingerprint and Deoxyribonucleic Acid evidence. Though the Minister pointed out two pivotal aspects, the Criminal Law (Forensic Procedure) Amendment Act No. 6 of 2010 was only about fingerprints investigation and the DNA Amendment Act was enacted later in year 2013, being the Criminal Law (Forensic Procedure) Amendment Act No. 37 of 2013. Both Acts elaborate on the procedures to be followed in each investigation of both pivotal aspects.

In his speech (as cited in News24, 2010), the Minister pointed out that SAPS had access only to the fingerprints stored in the SAPS AFIS system and they do not have direct access to the Home Affairs system where the fingerprints of 41 million citizens and 2.5 million foreigners are kept. The Minister further quoted statistics by mentioning that, the criminal justice system review office had found that 52% of perpetrators remained undetected in 2006/07 and 46% of perpetrators also remained undetected in 2007/08; suggesting that the new Act will reduce the number of undetected perpetrators. However, to this date these cases are still not detectable as there have been no changes in the LCRC database. Examples of crimes that rely on fingerprints for identification and apprehension of suspects are burglary to residential premises, burglary to business premises, theft of motor vehicles and theft from motor vehicles.

In the SAPS Annual Report 2020/2021 (2021: 201) several cases where suspect identification required fingerprint information were not taken to court. Only a few of the reported cases could be detected and taken to court. The following crime categories extracted from the SAPS Annual Report 2020/2021 (2021: 201) indicated the total number of complaints reported during 2020/2021 nationally and the total number of complaints which went to court during 2020/2021.

Figure 1: Number of Complaints reported, and cases taken to Court during 2020/2021

Crime Categories	Total Number of Complaints Reported	Detection Rate	Total Complaints in Court
Burglary (Residential Premises)	159 907	39 257	24 749
Burglary (Business Premises)	65 564	13 758	9 608
Theft of Motor Vehicle and Motorcycle	35 078	4 604	5 452
Theft from Motor Vehicle	83 291	12 448	6 048
Total	343 840	70 067	45 857

Therefore, the possibility of police having access to the fingerprint information of first-time offenders can enhance the quality of the investigations process by the police service in the country. Out of 343 840 reported cases only 70 067 suspects were detected.

1.4. Demarcation of the Study

This study was conducted in two provinces in South Africa, Gauteng and KwaZulu Natal. KwaZulu Natal, Durban Central SAPS had more than two thousand cases which required fingerprints investigation, which were reported during the 2018/2019 financial year (SAPS Crime Statistics 2018/2019, 2019: 139). This made Durban Central one of the areas in the country with a high number of cases that require fingerprint comparison and identification. It is evident that there is still a challenge with the property related crime since the statistics for 2022 first quarter shows that the problem still exists. According to SAPS Crime Statistics 2021/2022 (2022: 61) Durban Central SAPS still the highest number of property related crimes reported. Durban is also close to the researcher' place of residence and as such it allowed the researcher easy access to other participants. However there was a need to obtain more specialised data from other departments in the country and more information was obtained from the Gauteng province.

1.5. Research Aim and Objectives

According to De Vos, Strydom, Fouchè and Delport (2002:107-119) the aim of the study is like a dream that one imagines, and the objective is the step one has to take one by one within a certain timespan in order to attain the dream.

The aim of this study was:

- To explore how the fingerprints identification systems can be used to enhance the investigation of latent prints of first-time offenders.

The objectives set for this study were:

- To describe the process followed by the LCRC in identifying unknown suspects when latent prints are found at the crime scene.
- To explore the challenges faced by the SAPS LCRC in identifying first-time offender on fingerprints found at the crime scene.
- To investigate the role that can be played by departments such as the DHA and the DCS to assist the SAPS in identifying latent prints of first-time offenders.
- To highlight some of the international best practices on the identification of first –time offenders by means of fingerprints systems.
- To formulate recommendations based on the findings.

1.6. Research Questions

Porte (2010:43) suggested that the reader should be able to use the research questions to focus on the study, as they give direction and make it easier to follow. De Vos *et al.* (2002:107 & 119) mentioned that one aim of the qualitative method is to discover important questions, processes, and relationships.

The main research question of this study is:

- How can the sharing of fingerprints systems in South Africa be used to enhance the investigations of latent prints of first-time offenders?

The following sub-questions will assist the researcher to answer the main question**:**

- Which process is followed by the LCRC in identifying unknown suspects when latent prints are found at the crime scene?

- What challenges are faced by the SAPS/LCRC in identifying first-time offender whose fingerprints were found at a crime scene?

- Which role can be played by other departments within the CJS to assist the SAPS in identifying first-time offenders` latent prints?

- What are the international best practices on the identification of offenders by using fingerprints?

1.7. Study Significance

Terre Blanche, Durreihm and Painter (2011: 540) mentioned that the research question derives from different reasons including a personal speculation and experience.

1.7.1. South African Police Service

In this study the researcher was motivated by her personal experience as a former police investigator within the SAPS who experienced that many cases remained unresolved because suspect particulars were unknown. In addition to that, this study may contribute not only to academic body of knowledge but may also enhance the investigation of criminal cases in the country. Consequently, that will restore public confidence in the police investigations within the country.

1.7.2. Department of Correctional Services

This study will contribute to the coordination of resources and improved cooperation between the SAPS and the Department of Correctional Services. For example, sometimes the police encounter cases where they are looking for a suspect and that suspect has already been arrested and is serving a sentence in one of the South African correctional centres under a different name. Thus, the lack of access to databases containing offenders is a challenge for the police as they do not know who has already been arrested. The Department of Correctional Services will also benefit in terms of information sharing between them and the police. As mentioned in the White Paper on Remand Detention Management in South Africa (2014: 14), the departments face challenges because they use separate systems.

1.8. Definition of Key Concepts

De Vos *et al.* (2002: 30) mentioned that a concept expresses an abstraction formed by generalisation from particulars that are usually similarities. The researcher provides understanding and meaning to key words for the description of the phenomenon in this study. The following key concepts are used in the study as key words, and therefore they are clearly defined to describe the scope and nature of the study. The key concepts are defined as follows:

1.8.1. Crime Scene

Shaler (2012: 13) defined a crime scene as the place where the participants of the crime meet in time and space. According to this definition, the participants of the crime scene can also be suspects, the witnesses and or the victims. The crime scene can be in more than one place; for instance, where the crime started and where it ended. In a murder case, the crime scene can be where the victim was abducted e.g., the house where the victim was killed or where the body was buried or dumped. The crime scene (as in robbery case) can also be more than one location, starting from where the robbery took place and to where the money or the property was recovered.

1.8.2. Criminal

Henry and Lanier (2001: 20) defined the criminal as a person who has behaved in some way prohibited by criminal law and remains a criminal whether he/she has been convicted of the crime or not and whether this crime is known only to himself/herself or to anyone else. In this case, the word “criminal” is commonly used for any person who committed a crime whether identified or not, and whether convicted or released from a correctional centre. The word criminal is informally used by the community to call out or rank a person involved in criminal activity even if such person was never charged with any crime.

1.8.3. Data Integration

Data integration is defined as the set of processes used to extract or capture, restructure, move, and load or publish data in either operational or analytic data stores, in either real time or in batch mode (Giordano, 2011). In this study data integration is the sharing of information or people`s particulars of innocent people including criminal record information. Data integration will assist government departments in obtaining authentic information on individuals under scrutiny and it will prevent people from giving different identities in different government departments. For instance, a person applying for a grant support may claim that he is unemployed, but his employment status will be revealed via the Department of Employment and Labour.

1.8.4. Evidence

Siegel, Knupfer, and Saukko (2000: 28) and Shaler (2012: 25) regarded evidence as information, whether personal testimony, documents, or material objects, that is given in a legal investigation, to make a fact or proposition. Shaler (2012:25) pointed out that evidence can be defined in two ways, one when it is perceived as evidence during the scene investigation and the other when it is admitted in the legal proceedings. This implies that it can be evidence but not all evidence involved in a case is admissible in legal proceedings. Harber and Harber (2009: 5) suggested that all judges who make a ruling to admit fingerprint evidence treat identification based on fingerprint comparison as 100 percent certain.

1.8.5. Fingerprints

Shaler (2012: 212) explained that fingerprints at a crime scene result from someone touching a surface and leaving a residue. Shaler (2012: 212) further explained that the chemical of that residue is a mixture of secretions from sweat glands present in the skin as well as from exogenous contaminations, blood oils, cosmetics and so on. Identifying the fingerprint does not mean that the suspect has been found but it means that there may be a lead to the suspect. Fingerprints found at the crime scene may be of the people frequenting such place like workers, residents and maybe passers-by. Such fingerprints can be used as elimination prints to isolate the suspect`s prints which were not supposed to be found at the crime scene.

Evidence of fingerprints can be found in more than one crime scene for instance in a murder case, fingerprints can be found where the victim was abducted, where the victim was killed, and where the victim was buried or dumped. As indicated by Shaler (2012: 212) above, different forms of fingerprints can be found on any surface like metal, papers found on crime scene and any other surfaced items. If fingerprints have been found, but the suspect cannot be identified the docket is then closed as undetected. The National Instruction 325 as cited in the Consolidation Notice (2012: 3), instructed that whenever the investigation of a case has failed to disclose the perpetrator and it is further clear that an offence was actually committed, the case docket must invariably be closed as “Undetected”.

The Criminal Law (Forensic Procedure) Act 6 of 2010 states that its purpose is:

- To amend the SAPS Act 1995 to regulate the storing and the use of fingerprints.
- To provide for the keeping of databases and to allow for comparative searches against other databases.
- To make provision for the development of standard operating procedures regarding access to the databases of other state departments.
- To further regulate the powers in respect of fingerprints and body-prints for investigation purposes.

The Purpose of Criminal Law (Forensic Procedure) Act No. 6 of 2010 has a number of regulations that add to the above-mentioned to regulate the investigation of fingerprints which will assist in enhancing the investigation of fingerprints including latent prints.

1.8.6. Latent prints

Kriel (2011) mentioned the latent print as one of the forms of prints indicating that they are an impression which is produced by the ridged skin, known as friction ridges, on human fingers, palms, and soles of the feet. These fingerprints are analysed and compared to known fingerprints of individuals to make identifications or exclusions (Kriel, 2011).

1.8.7. Offender

Holtzhausen (2012: 6) described the offender as a person who has a tendency for criminality; that is the state, quality, and fact of being criminal. This implies that offender is the term used for a person who is frequently committing crime and whose identity is not known, the same as term criminal discussed above. Where fingerprint evidence is concerned, the first-time offender cannot be identified by the LCRC fingerprint system but an offender who was arrested before and charged can be identified by their fingerprint system. This study is concerned about first-time offenders who cannot be identified by the police system.

1.8.8. Suspect

According to Van Rooyen (2008: 14), a suspect is a person who law enforcement officers have reason to believe may have committed a crime. To identify a suspect in this study calls for a thorough investigation since not all fingerprints found on the crime scene are of the person who committed the crime. In addition, being a suspect does not mean that the person has indeed committed a crime; a person can also be eliminated as a potential suspect by the investigation or individualisation where more than one suspect have been involved in the case. Harber and Harber (2009: 54) stated that a skilled crime scene investigator predicts the location, the characteristics of the prints, and the specific fingers in the prints that he will find, given the perpetrator`s intentions at that location.

1.9. Systems Theory as Framework of the Study

Anfara and Mertz (2006: xxvi) defined a theoretical framework as any empirical or quasi-empirical theory of social and psychosocial processes at a variety of levels that can be applied to the understanding of phenomena. This study is underpinned by the systems theory because it discusses how the barriers within the organisation can impact negatively on the productivity of the employees.

Mele, Pels and Polese (2010: 126) described systems theory as an interdisciplinary theory about every system in nature, in society and in many scientific domains as well as a framework with which we can investigate phenomena from a general approach. The LCRC is a department which relies on a number of systems in order to work effectively. Before a case gets to the LCRC, it passes a number of departments, from the charge office to the first responder, the fingerprints officers uplifting the fingerprints and then the experts who compare fingerprints. A number of systems which are guarded by rules and regulations on their operation and same rules and regulations sometimes hinder smooth operations, for example, the Protection of Personal Information Act No. 4 of 2013 sometimes obstruct the effectiveness of investigations.

Many organisations have systems which may cause loss or low to zero productivity. Employees struggle to keep up with a system until they abandon any attempts of keeping up if management does not improve. Having the community complaining about services, while employees know they have tried their best, but the situation is beyond their control, is really demotivating and can result in future neglect. Investigations based on fingerprint detection, but lacking fingerprint information is the outcome of scarce resources; a lack which demoralises other employees.

Jali (2015: 24) pointed out that there are a number of factors which contribute to the non-performance of employees. Remuneration is a factor which has an impact on employees’ productivity, supervisors` behaviour towards employees as well as absenteeism as contributing factors towards non-performance. Similarly, Assiri (2016:118) identified a list of factors that may lead to loss of productivity namely, the lack of skills to use technology, poor work and employees’ management skills, inadequate resources (such as vehicles, offices or computers) and workplace stress (due to work overload). Other contributing factors which are caused by the organisation itself include: shortage of staff, causing backlog; rules and policies which affect employees` productivity and skills development programmes, Training and motivation can also impact negatively on the productivity of employees. These are systems designed to guide organisations, but sometimes work against organisations. This theoretical framework guided the researcher in identifying those systems or organisational factors that could enhance or hamper the success of police investigations.

1.10. Chapters Layout

Chapter 1: General Orientation. This chapter will discuss the study problem, the research aim and the rationale for this study.

Chapter 2: Research methodology. The focus of this chapter is on the research methods the researcher will adopt to achieve the aim of this study.

Chapter 3: In this chapter the discussion focuses on South African legislations governing the use and sharing of fingerprints. It will be explained how, when, why and by whom people's fingerprints can be used, as well as to discuss the purpose.

Chapter 4: The sharing of fingerprint systems between government departments for the investigation of latent prints of first-time offender. The discussion in this chapter is on the use of fingerprints within the Criminal Justice systems in and outside South Africa.

Chapter 5: Presentation of research findings, this chapter focuses on presenting the findings of the research. These are the answers to the research questions posed to research participants.

Chapter 6: Interpretation of research findings. This chapter discusses the themes and sub-themes to indicate the relevance of this study with the research objectives. The meaning and understanding of the researcher on the research findings is discussed in this chapter.

Chapter 7: Recommendations and conclusion. This chapter will summarise the entire research study, make recommendations and present conclusion to this study.

1.11. Study Limitations

There are three main limitations encountered in this study, namely:

1.11.1. **Access to information:** The Department of Home Affairs did not participate in the study, they indicated that this study investigates sensitive issues and therefore they could not participate. Therefore, the study relied on literature, published speeches, journals, news, and participants` views.

1.11.2. **Collection of data:** The outbreak of Covid-19 pandemic affected collection of information by means of face-to-face discussions and observations, and as a result, many participants responded to questions emailed to them, especially those who were outside the researcher`s province.

1.11.3. **Availability of fingerprint experts in the country:** The SAPS/ LCRC fingerprint experts tasked to work with the Department of Home Affairs to identify unidentified bodies are based at the National LCRC and they are fewer than five. Subsequently, the researcher was given two participants to participate in the study.

1.12. Summary

This chapter discussed the research problem that triggered the study. The problem discussed is that the Local Criminal Record Centre`s fingerprint system operating in the South African Police Service cannot identify latent prints of first -time offenders as the system can only identify previously charged persons. The researcher discussed the aim and the objectives of this study and also the method used to answer the research questions. Key concepts used were explained and discussed. This chapter discussed the purpose of this study and the theoretical framework to enhance the understanding of the research problem. The research methodology which was used in this study will be discussed in the next chapter.

CHAPTER TWO: RESEARCH DESIGN AND METHODOLOGY

2.1. Introduction

This chapter discussed the research methodology, the research approach and the design used in this study. The aim and the objectives discussed from the previous chapter, paved a way for the research methodology conducted for this study. The researcher adopted to achieve the aim of this study. A case study design was adopted because it allowed the researcher to understand how the Automated Fingerprint Identification System (AFIA), HANIS (Home Affairs National Identification System), ABIS (Automated Biometrics Identification System), IIMS (Integrated Inmate Management System) and PIVA (Person Identity Verification Application) function as well as their limitations. The researcher conducted this study using the qualitative research approach. Data were collected from participants by means of semi-structured interviews. The data analysis was conducted using a thematic analysis and a deductive approach.

2.2. Research Design

A research design is defined as a plan of conducting a study (Creswell, 2013: 49). Research design is a type of inquiry within qualitative, quantitative, or mixed method approaches that provide specific direction for procedures in a research study (Creswell, 2013: 12). De Vos, Strydom, Fouché and Delport (2011: 312) and Creswell (2013: 13) mentioned the types of research designs for qualitative research design as narrative ethnography, phenomenology, grounded theory and case study. In this study the researcher used a case study research design as De Vos *et al.* (2011: 320) explained that since qualitative researchers are primarily interested in the meaning subjects give to their life experiences, those researchers have to use some form of case study to immerse themselves in the activities of people to familiarise themselves with their social worlds.

Therefore, a case study design was adopted in this study because it allowed the researcher to understand how the AFIS, HANIS, ABIS, IIMS and PIVA fingerprint systems function and also to their limitations. Babbie and Mouton (2012: 281) indicated that case studies take perspective into account and attempt to understand the influences of multilevel social systems on subjects’ perspectives and behaviours. The fingerprint systems from two departments amongst the criminal justice system departments were scrutinised. The case study explained the process that was conducted during this research in the investigation of the SAPS and DCS operations in their different fingerprint systems. De Vos *et al.* (2011: 320) identified three types of case study a researcher may implement to conduct a study; namely descriptive, explanatory and collective case studies. The researcher therefore used a descriptive case study as De Vos *et al.* (2011: 321) indicated that a descriptive case study, also called an intrinsic case study, strives to describe, analyse, and interpret a phenomenon. The researcher intended to describe and analyse the sharing of fingerprints information between the South African government departments to enhance the investigation of latent prints of first-time offenders.

2.3. Research Approach

The researcher conducted this study using the qualitative research approach as De Vos *et al.* (2011: 91) mentioned that a qualitative approach aims to answer research questions that provide a more comprehensive understanding of a social problem from an intensive study of few people. Babbie and Mouton (2012: 270) pointed out that the primary goal of studies using qualitative approach is to describe and understand rather than explain human behaviour. Similarly, De Vos *et al.* (2011: 91) explicated that the qualitative researcher is concerned with understanding through naturalisation observation rather than controlled measurement. According to De Vos, Strydom, Fouché and Delport (2002: 78) qualitative research, in the broadest sense, refers to research that elicits accounts of meaning, experience, or perceptions. This approach was chosen for this study to enable the researcher to understand the study topic through the experiences of officials who are using AFIS (the SAPS fingerprints system), IIMS (Correctional Services fingerprint system) as well as PIVA (the system implemented by the Integrated Justice System).

2.4. Target Population and Sampling

This study focus was the Durban Central SAPS in KwaZulu Natal because of the rife in property related crimes of which most of them were not resolved. According to SAPS First Quarter Crime Statistics 2021/2022 (2022: 61) Durban Central is one of the police stations with the highest number of property related crimes reported. This study was conducted in two provinces in South Africa, Gauteng and KwaZulu Natal. Three criminal justice departments were targeted namely the South African Police Service, the Department of Correctional Services and the Department of Justice and Constitutional Development. Hagan (2014: 110) defined sampling as a procedure used in research which sub-units of a population is studied to analyse the entire population; while a population refers to all aspects that are being studied such as people, objects or animals. Hagan (2014: 110) explained that a small representative sample would yield a better estimate of the population than a much larger sample.

De Vos *et al.* (2002: 201) explained that probability sampling is based on randomisation, whilst non- probability sampling does not implement randomisation. In this study the researcher used non-probability sampling as it does not implement randomisation. De Vos *et al.* (2011: 232) explained that in non-probability sampling the researcher does not know the population size or the members of the population.

Additionally, the researcher further used purposive sampling which is one of the approaches used to conduct non-probability sampling. Bless, Higson-Smith and Sithole (2013: 177) clarified that purposive sampling is a qualitative approach where the researcher purposefully chooses participants on the basis of some specific criteria that are judged to be the essential targeted population. In this study the researcher purposefully selected participants who were directly involved in the identification, verification, and comparison of fingerprints.

- The fingerprint experts from the SAPS Local Criminal Record Centre (LCRC) are also known as AFIS experts. There is only one SAPS LCRC office in Durban, which is convenient to the researcher, and it consists of very few experts who are responsible for the comparison and identifying of fingerprints. The researcher therefore interviewed seven fingerprint experts: four from the Durban branch and three from the Pietermaritzburg branch.

- The researcher also interviewed two fingerprint experts from the Head Office LCRC, who are working closely with the Department of Home Affairs, responsible for the identification of fingerprints of unknown deceased people. There are two officers responsible for this identification nationally and the researcher interviewed both of them.

- From the DCS KwaZulu Natal three officials were interviewed; however the facility does not have a fingerprint system anymore. The researcher extended the research to Kgosi Mampuru Correctional Centre in Pretoria, Gauteng where a fingerprint system was found.

- The researcher interviewed four officials working with the fingerprint system in Kgosi Mampuru Correctional Centre: admitting and releasing offenders in and out of the correctional centre.

- The researcher further interviewed three Department of Justice officials who are working with the integrated justice system in the Integrated Justice System (IJS) Unit. They work closely with officials from other government departments, who are in charge of the newly implemented PIVA system.

The sample used for this study was small, since there are very few fingerprint experts working with fingerprint systems as well as experts who work closely with the Department of Home Affairs. Some fingerprints experts work with the fingerprints system, doing comparison and identification, but they do not work with the Department of Home Affairs. They work at the Local Criminal Record Centres, and they are the focus of this study.

Hagan (2014: 110) mentioned that the choice of sample size depends on the degree of accuracy required. The researcher is of the opinion that information obtained from the targeted sample group is accurate enough to conclude this study. De Vos *et al.* (2011: 232) and Hagan (2014: 117) agreed that purposive (judgmental) sampling represents the selection of an appropriate sample based on the researcher`s skill, judgement and needs.

The researcher chose purposive sampling because the participants that were targeted for this research were chosen on the basis of their expertise. For this study, nineteen research participants from the criminal justice system departments, namely the DCS, SAPS and the Department of Justice IJS were requested to form part of the sample group. As mentioned above the choice of sample was based on the opinion that information obtained from the targeted sample group was accurate enough to reach a conclusion in this study, as suggested by (Hagan, 2014: 110).

2.5. Data Collection Methods

De Vos *et al.* (2011: 342) stated that interviewing is the predominant mode of data collection in qualitative research. De Vos *et al.* (2002: 302) are of the opinion that researchers use semi-structured interviews to gain a detailed picture of a participant`s beliefs about, or perceptions of a particular topic. The researcher used semi structured interviews, which were suitable for this study. The researcher compiled a set of predetermined questions as the interview schedule to guide the interview.

The interviews were conducted face-to-face with the participants prior to the COVID 19 pandemic, while some interviews were conducted online by means of virtual platforms and other technical means amid the Covid-19 pandemic. Participant 18 was interviewed via Microsoft Teams, while other participants were interviewed by emailing them the interview schedules.

The communication with their respective supervisors was conducted, interview questions were emailed and returned through e-mails. Some questions were emailed and collected physically, whereas others were dropped off to the supervisor and were collected by hand. Information was acquired from library searches, the internet, and media for referencing to determine if there were any new developments in this study field. Information was collected from published books, government annual reports, law enforcement magazines, published journals and published speeches. Leedy and Ormrod (2015: 277) indicated that qualitative researchers must identify one or more appropriate sources from which to acquire data, as they are apt to rely heavily on observations and or interviews as sources of data.

2.5.1. Interviewing process

Lapan, Quartaroli and Riemer (2012: 152) mentioned that oral interviews do create a new primary source, or at least elicit information that otherwise would not be part of the public records. The researcher conducted face-to-face interviews with each participant separately, prior to the Covid-19 pandemic and via an online meeting during the Covid-19 pandemic. The questions came from the research aim and research questions. The researcher formulated questions using concepts that were familiar to the participants, and if questions were not clear, clarity was given with simpler concepts. Interviews were not audio recorded but were jotted down whilst attentively listening to the participant. The face-to-face interviews were conducted by means of semi-structured interviews. De Vos *et al.* (2002: 302) opined that a semi-structured interview gives the researcher and participants much more flexibility. Lapan *et al.* (2012: 152) also pointed out that it is up to the researcher not to overgeneralise an individual`s experience to those of all people. The researcher therefore ensured that information obtained from interviews like peoples` experiences was not overgeneralised to all people, but only to the respective individuals.

The researcher conducted interviews using the guidelines set out by Leedy and Ormrod (2015: 282) to ensure productive interviewing sessions with the participants. Some interviews were conducted via emails but, telephonic conversations were made before sending emails introducing the interview schedules. The following guidelines were used telephonically and face-to-face using semi-structured interviewing process.

- The researcher identified general interview questions according to the research aim and participants experiences.
- The researcher considered participants` background that might have influenced their responses.

- The researcher made sure that the sample included participants with information needed for the study. As the province intended for this study did not have enough information, the study was extended to another province.
- The researcher obtained written permission from the respective departments to conduct interviews with their employees, and also extended the University clearance to accommodate the selected provinces.
- The researcher found a suitable location in the participants` offices which were secured no for interruptions during the interviews, further ensuring that they were comfortable in their own spaces.
- The researcher established rapport by introducing herself, mentioning her own experiences and casually discussing hobbies whilst being cautious and respectful to ease any tensions formed during the interviews.
- The researcher mainly focused on the actual facts by asking questions about systems and methods used in the identification of suspects, rather than focusing on abstract ideas.
- The researcher always remembered that answers to questions may not be factual.
- The researcher listened attentively and was careful not to put words in the mouths of the interviewees.
- The researcher recorded responses verbatim in writing, as no voice recording was used. Responses were then read back to participants to ensure that the responses were correctly recorded. For the responses that were received via emails, the follow up was made telephonically for clarity and further information.
- The researcher did not show any emotion during the interviews so that she would not influence reactions and answers.

2.5.2. Observation Schedule

Leedy and Ormrod (2015: 281) suggested the following where the researcher decides to conduct observations as part of the qualitative study:

- Before the researcher begins the study, he/she must experiment with various forms of data recording e.g., field notes, identifying the particular method that work best for the study.
- There must be someone introducing the researcher to the people being observed.
- The researcher must remain quiet and inconspicuous, yet friendly to people he/she approaches.

At the Durban Westville Correctional Centre, the researcher was escorted to the fingerprints` section where the officials were seen obtaining fingerprints from offenders who were there for admission. A thumbprints appearing on a documents called a J7 which was the court warrant was also seen. The official obtained fingerprints from the offender, and those prints were compared with the thumbprint appearing on the J7. The researcher was also shown an office where the hub for the piloted fingerprints system was installed and that it was no longer working.

At the SAPS Durban branch, an officer pointed a computer which he uses to access the AFIS system which is available in his office.

With regards to the Integrated Justice System Unit, One participant used pictures as slides during the virtual meeting which was done via Microsoft Teams. During observation, the researcher recorded field notes for later referral.

2.5.3. Document Analysis

Documents that may be used in research include official documents, mass media and archival material (De Vos *et al.,* 2011: 379).

- **Official documents**

Official documents include minutes, and agendas of meetings, however the researcher had to keep in mind that the accessibility of official documents is often a problem due to legislation on the confidentiality of information (De Vos *et al.,* 2011: 379). In this study, the researcher used published documents, Standard Operating Procedures, Standing Orders/ National Instructions, Annual reports, statistics, and Annual Performances.

- **Mass media**

There are several mass media forms that disseminate information namely, radio, television, and websites. Websites represent commercial, governmental, educational, and other organisational interests. Other audio-visual mass media include newspapers, magazines, journals, and newsletters (De Vos *et al.,* 2011: 379).

- **Archival material**

According to De Vos *et al.* (2011: 379), archival material comprises documents and data preserved in archives for research purposes. In this study the researcher relied mostly on mass media documentation for the departments which did not participate in this study. The published statements and departments` reports like annual reports, yearbooks, magazines, and journals from other researchers played a vital role in this research to understand how other departments work with fingerprints databases.

2.5.4. Personal Experience

The researcher has been a criminal investigator for nine years working with different case dockets, including cases in which latent prints were involved. The researcher had been involved in cases where latent fingerprints were found on the crime scene, but the LCRC could not identify any suspects, because the individuals who left fingerprints at the crime scene were not on the LCRC fingerprints system. Those case dockets were therefore closed. As mentioned in Paragraph 2 (i) of National Instruction/Standing Order 325 issued by Consolidated Notice (2012: 5): a case docket with identifiable finger/palm prints, but no particulars of a suspect, should be closed as undetected with an endorsement of “positive fingerprints - Do not destroy”.

This aspect triggered the need for this research. Bracketing refers to a researcher`s identification of a vested interest, personal experience, cultural factors, or assumptions that could influence how he or she views the study`s data (Luts & Knox, 2014: 22). The researcher ensured that the study was not influenced by the researcher`s personal experience. The researcher remained impartial ensuring that individual knowledge was not used to interfere with data collected. With the assistance and guidance from the research supervisors, the study was not partial to any of the departments involved, information collected was used fairly and according to the university standard.

2.6. Data Analysis

Welman, Kruger and Mitchell (2012: 211-212) explained that during qualitative data analysis the researcher must identify themes like word repetitions, keywords, metaphors, etc. The researcher identified themes and interpreted them where it was necessary while keeping the original information as obtained from the participants.

The researcher interpreted data according to facts and personal experience as the research problem was also about the researcher`s personal experience. Guest, MacQueen and Namey (2012: 11) elucidated that in thematic analysis data codes are typically developed to represent the identified themes and then applied or linked to raw data. The researcher therefore analysed data by means of thematic analysis, which required more involvement and interpretation from the researcher, and focused on identifying and describing both implicit and explicit ideas within the data. Caulfield (2019) listed the following six phases of thematic analysis that are used to analyse data, namely: familiarising, coding, generating themes, reviewing themes, defining themes and reporting.

2.6.1. Familiarising

In the first step, the researcher reads and familiarises him/herself with the data collected from the participants and taking notes (Caulfield, 2019). In this study the researcher went through all the participants` written responses. Responses that were emailed, were printed for easy reading and easy reading to be scrutinised with the rest of the data collected.

2.6.2. Coding

The next stage involves coding. The researcher highlights similarities from interviews by colour-coding them according to their categories (Caulfield, 2019). As the scripts were printed and gathered with those obtained from face-to-face interviews, they were marked with different highlighters to identify similarities.

2.6.3. Generating themes

When the coding has been completed, the researcher identifies patterns and devise themes by combining codes into a single theme (Caulfield, 2019). In this study, the researcher then combined the coded information and matched them according to research objectives as themes and sub-questions as sub-themes.

2.6.4. Reviewing themes

The researcher goes through the themes and compares them with the collected data to ascertain if the themes are presented in the data (Caulfield, 2019). The researcher went through the objectives of this study and sub-questions from the interview schedule to align the generated themes with the objectives.

2.6.5. Defining and naming themes

Defining themes involves formulating a brief and easily understandable name for each theme (Caulfield, 2019). The researcher defined the themes as per the data collected from the sources and participants.

2.6.6. Reporting

The findings section addresses each theme, and the themes are discussed with examples as evidence (Caulfield, 2019). In this study, the researcher described the themes using examples, literature and information from participants.

2.7. Trustworthiness of the Study

Babbie and Mouton (2012: 277) pointed out that a qualitative study cannot be called transferable unless it is credible, and it cannot be deemed credible unless it is dependable. Therefore, in this study the meaning of these terms is discussed to assure the trustworthiness of this study. Credibility, transferability, dependability, and conformability will be discussed below.

2.7.1. Credibility/ Authenticity

De Vos *et al.* (2011: 419) viewed credibility as the alternative to internal validity in which the goal is to demonstrate that the inquiry was conducted in such a manner to ensure that the subject has been accurately identified and described. To safeguard the credibility of this study, the researcher collected data from participants who are involved in the investigation of fingerprints, or who have first-hand experience of being involved in the fingerprint identification processes within the departments which participated in this study.

2.7.2. Transferability

De Vos *et al.* (2011: 420) explained that in transferability the researcher asks whether the findings of the research can be transferred from the specific situation to other similar situations. Babbie and Mouton (2011: 277) are of the opinion that transferability refers to the extent to which the findings can be applied to other contexts or with other respondents. Bless, Higson-Smith and Sithole (2013: 157) mentioned that in qualitative research, external validity is referred to as transferability. According to them, external validity examines the extent to which the results of the study can be generalised. The researcher ensured that this study is transferable by outlining the process followed in the study, the challenges encountered as well as the profile of the research participants.

2.7.3. Dependability

De Vos *et al.* (2011: 420) cited that with regards to dependability, the researcher asks whether the research process is logical, well documented and audited. Babbie and Mouton (2012: 277) suggested that the study is dependable if its findings would be similar if it were to be repeated with the same respondents and in the same context. The researcher ensured that the process of this research was logical by gathering information according to the guidance provided by her supervisor and the language editor. Bless et al. (2013: 157) claimed that dependability as a concept is similar to, but not the same as, reliability, and that dependability demands that the researcher thoroughly describes and precisely follows a clear and thoughtful research strategy.

2.7.4. Conformability

De Vos *et al.* (2011: 421) stated that conformability captures the traditional concept of objectivity and that, regarding conformability, the question is whether the researcher provided the evidence that corroborates the findings and interpretations by means of auditing. Babbie and Mouton (2012: 277) are of the view that conformability refers to the degree to which the findings are the product of the focus of the study and not of the biases of the researcher. The researcher avoided biasness and followed all research procedures as per UNISA Policy on Research Ethics (Unisa, 2016:32). The researcher ensured that the study was not prejudice to any of the departments involved, personal experience was used proficiently to add value to this study.

2.8. Ethical Considerations

2.8.1. Permission to Conduct a Study

Creswell (2013: 57) emphasised that prior to conducting a study, it is necessary to obtain college or university approval from the institutional review board for the data collection involved in the study; as well as local permission to gather data from individuals and sites at an early stage in the research. In this study, the researcher applied for and obtained ethical clearance from the University of South Africa - Research Ethics committee, as stipulated in Paragraph 6.2.1 of the UNISA Policy on Research Ethics (Unisa, 2016: 05).

The researcher also obtained permission to conduct a study from the SAPS, the DCS and the Department of Justice (DOJ) as stipulated in Paragraph 8.1 of the UNISA Policy on Research Ethics (Unisa, 2016: 31). When the geographical area of the study required extension, the UNISA Ethics Committee was informed, and permission was granted. New submissions were made to relevant departments and permission was also granted.

2.8.2. Privacy

De Vos Strydom, Fouchè and Delport (2003: 67) remarked that violation of privacy, the right of self-determination and confidentiality can be viewed as being synonymous. Therefore, when participants requested to remain anonymous, their requests were respected and granted. Terre Blanche *et al.* (2011: 61) mentioned that the essential purpose of research ethics is to protect the welfare of research participants. Melville and Goddard (2007: 49) stated that “in order to avoid doing harm to people one must guard against both physical damage and psychological damage, people have a right to privacy and the researcher must keep data collected confidential.” The researcher then allocated codes to participants such as “Participant 1” to remember which participant provided the information.

In this study the researcher ensured that no names of participants were mentioned, and the data collected from participants were treated as confidential. Furthermore, the researcher provided the research participants with her personal cellular phone number and e-mail address in case they needed to ask her further information concerning the study. For confidentiality reasons, the researcher ensured that the research data are kept safe in a USB that is locked with a password.

2.8.3. Consent

De Vos et al. (2002: 74) mentioned that it should be ascertained that the consent of participants is voluntary and informed, without any implied deprivation or penalty for refusal to participate. Before commencing with the research study, the researcher explained to the research participants the purpose of this research study and the process that was to be followed throughout the research. The participants were treated with dignity and consent was requested from each research participant. All research participants were allowed to withdraw their participation at any time felt uncomfortable during the research study, only one participant from the DCS withdrew because of his busy schedule and unavailability, he was then replaced.

2.8.4. Plagiarism

Terre Blanche et al. (2011: 61) asserted that research ethics involves more than a focus on the welfare of research participants and extends into areas such as scientific misconduct and plagiarism. The researcher quoted sources and references as trained and as required. The researcher is aware of the consequences faced by unethical research; therefore, the researcher collected data and obtained information as required and of ethical standard. The researcher is also aware of UNISA`s student policies and rules on copyright infringement and plagiarism and is aware of the consequences faced by the student if such policies are violated. The researcher ensured that all citations are marked, and authors are acknowledged accordingly. The produced study is strictly the researcher` s own work. The research report was also put through the Turnitin software to detect plagiarised work and the certificate to prove that no information was plagiarised is attached to this document.

2.9. Summary

This chapter discussed research methodology, research approach, research design, and data collection. The focus was on the research methods which the researcher adopted in achieving the aim of this study. The researcher also discussed trustworthiness and personal experience which led to this study. Ethical consideration and consent procedures for the participants, the permission to conduct the study, as well as plagiarism in terms of UNISA students` rules were discussed. This study is based on fingerprints identification which involves people`s privacy and personal information, therefore the next chapter discussed the legislation that governs the use and sharing of fingerprints information.

CHAPTER THREE: LEGISLATION GOVERNING THE USE AND SHARING OF FINGERPRINTS SYSTEMS BETWEEN GOVERNMENT DEPARTMENTS

3.1. Introduction

In this chapter the discussion will be on South African legislations that governs the how, when, and why people's fingerprints are used, by whom as well as for what purpose. As indicated in the previous chapter that this study is based on fingerprints information which involves people`s privacy it is critically important to know the legislation that governs use and sharing of fingerprints information. Therefore, the following legislation will be discussed: Criminal Procedure Act 51 of 1977, the Constitution of the Republic of South Africa Act 108 of 1996, the Criminal Law (Forensic Procedures) Amendment Act No. 6 of 2010 and the Protection of Personal Information Act No. 4 of 2013 (POPI Act). Privacy and confidentiality in data matching as well as criminal justice system departments will be deliberated.

3.2. Section 36 of the Constitution of the Republic of South Africa No. 108 of 1996

Section 36 (1) of the Constitution of the Republic of South Africa (the Constitution) states that, the rights in the Bill of Rights may be limited only in terms of the law on condition that the limitation is reasonable and justifiable. Limitation should not violate a person`s dignity, equality, and freedom. The following should be taken into consideration:

a. The nature of the right.
b. The importance of the purpose of the limitation.
c. The nature and extent of the limitation.
d. The relation between the limitation and its purpose; and
e. Less restrictive means to achieve the purpose.

Section 36 (2) of the Constitution continues to state that no law may limit any right entrenched in the Bill of Rights, except as provided in subsection (1) or in any other provision of the Constitution. The Constitution emphasises the importance of humans` rights whilst leaving a gap for law enforcement and others to justify their acts. Infringing people`s rights is an offence, unless the official infringing the rights has justifications as mentioned above. Section 36C (1) of Criminal Law (Forensic Procedures) Act No. 6 of 2010 allows the police to take prints found on property and examine them if they believe that such prints will be valuable to the investigation of the crime. Limitation of rights allows officials working with prints to go through private and personal information contained in fingerprints systems without the consent of the owner of the information. Limitation of rights limits the POPI Act, the Bill of Rights which is the right to privacy. However, this clause applies to the use of information for investigation purposes. Accessing such information for personal use or sharing of such information illegally does not apply to the limitation of rights. Such person will be charged for unauthorised sharing of information in terms of POPI Act or in terms of the Bill of Rights.

There are investigators who access information for investigation purposes but without following the correct procedures of obtaining such information; and if a transgression has been established, such information is inadmissible in the court of law. For example, the police use cell-phone records as evidence in cases to prove communication, to prove location of the suspect at the time of an offence, or to prove ownership of the cell-phone number involved. Such information is obtained from the service provider. The investigator requiring such information can easily obtain such information from a friend if the friend has access to cell-phone records at the service provider, the information is indeed for investigation purposes but has been illegally obtained and will be inadmissible in court.

The correct procedure is to apply in court for a subpoena to be issued to the service provider for the information required. This is done in terms of the Section 205 of the Criminal Procedure Act No. 57 of 1977 which authorises the person who is likely to give material or relevant information to an alleged offence, whether it is known by the person who committed the offence or not. This implies that the owner of the cell-phone does not have to know that his information will be requested from the service

provider, as he/she does not have to give consent to the service provider to provide such information. Therefore Section 205 of the Criminal Procedure Act limits the right to privacy, protection of Personal Information Act.
Section 15D of the Criminal Law (Forensic Procedure) Act No. 6 of 2010 gives directives to the departments to work together while ensuring protection of people`s privacy. The police in this case can use Section 36 of Bill of Rights if there is need, however other violations and limitation of rights require authorisation from the DPP or courts to avoid unnecessary litigations.

3.3. Protection of Personal Information Act No. 4 of 2013

The Protection of Personal Information Act No. 4 of 2013 (POPI Act) is aimed at ensuring that people do not share other people`s information without permission. Whether it is shared by the police or the court, illegal sharing of information is still an offence for these agencies. Sharing of information between the departments requires departments to be cautious of the protection of people`s information. This study discusses the sharing of information with the LCRC therefore, it is vital that the protection of such information is also discussed. The LCRC verification and identification of fingerprints depend on fingerprint information received from other departments. Section 9 of Protection of Personal Information Act No. 4 of 2013 states that personal information must be processed:

a) Lawfully and
b) In a reasonable manner that does not infringe the privacy of the data subject.

This requires the departments in the criminal justice system to protect personal information at their disposal whilst utilising the database that contains citizens` personal information. As mentioned earlier, Section 15D (4) of Criminal Law (Forensic Procedure) Act 6 of 2010 states that the departments must develop a standard operating procedure which will be used when sharing databases without violating people`s privacy.

Proper confidentiality amongst members delegated with such duties is required to ensure that people`s information is safe, they are not exposed to fraud and identity fraud, and to protect them against risks that come with the exposure of their information. Christen (2012: 15) pointed out that identity crimes are on the rise in many countries, resulting in losses of billions of monies to financial organisations and sometimes with grave social implications for the individuals concerned. Christen (2012: 15) further defined identity crime as a crime that occur when a fraudster gains access to services and benefits by using a false identity.

Section 10 of the Constitution states that every person has inherent dignity and the right to have their dignity respected and Section 14 of the Constitution states that every person has the right to privacy. Section 35 (5) of the Constitution states that evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence would render the trial unfair. The use of fingerprints as an authentication measure in accessing the fingerprint system is another form of protecting the confidentiality and privacy of people, while serving as a measure to prevent fraud by officials accessing the system. When the system is unlocked, it is known who had access to the system at a particular time.

Passwords can be stolen and misused by fraudsters. Exchange of information has been a concern when it comes to privacy and confidentiality of information. Not only because people do not want to be known or traced, but because of rifeness of the identity fraud. People have been victims of fraud and other crimes unknowingly, because sensitive information is shared among different organizations or hacked and shared for fraudulent purposes. In March 2022 Credit bureau TransUnion was hacked for ransom, News24 (2022) reported that Credit bureau TransUnion was hacked for ransom and hundreds of companies were under threat. News24 (2022) further reported that the hackers described as a criminal third party gained access to the credit bureau server by misusing an authorised client's credentials.

News24 also mentioned a number of data breaches including that of Experian credit bureau which suffered a data exposure in 2020 where information of twenty four million South Africans was exposed. Also according to the Timeslive (2023) in September 2021 the Department of Justice and Constitutional Development contravened the POPI Act where more than one thousand two hundred files were lost. Timeslive (2023) added the Information Regulator issued the Department of Justice with an enforcement notice. The breaching took place when the department failed to renew its security license which was monitoring the unusual activity and to back up log files.

Krimsky and Simoncelli (2012: 157) agreed that a population-wide database of fingerprints can be misused in violation of one`s privacy and spatial anonymity. In this study, the information that is to be shared involves identity numbers and addresses. With an identity number a lot of sensitive information can be retrieved by fraudsters which puts the lives of citizens at risk.

Wells, Bradford, Gilbert, Kramer, Ratley and Robertson (2012: 1.780) mentioned the logical access control, describing it as the process by which users are identified and granted certain privileges to information, systems, and resources. Wells *et al.* (2012: 1.780) further explain that access controls are designed to protect the confidentiality, integrity, and availability of information resources by verifying the identity of persons trying to enter system.

To reduce misconduct in the workplace, government departments have offices which were implemented to investigate internal misconduct. The Department of Home Affairs (DHA) developed the Counter Corruption and Security Services. The DHA Annual Report (2017/2018: 113) explained that the mandate of the DHA Counter Corruption and Security Services is to prevent and combat corruption to protect and promote the integrity of the department. Their purpose is also to ensure that DHA operations are conducted in a safe and corruption-free environment and that all DHA employees, clients and assets are safeguarded. In addition, the directorate is also tasked with undertaking awareness initiatives on ethics, fraud prevention and counter-corruption within the department. The DHA took these initiatives to maintain an ethical workforce. Therefore, the DHA is concerned about the safety of people`s information and tries to fight any contravention of their policies. If, for instance, the LCRC violates any of the DHA policies on information security, the DHA can also charge the LCRC officer because the information was only supplied to the DHA and the DHA has the responsibility to protect that information.

Section 11 (4) of the POPI Act stated that if a data subject has objected to the processing of personal information in terms of subsection (3), the responsible party may no longer process the personal information.

To protect people`s personal information, Gibbons (1991: 15) stated mentioned that in the United State of America (USA), the NCIC (National Crime Information Centre) developed procedures to protect the NCIC network from unauthorised use, sabotage, and other physical technical, and personnel security breaches. As a matter of concern, the staff that are directly involved in the sharing and identification process, should be trusted with handling other people`s privacy. Training and sensitization should be provided about the consequences to be faced by wrong doers.

The detection of suspects in these cases would rely more on fingerprints uplifted from the crime scene than relying on witnesses and other investigation techniques. Section 14 of the Constitution states that every person has a right to privacy. Section 6 of POPI Act as discussed above, states that protection of personal information does not apply to the processing of information by a public body (Department or organ of State) if it is for the purpose of prevention, detection, including assistance in the identification of money laundering activities, investigation, proof of offences, etc.

Section 19 of POPI Act provides that a responsible party must ensure the integrity and confidentiality of the personal information in its possession by putting appropriate and reasonable technical and organisational measures in place to prevent the loss of, damage to, unauthorised destruction of, unlawful access to, or unlawful processing of personal information. The POPI Act is emphasising the implementation of username and password protection to control access to personal information. In other systems which are password protected, some officials take advantage of their colleagues by requesting to use their passwords if their own passwords are blocked.

The Office of the Premier (2017: 6) stated that the Province of KwaZulu Natal has adopted the Biometric Access Control System (BACS) as an additional security layer; a PERSAL user must now use a fingerprint identification to log into the mainframe and thereafter uses User ID and password to log into the system as in BACS system. This reduces using other peoples` log in credentials in their absence. Colleagues often trust one another so much that they share login credentials, even where they are aware of the consequences of such conduct; therefore, the implementation of fingerprint login reduces such conduct.

In the USA, the FBI launched a system called Next Generation Identification (NGI), a database that contains the biometric data of millions of Americans to enhance background the search of criminals and non-criminal searches. The FBI further released a final rule claiming several Privacy Act Exemption, meaning they wanted to be exempted from certain laws in order to have access to all information available. This implied that FBI is exempted from other privacy laws for the purpose of enhancing investigations and other identification purposes. However, the Electronic Privacy Information Center (EPIC) opposes the program, saying the program raises privacy issues that implicate the rights of Americans across the country.

The AFIS has been replaced by an Automated Biometric Identification System (ABIS) that allows the identification and verification by fingerprint, facial, iris recognition and other means (DHA Annual Report, 2017/2018: 10). The Annual Report further indicated that the ABIS has been implemented to integrate all systems and use biometrics as a unified/unique person identifier. The use of this system has been a success in commercial banks, but the LCRC still has no access to the system. During interviews the participants emphasised that there is absolutely no liaison with the DHA. Christen (2012: 187) suggests that if data matching is conducted within a single organization and between databases owned by the same organization, privacy and confidentiality are generally not of concern. Christen (2012: 187) further indicates that in most cases it is assumed that people who conduct data matching projects within organizations are aware of all relevant policies and regulations with regard to handling the private and confidential data that are being matched. They would not have malicious intent to disclose identifying or other sensitive information, or the matched data, outside of their organizations for personal gain (Christen, 2012: 187). Individuals conducting fingerprint identification in departments like the DHA, DCS and DHA should be made aware of other legislations that prohibit illegal sharing of people`s information, beside the POPI Act. There are strict measures in place dealing with the unlawful handling of personal information; Section 19 of POPI Act provides that:

(1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent:

a) Loss of, damage to or unauthorised destruction of personal information; and
b) Unlawful access to or processing of personal information.

3.4. Privacy and confidentiality in data matching

Christen (2012: 187) reiterated that if matched data are used for purposes internal to an organization only, such as for internal fraud detection, generating customer mailing lists, or internal research studies; no privacy or confidential matters will occur; however, the necessary steps should be taken to prevent unauthorized access to the matched data and no detailed results of a matching exercise should be made public. Exchange of information has been a concern when it comes to privacy and confidentiality of information. Not only because people do not want to be known or traced, but because of the fact identity fraud has become rife. People have been victims of fraud and other crimes unknowingly because sensitive information is shared amongst different organizations or hacked from organizations for fraudulent purposes.

Krimsky and Simoncelli (2012: 157) agreed that a population wide database of fingerprints can be misused in violation of the victims' privacy and spatial anonymity. People give consent to one organization to use their information for marketing purposes without realising to what extent the information is shared for marketing purposes. In this study, the purpose of data sharing is to compare or match the unknown fingerprint with the fingerprints contained in the DHA or the DCS and hopefully the DOT databases and when a match is found, the details (name, surname, and address) of that fingerprint will be used as the identity of the unknown fingerprint. Christen (2012:6) confirmed that data matching relies on personal information such as names, addresses and dates of birth of individuals. Christen (2012: 6) also emphasises that privacy and confidentiality in data matching need to be carefully considered where databases are matched between organizations.

In this study the information that is to be shared involves identity numbers and addresses. With an identity number a lot of sensitive information can be retrieved by fraudsters. Gibbons (1991: 15) pointed out that in the United States of America (USA), fingerprint identification files and criminal history records maintained by Ident were more sensitive than the hot files maintained by National Crime Information Centre (NCIC). The NCIC subsequently developed procedures to protect the NCIC network from unauthorized use, sabotage, and other physical technical, and personnel security breaches. As a matter of concern, the staff members that will be directly involved in the integration and identification process, should be trusted with handling other people`s privacy. Training and sensitization should be provided and possible consequences of fraudulent use/misappropriation of information should be communicated.

A person caught violating people`s privacy can be charged departmentally and criminally for fraud and contravention of acts which protect people`s privacy. Fraud is an unlawful and intentional making of a misrepresentation which causes actual or potential prejudice to another (Van Rooyen, 2013: 19). Therefore, the unauthorized retrieval of another person`s information for the purpose of self-gain may amount to fraud. To prevent fraud, fraud examiners believe that detection, investigation, and deterrence can prevent or minimize the risks of fraud. Deterrence, as discussed above involves punishment of members caught committing fraud should be made known to other members to instill fear of punishment imposed for similar offences. Deterrence is designed to detect law violations, determine who is responsible, and penalize the offender to deter future violations (Wells, 2012: 4.415).

Wells *et al.* (2012: 4.503) refer to Cressy` s fraud triangle which has three pillars namely the perceived opportunity, the pressure and rationalisation which are described as reason coerce/compel fraudsters to commit fraud. Members working with people`s information can feel threatened if information is illegally demanded from them or pressure to possess such information for personal gain; whilst perceived opportunity can be the reason why the member may contemplate playing system and obtaining the information for fun or for personal gain. Rationalisation is when the person tries to explain reasons why he possesses such information and trying to make it legal. These kinds of conduct can be prevented by clearly communicating the consequences of such conduct to all concerned.

Innocent citizens fear identity fraud and integrating people`s information with other government departments will get people divided, as some will understand and be enthusiastic about the idea whereas others will have concerns about the protection of their own information. The people who are concerned about the integration of the fingerprint systems are those in offices that look at violation of people`s rights, as experienced by the FBI. As mentioned above the FBI launched the NGI system, a database with the information of millions of Americans to have access to certain kinds of information, but they are opposed by the EPIC, saying that the program raises privacy concern.

Christen (2012: 187) pointed out that individuals who conduct data matching projects within an organization should not have malicious intention to identifying or other sensitive information outside the organizations for personal gain. The training and sensitising of employees regarding the confidentiality of information they work with is important and it is therefore extremely important to communicate consequences which may be faced by violators. In 2002, South Africa introduced a new system in which customers have to produce identity documents and addresses to purchase SIM-cards or cellular telephones.

Section 62C (1) of the Regulation of Interception of Communications and provision of communication-related information Act (RICA) Act No. 70 of 2002 states that: before handing over a SIM card to another person, record the particulars as required in section 40(2) and the date on and period for which the SIM card is provided and verify the full name, surname, identity number of the person to whom the SIM card is provided and the address contemplated in section 40(3) (iii) by means of documentation contemplated in Section 40 (3) (b). This system frustrated people as it was no longer easy to purchase SIM cards. To supply Identity documents and addresses made many people uncomfortable, fearing that they may be followed or scammed, as every shop no matter how small, requires these documents when purchasing.

To protect customers` information, Section 42 of the Act provides that no person may disclose any information which he or she obtained in the exercising of his or her powers or the performance of his or her duties in terms of the Act. This section prohibits employees who work with people`s information to provide to unauthorised people for personal gain. Similarly, the process of sharing of fingerprint information between the criminal justice system departments may protect people`s information by giving specific directives to employees who are responsible for the comparison and identification of fingerprints; and consequences of any contravention should be communicated to such employees to prevent malicious intentions of providing such information outside the organizations for personal gain. Section 19 (1) (a) and (b) of the Protection of Personal Information Act No. 4 of 2014 provides that a responsible party must ensure the integrity and confidentiality of the personal information in its possession by putting appropriate and reasonable technical and organisational measures in place to prevent the loss of or damage to; unauthorised destruction of, unlawful access to or unlawful processing of personal information.

Gibbons (1991: 15) explained that authorized law enforcement and criminal justice personnel may access the NCIC and that the NCIC places a high priority on a secure, tightly controlled network. The Advisory Policy Board (APB) suggested that noncriminal justice users such as employment checks etc. may obtain NCIC information but only for authorized purposes and with access provided through authorized law enforcement. Where the accused had given wrong particulars during arrest, the information given can be compared with the information in the DHA or the DCS systems to establish whether the information given is authentic or not. Some offenders have the tendency of changing their names in different cases to lessen or to avoid sentences.

However, that conduct can be picked up by the SAPS LCRC through fingerprints on which that the suspect was arrested before and supplied certain names. Sometimes such information is made available after the accused has been released and already at large as the LCRC releases such results/information a few weeks after the arrest, and by that time the accused is already released on bail or has paid admission of guilt. The problem in this kind of act is that the real name (birth particulars) of the suspect remains unknown. Also, since the implemented PIVA system is available in police stations, this will not be the case anymore. The offender`s real particulars will be picked up by the PIVA system at the police station and the false information will be scrapped.

The USA National Crime Information Centre (NCIC) has an audit procedure where the record quality of files is audited, which includes comparison of the entries in the NCIC national files with the corresponding entries in the State/local files based on a random sample of the record from each file. Erroneous information or discrepancies are therefore discussed with the appropriate State or local criminal justice officials (Gibbons, 1991: 15). The same can be done where departments will audit information stored by each department to see if the department have the same or different information on their databases. This can be effective to avoid duplicated information where people intentionally give wrong particulars which may only be discovered with a set of fingerprints or a thumb print. Stuart, Nordby and Bell (2014: 343) indicated that fingerprint examiners are generally extensively trained and required to accumulate significant experience before being entrusted with the responsibility of making identifications. This implies that they are trusted with confidentiality, authenticity, integrity and loyalty when it comes to performing their duties.

3.5. Closing of Case Dockets Undetected

The National Instruction 325 as cited in the Consolidation Notice (2012), lists a number of reasons for closing case dockets but dockets are not closed because there is insufficient evidence to prosecute. Dockets may be closed with ample evidence but with certain circumstances compelling the closure of such a docket. The following reasons will be discussed:

- **Undetected** e.g., when there is no lead to act, meaning when there are no fingerprints or no witness or any useful information that can guide the investigator how to go about investigating, when and where.

- **Further investigation** is required e.g., when a suspect cannot be identified by means of the fingerprints lifted from the crime scene.

- **Case is finalised** e.g., when the case was withdrawn or when the suspect is found not guilty or under nolle prosequi (dismissal of charges by prosecutor). Also, when the accused is convicted and sentenced, the case docket is closed with file final.

- **No Complainant.** There are complainants or victims who open cases and then they lose interest to proceed, either because of threats and fearing the suspect or because the stolen property has been recovered; or because the suspect has apologised and there is an agreement. Although the complainant or the victim voluntarily withdraws the case, investigators are trained not to believe on first occasion that the withdrawal is voluntary, especially in domestic violence cases. Unless the complainant insists and does not show up for appointments the case is closed on the complainant`s withdrawal. In some cases, dockets are closed because complainants cannot be traced; either the address is vague, or the complainant relocated, and left no contact details or the complainant gave the wrong address on purpose to get a case number.

National Instruction/ Standing Order 325 as cited in the Consolidation Notice (2012) further indicates the following:

- Whenever the investigation of a case has failed to disclose the offender and it is furthermore clear that the offence was actually committed, the case docket shall invariably be closed as "Undetected".
- If a complainant who reported a case cannot be traced, the case docket shall always be closed as "Undetected - complainant not traced".
- If a warrant has been issued for the arrest of a person whose identity is known, the case docket shall be closed as "Undetected - Warrant Issued".
- The case docket with identifiable finger/palm prints but no particulars of a suspect, should be closed as “Undetected - “Positive fingerprints - Do not destroy”.

This study focuses on case dockets closed undetected where fingerprints were found but were not identifiable. In this case the case is undetected because there are no leads, there are fingerprints but there is no name or address that can guide the investigator on how to go about finding the suspect.

As mentioned in Chapter One, the reason of closing dockets undetected may be that fingerprints uplifted from the crime scene are not identifiable by the LCRC (Local Criminal Record Centre) because the person who left the fingerprints at the crime scene has never been charged before.

Therefore, such cases are closed undetected. Closing the docket with positive fingerprints and the suspect is unknown means that the fingerprints were detected and readable, but not identifiable as there are no records of the person on the LCRC database. Those fingerprints are not destroyed but they are stored on the LCRC database. Such docket is then closed as “Undetected” by the police station. Paragraph 2 (i) of National Instruction/Standing Order 325 issued by Consolidated Notice (2012: 5) provided that the Commander closing the case docket as “Undetected” where identifiable finger/palm prints were found, must make the endorsement in red ink on the cover of the case docket “positive fingerprints- Do not destroy before the date endorsed”.

Komarinski (2005: 84) confirmed that if the information is not found on the criminal record database the examiner then initiates another search where unknown latent prints are searched against a database of unknown latent prints. These dockets are closed and filed but if the same person commits a crime, is arrested and charged, the LCRC picks up the stored and unknown fingerprints and links them with the new information when an arrest was made, and they then alert the police station of the filed docket and the offender will be charged on the linked old case. Komarinski (2005: 84) confirmed that if there is no match the examiner can notify the investigator that another police station is working on a case in which matching fingerprints were found and the collaboration can therefore lead to an identification of a suspect for the filed case which may lead to arrest.

Paragraph 2 (h) of National Instruction 325 issued by Consolidated Notice (2012: 3), provided that a Commander closing the case docket “undetected” where property such as a firearm was stolen, the docket must be endorsed to be brought forward after five years and the Commander must determine the month and the year when the docket must receive attention; and endorse the docket with “circulated-do not destroy before the date endorsed.” Paragraph 2 (c) of National Instruction 325, issued by Consolidated Notice (2012: 4), stated that if a warrant has been issued for the arrest of a person whose identity is known the case docket must be closed as “Undetected-Warrant Issued”. The commander must also determine a “Brought forward date” on which the docket will be reopened to trace the suspect. According to the researcher’s experience, dockets are brought back from the archives every month, as they have reached their five-year brought forward period, and they are normally handed to various investigators for further tracing of suspects.

Paragraph 2 (j) of National Instruction 325, issued by Consolidated Notice (2012: 6), stated that in cases where it was established that a particular criminal is also responsible for other offences committed at diverse places, without the name of the criminal being known, the docket must be kept for 10 years before being destroyed; and the commander closing the docket must endorse a “Brought forward date” -in red ink and endorse it with “Do not destroy before the date endorsed. This can happen when the same fingerprints are found in different crime scenes, but the person has never been arrested, as he/she is not on the LCRC database. That is where other departments can assist in locating the suspect, as it may happen that the suspect is registered by Home Affairs, he has an ID book where his full names, surname and home address can be found, or he has a driver`s license which is renewed every five years.

The Department of Transport might have a recent home address for the wanted person. With the current government assistance to unemployed South Africans due to COVD-19, the Department of Employment and Labour might also have recent particulars of the person if such person had applied for the COVID-19 relief fund. Although the system does not use fingerprints for applications, an ID number retrieved from the DHA database can be used in every database to locate recent particulars of the wanted person. If all these departments can be linked with the AFIS or the LCRC, wanted criminals and first-time offenders may be identified immediately.

Section 36C (1) (a) of Criminal Law (Forensic Procedures) Amendment Act 6 of 2010 states that any police official may, without a warrant, take fingerprints or body prints of a person or a group of persons, if there are reasonable grounds to suspect that the person(s) has committed an offence. Section 36C (2) states that such prints may be examined and be subjected to a comparative search. This implies that not only an arrested person`s fingerprints may be taken by the police, but also that if fingerprints are requested, it does not mean that the person has committed a crime. Fingerprints can be requested for verification without a warrant if the person`s fingerprints are found on the crime scene; and for elimination purposes if the place has been utilized by different people.

Section 36C (3) (a) (i) states that any fingerprints taken under any power conferred by this Section, must upon the conviction of an adult person be retained on a database referred to in Chapter 5A of the SAPS Act. Section 36C (3) (b) states that fingerprints which may be retained in terms of this section may only be used for purposes related to the detection of crime, the investigation of an offence, the identification of a missing person, identification of an unidentified human remains, or the conducting of a prosecution. These are the fingerprints records that assist in the investigation which, shows if the suspect has previous convictions or not and if there are previous convictions, what type of offences the criminal has been convicted for. These records assist the court in making a decision during sentencing; however a conviction which happened ten years earlier may not be used against the accused person, as after ten years the conviction record is voided by the court, but it can still appear in the SAP 69 (previous convictions history).

Similarly, Section 36C (3) (a) (iii) states that any fingerprints taken under any power conferred by this Section, in a case where the decision was made not to prosecute, the person found not guilty, a conviction is set aside, or the prosecution declines to prosecute, must be destroyed within 30 days after Criminal Record Centre has been notified of such decision. The destroyed fingerprint records show that the person investigated does not have previous convictions; however the CRC records (SAP 69) does show that the person was charged, and charges were withdrawn. That information does not affect the court decision, and the same as that of a conviction that happened tens of years ago, but it does assist investigators to see the offender`s pattern behavior or the trend of the suspect.

3.6. Blaming Criminal Justice System

The closing of dockets where there is a lead to the perpetrator but no resources to detect such is an embarrassment to the police, because the community loses trust if their expectations are not met. Daigle (2012: 85) explained that when police meet victims` expectations; people report high levels of satisfaction. However, when the police are failing the community, they are regarded as useless and not to be trusted whether they can do the job or not. Smit, Minaar and Schnetler (2004: 225) indicated that people do not approach the police, because of their lack of faith in the police. Daigle (2012: 85) is of the view that police are the doorstep of criminal justice, the responses that the public receives from the police may shape how they view the criminal justice system, and it may impact their future dealings with the justice system.

Some people in the community call for the reinstatement of the death sentence, especially for crimes against women and children. Many people feel that the justice system is weak and powerless, while others take matters into their own hands (vigilantism). In some cases it is not justice as they say, but it is caused by the fact that perpetrators are not arrested. At one stage, after the death of the South African teenage girl, Uyinene in 2019, the community created an online petition for people to vote to "*bring back the death sentence"* because they were tired of femicide in the country, and they felt that the justice system was failing the people of South Africa. According to Change.org (2019)

> *"1 000 000 (one million) signatures, this petition became one of the top signed on Change.org. Crimes against women in South Africa has become an uncontrollable vicious cycle where women and children are sexually assaulted and murdered with little to no justice for the ones that are left behind to pick up the pieces."*

The community lost hope, which implies that it is not just because of one case where the police failed to meet people`s expectations, but a number of cases until the community had enough. This case has nothing to do with fingerprint investigations; but the justice system has been blamed where perpetrators walk free after few years in prison, where perpetrators are not arrested because of lack of evidence and where perpetrators are not detected at all. Property crimes where fingerprints are involved has a multitude of cases where the detection rate was low (not detected). This is according to statistics, as discussed in Chapter 1 and the following chapters. These kinds of unresolved cases have victims or complainants who, if interviewed, would openly express their dissatisfaction with the outcome of their cases. It is obvious that not every citizen will be pleased with the standard of the police work, but a reduction in the number of disgruntled citizens may restore trust in the police. If the citizens of South Africa do not trust and believe in the police, it creates a bad image of the country and for its economy, as no international investors will invest in the country where the security of its citizens is unmanageable.

To reduce undetected cases with positive identification of fingerprints can restore trust in the police. In minor cases where fingerprints are found and no arrests were made, victims complain of poor investigating skills when they know that fingerprints were found but no one was arrested. According to this study is reasons for not effecting an arrest may be that the LCRC cannot identify fingerprints of a first-time offender because such fingerprint information is not on the AFIS of the LCRC database, unless they can obtain access to the Department of Home Affairs database or the PIVA system where all citizens' fingerprints are stored. As mentioned earlier, former Justice Minister Jeff Hadebe (as cited in News24, 2010) quoted statistics indicating that, the criminal justice system review office had found that in 2006/07 52% of perpetrators remained undetected while 46% perpetrators also remained undetected in 2007/08; suggesting that the new Act will reduce the number of undetected perpetrators.

The Minister pointed out that the SAPS had access only to the fingerprints stored on the SAPS AFIS system and had no direct access to the Home Affairs system where the fingerprints of 41 million citizens and 2.5 million foreigners were kept. The proposed fully operational detection of latent fingerprints for every latent print uplifted from the crime scene remains still an expectation, but it seems promising in the long run. This promise was released in 2007/2008, but to this date the LCRC is still unable to detect a suspect on latent prints left by first-time offenders. Even with the new PIVA system which has now integrated information from other departments, the LCRC is still unable to detect first-time offenders because the PIVA system does not identify latent prints. There is a lot of work to be done by experts on latent prints before they can be searched for identification and that cannot be done at police station level.

According to Wells et al. (2012: 4.415), deterrence is designed to detect law violations, determine who is responsible, and penalize the offender to deter future violations. This means that to prevent wrong doing, such perpetrators must be punished to instil fear into others who contemplate doing the same thing. If offenders walk free because they cannot be traced it will encourage others to do the same or the same offenders to repeat what they have done.

3.6.1. The Criminal Justice System Departments

Smit, Minaar and Schnetler (2004: 255) described the Criminal Justice System as the term used to include all participants in the process of identification of a crime which includes police, justice and correctional services but not limited, to also include social services and non-governmental service providers. Cross (2010: 9) in his list of criminal justice system departments, adds other departments like Home Affairs and the Ministry of Justice. Davies, Croall and Tyrer (2010: 4) mentioned several agencies that are involved in criminal justice, namely the police, prosecutors, criminal defence services, and courts, ministry of justice probation, correctional centres and youth justice.

In the United States of America (USA) the FBI`s Criminal Justice Information Services (CJIS) developed a new system to replace the integrated IAFS, the system called Next Generation Identification (NGI). This system provides the criminal justice community with the world`s largest electronic repository of biometric and criminal history information (FBI, 2013). The EPIC (Electronic Privacy Information Centre) rejected the development of the system arguing about the privacy of USA citizens, while EPIC (2013) argued that most records contained in the NGI database will be of US citizens and millions of individuals who are neither criminals nor suspects. The EPIC (2017) which is concerned with the privacy of individuals, has urged the FBI to expand its use of name-based checks for noncriminal purposes, such as government employment, licences, child care providers, teachers, firearm purchasers and others, rather than fingerprint-based background checks.

The fingerprint check is an effective and trusted way of conducting checks, whether it is criminal or a non-criminal checks. Therefore, these fingerprints should be stored to assist investigations at a later stage. In South Africa security checks are done by police. While the LCRC and security checks are done innocently by people in desperate of something therefore these people provide their correct identities it will be very useful for LCRC to keep these details so that whenever latent prints are found on a scene, but their details are not detected on the AFIS, then the LCRC must search from this database where security checks are stored.

3.6.2. South African Police Service Local Criminal Record Centre

The first case where fingerprint evidence was presented in a South African court was in the case of The Crown vs Umfubayana on 16/02/1905 at Pietermaritzburg. In this case only 5 points were indicated by the fingerprint expert, Mr Pinto-Leite, and it was accepted by the court as sufficient evidence. On 01 April 1925 the SAP Criminal Record Centre was established and has been in existence since then (SAPS CRC Training Committee, 1999: 2 & 5). The SAPS CRC Training Committee (1999: 3) explained that the official South African criterion for individualizing a fingerprint, palm print, and footprints were formulated by the SAP Criminal Record Centre to be 7 ridge characteristics that can be identified on both prints, corresponding with the type, size, direction, position, and relation to each other and was later accepted by the International Association for Identification.

The police Automated Fingerprint Identification System (AFIS), consists of two principal applications, first searching large files for the presence of a ten-print set of prints taken from a person; the second application is searching large files for single prints, usually developed latent fingerprints from the crime scene (James, Nordby & Bell, 2014: 335). James et al. (2014: 335) continued to say that as the AFIS database holds two types of files, one for known individuals and known as the forensic file/ database. James *et al.* (2014: 335) explained that the one for known individuals can be used to search questioned specimens, images or profile. The forensic database contains images or profiles from unsolved cases. The AFIS forensic files consist of images of developed latent single fingerprints from unresolved cases of, fingerprints that have not yet been identified.

Ogle and Plotkin (2018: 119) pointed out that if the surface is severely contaminated with grease or oils, powders and small particle reagents will usually blanket the surface so that the latent print does not stand out from the background. Fingerprint contamination occurs in rainy or very hot weather if the crime scene is outside in the open. Contamination of prints can also occur deliberately when a suspect tries to wipe fingerprints to hide his/her identity. It is commonly known that some suspects use gloves to hide their identity, or some try to destroy them. Lyle (2012: 258) stated that to completely obliterate a print is difficult and any scars on a finger that remain will create new individual characteristics an examiner can use for a match.

Lye (2012: 258) quoted the case of John Dillinger who burnt his fingers in order to mislead the police. After John Dillinger had been shot dead, he was identified by his fingerprints in the morgue. Lye (2012: 258) added that original fingerprints can grow back and be visible again. This means that fingerprints cannot be completely changed even after the fingers had been injured, causing scars. Kriel (2011) emphasised that the uniqueness, permanence, and arrangement of the friction ridges allow examiners to positively match two prints and to determine whether two friction ridge impressions originated from one source. The majority of fingerprints found at the crime scene, or on crime articles are partly smudged and the experienced fingerprint expert should be able to say whether a mark is usable as fingerprint evidence or not (Nath, 2010: 120). This aspect emphasizes the importance of using properly trained officers to uplift and compare prints.

Gibbons (1991: 17) revealed that there are departments that use law enforcement systems (e.g., the SAPS system) to check criminal records on their applicants to see if the applicant has criminal convictions and such information is retrieved by means of fingerprints. As discussed above, this is a known procedure in South Africa that when a person is applying for employment, a visa, and other documentation, he/she is first checked for convictions known as clearance. Section 113 (2) (iii) of the Firearms Control Act provides that the person who has control over prints or has taken them in terms of this section may examine them for the purpose of the investigation. Fingerprint experts identifying or comparing fingerprints are authorised by law to give identification findings to be used in court proceedings, whether positive or negative. The experts may be used in court as prima facie proof for the results they established during fingerprint comparisons as long as the results or findings are accompanied by an affidavit of that expert detailing them. Section 212 (4) (a) (vi) of the Criminal Procedure Act 1977 states that an affidavit made by a person who alleges that he/she is in the service of the State and that he established such facts by means of an examination shall be prima facie proof of such fact.

Similarly, Section 36C (1) of Criminal Law (Forensic Procedures) Act No. 6 of 2010 allows the police to take prints found on the property and examine them if they believe that such prints will be valuable to the investigation of crime. This Act regulates uplifting of fingerprints from the crime scene so that not all people are allowed to pick up fingerprints from a crime scene. Fingerprint experts uplifting fingerprints from the crime scene are required to submit affidavits as a confirmation that the fingerprints were uplifted by an authorised and trained person performing his official duties. This will avoid delaying questions or tactics during cross examinations.

Section 225 (1) (a) of the Criminal Procedure Act, No. 57 of 1977 states that whenever it is relevant at criminal proceedings to ascertain whether any fingerprint of an accused corresponds to any other fingerprint shall not be inadmissible by reason that the fingerprint was not taken in accordance with the provisions of section 37, or that it was taken or ascertained against the wish, or the will of the accused concerned. This implies that people cannot refuse to submit fingerprints if the police want to ascertain if the fingerprints correspond with other fingerprints under investigation and the outcome of that investigation should be admissible in court.

According to the South African Police Service Act, No. 68 of 1995, the functions of the SAPS are as follows, to:

- Ensure the safety and security of all persons and property in the national territory.
- Uphold and safeguard the fundamental rights of every person.
- Ensure co-operation between the Service and the communities it serves in the combating of crime.
- Reflect respect for victims of crime and an understanding of their needs.
- Ensure effective civilian supervision over the Services.

The SAPS has the function of safeguarding the fundamental rights of citizens which includes the right to privacy. It is the reason why police can be trusted with information at their disposal. The SAPS have policies and standing orders regulating the use of highly confidential information.

The objectives of the SAPS as per Section 205 of the Constitution are to:

- Prevent, combat, and investigate crime.
- Maintain public order.

- Protect and secure the inhabitants of South Africa and their property.
- Uphold and enforce the law.

The SAPS has a mission to accomplish, and therefore there should be support or assistance from other criminal justice system departments who have the same goal. The goal of the police is to ensure that the citizens of South Africa live in a safe country without fearing any harm; however it is impossible to achieve such goal without having to involve sister departments in the process. Living in a crime free country is the dream of every citizen. When a criminal commits a crime and flees the scene, leaving fingerprints behind, no matter how small the crime is, the person reporting that crime believes that the police will catch the offender because of the fingerprints present at the crime scene, unaware of the fact that the police powers are limited.

3.6.3. Department of Home Affairs (DHA)

Section 10 of the Identification Act, No. 68 of 1997 states that every person who has reached the age of 16 years shall, when he/she applies for an identity card, gets his/her fingerprints taken in the prescribed manner so that they may be included in the population register. The Identification Act defines the population register as the register containing details of the population of the Republic of South Africa. This implies that the details of every person over the age of 16 in South Africa will be available in the DHA population register.

Section 2 of the Identification Act, No. 68 of 1997 states that the information contained in the population register which existed immediately prior to the commencement of this Act, as well as the information contained in any document kept by the Director-General under any law, which are appropriate for the compilation and maintenance of the population register be utilised by the Director-General for that purpose. The Act restricts access to the population register since Section 6 of the Identification Act states that subject to the provisions of this Act, no person shall have access to the population register and no person shall record or amend any particulars in such register unless specifically authorised thereto by the Director-General.

According to Section 12 (a) and (b) of the Identification Act, No. 68 of 1997, the Director-General may:

a) Request any person to furnish the Director-General with proof of the correctness of any particulars which have been furnished in respect of such person in any document in terms of this Act.
b) Investigate or cause to be investigated any matter in respect of particulars required to be recorded in the population register.

Section 21 (1) of the Identification Act, No. 68 of 1997 states that no person shall publish or communicate to any other person any information recorded in the population register. The Identification Act further authorises issuing of information on the population register if the person requesting the information is included in the population register. The Department of Home Affairs protects the information because of these Acts. It is advantageous that the DHA can be trusted with information, but as part of government they should also protect police credibility by providing the police with information that is needed in order to solve cases. Many cases which are closed as undetected lack the suspects` fingerprint information, but when the DHA has the information, Section 36 should be used in investigations as discussed above.

Section 21 (2) of the of the Identification Act, No. 68 of 1997 states that the Director-General may furnish any information in respect of a person whose name is included in the population register to:

a) Any person or institution on behalf of, and on the written instruction of, any such person.
b) Any state department, municipality, or statutory body.
c) Any organisation, body, society, or institution whose main activity is insurance business as defined in the Insurance Act, 1943 (No. 27 of 1943), or banking as contemplated in the Banks Act, 1990 (No. 94 of 1990); or
d) Any other organisation, body, society or institution, subject to the restrictions, conditions, exclusions, directives and fees as may be prescribed.

This covers the requests done by the police, as the SAPS is a public body and the police are included in the population register as citizens and as law enforcement officers. Section 21 (3) does not authorise the issuing of information from the population register unless the information is required for the exercise or protection of rights or public interest. The DHA Annual Report (2017/2018: 67) reported that the DHA has developed a new system and data migration which is the cornerstone of the National Identity System (NIS). This new system was planned for the 2018/19 financial year. According to the DHA Annual Report (2017/2018: 67) it will enable effective e-government initiatives, with all departments and government entities that require instant identification and verification during service delivery having central access to the ABIS. This system will enable departments to utilise it without wasting time as it is said to enable effective e-government initiatives.

3.6.4. Department of Correctional Services

The Department of Correctional Services Performance Plan 2017/2018 (2018: 8) indicated that the use of biometric technology is the key to positive identification of inmates within the correctional system, to effect admission and release of inmates with greater accuracy and efficiency. Biometrics at the correctional services is an important tool, especially since there is always a risk of escapes whenever there are court transportations. Having the integrated system with the DCS will assist in quick reporting and broadcasting of escaped offenders for swift responses. Integrated information will also assist the DCS with possible recent addresses where offenders may seek refuge.

According to the Department of Correctional Services Procedure Manual (2019: 41), two sets of fingerprints must be taken in respect of offenders on the SAP 76, one set of fingerprints must be filed in the offender’s case file while the other set must be forwarded to the SAPS LCRC. The Procedure manual states that all efforts must be made to obtain the SAP 69(c) for previous convictions before admission into the system of community corrections. From the researchers experience, in most cases SAP 69s are not available at the time the offender goes to the correctional centre, and some offenders are sent to the correctional centre with their SAP 76 still lying on the administrator`s desk waiting to be captured and sent to the LCRC; unless the detective does his own capturing (charging the suspect on CAS system doing 5.3) and drives to the LCRC to get the criminal record (SAPS 69). However, with the new integrated system, the PIVA which is available at the police stations, getting such information before going or appearing in court might be possible. The DCS can obtain the information about the previous convictions from the police station where the offender is detained. However, it will be more convenient for the DCS to retrieve such information if the PIVA system was also implemented at the correctional centres. According to the interviews conducted, this system has not reached the correctional centres which participated in this study; and this was the main request by participants to have the integrated fingerprint systems for convenient filing of information.

The DCS procedure Manual (2019: 41) indicated that upon admission, the following information must be captured on the Community Corrections computer system and also be recorded in the reporting register (G439) which must be divided as follows: Registration number; Surname and initials; ID number; date of birth; race; sex; SAPS Case no; Court case no; offence; date of sentence; sentence/court order; date referred by court official; set date and time of reporting; date and time reported; residential address and telephone number; work address and telephone number. If the offenders are registered with ID numbers at the time of admission in the facility as mentioned above, there will be no double identities, there will be no wrong names registration, this implies that this requirement is ignored or it lacks computer systems that will refuse to store an offender`s information without an Identity Number. Having offenders recorded with ID numbers, will reduce fraudulent activities which are committed by people who are free, using identity numbers of people who are serving sentences.

According to the DCS Procedure Manual on an integrated and coordinated service delivery by Justice System, offices must preferably be located as close as possible to the local Departments of Justice and Constitutional Development (Courts), the SAPS and Social Development to promote an integrated and coordinated Criminal Justice System. The planned relocation of such departments must be ascertained to assist in determining the office location.

3.7. Standard Operating Procedure

There are criminal justice system departments which obtain people`s information directly from owners of information (clients) with possible correct information, like the Department of Transport, the Department of Home Affairs, the Department of Social Development, the Department of Labour and others. These departments collect fingerprints and information directly from clients and they provide their particulars voluntarily without any prejudice; unlike the SAPS and the DCS.

Offenders on the other hand, provide their particulars under pressure because they have to they sometimes even allege that information was given under pressure. Obtaining information directly from the owner of that information is stipulated by Section 12 (1) of POPI Act which states that personal information must be collected directly from the data subject and by that, they mostly get genuine, reliable information. The LCRC can obtain such information from other departments as provided by Section 12 (2) of POPI Act which provides that it is not necessary to collect data directly from the data subject if information is contained or derived from a public record or has been made public by the data subject. This implies that government departments as public entities can share people`s information, since people submitted their information voluntarily to other government departments, including the LCRC (Local Criminal Record Centre) as a government department.

Leseba (2015), the Chairperson of IJSB indicated in his presentation to the police committee that the PIVA was ready for deployment pending the sign-off of the Standard Operating Procedures. The PIVA (Person Identity Verification Application) has now been rolled out and is available in most police stations. Therefore, the current standard operating procedure where departments share information is PIVA. However, the LCRC members who participated in this study did not know about such system. This implies that the PIVA is indeed not for the LCRC or forensic investigation. It mainly assists courts with management of cases where docket information is shared amongst role players of court proceedings. This has been mentioned in the IJS PIVA report (2017: 6) that case management business applications have been developed and implemented for the SAPS, the NPA and the DOJ&CD.

The SAPS has the LCRC office which does comparison, verifying and identification of fingerprints. Where an identification of an unknown deceased is required, the fingerprints of the deceased are sent to National CRC who then provides the identification of the unknown deceased via DHA. This procedure not only protects vulnerability of the DHA information, but it is also effective in controlling the traffic of investigators going to and from DHA offices for identification. However, it does not assist the local or provincial CRC where a multitude of property crimes where fingerprints are involved are closed undetected. Currently this is the situation for the LCRC which does not help investigation, since the PIVA system integrates information on case management and offender movement. The PIVA is more operational and effective after the arrest of the offender whilst the LCRC needs information for the arrest. The IJS Report (2017: 7) indicated that the new integration system will assist the forwarding of docket information from the SAPS to court electronically, and automatically share it with the NPA by means of the IJS Transversal Hub. This confirms that the PIVA in police stations is mainly for sharing information between the court, the SAPS and NPA and maybe DCS at a later stage.

The National Identity System (NIS) once integrated or powered by the ABIS, will enable a system of national identification for South Africa and the full modernisation of the DHA systems (DHA Annual Report 2017/2018: 67). Once the DHA fully develops the ABIS, departments will acquire identification information; and retrieve accurate information since the subject of information provides the true information about himself/herself. Departments with personal information can share information for investigation purposes and or prosecution purposes as stipulated in several legislations. If Local Criminal Record Centre can have access to information contained in other departments, information can also be compared for authenticity. It will assist in obtaining genuine information of suspects especially from the departments where people are honestly providing information without fear of being targeted.

Information contained in the Department of Home Affairs, the Department of Transport and the Department of Social Development may be more trustworthy than that controlled by the SAPS. From the researcher` s experience, some offenders give false information during arrest fearing to be traced and to be recognised as a repeat offender. Information contained in SAPS system can have more than one name with the same set of fingerprints and the real name remains unknown.

3.7.1. Systems that are shared by government departments

Section 15D (4) of Criminal Law (Forensic Procedure) Act 6 No. of 2010 No. states that the departments must develop a standard operating procedure regarding access to the database and security measures to protect privacy of people`s information. There are systems that are shared by government departments where sensitive information of employees is stored, where government payments are made and where the information of private businesses are kept for referral purposes. These systems are protected and people working with these systems are trusted, sensitized and warned about illegal use of information.

- **Basic Accounting System (BAS)**

There is another system called the Basic Accounting System (BAS) where all government payments are made there are also restrictions of who is eligible to access such system. Mamoojee, the Accountant General (2001) explained that during January 2001 the National Treasury took a decision to implement the BAS at all National Departments utilising Financial Management System to consolidate financial systems in government to a single platform. The Department of National Treasury (2007) emphasised that due to the sensitive nature of the accounting system and the number of users using the system, it was necessary to include various security features to prevent misuse of the system and the following measures were put in place to protect the system:

- Individual User IDs for every person utilising the system.
- Self-chosen passwords for everyone that expires after a predetermined period.
- The ability to deactivate or activate individual User IDs.
- Immediate BAS Function locking facility; and
- Limited number of login attempts.

The Department of National Treasury (2007) pointed out that users of the system are given a certain level of clearance based on the tasks they need to perform their jobs and, depending which level of clearance they have, are assigned access to a group, which is set up and maintained by the Systems Administrator. This implies that BAS users are people nominated according to the tasks that they perform.

- **PERSAL System**

In 1986 Government decided to implement a computerised Personnel and Salary System which gave birth to PERSAL, the word PERSAL is the acronym for Personnel and Salary (Office of the Premier, 2017: 4). The Office of the Premier (2017: 4) explained that the PERSAL system was designed to cater for all aspects of government regulations, prescripts, treasury instructions and policies and it is used by all National and Provincial government departments. Access to this system is controlled by means of User ID, password and a fingerprint, which means no second person can log onto the system by means someone else`s logon details.

- **Central Suppliers Database (CSD)**

Government has another system shared by all government departments known as the Central Supplier Database (CSD). The Department of National Treasury describes the CSD as the system which maintains a database of organisations, institutions and individuals who can provide goods and services to the government. The Department of National Treasury further explains that the CSD serves as a single source of key supplier information for organs of state, providing consolidated, accurate, up-to-date, complete, and verified supplier information to procuring organs of state. Practically, when business suppliers apply for advertised government tenders, the Supply Chain Management (SCM) officers from various government departments first log into the system to see if the companies are registered on CSD or not. This assists government departments to confirm the company details before awarding the tenders and to see if the companies do provide services advertised before tenders are awarded to them.

This is also an example of a successful sharing of information by government departments where not all government officials can access the system, but certain individuals are authorised access to protect people`s information.

Another method that can be used to create passwords to ensure protection of people`s privacy, is by the creation of face recognition features. The ABIS system as indicated by the DHA Annual Report, 2017/2018 (2018: 10), allows the identification and verification by fingerprint, facial, iris recognition and other means. These features are meant for suspects and any person required to be verified, they can also be used for the protection of information, where officials working with such information can be authenticated by means of facial recognition. Shu Chang (2022: Para 19) in his study for the face recognition security, emphasised that the face recognition security feature does not mean the use of ID cards with pictures, but the face recognition feature must have the face edge information as the main observation feature. This security feature will also reduce sharing of passwords. As indicated earlier that ABIS already has the face recognition feature for the wanted suspects and people required for verification.

3.8. Summary

This chapter discussed South African legislation that govern the use of fingerprints. In Chapter 2 of the Constitution of the Republic of South Africa No. 108 of 1996, the Bill of Rights and Protection of Personal Information Act No, 4 of 2013 provide restrictions to access other people`s personal information, unless permission was obtained from the person in question, or the subject of information was present during the accessing of information. Section 12 (1) of POPI Act provides that personal information must be collected directly from the data subject. However, for the purpose of criminal investigations, Criminal Law (Forensic Procedure) Amendment Act No. 6 of 2010 authorises the police to have access to people`s information contained in databases of other government departments which is discussed in the next chapter. Chapter 4 provides the literature review on the fingerprints identification systems that can be used for the investigation of latent prints of first-time offenders.

CHAPTER FOUR: THE FINGERPRINTS IDENTIFICATION SYSTEMS THAT CAN BE USED ON THE INVESTIGATION OF LATENT PRINTS OF FIRST-TIME OFFENDERS.

4.1. Introduction

The closing of cases as “undetected” because suspects cannot be identified is an embarrassment to the community who rely on the police for the detection of suspects. Criminals take advantage of the criminal justice system because they have the perception that they will never get caught. The previous chapter discussed the closing of dockets and a number of legislations which are against the use and sharing of people`s information and how it impacts on service delivery. The chapter also discussed the legislation which justifies the sharing of information for investigation purposes.

This chapter discusses the main objective of this study which is the importance of sharing fingerprint systems between government departments to enhance the investigation of latent prints of first-time offender. Different government departments will be discussed to explore on how their fingerprints systems can contribute in the investigation of latent prints of first-time offenders. This chapter also discusses the use of fingerprints when they are extracted from the crime scene and when they are used in the court of law to charge the suspect. The current standard operating procedures that are in place in other private and government departments to ensure that people’ privacy is protected is also discussed.

4.2. Fingerprints

Fingerprints, along with the DNA of a person, are powerful methods for establishing identity (Lyle, 2012: 243). As mentioned in Chapter 1, James, Nordby and Bell (2016: 328) explained that fingerprints are unique and because of its uniqueness they are commonly used to identify people. According to Shaler (2012: 211), there are three forms in which fingerprints occur namely latent (invisible), patent (visible), and impression or plastic which will be discussed below.

4.3. The use of fingerprints identification systems on latent prints of first-time offenders

Daluz (2015: 83) is of the view that identifying an individual’s is possible because fingerprints are both unique and permanent. Irrespective of the form of a fingerprint found at the crime scene, the ultimate purpose of uplifting fingerprints is to identify the individual that had physical contact with such crime scene. As Locard` s principle states, each contact leaves a trace. Newburn, Williamson and Wright (2011: 320) affirmed that every time a person makes contact with another person, place, or anything else, it results in an exchange of physical materials. Therefore, identifying fingerprints at the crime scene is critically important to trace perpetrators.

Fingerprints are not picked up by any police officer but must be lifted by a trained fingerprints expert. Kriel (2011) indicated that a variety of techniques, including the use of chemicals, powders, lasers, alternate light sources, and other physical means, are employed in the detection and development of latent prints. Police officers (first responders) at the crime scene can assist the investigation by identifying visible prints which are visible to the naked eye; as Lyle (2012: 254) explained that some prints are readily visible while others require diligent searching.

Police officers can assist to protect the crime scene by physically avoiding contact with the surface containing fingerprints and by removing witnesses from the crime scene. Lyle (2012: 32) pointed out that since the police officer might not know if the suspect is amongst the witnesses, he must prevent all of them from entering the scene. Since a witness can also be a suspect, the police must then avoid losing evidence or getting evidence destroyed. Kriel (2011) emphasised that all objects at the scene of the crime should be considered as possible sources of fingerprints that may lead to the identification of the offender. Careful attention is needed when dealing with crime scene to avoid contaminating invisible prints that can only be identified by an expert.

Not every crime scene will have fingerprints available as discussed however, there are techniques that may assist trying to locate fingerprints that are not visible to the naked eye. As mentioned by Ogle and Plotkin (2018: 10) prior to the comparison of the questioned item to the known item, a thorough examination of the questioned item is accomplished by means of one or more of the following techniques unaided eye, magnifier, stereoscopic microscope, or an alternate light source. Some of these techniques are used in crime scenes to locate or identify fingerprints.

Saferstein (2011:86) opined that the process of identification requires the adoption of testing procedures that give characteristic results for a specific standard material. Once these test results have been established, they may be permanently recorded and used repeatedly to prove the identity of suspect material. According to Shaler (2012: 211) there are three forms that fingerprints can manifest: latent, patent and impression prints.

4.3.1. Latent (invisible)

Kriel (2011) described latent prints as impressions produced by the ridged skin, known as friction ridges, on human fingers, palms, and the soles of the feet. Kriel (2011) further explained that examiners analyse and compare latent prints to known prints of individual to make identifications or exclusions. This confirms that unknown fingerprints are identifiable and can be linked to only one person, and an unknown suspect can be identified by fingerprint examiners. Kriel (2011) stated that points out that in instances where latent prints have limited quality and quantity of detail, personnel may perform a microscopic examination to make conclusive comparisons. This procedure can assist in cases where fingerprints are less visible.

Lyle (2012: 254) explained that latent prints are not visible and cannot be seen without special lighting or processing. This confirms that the uplifting of latent prints and subsequent comparison can only be done by a trained official, not by any police officer at police station. Since the current integrated fingerprint system is implemented at police stations, police officers who are not fingerprint experts cannot uplift latent prints and verify them on the PIVA (Person Identification Verification Application) system.

Kriel (2011) added that latent prints are among the most valuable and common types of physical evidence. It is therefore important to be able to identify those fingerprints. And all objects at the scene of the crime should be considered as possible sources of fingerprints that may lead to the identification of the offender.

Harber and Harber (2009: 58) referred to three characteristics of latent fingerprints which require further manipulation: -

- Crime scene latent prints are always small.
- There may be interference with the ridge patterns from details already on the surface
- Their visibility and contrast may not be adequate.

Mokwele (2015: 39) a former fingerprint expert, described latent print as the print that is left at the crime scene by the perpetrator, but it is not visible. All latent prints are regarded as prints made under unfavourable conditions and in most cases, they are not visible to the naked eye, but they are developed by means of fingerprint powders or chemicals in a laboratory to make them more visible.

4.3.2. Patent (visible to the naked eye)

Shaler (2012: 211) reiterated mentioned that patent prints may require nothing more than photography followed by using a method to lift the print. On the other hand, a patent print might require a well-thought-out strategy to enhance that which is visible and that which is latent. A patent print is said to occur when someone has a substance on his/her fingers like blood, grease, ink, or anything that leaves a visible print on a surface, unlike a latent print which is not visible. Patent prints are common in serious crimes like murder, where blood prints are found on the crime scene. Therefore, if a blood print or patent fingerprint is left by a killer who is a first-time offender, who is not on LCRC database, the PIVA system containing fingerprint information from other departments, including the Department of Home Affairs (DHA) will be very useful in identifying the killer.

Lyle (2012: 254) mentioned that patent prints are visible to the naked eye, as they occur when the perpetrator gets a substance such as blood, ink, paint or grease on his fingers and leaves behind a visible print. These fingerprints are easy to identify on the crime scene and they are easy to avoid for contamination. Access to the areas where patent fingerprints have been identified should be prohibited until the fingerprints expert has visited the scene. This is normally handled by the police who are known as the first responders at the crime scene.

4.3.3. Impression or plastic.

Lyle (2012: 255) defined plastic prints as three dimensional and occurs when the perpetrator impresses a print into a soft substance such as wax, putty, caulk, soap, moist paint, or even cold butter. Shaler (2012: 211) explained that if the print is plastic, that is, impressed into a soft surface, the scene scientist/investigator might decide to cast it using silicone-based material.

4.4. The process followed by the South African Police Service Local Criminal Record Centre in identifying unknown suspects` latent prints at crime scenes.

Saferstein (2011: 87) declared that comparison analysis subjects a suspect specimen and a standard/reference specimen to the same tests and examination to determine whether they have a common origin. Criminal Procedure Act No. 51 of 1977 section 225 authorises the comparison of fingerprints whether the fingerprints were obtained consensual or not: Section 225 (2) stated that any fingerprint which corresponds with the fingerprint of an accused cannot be inadmissible because it was obtained against the will of the accused. Section 113 (2) (IV) of Firearms Act No 60 of 2000 provides that may cause any prints taken under any power conferred by this section to be subjected to a comparative search. Ogle and Plotkin (2018: 12) believed that the quality of the laboratory analysis depends profoundly on the collection and submission of proper standards and controls for each item submitted.

Ogle and Plotkin (2018: 12) categorised known comparison of fingerprints in two forms namely the comparison standards and the exemplar:

- **The Comparison Standards**

There is described as those materials collected from a known source for comparison with a question sample, in order to determine whether the questioned sample came from the same source as the comparison standard**.** In this case, comparison standard is the set of prints collected from a suspect (known suspect) to compare with the fingerprints collected from a crime scene.

- **The Exemplars**

This term is used to describe either a sample of the comparison standard collected for the purpose of comparison with the question item or the entire comparison standard used for comparison with the questioned item (Ogle & Plotkin, 2018: 12). Items derived from the standards for use in laboratory comparison with the questioned items are referred to as exemplar items.

Saferstein (2011: 95) clarified the following on how comparison and identification of fingerprints process is done:-

> *"Once the quality of the print is deemed suitable for the IAFIS search, the latent-print examiner creates a digital image of the print with either a digital camera or a scanner, marks points of the print to guide the computerized search. The print is then electronically submitted to IAFIS and within minutes the search is completed against all fingerprint images in IAFIS, the examiner may receive a list of potential candidates and their corresponding fingerprints for comparison and identification".*

The purpose of fingerprint comparison is to identify an unknown suspect, to individualise or isolate the suspect from other suspects, or to eliminate an innocent witness from the suspects. In a robbery case for instance, witnesses' fingerprints can be confused with suspects' fingerprints, and the witnesses` fingerprints can be collected and eliminated from foreign fingerprints found on the crime scene, and the foreign prints can be identified as those of a suspect. Ogle and Plotkin (2018: 10) mentioned that the purpose of the laboratory analysis is to individualise the physical evidence. In a robbery case where the victim was shot, the firearm recovered, and the suspects arrested; fingerprints lifted from the firearm can reveal that only one suspect fired the shots, and that suspect can be individualised from other suspects as the one who pulled the trigger. All the suspects may be charged for murder, but sentencing may differ as a result of the individualisation of the prints.

Ogle and Plotkin (2018: 10) defined individualisation as the identification of the individual source of the evidence item. Kriel (2011) pointed out that by examining the evidence submitted, the laboratory may be able to:

- Determine the presence of latent prints
- Determine if latent prints are identifiable
- Compare and identify latent prints with the inked prints of suspects and with others for elimination purposes.
- Establish the identity of unknown deceased persons
- Identify the prints via the Automated Fingerprints Identification System (AFIS).

Fingerprints experts summoned to crime scenes are expected to find and uplift fingerprints pointed out by either witnesses or police officers already at the crime scene. It is therefore important to note that not all fingerprints are identifiable if they are present at all. In other cases, fingerprint experts fail to find fingerprints because they have been contaminated or smudged. It is also important for the case to uplift latent prints and then obtain fingerprints from individuals who frequently operate in the place on to eliminate them from the case so that they are not regarded as suspects. Ogle and Plotkin (2018: 12) suggested that the quality of the laboratory analysis depends heavily on the collection and submission of proper standards and controls for each item submitted. Experts uplifting the prints from the crime scenes are not the same as those who have to do the comparison.

Therefore, proper uplifting is vital for the ones doing the comparison. Similar to the obtaining of fingerprints from suspects, the police who uplift the fingerprints are forced to do it meticulously, because the obtained prints (SAP 76) are sent to the LCRC for fingerprints experts to determine if the charged person has a criminal record or not and to put the current crime on record. If the set of fingerprints is not clear, the experts do not use the SAP 76 form, and the offence will not be recorded against the offender. The police are then told to retake another set of fingerprints, which can happen if the charged person is still in custody. In other cases where the person was given bail, the investigating officer waits for the court date and the accused is requested for a redo of prints inside the court. This procedure is according to the researcher`s experience as a former detective.

A process of elimination process is also used in cases where police officers have attended a case and their fingerprints are also found at the crime scene; for example in a hijacking case, the fingerprints of hijackers and police officers who recovered the vehicle, are normally found on the hijacked vehicle. It is the duty of the investigating officer to eliminate the information found and excludes the SAPS members from the list of suspects. This can only happen after establishing which SAPS members were present during the recovery of the vehicle, so that their prints can be eliminated from those who may be suspects. Harber and Harber (2009: 54) were of the view that a skilled crime scene investigator predicts the location, the characteristics of the prints, and the specific fingers in the prints that he/she will find, given the perpetrator`s intentions at that location.

Daluz (2015: 83) explained the purpose of comparing fingerprints as; to determine whether an unknown latent fingerprint and a known fingerprint come from the same source. Police officers` fingerprints are stored in the police database as employees and they are easily identified if found on crime scenes although those prints are not stored in Criminal Record Centre as criminals. Daluz (2015: 83) claimed that identifying an individual as the source of a latent print is possible because fingerprints are both unique and permanent as discussed above, that fingerprints can be identified even after the person had tried to destroy his fingerprints with acid poured into his hands.

Harber and Harber (2009: 5) indicated that all judges who have made a ruling to admit fingerprint evidence treat the identification based on fingerprint comparison as 100 percent accurate. Identity obtained through fingerprint evidence is admissible and treated as proof beyond reasonable doubts that the person who left the prints is the person identified by the examiner. An item with an unknown source that is to be compared with an item from a known source in order to establish whether or not the questioned and known sample share the same source (Ogle and Plotkin, 2018: 12). This implies that an unknown fingerprint is compared with a known fingerprint to establish whether the unknown fingerprint and the known fingerprint are from the same person.

There is a distinctive link between Criminal Law (Forensic Procedures) Amendment Act 6 of 2010 and Criminal Law (Forensic Procedures) Amendment Act No. 37 of 2013; these Acts are a continuation of each other, and they are not an amendment of each other. Section 1 of the Criminal Law (Forensic Procedures) Amendment Act No. 37 of 2013, links the fingerprints of offenders with their DNA by stating that:

a. When a buccal sample is collected from an arrested person, the DNA Reference (buccal) Collection kit must be utilised and his/her fingerprints must be taken on form SAPS 76.

b. The unique barcode form reference number of the DNA Reference (buccal) Collection kit must be recorded on the fingerprint form SAPS 76 and on the collection form (provided with the DNA Reference (buccal) Collection kit).

This implies that the fingerprints of an offender are now connected to the DNA and the DNA is stored in the DNA database, and the DNA barcode is recorded on SAP 76 which is stored in the fingerprint database at the LCRC. The details of an offender are now found in the fingerprint database and in the DNA database making it easier to identify repeat offenders. However, this still does not assist with first-time offenders` information.

This, however, has been emphasised earlier that if SAPS can store information of all security checks applications, they will have a database with most of South African citizens if not all. As discussed above about the collection of DNA, the DNA Act authorises police to collect DNA samples from all people arrested and charged on all types of crime not only on sexual offences. The SAPS also collects DNA samples from all SAPS employees and new recruits to have everybody`s DNA stored on the DNA database. Prior to the Criminal Law (Forensic Procedures) Amendment Act No. 37 of 2013, DNA samples were only collected from people charged with rape and other cases where a DNA investigation was involved. In similar fashion, the collection and the creation of such fingerprint database will assist the LCRC with more information to work on, so that they do not rely on the criminal record database only. Currently the LCRC does have a system of SAPS employees which supplies police information on hijacked vehicles and thereafter those police officers are not recorded as criminals and are not charged as the stored information indicates that they are SAPS employees or former SAPS employees.

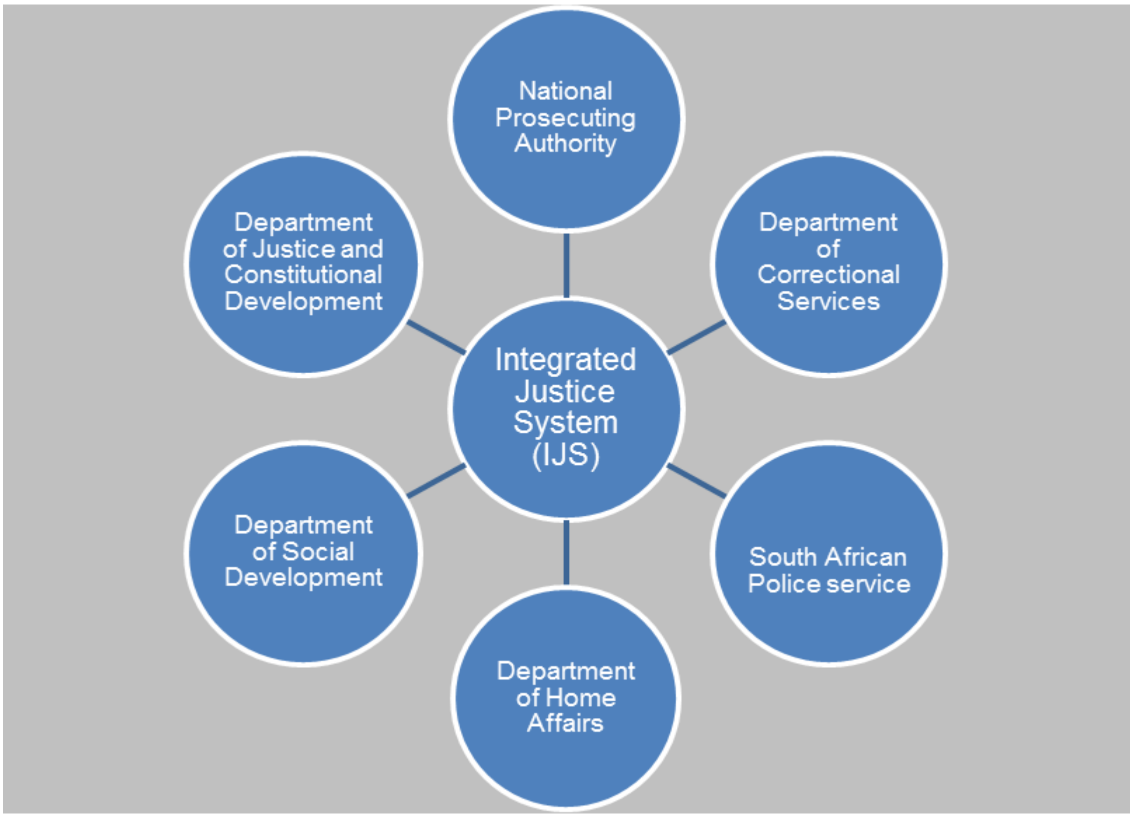
4.5. The challenges faced by the South African Police Service Local Criminal Record Centre in identifying first-time offender on fingerprints at crime scene.

Cross (2010: 13) believed that without criminal justice, criminal law cannot be enforced. Also, without criminal law, criminal justice has nothing to enforce, therefore criminal law and criminal justice should work hand in hand. Similarly, Davies *et al.* (2010: 8) state that criminal justice is about society`s formal response to crime and is defined in terms of a series of decisions and actions taken by a series of agencies in response to crime. The White Paper on Remand Detention Management in South Africa (2014: 2) regarded the critical partners in the implementation of the White Paper to be the South African Police Service, the Department of Social Development, the National Prosecuting Authority, the Department of Justice and Constitutional Development and the Legal Aid South Africa.

For the purpose of this study, the departments that will be discussed as part of criminal justice system are those departments pointed out by the Criminal Law (Forensic Procedure) Amendment Act No. 6 of 2010 and by the The White Paper on Remand Detention Management in South Africa, the South African Police Service (SAPS), the Department of Justice and Constitutional Development, the Department of Correctional Service (DCS), the Department of Home Affairs (DHA), the Department of Social Development (DSD), National Prosecuting Authority (NPA) and the Legal Aid South Africa.

It is crucial that the information system of every department is integrated to avoid dishonest and false information. The IJS Report (2017: 6) reported that the Integrated Justice System programme has worked together with other departments to establish electronic case management and workflow applications that support the core business processes of the department. This implies that the DOJ/IJS was concerned about service delivery, and they implemented this case management programme. Similarly, the sharing of personal information is important to assist other departments for effective service delivery. When the community blames the criminal justice system, they blame all role players. One department cannot fail to trace a suspect whereas, another department has all the information to locate the suspect and it is regarded as lack of unity and collaboration. The IJS Report (2017: 7) indicated that an integration milestone was achieved in March 2016; with the electronic integration of SAPS, NPA and DOJ & CD for the exchange of docket and case information. This case management solution has expanded to a national footprint of 509 Courts and 1,144 police stations across the RSA. Participants from the Integrated Justice System (IJS) were asked which government departments were currently involved in the integrated justice system and the participants indicated that as of 2021 it is the SAPS, the Department of Home Affairs (DHA), the National Prosecuting Authority (NPA), the Department of Justice and the Constitutional Development (DOJ & CD), DCS, the Department of Social Development (DSD), Legal Aid South Africa, the Office of the Chief Justice (OCJ) and South African Social Security Agency (SASSA).

Figure 2: Integrated Justice System


National Prosecuting Authority
Department of Justice and Constitutional Development
Department of Correctional Services
Integrated Justice System (IJS)
Department of Social Development
South African Police service
Department of Home Affairs

IJS Report (2017: 6) indicated that case management business applications had been developed and implemented for the SAPS, the NPA and the DOJ & CD. System development processes have already commenced for Legal Aid SA, the Department of Social Development and the Department of Correctional Services, with anticipated implementation of the case integration for these three departments in the 2017/18 financial year. It has been confirmed through interviews that the PIVA system is already in operation in police stations. The integration will not only assist law enforcement agencies but other departments which do not work with criminal cases will also benefit in fighting fraud and will save thousands of rand for the government. The involvement of the Department of Employment and Labour has not been mentioned yet. The Auditor General Makwethu (2020: 5) mentioned that the reason why Covid-19 relief grants were paid to undeserving individuals is because all the government department systems are not integrated.

The Integrated Justice System has been in operation decades ago, and the intention to fight crime together as government departments has been there since 1998. The DOJ & CD Annual Report (1998/1999: 32) reported that in order to address the inefficiencies within the criminal justice system, Government commissioned a project called the Integrated Justice System (IJS) project; and the overall aim was to transform the system so that it functioned in an integrated, rather than in a compartmentalised manner. In this report, the IJS mentioned the separation of four departments (Department of Justice, Safety and Security, Department of Social Development and Department of Correctional Services) as one of the causes for the inadequate response of the justice system to the problems related to crime.

Nevertheless, the integration in this manner, as proposed by this study and as mentioned in the Criminal Law (Forensic Procedures) Amendment Act No. 6 of 2010 has not been successful, because the statistics on the detection rate of priority crimes is still very low as indicated in the number of complaints reported in figure 1 and figure 3. The DOJ & CD Annual Report (1998/1999: 32) reported that some of the reasons for the inadequate response of the system to the problem of crime are the following:

- Inefficient and ineffective functioning within the four departments in the criminal justice cluster Justice, Safety and Security, Welfare and Correctional Services.
- A lack of integration of the activities, systems, processes, and information within the core departments.

- Poor teamwork and insufficient joint training.
- A low level of automation of systems and processes.
- A high degree of duplication within and between departments.
- A lack of timely positive identification of offenders.

The problem that is currently being resolved on integrating government departments as per the Criminal Law (Forensic Procedure) Amendment Act No. 6 of 2010 has been an issue since 1998, as well as integrating activities, systems, processes and information. Government loses huge amount of money on fraudulent social grants to non-existing children, and to fight this scourge, the sharing of fingerprint information between the Department of Home Affairs and the Department of Social Development can be a solution to this problem. The lack of integration and operating independently and isolation between government departments had cost the Department of Social Department much money during the COVID-19 Pandemic. Fraudsters managed to register deceased people and sentenced inmates for the Covid-19 relief fund.

According to Makwethu the Auditor General (2020: 5) after a thorough analysis of payments and checking with other government departments, a large number of payments were made to people who are not eligible for the relief fund, for instance, deceased, people working in government, people receiving social grants and students funded by NSFAS (National Student Financial Aid Scheme). If the Department had access to the DCS and the DHA systems such activities would have been stopped. The Department of Employment and Labour only had access to its information system during these applications and errors were picked up after the damage had already been done. During the application process some applications were declined as the system managed to detect those applicants as being employed.

During interviews with the Department of Correctional Services, it emerged that inmates are admitted at the facilities without the requirement of an official Identity document therefore the inmates can use false names making it difficult to be traced. If the inmates were admitted with their ID Books in the correctional centre such information would have been available to other departments including the

Department of Employment and Labour as they would have detected that such people with those ID numbers were serving sentences in correctional centres.

> *"The information technology systems across government carry data on almost everyone in the country; for example, there is information on the Home Affairs databases on identity numbers and deceased people, the South African Revenue Service databases include information on the earnings of people, the details of grant recipients are on the social pension systems, and the salary systems of public sector entities carry information on government employees. But this rich data is not integrated, shared across government, or effectively used by the UIF and Sassa (and similar entities) to check if people applying for benefits and grants qualify for these,"* (Makwethu, 2020: 4).

4.5.1. South African Police Service

Section 37 (1) of the Criminal Procedure Act No. 57 of 1977 states that any police official may take the finger-prints, palm-prints or foot-prints or may request any such prints to be taken, of any person arrested upon any charge; of any such person released on bail or on warning under section 72, of any person arrested in respect of any matter and of any person upon whom summons has been issued in respect of an offence. Similarly, Section 113 (1) of Firearms Control Act No. 60 of 2000 states that any police official may without warrant take fingerprints or body-prints and bodily samples of a person or a group of persons or may request any such prints if there are reasonable grounds to suspect that that person has committed an offence and if there are reasonable grounds to believe that the prints will be of value in the investigation.

This is the reason why AFIS the police fingerprint system has fingerprints limited to criminal records only. It is because they only keep fingerprints of people charged or arrested and fingerprints of SAPS employees. This system is not shared or integrated with the Department of Correctional Services the IIMS (Integrated Inmate Management System) and it is not shared with any of the law enforcement agencies. Section 113 (1) of the Firearms Control Act states that any police official may without warrant take fingerprints or body-prints and bodily samples of a person or a group of persons.

This section gives powers to the police to obtain fingerprints from anybody for the purposes of investigation. Storing of fingerprints for future use like the DNA will not mean that the person giving fingerprints is charged. Police do not even store fingerprints of people who come to them for security clearances, like firearm applications, employment security clearance, travelling security clearance, etc. This fingerprint information should be stored in database different from the criminal record database like how they keep fingerprints information of SAPS employees; just like the DNA database that is done even on innocent SAPS employees, new recruits and offenders in all sorts of cases.

4.5.2. Department of Justice and Constitutional Development (DOJ & CD)

According to Thomas (2009: 8) the Chairperson of the Integrated Justice System Board (IJSB), the IJSB made a submission to the police portfolio committee in respect of considerations arising from the proposed criminal law (forensic services) amendment Bill. The IJSB consists of the following departments, the Department of Justice and Constitutional Development, the National Prosecuting Authority, the Department of Social Development, the Department of Correctional Services and the South African Police Service (Thomas, 2009; 8). The word “proposed” implies that at that time the Bill was not enacted but was still in process.

In March 2009 the IJSB facilitated a two-day workshop with the parties and representatives of the Office of Criminal Justice Reform (OCJR) this workshop was facilitated to clarify requirements and system limitations that needed to be considered in devising an appropriate information sharing strategy between the SAPS, the DHA and the DOT. Thomas (2009: 2) provided an initial assessment of the impact on systems that were in place and broad estimates of timescales, together with the anticipated costs arising from the promulgation of the proposed Criminal Law Forensic Services Amendment bill. All role players in the integrated justice system were concerned about service delivery and the quality service to the community which was the main focus.

The Integrated Justice System Board made the submission to the police committee in November 2009 before the Criminal Law Forensic Procedure Act No. 6 of 2010 was promulgated or published since it was promulgated in October 2010. This indicates that the Department of Justice and Constitutional Development saw the need for the identification and verification of suspects on the investigation side to enhance the investigation by means of fingerprints and DNA.

The Department of Justice implemented an integrated justice system to manage the backlog of criminal cases, the development and finalisation of the Integrated Criminal Justice Strategy (ICJS) which would lead to a better coordination and the realisation of the National Development Plan (NDP)'s Vision 2030 (DOJ and CD Annual Report, 2017/2018: 47). The Integrated Justice System (2017: 3) described Integrated Justice System (IJS) programme as government`s initiative to improve the efficiency and effectiveness of the South African criminal justice process; it is driving a multidepartment effort to increase the probability of successful investigation, prosecution, punishment, and ultimately the rehabilitation of offenders and their restoration back into society to realise a national objective that all South Africans are safe and they do feel safe.

4.5.3. Department of Correctional Services

According to PMG the Parliamentary Monitoring Group (2001) the Minister of Correctional Services Ben Skosana told the Committee on the briefing of Automated Fingerprint System, that the integrated criminal justice system approach envisaged in terms of the National Crime Prevention Strategy has necessitated a review of the strategic role played by correctional services in crime prevention. The Committee was told that:

> *"The automated fingerprint system would be used in the integrated justice system consisting of the Department of Correctional Services, Social Development, Safety and Security, and Justice. This system will allow the Department to track offenders electronically without using the old manual system. This system is meant for verification primarily within the processes of admission, releases and releases to court, roll calls, visitations as well as movement management of offenders where their identification is required. Focusing on rehabilitation during the time of imprisonment was also emphasized."*

Thomas (2009: 4) the Chairperson of Integrated Justice System Board (IJSB) indicated that the DCS was busy with the development of a fingerprint and photographic enrolment module for their Admissions and Release System (A&R) for the future Remand Detainee Offender Management System (RDOMS). The DCS consists of different persons, not only people who are arrested and charged by the police. There are people who are detained by home affairs (illegal migrations), people who are detained by the courts due to mental illness and then people who are detained via SAPS. The following is the detailed categories of people detained in Correctional centres.

The DCS Annual Performance Plan (2017/2018: 14) explained that the Department of Correctional Services detains sentenced and un-sentenced inmates. The un-sentenced inmates consist of remand detainees, state patients and the deportation group. Below is the category of the different types of detainees in the correctional centres.

Remand Detainees

- Accused persons who have been detained after the first court appearance whose trial have not commenced.
- Accused persons in detention whose cases are in the process of being heard by the courts, those who are in the trial phase.
- Accused persons detained by the DCS pending observation at designated Mental Health Establishments (Observation cases)
- Accused persons who are detained mainly for extradition in line with section 9 of the Extradition Act 67 of 1962
- Accused persons who are convicted and waiting for sentencing.

The Deportation group consists of detainees who fall under the mandate of the Department of Home Affairs (DHA) and are not the clients of the Criminal Justice System. They are detained and released through the warrants from the DHA.

State patients are un-sentenced persons who are classified as such by courts and detained in the DCS while awaiting placement at designated Mental Health Institutions.

The above categories confirm that not all inmates are offenders, which also confirms that the DCS may have inmates which are not available of the AFIS (the police system). During the interviews some participants argued that there are no inmates detained at correctional centres that the SAPS does not know about, some participants were of the view that correctional centres only have arrested and charged persons; but this report proves otherwise. If the IIMS the DCS fingerprints system can be shared with other departments, people committing fraud by applying for grants using details of mentally ill people who are detained mentally as state patients will be stopped from doing that. These patients will be on the DCS system but not on the AFIS. Therefore, having the systems shared either by the PIVA system or amongst them will prevent crime to a large extent.

4.5.3.1. Challenges faced by the Department of Correctional Services

During the interviews, the DCS participants confirmed that they used to have a fingerprint system, but it stopped working and it was linked with other departments. The AFIS has been rolled out in the DHA and replaced with the HANIS and now the ABIS before it could be used as mentioned above. Had the departments really shared the AFIS LCRC, it would not have had a problem in identifying first-time offenders, because all departments would have been storing information on the AFIS and authorize others to access the information. Now only the SAPS LCRC is use the AFIS, as the DCS uses IIMS and the DHA uses ABIS and the IJS uses the PIVA for integration, all of which limits access to police stations only and not to the LCRC.

During interviews and observation at the Records Section of Westville Correctional Centre, no biometrics or fingerprint system was in use, except that officials were still using a manual system and uses the LCRC for criminal record checks. According to the participants, the biometric system that was used in the awaiting trial section to record new admissions, discontinued long ago. The South Africa Yearbook 2012/2013 Justice and Correctional Services (2013: 435) reported under the Automated Fingerprints Identification System that:

> *DCS initiated the roll-out of Afis in correctional centres around the country. By 2011, facilities for capturing and storage of fingerprint data had been installed at 145 sites. In 2012, it was decided that it was not feasible to use the*

> *Department of Home Affairs’ Afis database, as offenders do not necessarily provide the Department of Correctional Services with their identity numbers upon admission.*

Similarly, the South Africa Yearbook Justice and Correctional Services 2016/2017 (2017: 324) indicated that the DCS initiated the roll-out of the AFIS in correctional centres around the country and now has the Automated Personal Identity System (APIS) which interfaces with the Department of Home Affairs database to verify the identity of offenders; the APIS is available in 32 correctional centres and 99 community correctional offices. The APIS being for the DCS; NIS/ABIS being for DHA and AFIS being for SAPS shows that the departments have different identification systems, and they need to have either a separate system where all departments meet and share information (integration) or let each department have access to other departments` systems (sharing).

During an interview with DCS officials, it was discovered that there is no system currently in place since the cancellation of the Inmate Tracking System (ITS). The fingerprints system was not replaced, and inmates are recorded manually with fingerprints also obtained manually. Officials did not know about the PIVA system as has not yet been implemented in their facilities. Mngcungusa (2005) indicated that the Department of Correctional Services deployed biometric technology in correctional centres that started in June 2005 in three provinces namely Gauteng, Eastern Cape and KwaZulu-Natal. It was implemented to control and monitor access in correctional centres. Mngcungusa (2005) continued to say that the biometric technology discontinued as it was piloted to test whether such technology would be effective or not.

4.5.3.2. Department of Correctional Services fingerprint Systems

The PMG (2008) indicated that there was an evaluation done to ascertain the functionality, efficiency and sustainability of the Inmate Tracking System (ITS), the findings of the Evaluation Committee concluded that although the system was sustainable and was considered of great value to the Correctional Centres, the Personal Tracking Devices were deemed as inefficient and non-durable. This confirms that the fingerprint system used in Westville Correctional Centre was only for a short period to test its effectiveness. The importance of having a reliable identification system in the correctional centre has been stressed by members and it is indeed important to have control and easy access to inmates` information.

Without fingerprint systems the departments cannot share information as suggested in the Criminal Law (Forensic Procedure) Act No. 6 of 2010. As discussed previously that the Act proposes integration of departments but with the DCS and other departments still using manual recording of information, it implies that transformation will not be possible. Wyllie (2017) indicated that the large number of offenders in correctional centres makes it difficult to manage identification records securely, therefore many correctional centres in the USA are moving away from collecting fingerprints manually and are adopting biometric fingerprint identification technology.

Wyllie (2017) emphasized that during the booking process, one of the most important things a correctional centre must do is to establish the subject's identity by collecting readable fingerprints because failure to do so, can present a host of problems including having an offender go through the entire criminal justice process of booking, sentencing, incarceration and release without having had his or her fingerprints properly captured. This was the concern stressed by the DCS participants, indicating that unclear prints or failure to identify prints properly on warrants with prints obtained by them may result in wrongly admitting an inmate with particulars of another inmate.

The participants briefly explained that during admission of inmates, sometimes two or three inmates share the same names, if the officer calls "Sandile Ngcobo" an inmate responds, his fingerprints are obtained and compared with fingerprints appearing on the warrant and that is when it may be discovered that the wrong inmate responded. Participants emphasised on the use of biometrics as with the use of fingerprint scanners such mistakes can be avoided. Wyllie (2017) explained that once an electronic fingerprint is scanned, it is attached to that inmate's records so that any time there is a need to verify a person`s identity, the information is immediately available in the facility database.

Commissioner Motseki, the former Chief Deputy Commissioner in the Department of Correctional DCS, explained that the objectives of an inmate tracking system was intended to decrease the detention cycle time of awaiting trial detainees. He further indicated that there were two pilot sites where the system was being tested, namely the Durban-Westville and Johannesburg Correctional Centres (PMG, 2008). According to the IJS Progress Report (2017: 8) the Department of Correctional Services successfully implemented the Integrated Inmate Management System (IIMS) at Kgosi Mampuru in Pretoria. The Report continued to indicate that the planned electronic integrations included:

- Enabling the DCS to use the PIVA service integration with the DHA to verify the identity of detainees during the admission and receipt process.

- Establishing an electronic mechanism for the DCS to receive the J7 warrant of detention directly from the Department of Justice which will bring efficiencies by eliminating the need for the DCS to recapture information during the admission and receipt process.

The fingerprint system at Kgosi Mampuru is in operation and in good order. During the interviews the participants confirmed that the system is very convenient and user-friendly, compared to the manual verification of detainees. The IJS Progress Report (2017: 8) conveyed that the IIMS application is a centralised application which is developed by the DCS to manage the full inmate lifecycle and it is an essential component to the IJS programme, providing the basis for the DCS electronic integration.

The IJS Report further indicated that DCS has also leveraged the availability of smart mobile devices, enabling the DCS officials to capture and verify fingerprints, as well as location and status information of detainees during daily lock and unlock counts operations facilities. However, this system is not operational in all correctional centres. Westville correctional centre had the system for few months, and it stopped working. The staff at the centre confirmed that it was an effective system to trace and locate inmates, but it could not provide the exact location of the inmates. The White Paper for Remand Detention Management in South Africa (2014: 51) mentioned the following challenges as being faced by the Department of Correctional Services in the management of detainees:

- *The use of multiple identities by Remand Detainees who are clients of the Criminal Justice System (CJS) which leads to the creation of aliases within the CJS system and redundant information.*

A client of the CJS refers to a person who continues to break the law in one or other way. This person may be incarcerated in correctional centres multiple times, but with different identities. This was confirmed by participants during the interviews at the DCS who mentioned that some inmates use names of other people accidentally or intentionally. The White Paper for Remand Detention Management in South Africa (2014: 51) also explained that the exchanging identity takes place when the remand detainee intimidates or conspires with another remand detainee to exchange identities to defeat the ends of justice. This is the reason why the fingerprint system is so important because they are doing that because they are aware that the manual identification system does not work effectively. If they know that the fingerprints are required for verification and that the system is very effective, they will not even try to exchange identities.

- *The slow process of verification of identities with the Department of Home Affairs (DHA).*

Participants confirmed that another process that is followed to verify inmate information, is by sending fingerprints to the Department of Home Affairs, but this process takes long, and by the time the results return from the DHA the inmate has already been released. Meantime if the systems are linked or are shared, such information can be available in the facility whilst the inmate is still detained.

- *A lack of access to systems of other Departments e.g., access by the SAPS to details of inmates in the DCS.*

This is the focus of the study for the SAPS to have access to other department systems. This will remain a challenge in facilities where there are no fingerprint systems.

- *Inadequate systems for the identification of accused persons within the Criminal Justice System which results in each institution utilising its own identification from arrest to detention.*

- *The situation is compounded by the fact that remand detention institutions are provided with limited information, presented in the Warrant of Detention (J7); this leads to difficulties in tracing and tracking remand detainees in general and managing the court appearances of remand detainees with multiple charges who are required to appear in different courts within and across provinces.*

Participants pointed out that the use of J7 warrants is a challenge and time-consuming as information is verified manually and sometimes the thumb print in the J7 has been poorly obtained, making it difficult to confirm if the person received is the owner of the fingerprint appearing in the J7, as this verification is done by physically comparing the prints.

- Regular and repeated administrative processes for the admission and release of RDs from detention institutions for court appearances and other temporary releases.
- A lack of communication of the security risk or threat in relation to certain categories of remand detainees to remand detention institutions thus leading to improper housing and the risk of escape.
- The failure to arrive or late coming of some categories of remand detainees for court appearances.

The challenges mentioned in the White Paper were also mentioned by the participants in the Correctional Centre, emphasizing the necessity of having a working and integrated fingerprints system. In this case the PIVA system which has already been installed in police stations, will be perfect for the Department of Correctional Services to record inmates' particulars and verify their particulars before admission, therefore will be no need to verify those aspects with the DHA.

4.5.3.3. Strategies to overcome the challenges

The White Paper for Remand Detention Management in South Africa (2014: 51) further mentioned the following strategies to address the challenges as the seven point-plan approved by the Cabinet:

- *Establishment of an integrated and seamless national Criminal Justice System IT database/system containing all information relevant to the Criminal Justice System.*
- *The remand detention institutions and courts should have electronic systems for verification of the identities of remand detainees (RDs) and identities are to be verified with every release undertaken by the remand detention institutions.*
- *This challenge of multiple identities by the accused will be addressed through the development of a unique identification system for all accused who enter the Criminal Justice System; the identity number given to an accused will be attached to the personal identification information and multiple biometrics.*

According to the PMG (2001), the Correctional Services Portfolio Committee held a meeting on the Automatic Fingerprinting Identification System (AFIS), in which Chief Deputy Commissioner, Mr Esmeraldo, indicated that the automated fingerprint system would be used in the integrated justice system which will consist of the Department of Correctional Services, Social Development, Safety and Security, and Justice.

Mr Esmeraldo explained that fingerprint biometrics verification is an automated technology designed to replace the manual verification systems used throughout the criminal justice process and that in the Department of Correctional Services, fingerprint biometrics verification will be used to process admissions, releases, releases to court, roll calls, and visitations, as well as any movement management of prisoners where their identification is required.

As mentioned previously, the IJS has implemented the PIVA system which is supposed to be implemented at all the correctional centres. The process seems to be very slow, since the White Paper was published in 2014 and there is still no promise of the PIVA or any other fingerprint system in other correctional centres.

There are a few strategies obtained from the White Paper of Remand Detainees Management South Africa. These strategies will only come to life when the integration of information is successfully implemented; while the facilities where there is no system at all are still waiting for such changes.

4.6. Department of Home Affairs (DHA)

The DHA Annual Report (2017/2018: 15) confirmed that the criminal justice system departments are willing to integrate or share information. In the annual report it is mentioned that:

> *"An important advance over the period under review was the appointment of a service provider to develop the ABIS, as the current HANIS is nearing the end of its contract. It is envisaged that the system will go live during the 2018/19 financial year. The department received funding of R264 million from the South African Police Service during the current year and will receive additional funding of R156 million over the next two financial years from the Department of Justice and Constitutional Development, to develop and maintain the system. This is a significant milestone for government departments working together to achieve integrated systems in the public sector and eliminate a silo approach. The ABIS will interface online, in real time with other systems of criminal justice institutions and entities, which will also enhance cooperation and information sharing between the law enforcement agencies."*

The DHA is the custodian, protector and verifier of the identity and status of citizens and other persons residing in South Africa, Secondly, the DHA controls, regulates, and facilitates immigration and the movement of persons through ports of entry (DHA Annual Report 2017/2018: 67). Therefore, having the DHA as part of the criminal justice system departments can assist one another in sharing information for identification purposes will be of great assistance and possible breakthroughs in many cases.

The DHA Annual Report (2017/2018: 67) reported that the DHA is implementing the modernised roadmap ABIS system to integrate all systems and use biometrics as a unified/unique person identifier to enable advanced search capabilities and enable fingerprint verification and identification in the country. The search capabilities will increase of the response rate and the ability to do latency searches. Latent searches are important fingerprint searches in the investigation where evidence uplifted from the crime scene is scrutinised. It is important to know that the DHA has developed such a system to assist in latency searches.

Thomas (2009: 4) indicated that the DHA has historically been able to provide information to the SAPS under certain conditions. The DHA will be able to carry on supporting requests, provided that the requests do not unduly burden their current personnel capacity. This then confirms the concerns of the people and the investigators who wonder why it is difficult for the police to get information from the DHA when there are fingerprints involved. It might be that the agreement between the SAPS and the DHA was limited to priority crimes and all unidentified deceased, as mentioned above that the DHA has historically been able to assist the SAPS under certain conditions. With this concern in mind, it is commendable that the DHA has agreed to be part of integration and to be included in the PIVA system, so that any department which requires information from the DHA can access it on their own without burdening their current personnel capacity.

Thomas (2009: 4) pointed out that the ABIS is not equipped to provide information on latent (crime scene) searches and that the ABIS previously known as the HANIS, had a hot standby system which could provide additional 10-P search capacity if required. This is another reason why the DHA ABIS cannot assist the LCRC with latent searches. Latent search is the responsibility of the police in the LCRC who are trained to develop and turn latent prints to readable fingerprints. It is therefore important that the LCRC is equipped with a system that will have fingerprint information, or the current systems (PIVA) be developed to read and detect latent prints so that no docket is closed with positive fingerprints waiting for the suspect to be arrested on another criminal case.

Christen (2012: 15) suggested that data matching is a crucial component to identify verification as it allows matching of the identifying details that contain verified and accurate entity records and such databases that include voter registrations, drivers` licence and social security databases, and telephone directories. This confirms that integration or verification of information is not limited to certain departments, as mentioned earlier that even cell-phone service providers can be used for verification of information as they possess the latest information of their clients. People registering their cell-phones might provide accurate information out of desperation to avoid not being able to register a cell-phone.

4.7. Department of Transport (DOT)

The DOT Annual Report 2017/2018 reported that the DOT is currently in the process of integrating their own systems and it has started successfully in some municipalities. The Department of Transport issues vehicle licenses, roadworthy certificates, they also issue drivers` licences, Professional Driving Permits (PRDPs) and driving learners` permits. The DOT is responsible for Road Transport, Rail Transport, Aviation Transport and Maritime Transport.

The DOT may have accurate client information, rather than that of the information from the SAPS has, as people submitting information to the DOT are desperately seeking driving licences and learners` permits, and do not fear to be traced. However, there are people who give false addresses with the intention to escape fines for traffic offences. The Department of Transport also requires security checks from drivers before they issue them with PRDPs. Professional Driving Permits are permits which authorize drivers to drive buses, taxis, and any other forms of public transport. Drivers can do their own security checks, or they submit their fingerprints at the DOT during the PRDP application. The Muvoni Technology Group (2013: Para 4) explained that to operate as a professional driver, a person must have a valid driver`s license which incorporates a PRDP. The Muvoni Technology Group (2013: Para 4) further stated that a fingerprint clearance which is required for the PRDP involves a number of steps, namely:

- At the DLTC (Drivers` License Testing Centre) fingerprints are captured electronically and attached to the PRDP applications,
- The DLTC then forwards them to the South African Police Service via the afiswitch interface,
- Once checked, the SAPS provides a report to Afiswitch interface,

- The Afiswitch then sends the report to the DLTC.

DOT systems are still in process of integration themselves; currently only a few municipalities are integrated, let alone provinces. Previously, traffic offences that took place in another province ended there, and the traffic fine was not sent to the responsible driver if he is from another province. Also currently, vehicles of different municipalities are registered and renewed in their own municipalities. The DOT Annual Report (2017/2018: 43) reported that in 2015/2016 municipalities continued to implement Integrated Public Transport Networks and that initial services have started in Tshwane, Johannesburg, Cape Town and George.

Thomas (2009: 4) explained in his submission that manual requests for information using a SA-ID number on the eNATIS (Electronic National Administration Traffic Information System) database can be provided by the DOT. Currently fingerprint based searches are not possible on the eNATIS system, as this information is used in the driver's licence card processing facility and is not directly accessible. However, Thomas (2009: 4) also pointed out that fingerprints are envisaged to be used for verification of drivers in the issue of licensing, as this information would not be of immediate usefulness to the SAPS as the latest suspect photograph and registered address information would be accessible through the SA-ID number.

It is therefore noted that Thomas (2009: 4) does not agree with the Criminal Law (Forensic Procedure) Amendment Act No. 6 of 2010, because the DOT system is currently not suitable for integration. For investigation purposes investigators can manually request certain verification for confirmation with what they have from shared fingerprints systems. The DOT renews vehicle licenses annually and they renew drivers` licenses every five years, whereas PRDPs are renewed every two years. This department may assist with the latest information of South Africans, as drivers have to renew their driving licences with their latest details, whereas Home Affairs may have details of people as old as when they first registered their ID documents. The DCS will have similar information, if not the same as what SAPS has. It is unlikely that the DCS will have details of a suspect or first-time offender if SAPS does not have them, because most offenders are admitted in correctional centres from the police (SAPS) or Department of Home Affairs or the Department of Justice. The DOT has useful and important information of its clients, but the DOT is currently not involved in the PIVA integration. The DOT should form part of the PIVA as they will assist sister departments in the prevention of crime and in the tracing of and verification of information.

4.8. Department of Social Development (DSD)

The DSD also has information of minor offenders. The National Crime Prevention Strategy (NCPS) consists of programmes dealing with crime and minor offenders, and the NCPS programmes include the Diversion Programme for Minor Offenders and Secure Care for Juveniles. The National Programme on Diversion for Minor Offenders argued that youthful offenders should not be held in standard detention facilities or police cells, but they should be held in an environment that limits trauma and strengthens the likelihood of reintegrating into society (White Paper on Remand Detention Management in South Africa, 2014: 34).

The Department of Social Development, as mentioned by Christen (2012: 15), can also assist with accurate information because people also turn to social development for life support or assistance in desperate times. Social Development also uses fingerprints and has a database that contains particulars of their clients, and they may therefore have latest and updated information of people registered in their databases. Social Development has information of people registering for support grants, child grants, pensions, and disability grants. Sharing of these databases can also assist the Department of Social Development in verifying information of new applicants with information contained in any of the criminal justice system departments. The IJS Report (2017: 12) mentioned the inclusion of South African Social Security Agency (SASSA) in the PIVA system, stating that PIVA SASSA will be able to establish the eligible and ineligible beneficiaries in order to prevent fraudulent activities.

> *"The Integrated Justice System PIVA service will also be leveraged to assist the South African Social Security Agency in its efforts to combat fraud. It is envisaged that all beneficiaries of social grants will be verified against the Department of Home Affairs national population register as part of their enrolment process. A proof of concept with SASSA is currently underway and is at an advanced stage. Network connectivity between SASSA and the IJS*

> *Transversal Hub has been established, while SASSA has successfully deployed necessary server infrastructure within their environment to utilise the PIVA services." (IJS Report, 2017: 12).*

Sharing of government fingerprint databases will reduce fraudulent registrations where people give false information to benefit on government handouts or for personal gain. There are people who register children that do not exist to access child grant support. This registration requires the applicant to go through three departments before the registration is complete, namely the Department of Health (where the child was born), the Department of Home Affairs where the child`s birth is registered and the Department of Social Development where the child support grant is registered. Sharing of government databases can reduce or even avoid such false benefits and registrations. The Department of Health does not use a fingerprint system and does not require proof of identity for any medical treatment.

The PIVA system will also assist the DSD with information when a minor has been arrested. The IJS Report (2020: 5) indicated when a child is apprehended by the SAPS, the arrest information recorded on the SAPS sends notification to the Department of Social Development (DSD), so that a probation officer can be immediately assigned.

4.9. The roles that can be played by other departments to assist the South African Police Service in identifying latent prints of first-time offenders.

Linthicum (2000) defined data integration as a set of processes used to extract or capture, restructure, move, load, or publish data, in either operational or analytic data stores, in either real time or in batch mode. According to Christen (2012: 3), the analysing of data from different sources either within an organisation or between different organisations, can lead to much improved benefits compared to analyses databases in isolation. The sharing of fingerprints, as discussed in the previous chapter is vital for all organisations or entities that require authentic information on individuals. Sharing of information on fingerprint systems is not only needed by government (DHA, SAPS and DCS), but it is also in used by commercial banks to verify information submitted by bank clients which will be discussed below. The banking industry now works together with the Department of Home Affairs using their fingerprint database HANIS or the new system ABI to verify applicants and clients` information by means of fingerprints.

The South African Government Communications and Information System (2017: 324) explained that the Integrated Justice System aims to increase the efficiency and effectiveness of the entire criminal justice process by increasing the probability of successful investigation, prosecution, and punishment for priority crimes. This suggested information sharing is very important as it can show unity in all criminal justice systems. However, it should not be limited to priority crimes only, but cases should be treated equally. Criminals sometimes take advantage of the criminal justice system with the idea that there is no connection between fingerprint systems and there are differences in operating standards. The Government Communications and Information System (2017: 324) further indicated that the South African Government wants to eliminate duplication of services and programmes at all levels. The benefits of such alignments are mentioned as:

- Less duplication of services.
- The effective use of scarce and limited resources and skills.
- Joint strategic planning and a planned approach instead of simply reacting to problems.

The SAPS Annual Report (2015/2016: 54) mentioned that the Department of Home Affairs (DHA) is assisting the SAPS to identify fingerprints of circulated persons (missing and wanted persons) and vehicles. However, this system can only identify a suspect who has been arrested before and has a warrant on his name or is a missing person. During the interview with the DCS participants it was discovered that there is no sharing of information between departments. Participants indicated that they manually request verification of information from the DHA. The current procedure is that they send inmates` fingerprints to the DHA manually for verification and the DHA sends information to DCS on another day. The DCS Participants raised concerns of the time it takes to get the results back, since sometimes they only receive feedback when the inmate has already been released.

4.10. Sharing of Information between criminal justice system departments

Thomas (2009: 8) indicated that there was a service which was integrated to the Department of Home Affairs' ABIS, where Integrated Justice System participating departments were to confirm the details of a South African ID number holder. Their mandate was to use a South African ID for the verification of firearm and licence applications, suspect identities, complainants, bail payees, visitors to correctional facilities and other applications for other permits and civilian clearances.

Thomas (2009: 9) submitted that this project had already been initiated, with the client-side application development being completed and ready for testing; while the integration specifications were in the process of being finalised with the DHA to establish the integration between the Integrated Justice System transversal hub and the HANS/ABIS verification capability to complete the development of the PIVA. It was further indicated that the DHA was committed under the Cabinet Programme of Action to complete the integration by December 2009. Leseba (2015), the Chairperson of the IJSB explained to the police committee that the PIVA solution entails instant verification of SA IDs via the DHA HANIS/ABIS system using biometric devices.

The PIVA has been deployed to production and is being used by SAPS at several specialised units, as well as at the OR Tambo International Airport (PIVA Report, 2017: 12). The PIVA provided a platform for the identity of an individual to be verified against the Department of Home Affairs records by means of fingerprints. Identity verification is a common requirement across all IJS member departments, and the development of the application was a combined effort. The SAPS is the CJS entry point, and it is the first department to implement the PIVA (PIVA Report, 2017: 12).

The IJS PIVA has a Transversal Hub where criminal justice system departments can share information. Each department needs a single connection to the IJS Hub and can exchange data with all the departments already connected. Already there are departments that are connected to the IJS Transversal hub, and they are exchanging information between their systems (IJS Report, 2020). This information promises that implementation of the system will only require a single connection which sounds easy and quick to implement in other departments. However, the implementation is still in progress and not all departments have this system and not all police officers know about the system. At the time of interviews, some of the Local Criminal Record Centres (LCRC) and DCS officials who work with fingerprint identification did not know about the PIVA system, but the LCRC participants in Pretoria confirmed knowledge of the system, although they do not use it.

The IJS Report (2017: 7) indicated that the new integration system will assist the forwarding of docket information from the SAPS to court electronically, and automatically share such with the NPA by means of the IJS Transversal Hub. This implies that docket information will be available in the docket itself, the SAP Case Administration system (CAS) and it will be in the court system. This sharing of information will not only be convenient for the role players, but it will also protect dockets from being misplaced. Dockets will be safe because whenever it disappears, it will be restored.

Participant 16 confirmed that the system of integrating docket information was successfully implemented. He explained that in July 2019, a key milestone was reached through the undertaking of the first fully paperless case trial simulation where all parties in court were able to use their own devices to access and refer to digital versions of case materials. The PIVA system will assist in cases which are postponed in court because dockets are not brought to court. Prosecutors and court administrators will be able to print the docket information for the court to proceed. This system is different from the system that can identify latent prints because the system that is able to identify latent prints is on SAPS Local Criminal Record Centre only and not linked with the courts, the Justice System or even PIVA system.

The IJS (2020: 5) reported indicated that the PIVA is available at police stations because its purpose is to integrate case information with courts, for example:

- The SAPS has developed the Integrated Case and Docket Management System (ICDMS) that is used manually for the administration of all dockets within SAPS police stations nationally.
- Similarly, the NPA has developed the Electronic Case Management System (ECMS), a system that the NPA designed for prosecutors to work on electronic dockets, screen and enroll cases, and record necessary case tracking performance information.

- The DOJCD Integrated Case Management System (ICMS), which enables the administration of cases at the courts.
- Similarly, when a child is apprehended by the SAPS, the arrest information recorded by SAPS sends notification to the Department of Social Development (DSD), so that a probation officer can be immediately assigned.

Therefore, these systems mirror the case flow and allow departments to capture key events at each step. This also confirms that one of the purposes for the integrated systems is mainly for the case management process from the time the case is reported to the sentencing and the release of the offender.

It has been confirmed that this system is available in several police stations, but it does not identify latent prints left by first-time offenders. The latent prints uplifted from the crime scene are not scanned and checked by the police stations. They are uplifted by fingerprint experts who then take them to another fingerprint expert working with the fingerprint identification system and then checks the prints if the information is available in the database. This means that the PIVA system must either be implemented at the Criminal Record Centres for fingerprint experts, or the system must be upgraded to be able to scan and identify latent prints.

The PIVA works with the thumbprint presented physically and scanning of ID document or ID numbers, it can also scan images, faces etc. but not uplift latent prints. The IJS participant confirmed that the PIVA process starts when an individual presents him/herself and an identity document to a government official as part of an existing business process, such as an application for a firearm licence, social grant application or apprehended by a SAPS official. In the PIVA system, the person investigated must present his fingerprints, the information is then retrieved in his/her presence. The information of the arrested is also captured on the PIVA system in his/her presence.

The PIVA also retrieves information by means of ID numbers. This can assist departments like the Department of Social and the Development and Department of Correctional Services and others who need to verify information before processing applications. The LCRC verifies and compares fingerprints in the absence of the owner of fingerprints, but the fingerprint expert at the LCRC does not need permission from the owner of fingerprints to access his or her information, since the LCRC work with investigations. Only in clearance checks the owner of information has to give consent or permission for the retrieval of personal information. The PIVA system is available at police stations because it assists criminal justice system departments with integration and sharing of case information.

As discussed in earlier chapters, the SAPS CRC Training Committee (1999: 3) explained that the official South African criteria for individualizing a fingerprint, palm print, or a footprint were formulated by the SAP Criminal Record Centre to be seven ridge characteristics that can be identified on both prints corresponding the type, size, direction, position, and relation to each other, and those criteria were later accepted by the International Association for Identification. This implies that there must be rigorous training before an officer can work on latent prints developing them to fingerprints. This cannot be done at police stations. Therefore, the PIVA system cannot assist with identifying latent prints because it operates in police stations, and it has not been designed to identify latent prints. However, the PIVA database will be a great tool to identify first-time offenders as it contains information of few government departments.

It is evident that not all crime scenes will have positive and readable prints, as some crime scenes will have smudged, contaminated prints or no prints at all if the offender had used gloves during the commission of the offence. However, the integration or sharing of information will assist in those latent prints which are developed successfully and are readable; in such a case no dockets with positive fingerprints will be closed and filed undetected unless the offender is deceased. As mentioned above, the National Instruction/ Standing Order 325, as cited in the Consolidation Notice (2012), provided that the status of case docket where finger/palm prints were identifiable but with no particulars of a suspect, should be closed *“Undetected - “Positive fingerprints - Do not destroy”.*

4.11. The international best practices on the identification of first-time offenders by means of fingerprints systems.

Commercial banks are already collaborating with the Department of Home Affairs by using their fingerprint database (Home Affairs National Identification System) to verify applicants by means of fingerprints. The Minister of Home Affairs Gigaba (2016) confirmed the effectiveness of the system during a meeting with SABRIC (South African Banking Risk Information Centre) by stating that:

> *"We formalised our collaboration through a joint partnership between the Department of Home Affairs and the South African Banking Risk Information Centre (SABRIC) expressly to combat fraud and corruption that had robbed banks and our people of millions of rand. For this to work, we allowed, as Home Affairs, the banks access to the Home Affairs ABIS (previously known as National Identification System (HANIS)), so they could verify the identity of their prospective and current clients, using their fingerprints".*

Minister of Home Affairs Malusi Gigaba (2016) further mentioned that the success in this regard had been phenomenal. Therefore, the same system of identifying suspects through the DHA system can bring successes in cases provided that the integrity of information is protected. Although it is commonly accepted that bank clients give their consent to privacy when they open or manage accounts, the important point is that the involvement of the DHA in the process is feasible. The sharing of fingerprints information sharing will reduce identity fraud.

Identity fraud cases are common where victims are left with debts they have not incurred, and banks and retail stores lose large amounts of money to compensate victims or to criminals who do not repay loans. As mentioned above, commercial banks which are private entities are linked with the Department of Home Affairs but SAPS access to Home Affairs is limited to specific conditions. As pointed out by Thomas (2009: 4) that the DHA has been able to provide information to the SAPS under certain conditions whereas the banks can verify information of every applicant. This is unfair to the victims of crime and the community at large who put their hopes in the police. Police investigation should be the priority to prevent and deter crime.

Lyle (2010: 118) indicated that in India money lenders prefer to take thumb prints of the debtors on a hand note rather than a signature. The extent of fraud is compelling money landers to be more cautious when it comes to lending money. A fingerprint can be compared to the information stored on the bank`s database to confirm that the fingerprint produced is that of a person authenticated during the opening of an account. Christen (2012: 15) was of the view that data matching is a crucial component to identify verification as it allows matching of the identifying details provided by an individual with a variety of databases that contains verified and accurate entity records.

Saferstein (2011: 95) mentioned that in the USA, FBI (Federal Bureau of Investigation) has an IAFIS system which is the national and criminal history system which contains fingerprints that are submitted voluntarily by state, local, and federal law enforcement agencies. James, Nordby and Bell (2014: 335) emphasised that the AFIS has become a successful tool in the apprehension of unknown offenders. James *et al.* (2014: 336) further explained that the FBI has made their criminal database of known fingerprint cards available to other law enforcement agencies through its Integrated Automated Fingerprint Identification System (IAFIS), which allows a latent print examiner to search unknown latent impressions in a neighbouring state or in several states.

INTERPOL (2018: 1) indicated that at the INTERPOL General Assembly held in 2009, heads of the Organization’s National Central Bureaus voted unanimously to develop the systematic sharing and updating of fingerprints, including finger marks from unsolved crimes, as well as fingerprint profiles taken from offenders who are citizens of other countries, and to date this still applies. INTERPOL, (2018: 1) further reported that in 2017 INTERPOL the organisation was able to make more than 1,700 identifications because of increased data sharing and comparison by member countries.

INTERPOL (2012: 2) further explained that the INTERPOL Gateway Project allows member countries to access the INTERPOL Central AFIS remotely and to run searches of fingerprints and latent prints against all data stored in the AFIS database at the IPSG in Lyon. INTERPOL (2012: 3) further supplied directives to countries seeking information from INTERPOL`s fingerprints database by indicating that member countries should forward, fingerprints of person suspected or convicted of crimes who is not a national of the country in question to, INTERPOL. In this case the fingerprints are searched and stored in the INTERPOL AFIS database. INTERPOL actually shares information they have on foreign national with other countries. In the case where the SAPS arrests a foreigner, fingerprints must be shared with INTERPOL that can establish how dangerous the arrested person is, they can also provide crucial information about that person whether he/she is a fugitive or a terrorist. Distribution of such information can assist the country who is looking for that person.

Working with the DHA and other government departments to identify latent prints of first-time offenders is important as the DHA contains information of all people living in South Africa. As discussed above in paragraph 3.7.4 Section 10 of the Identification Act No. 68 of 1997 orders every person who has attained the age of 16 years to be included in the population register. Therefore, the DHA is the best source of information when it comes to seeking first time offenders or innocent persons. However, some people, for instance, in rural areas may take long to register their children at Home Affairs or to register a death so that some deceased citizens are still indicated as alive in the DHA registers when they are already deceased.

The South African Police Service also currently runs a DNA database in which all arrested persons have to submit their DNA samples for future reference. This process was suggested by the Criminal Law (Forensic Procedures) Amendment Act No. 6 of 2010, together with the integration of fingerprint systems. Acting National Commissioner Phahlane (2017), while addressing the 4th Forensic Services Conference hosted by SAPS, announced that the Forensic Database Management which is responsible for managing the National Forensic DNA Database has become the first section in the South African Police Service to be successfully registered for certification compliance to the international ISO 9001: 2015 standard.

The implemented DNA database procedure is working phenomenally well in that current criminals are linked with old cases which were closed as undetected because suspects being unknown. In a specific case, an attempted murder victim who had been sexually assaulted and left unconscious could not describe or identify her suspect, but in 2017 her suspect committed another crime, and his DNA was obtained. He was positively linked and charged on the old case. He pleaded guilty, and he was sentenced even though the victim could not even identify him. The former Acting National Commissioner Phahlane (2017), confirmed that by means of the DNA database, forensic DNA investigative leads successfully linked persons to 15 531 cases and linked 10 496 different cases have been reported to investigating officers since the operational date of the Act.

Krimsky and Simoncelli (2012: 157) argued that the Universal DNA databank has greater opportunities of privacy being violated than with the fingerprint database. Krimsky and Simoncelli (2012: 157) explained that the DNA has large amount of information that can be revealed about a person as the DNA contains the blueprint of human life, revealing a person`s genetic predisposition to disease, physical and mental characteristics, while the fingerprints cannot reveal any such information about the person, except for security information. This implies that the DNA database is riskier than a fingerprint database when it comes to the violation of people`s privacy.

4.12. Summary

This chapter discussed the literature review on the fingerprints identification systems that can be used for the investigation of latent prints of first-time offenders, on how other departments can assist LCRC and how they can assist each other. The use of fingerprints within the Criminal Justice System from when they are uplifted from the crime scene until they are used in the court and the current standard operating procedures were discussed. There is no cooperation between the departments when it comes to integration. The PIVA implemented by the Integrated Justice System (IJS) is currently with the SAPS and is available in police stations assisting courts with case management. The PIVA consists of integrated information from various departments, but it cannot identify latent prints. Most correctional centres still use manual filing of information as they do not have a fingerprint system. In the next chapter the data collected using the objectives of this study, will be discussed and analysed using objectives and sub-themes.

CHAPTER FIVE: PRESENTATION OF RESEARCH FINDINGS

5.1. Introduction

The previous chapter provided literature review on the aim and the objective of this study which was the use of fingerprints identification systems to enhance the investigation of latent prints of first-time offenders. The data collected from participants and literature is discussed and analysed in this chapter using objectives and sub-objectives.

In order to achieve the main aim of the study, the following objectives were utilised:

- To describe the process followed by the LCRC in identifying unknown suspects when latent prints are found at the crime scene.
- To explore the challenges faced by the SAPS LCRC in identifying first-time offender on fingerprints found at the crime scene.
- To investigate the role that may be played by departments such as the DHA and the DCS to assist the SAPS in identifying latent prints of first-time offenders.
- To highlight some of the international best practices on the identification of first-time offenders by means of fingerprint systems.

5.2. Profiling of Fingerprints experts in SAPS, DCS, and IJS

5.2.1. SAPS: Local Criminal Record Centre

At the LCRC the researcher interviewed nine fingerprints experts who work with the AFIS with experience in fingerprints comparison. All the interviewed officers had undergone internal training and have educational qualifications in different spheres of education, but within the range of law enforcement and Information Technology.

The SAPS has fingerprint experts with different roles, there are local fingerprint experts based in all provinces at cluster level and there are national fingerprint experts based in the SAPS Head Office (Pretoria) who work closely with the Department of Home Affairs. All these experts use the Automated Fingerprints Identification System (AFIS).

5.2.2. Department of Correctional Services (DCS)

At the Department of Correctional Service, seven of the fingerprint officials and former fingerprints officials were interviewed. All interviewed participants had undergone internal training on fingerprint verification with a number of years' experience. The fingerprint system used by Correctional Services is the Integrated Inmate Management System (IIMS), mainly used for recording the admission and the release of offenders, it can also identify offenders whose fingerprints are stored in the system.

5.2.3. Integrated Justice System (IJS)

At the Department of Justice, three officials who are working at the IJS Unit responsible for the management of PIVA system were interviewed. The Integrated Justice System (IJS) office work with a number of departments under the umbrella of the criminal justice system. The IJS is part of the Department of Justice & Constitutional Development and is based at the DOJ & CD head office in Pretoria. The officials that were interviewed work closely with other departments and they are responsible for the functioning of the PIVA system, the system that integrates fingerprints information from different departments. Three of these officials were interviewed, because this office has very few officials.

5.2.4. Demographical information of Participants

The table below indicate the demographic details of the code given to each participant, the gender, years of experience, the area where the participant is located and the employment position. The areas are named as follows:

- LCRC DBN: Local Criminal Record Centre Durban
- LCRC PTA: Local Criminal Record Centre Pretoria
- DCS DBN: Department of Correctional Services Durban
- DCS PTA: Department of Correctional Services Pretoria
- IJS PTA: Integrated Justice System Pretoria

Figure 3: Demographic information of the participants

Participant Number	Gender	Years of Experience	Geographical	Current Position
1	Female	8 years	LCRC DBN	Constable Fingerprints Expert
2	Male	24 years	LCRC DBN	Warrant Officer Fingerprints Expert
3	Male	18 years	LCRC DBN	Warrant Officer Fingerprints Expert
4	Male	18 years	LCRC DBN	Warrant Officer Fingerprints Expert
5	Male	20 years	LCRC DBN	Lt Colonel Experts` Supervisor
6	Male	19 years	LCRC DBN	Warrant Officer Fingerprints Expert
7	Male	30 years	LCRC PTA	Lt Colonel Fingerprints Expert
8	Male	15 years	LCRC PTA	Warrant Officer Fingerprints Expert
9	Male	12 years	DCS DBN	Warrant Officer Fingerprints Expert
10	Male	14 years	DCS DBN	Fingerprints Officer
11	Male	4 years	DCS PTA	Fingerprints Officer
12	Male	4 years	DCS PTA	Fingerprints Officer
13	Male	3 years	DCS PTA	Fingerprints Officer
14	Male	24 years	DCS PTA	Fingerprints Officers` Supervisor
15	Male	4 years	IJS PTA	Unknown
16	Male	13 years	IJS PTA	Unknown
17	Female	Unknown	LCRC DBN	Captain Experts Supervisor
18	Male	Unknown	IJS PTA	Former IJS Supervisor
19	Male	Unknown	DCS DBN	Fingerprints Officers` Supervisor

5.3. Research findings and Discussions

Guest, MacQueen and Namey (2012: 11) and Caulfield (2019) described the thematic analysis as a method of analysing qualitative data and point out that thematic analysis is applied to a set of texts, such as an interview or transcripts; and the researcher examines the data to identify common themes, topics, ideas and patterns of meaning that arise repeatedly. As indicated in Chapter 2, the researcher analysed the data, using thematic analysis with data codes which were developed to represent the identified themes linked to the raw data. Following the process of thematic analysis, the researcher assembled all the responses from the participants, read through them one by one, and compared different answers to the same question asked. Similar answers were noted and recorded while, different answers were also noted and recorded separately.

The researcher formulated themes and sub-themes by means of a deductive approach. Skjott Linneberg and Korsgaard (2019) explained that in the deductive approach the researcher begin with a set of codes and continue with the set, whereas in the inductive approach, the researcher creates codes as he/she reads the data. Skjott Linneberg and Korsgaard (2019) emphasised that the objectives and the research questions are important imperative to define the data in order to complete the project successfully. Subsequently the researcher analysed the data in line with the objectives and as themes while the questions that appeared in the process were recorded as sub-themes. The table below categorises the themes and sub-themes and defines the categories.

Figure 4: The fingerprint identification systems to be used on the investigation of latent prints of first-time offenders.

Study Objectives	Identified study themes and sub-themes	Definitions
OBJECTIVE 1: The process followed by the LCRC in identifying unknown suspects when latent prints are found at the crime scene.	Fingerprints identified by the LCRC.	The LCRC uses AFIS system for comparison, identification verification and recording of criminal records. The system is not linked with any of the CJS departments
	Fingerprints identified by the DCS.	The DCS uses the IIMS for admission and releasing the inmates and the system is not linked with any CJS department
	Current standard operating procedure.	Verification is done manually by referring to the DHA. There is no standard operating procedure
OBJECTIVE 2: The Challenges faced by the SAPS LCRC in identifying first-time offenders on fingerprints found at the crime scene.	Previously charged persons.	The LCRC can only identify fingerprints of previously charged persons, and first-time offenders cannot be identified
	Poorly obtained fingerprints.	All participants complained of poorly obtained fingerprints, fingerprints form not clear.
	No fingerprints systems.	Some correctional centres do not have fingerprint systems and are admitting and releasing offenders manually
OBJECTIVE 3: The role that should be played by other departments.	No correlation between the departments	There is no relationship between the departments all departments are working independently.
	People`s privacy.	The duty to protect people`s information in terms of POPI Act is hindering the sharing of information requirement
OBJECTIVE 4: The international best practices	Sharing of information	Interpol suggested the sharing of information with other member states via integration,
	National Fingerprints database from Security Clearance	The USA has implemented a database containing non-criminals using information obtained during security clearances.
	The use of digital scanners in obtaining fingerprints	The USA is working towards obtaining fingerprints using fingerprints scanners to avoid poorly obtained fingerprints

5.3.1. Objective 1: The process followed by the LCRC in identifying unknown suspects when latent prints are found at the crime scene.

The LCRC uses the AFIS system to record criminal offences on an individual by means of fingerprints. Criminal records of people are obtained from the AFIS database for investigation purposes, court purposes, and security clearance for employment or travelling visas and any other checks that requires security clearance. Local fingerprint experts are those fingerprints experts based in all provinces with the number of offices allocated according to clusters.

These experts are responsible for comparing and identifying fingerprints uplifted from the crime scene, identifying fingerprints obtained from the charged suspects to establish whether the suspect has previous convictions or not. They are also responsible for security clearance to check whether a person has a criminal record for court purposes or not. They also conduct security clearances for employment purposes or for application of firearm licenses or travelling visas etc.

This study was based at the functioning of these fingerprint experts because they deal with so-called minor property crimes. They are regarded as minor crimes because they are not priority crimes. Priority crimes, as discussed in earlier chapters, do have the privilege of being sent to the National Criminal Record Centre experts who are able to detect first-time offenders using Department of Home Affairs or any other verification approach. As mentioned in Chapter 1, Section 15D (4) of the Criminal Law (Forensic Procedure) Act No. 6 of 2010 suggested that the departments should develop a standard operating procedure which will be used when sharing information. There is a successful implemented integration of fingerprints databases from different government departments, called the PIVA (Person Identification Verification Application). However, this system does not assist the LCRC with latent prints found at a crime scene of a first-time offender.

5.3.1.1. Sub-theme 1: Fingerprints identified by the Local Criminal Record Centre

The LCRC from provincial Criminal Record Centre cannot identify latent prints if the person who left the prints is not on their criminal record system or has never been arrested. According to a number of property-related cases reported during 2020 to 2022 (two years), it is evident that the detection of suspects in these cases is still a challenge, as a number of cases were not detected and only a few were detected.

The table below indicated the exact numbers as per SAPS Annual Reports for 2020/2021 to 2021/2022 (SAPS Annual Report, 2022: 213).

Figure 5: Number of Complaints Reported during 2020/2021 and 2021/2022

Crime Reported	**2020/2021**		**2021/2022**	
	Reported	**Detected**	**Reported**	**Detected**
Burglary at residential premises	159 907	39 257	206 129	47 595
Burglary at non-residential premises	65 564	13 758	69 762	13 971
Theft of motor vehicle and motorcycle	35 078	4 604	46 966	5 741
Theft out of or from motor vehicle	83 291	12 448	118 278	14 915
Total	343 840	70 067	441 135	82 222

SAPS Annual Report 2021/2022 (2022: 201) showed that there is still a problem with the detection rate of property crimes. The report indicated a number of factors that prevents LCRC from achieving their target. This is a confirmation that the LCRC still does not have fingerprints system that will assist them with fingerprints information. They are still working independently using AFIS. In the report on a forensic services column, there is no mention of PIVA system assisting with the identification of fingerprints. However, PIVA system it is mentioned on other columns where it contributed in reducing levels of contact crimes. The report indicated the following:

> *"Target not achieved, extraordinary circumstances prevailed during quarters 3 and 4, of 2021/22. In the month of January there was a planned transitional period for the new AFIS implementation and switch over, from 17 to 24 January 2022. Certain activities were halted prior to shut down, in order to reduce the work load on the system. From the time the new AFIS started, the expected processing of all transactions was slower than normal.* There are still unresolved issues associated with transitional activities, which are attended to.*"*

SAPS Annual Report 2021/2022 (2022: 195) showed that the integrated PIVA system is working effectively in police stations and the targets were achieved during 2021/2022.

> *"Target achieved, increased utilisation of the PIVA System, enhanced profiling of suspects."*

In the mentioned cases the victim will not know who broke into the house or the vehicle if there are no witnesses, informers or cameras. The only evidence that can be used to detect the suspect is by means of fingerprints. Fingerprints or the DNA (hair or blood) is the most reliable tool to detect a suspect in the above-mentioned cases. In the above-mentioned cases there were no detection, it is unknown whether there were no fingerprints found at the crime scene (contaminated/ gloves used) or they were found but were undetected since the LCRC does not have the resources needed to detect latent prints of a first-time offender.

During interviews the participants confirmed that they cannot identify fingerprints of innocent persons. Participant 13 indicated that:

> *"I can only verify fingerprints of an inmate who was detained before and that is after the system was introduced"*

Another LCRC participant explained that even after the person has been arrested and charged but found not guilty in court, the SAPS destroys those fingerprints, and his/her name is removed from the database. This person will still appear as a first-time offender if his/her name has been cleared on the LCRC database. All LCRC participants were asked during interviews, to enumerate the types of individuals who be identified by their system; and they all indicated that their system can identify fingerprints of a person who was arrested and charged previously and that those fingerprint information is available on their database. It was also established that there is no memorandum of understanding between the government departments when it comes to identification of latent prints of first-time offenders.

5.3.1.2. Sub-theme 2: Fingerprints identified by the Department of Correctional Services

During an interview with the Department of Correctional Services, the Correctional centre under review did not have a fingerprint system. The participants indicated that they did have a fingerprint system, but it crashed and was never replaced. The participants emphasized that fingerprint system was advantageous as admitting and releasing offenders was easy and fast. The use of the now fingerprint system was commended because of its convenience in keeping records, compared to the manual system currently in place, which is time-consuming and the manual filing of fingerprints seems to be a problem.

Participants indicated that they are manually obtaining fingerprints on admission, releasing and filing offenders` information. The challenge faced by this Correctional centre is that sometimes there are difficulties in authenticating information obtained from offenders, for instance having more than one person using the same name and surname. The participants confirmed that in some instances they do work with the DHA in confirming some offenders` details but it is also time consuming, since this too is done manually. In addition, the DHA takes time to respond with the correct information of the offender. The participants indicated that verification done with Home Affairs takes so that by the time the verification is received from Home Affairs, the offender has already been released.

The integration proposed by the Act Section 15D (4) of Criminal Law (Forensic Procedure) Act No. 6 of 2010 has the involvement of the Department of Correctional Services (DCS) but the DCS still operates on dated system. The use of manual recording and filing is outdated school and has its own challenges. As a custodian of offenders, the DCS should be equipped with hi-tech and advanced technology to be one step ahead of criminals who plan to manipulate the system like those mentioned above who supply false identities and thereby blaming their transgressions on other people.

The participants at the Correctional Centre which has a fingerprint system were asked which fingerprint system they used and whether their system was linked with any of the other government departments. The participants indicated that they were using the IIMS (Integrated Inmate Management System). They indicated that there was no operating procedure in place with other departments, because the IIMS is limited to the Department of Correctional Services only. Their system is not integrated with the SAPS or the Department of Home Affairs. In addition, the participants emphasised that it would be very easy to admit offenders if their fingerprint system were linked with other departments since during admission of an offender, officials will only scan a thumbprint and the offender`s information would appear on screen. Although they had not experienced it, they explained that the court will record offenders who are transferred to the correctional Centre instead of doing it in a warrant (J7), and the Correctional Centre will have the information already stored on the system.

5.3.1.3. Sub-theme 3: Standard operating procedure

Sharing of information is stipulated in Section 15D (4) of Criminal Law (Forensic Procedure) Act No. 6 of 2010. This is the Act that triggered this study, as it states that departments must develop a standard operating procedure that will enable them to share information.

During interviews, participant 10 and 2, from the LCRC and the DCS respectively, indicated that there is no standard operating procedure or memorandum of understanding between departments. The following was indicated:

> *"There is no operating procedure, as members we do communicate with colleagues from other departments not because it is a standard procedure, we do ask SAPS members that we know for information on inmates" (Participant 10).*
>
> *"There are no standard operating procedures between the departments" (Participant 2)*

Participants confirmed that all departments are working independently, consequently there is no integration or sharing of information as standard procedure. However, participants from the Integrated Justice System confirmed that there is a new implemented system known as the PIVA that has been installed in police stations. The PIVA integrates information from a number of departments, and it is meant to provide information to Criminal Justice System departments, sharing information on the movement of the accused and docket information.

Leseba (2015) the Chairperson of the IJSB indicated in his presentation to the police committee that the PIVA was ready for deployment, pending the sign-off of the Standard Operating Procedures. The PIVA (Person Identity Verification Application) has now been rolled out and is available in most police stations. However, the PIVA`s implementation at police stations assists police stations and courts only. It does not verify latent prints; in fact it does not assist fingerprints experts in Local Criminal Record Centres. All participants from the local LCRC did not know about the PIVA. Participant 7 from National LCRC confirmed knowledgeable about the PIVA but did not work with the PIVA. He said the following:

> *"It is a system that verifies a person identification (No)"*

All participants from the Department of Correctional Services denied any knowledge about the PIVA system. Another participant from National LCRC he was asked and answered:

> *"No idea" (Participant 8)*

Participant 16 from the IJS (Integrated Justice System) indicated that:

> *"Regarding the sharing of fingerprints information, a JCPS (Justice Crime Prevention and Security) Fingerprint and Photographic Images Database Protocol is currently in place. Parties to the protocol include, but not limited to South African Police Service, Department of Justice & Constitutional Development, Department of Home Affairs, Department of Transport, Department of Correctional Services, State Security Agency (SSA) and Department of Social Development."*

5.3.2. Objective 2: The challenges faced by the SAPS LCRC in identifying first-time offender on fingerprints found at the crime scene.

5.3.2.1. Sub-theme 4: Previously charged persons.

The LCRC`s fingerprint system the AFIS can only verify fingerprints that are stored in their database and therefore people with no criminal record cannot be traced on the LCRC database. Participants indicated the following:

> *"Those that are charged and have cases pending" (Participant 4).*

> *"Those who have been formally charged and who have previous records of conviction" (Participant 6).*

Another participant indicated that only previously charged persons can be traced on the AFIS, however if the person is found not guilty after the arrest, his/her fingerprints must be destroyed. This implies that even a person who had been arrested and charged before, and was found not guilty, would not be traced on the LCRC, because his/her history has been removed from the database. This participant explained:

> *"AFIS system has fingerprints for people with previous conviction/s, it must be remembered that according to the Criminal Procedure Act, SAPS must not keep fingerprints for any other people other than those that are convicted. This means that if a person is arrested, and he is not found guilty in court, their fingerprints (SAP 76) must be destroyed, so if the person is a first offender that will mean AFIS will not have their fingerprints anymore after destruction. (Participant 5).*

Section 36B 6 (iii) of the Criminal Procedure Act 57 of 1977 confirmed the indication by the participant that any person arrested but found not guilty by court should be cleared from the+ criminal record register. The Act states the following:

> *"Any fingerprints, taken under any power conferred by this section in a case where a decision was made not to prosecute a person, if the person is found not guilty at his or her trial, or if his or her conviction is set aside by a superior*

> *court or if he or she is discharged at a preparatory examination or if no criminal proceedings with reference to such fingerprints or body-prints were instituted against the person concerned in*
> *any court or if the prosecution declines to prosecute, must be destroyed within 30 days after the officer commanding the Division responsible for criminal records referred to in Chapter 5A of the South African Police Service Act has been notified."*

This implies that a suspect arrested and charged, and who appeared on the criminal record database can also not be traced at a later stage if he is found not guilty of the crime charged with. According to the South African Government (2022) a person can apply to have a criminal record expunged in terms of Criminal Procedure Act No. 57 of 1977 when:

- A period of 10 years has passed after the date of the conviction for that offence.
- The person has not been convicted and sentenced to a period of imprisonment without the option of a fine during those 10 years.
- The sentence was corporal punishment.
- The sentence was postponed, or you were cautioned and discharged.
- The sentence was a fine not exceeding R20 000.
- The sentence was imprisonment with the option to pay a fine (not more than R20 000) instead of serving the period of imprisonment.
- The sentence of imprisonment was entirely suspended.

This implies that an individual can be charged and cleared on the database and after the record has been cleared, he/she commits another crime and are released because the LCRC cannot identify his/her fingerprints and cannot approach the Department of Home Affairs because the first crime has not been a serious crime.

Correctional Centres with a fingerprint system, the IIMS, can also identify persons who were detained in their facilities. Other correctional centres do not have fingerprint systems and they admit and release offenders manually. When the participants were asked whose fingerprints they can identify on their system, participants from the Department of Correctional Services indicated the following:

"Only the ones admitted at our Centre" (Participant 14)

Other participants from the Correctional Centre were asked the question and they indicated the following:

"There is no fingerprints system" (Participant 10)

"There is no fingerprints system in place" (Participant 9)

The Minister of Correctional Services Ben Skosana (as cited in the Parliamentary Monitoring Group, 2001) told the Committee on the briefing of the Automated Fingerprint System that the Automated Fingerprints system was meant for verification during admission, releasing as well as releases to court, roll calls, visitations; and movement management of offenders if their identification is required. This, however, does not happen in some of the correctional centres.

During the interviews, there was also an observation of the admission process. The admission section in one of the facilities had inmates coming in and indeed they were called by names according to the warrants. In the SAPS according to the researcher`s observation and experience the admission of a suspect after the arrest is documented manually in the cells register known as the SAP 14, at the same time the information of the arrest including the Cell Number known as the SAP 14 number and the fingerprints form number (serial number), are captured in the system. This process is known as the 5.3, this function is for charging of the suspects.

5.3.2.2. Sub-theme 5: Poorly obtained fingerprints not readable

When the participants were asked about the challenges they face when working with fingerprints, most participants revealed that there is a major concern of poorly visible fingerprints which may result in unsuccessful identification and recording of the fingerprints. The participants from the Department of Correctional Services indicated the following:

"Fingerprints which are not clear, this is normally done on warrants from court, some people allow inmates to take their own prints". (Participant 9).
"Sometimes fingerprints on warrants are not clearly obtained" (Participant 10).

> *“Normally the fingerprints taken at court are not clear” (Participant 14).*
>
> *Challenge maybe the fingerprints taken on the warrant not visible enough to establish a positive identification” (Participant 13).*

Other participants from the Local Criminal Record Centre indicated the following:

> *Fingerprints are sometimes badly taken, or crime scene prints are badly lifted” (Participant 2).*
>
> *Poor quality of the prints when being taken” (Participant 2).*
> *Poor quality, not in sequence” (Participant 7).*
> *Poorly taken prints on fingerprints forms and prints from crime scene developed powders and reagents being bits and pieces” (Participant 8).*

The study found that manually obtained fingerprints are sometimes not readable because of being poorly obtained. If fingerprints are not readable there is a possibility that suspects` criminal records might not be recorded. This may result in suspects having clear criminal records. Wyllie (2017) indicated that the large number of offenders in correctional centres makes it difficult to manage identification records, therefore correctional centres in the USA are moving away from manually obtaining fingerprints and they are adopting fingerprints identification systems.

5.3.2.3. Sub-theme 6: DCS Correctional Centres not having fingerprints systems

All participants who were involved in this study indicated that the there is no sharing of information between the departments, there is no integration. Participants nevertheless saw the need for departments to integrate information. Participants from the Department of Correctional Services saw the need to integrate information with courts. Participant 10 raised concerns about the use of manual operation with offenders from court by means of a warrant also known as a J7. The participant mentioned that the J7 comes with thumb print obtained by court personnel, when the offender gets to the facility another set of fingerprints are also obtained. The fingerprints obtained are compared with the naked eye with the thumb print appearing in the J7. They suggested that if the court can have fingerprints system, the offender`s fingerprints will be obtained and stored by the court and on the admission at the Correctional Centre only the thumb print will be obtained and verified with what the court and the SAPS already have.

5.3.3. Objective 3: The role that can be played by departments such as the DHA and DCS in identifying latent prints of first-time offenders.

The Department of Home Affairs is mandated to ensure the security of the country by protecting its information interface; and in the same way in the Criminal Law (Forensic Procedure) Act No. 6 of 2010, it is pointed out that departments should implement safety measures to protect the integrity of information contained on the relevant databases. The Criminal Law (Forensic Procedure) Act No. 6 of 2010 takes into consideration the privacy of people stating that National Commissioners must implement safety measures to protect the integrity of information contained on the databases.

The major concern of the safety of information is the same aspect that hampers the successful resolving of cases. The successful resolution of cases requires investigation to access the protected information to identify an offender. For example, a house has been broken into and valuable items have been stolen. The fingerprints expert managed to transform latent prints to readable fingerprints, but fingerprints information is not available on their database the AFIS. It is at this stage that the fingerprint expert must either access another department`s fingerprints database or let the offender or the intruder walk free.

5.3.3.1. Sub-theme 7: No correlation between the departments

The study revealed that there is no relationship between the criminal justice system departments. When the participants were asked about the current operating procedure, it emerged that all departments are working on their own and in isolation.

Participants from the correctional Centre indicated the following:

> *“There is no system or communication with SAPS or Home Affairs because we are not informed how many offenders are coming to the facility, e.g. new ones” (Participant 9).*

Auditor General Makwethu (2020: 5) stressed the importance of integration and the sharing of information between the government departments, as such information could have been used by SASSA to check if the people applying for such grants were eligible or not.

The Local Criminal Record Centre had different views regarding the integration of fingerprint systems. One of the officers was very positive and keen to have fingerprints information integrated, arguing that all people should be treated the same when it comes to resolving cases. The main issue during the discussion was that for normal cases the local LCRC is still limited in identifying latent prints unlike the case with high profile.

5.3.3.2. Sub-theme 8: People`s privacy

Section 15D (4) (b) of the Criminal Law (Forensic Procedure) Act No. 6 of 2010 provided that the departments must under the chairpersonship of the National Police Commissioner develop standard operational procedures regarding access to the databases and implementation of safety measures to protect the integrity of information.

During the interviews when asked about the protection of people`s privacy, all participants indicated that the only way available to protect people`s information is by using username and password authenticating credentials. Three participants went as far as mentioning that by employing passwords, the system will be able to detect who accessed a certain individual`s personal information. Modern technology is so advanced that investigative techniques are capable to detect violators easily. The use of credentials to access information systems to expose employees who are stealing information or processing fraudulent payments is common practice in many companies.

When participants were asked about the people`s privacy when sharing fingerprint information, participants indicated the following:

> *“There are regulations which are regulating the unauthorised use of information, person caught infringing other people`s information can be charged in terms of the laws” (Participant 16)*
>
> *“Each person uses their own username a password to login, and they sign a confidentiality clause” (Participant 1)*

Participants emphasised the importance of training and sensitisation of officials who would be tasked to work with the fingerprint system that contains other people`s information. This implies that the use of credentials and the use of laws are sufficient they are enough to deal with the protection of information. With regards to the selection of officials, it was also suggested that the number of officials in a specific department having access to the information must be limited; and that those given access should be vetted to be trusted with other people`s information.

However, vetting of employees does not guarantee that he/she is trustworthy, but vetting reduces the number of risky people as vetting usually indicates whether the vetted employee may be a risky choice or not. The employer or then has the choice whether to place that employee in that section or not. For instance, if the results of vetting indicate that the employee is a risk potential, such employee should not be made a financial manager. Van Rooyen (2016: Para 6) with regards to pre-employment vetting, pointed out that even if a person has never showed any risk-bearing behaviour, in the past, it does not mean that the person will never do so and if a person at the time of vetting showed no risk-bearing in the past, it does not mean that it will happen again.

Another participant mentioned that people need to give permission to officials to access their information because of the POPI Act, the Constitution and the Criminal Procedure Act. This however, is not valid when fingerprints uplifted from the crime scene are investigated, as the person to give permission to access his/her information on the system will not be present. The only way to ask the person permission is if that person is implicated and his/her fingerprints were found at the crime scene. Another way of getting permission to access another person`s information is if that person has requested security clearance where fingerprints are given voluntarily. Conversely when a person has been arrested and the fingerprints are obtained in terms of the Criminal Procedure Act, those fingerprints are obtained whether the suspect authorizes the officer or not.

On the other hand, Participant 5 was deeply concerned about the information which will be obtained from the DHA, pointing out that the DHA consists of all citizens' including that of innocent people. Another participant indicated that:

> *"The participant indicated that innocent people will be arrested as there will be a case where innocent fingerprints will be found at the crime scene". (Participant 5).*

This participant used the example of a hijacking case, where a taxi that had been hijacked and when recovered, would have fingerprints of innocent passengers as well as those of hijackers. The concern was that if all fingerprints are referred to the DHA for identification, how will it be determined who the hijacker was and who were the innocent passenger. In such a case the investigator`s skills will be indispensable, as his/her investigative skills will have to separate the innocent from the offender, and if there is no conclusive evidence, he/she will have to use discretion and decide who should be investigated.

Orthmann and Hess (2013: 11) described the investigator as a person who systematically seeks evidence to identify the individual, who committed a crime, locates the individual and obtains enough evidence to prove the case beyond reasonable doubt. When using discretion, it does not mean the investigator is convicting the suspected, but it means to investigate further and scrutinising the suspected fingerprints more carefully. Subsequently the case may be sent to the prosecutor for a decision to prosecute or not to prosecute. The investigator of the case does not only rely on fingerprints evidence. More evidence may also be detected, and more eliminating evidence may also be detected on innocent people. The skills of the investigator are coupled with the years of experience in the same field, the level of education and the relevant qualifications obtained during their careers. Where there is a lack of evidence, the investigator closes the case or sends the docket to court prosecutors for guidance and a decision before making an arrest.

Therefore, where several fingerprints are found from the crime scene of a hijacked taxi, innocent people will be eliminated, and hijackers will be arrested. It is up to the investigator`s discretion to decide whether they were all involved in a crime or not. During the police and detective training, tutors emphasise the fact that the police are faced with a task of making prompt decisions and using their discretion on cases. This emphasis equips the police and sensitizes them in making correct and careful decisions to avoid litigations on unlawful arrests.

Upon receiving fingerprint information from the LCRC police detectives have to decide on whether to make an arrest or not. The procedure followed by the police upon receiving fingerprint information is the following:

- The investigator searches for that individual, interviews the person regarding the reason why the fingerprints were found at the crime scene; and if the explanation is not satisfactory, that person will be arrested and taken to court.
- If the investigator is not certain about the response, the person`s explanation will be sent to court for a decision. The Director of Public Prosecution (DPP) will issue summons or a warrant of arrest for the person to be arrested or the DPP will decline to prosecute, and the person will not be arrested though fingerprints had been found at the crime scene.

It has been mentioned previously that identification of the fingerprints does not mean that the suspect has been found, but the investigation may continue to apprehend suspects.

5.3.3.3. Sub-theme 9: PIVA system and People`s Privacy

Government department have a number of integrated systems where information is shared, as discussed in Chapter 3.7, namely the BAS system (Payments), the PERSAL system (Human Resources) and the CSD (Central Suppliers Database). These integrated systems contain sensitive information from peoples` addresses to bank details to family histories and even their wealth, but their information is undoubtedly safe and protected.

Not all officials have access to these systems, and only a few are authorized and clearly warned against divulging information. The PIVA system is also believed to be safe with regard to sensitive information. As explained above, only few officials are selected to work with PIVA system. The officials working with these biometrics systems have been warned trained, sensitized about the confidentiality of information and warned against contravention of privacy regulations. One of the officials who attended the PIVA workshop confirmed that the information contained in PIVA system is sensitive and emphasizes how dangerous it is to divulge such information illegally.

The officials working with these systems are aware of the consequences they may face if ant information has been illegally disclosed. All SAPS participants indicated that before receiving credentials to access the database, officials are made to sign an Undertaking/ Confidentiality Clause where officers are declaring under oath that they will not share information contained in the system and that they will not use the information on the system for personal reasons. Participant 6 indicated the following:

> *"The database is highly protected users of the system also use access codes it may just be a challenge due to rogue individuals. People unfortunately need to give an explicit authorization for the government departments to share their information that is protected by law and the constitution." (Participant 6).*

This implies that where an investigator or detective requests information from the PIVA system, the officer supplying the information will encrypt it and only the person who requested the information will have access to it. Nonetheless, the detective cannot request fingerprints information from PIVA officers because PIVA cannot scan latent prints.

The participant working with the PIVA system indicated that:

> *"People`s privacy is protected, the interface can only be accessed by the authorized personnel managed by each government department, and all data captured and communicated is encrypted." (Participant 16).*

About the safety of information and access to the PIVA, another officer from a police station confirmed that there are three offices with access to the PIVA system in his police station and that only three police officers have access to PIVA. The procedure to be followed is that, police officials are compelled to take suspects to these officers for piving (as they call it). The officer continued to state that there was a PIVA workshop which was attended by members who would have access to PIVA, and he also attended the course. They were sensitised about the confidentiality of information contained in the PIVA system and therefore they would not access information illegally.

5.3.4. Objective 4: The international best practices on the identification of first-time offender using fingerprints.

5.3.4.1. Sub-theme 10: Sharing of information.

The use of fingerprint systems for people`s information is used across the world and a preferred method of record keeping. Some countries even share fingerprint information with INTERPOL the international police organisation. INTERPOL assists every country to search for an offender all over the world. As discussed earlier, INTERPOL (2012: 3) gave directives to countries seeking information from INTERPOL`s fingerprint database by indicating that member countries should forward fingerprints of a person suspected or convicted of crimes who is not a national of the country in question to INTERPOL, and INTERPOL will assist by tracing the person who is wanted just by means of fingerprints. Sharing of fingerprints information for investigation purposes is made increasingly.

Every government department should have a fingerprint system for easy sharing of information between government departments, and it is even more difficult in cases where some departments cannot even share information amongst themselves like some of the Correctional Centres.

5.3.4.2. Sub-theme 11: National fingerprints Database created from security clearance.

It has been established that many countries do store information of people who are doing security checks with law enforcement agencies. Saferstein (2011: 95) indicated that in the USA, the FBI (Federal Bureau of Investigation) has an IAFIS system which is the national and criminal history system which contains fingerprints that are submitted voluntarily by State, local, and Federal law enforcement agencies. This collection of fingerprints will assist the LCRC to have fingerprints all South Africans in their database beside those being criminally charged, and their system should store all those fingerprints. This is however does not mean all people will be doing security checks, but the LCRC database will slowly grow.

Most people who do security checks are not likely to be on the wrong side of the law as they might be employed, whilst the people who do housebreaking, theft from motor vehicles might be people who are unemployed and would not be requiring security checks for employment. However, those people, might apply for firearms, visas and Professional Driving Permits (PRDPs). As discussed in Chapter 4 the Department of Transport also requires security checks from drivers before they can be issued with PRDPs. Professional Driving Permits are permits that authorize drivers to drive buses, taxis and any other public transport. Drivers can do their own security checks, or they submit their fingerprints at the DOT during the PRDP application.

Muvoni Technology Group (2013) indicated that the drivers of all buses, heavy goods vehicles and taxis must have PRDPs. In the USA, the FBI launched a system called the Next Generation Identification (NGI), a database that contains the biometric data of millions of Americans to enhance background searches; of criminals and non-criminals (FBI, 2013). This NGI database is mainly for enhancing background searches; this implies that it is a system similar to the PIVA system; since PIVA system contains data from all departments, it also contains information on criminal records. However, the system needs to be enhanced for latent searches as well and be extended to local Criminal Record Centres for fingerprints to enable fingerprint experts to do latent searches.

5.4. Summary

This chapter discussed findings from the literature study and from the participants. All participants were experienced and fully aware of the subject under discussions. The discussion clearly shows that there is no relationship between departments and that there is no standard operating procedure. The implemented fingerprint system, the PIVA which integrates information from other departments, does not assist the

LCRC with the identification of latent prints of first-time offenders. Some correctional centres in the Department of Correctional Services still manually capture the fingerprints of offenders. Offenders are admitted and released manually. The verification of offenders` identities is manually sent to Home Affairs and by the time the true identity of the offender is returned to the Correctional Centre the offender has already been released. These findings on this chapter and previous chapters will be discussed and interpreted in the next chapter.

CHAPTER SIX: INTERPRETATION OF RESEARCH FINDINGS AND DISCUSSIONS

6.1. Introduction

The previous chapter presented data collected from literature and participants, in this chapter the researcher interprets the findings telling the reader what has been learned from the previous chapters. The researcher discusses the objectives to indicate the relevance of this study.

The following objectives are discussed:

- The process to be followed by the LCRC in identifying latent prints of a first-time offender.
- The challenges faced by the SAPS LCRC in identifying first-time offenders.
- The roles to be played by other government departments to assist the SAPS in identifying latent prints.
- The international best practices on the identification of first-time offenders.

6.2. The process to be followed by the LCRC in identifying latent prints of a first-time offender and the DCS standard operations

There are crimes which are not resolved because there is no information leading to the offender. Failure to solve such crimes results in criminals arrogantly committing crimes without fear of being caught by law enforcement. This is the reason why the community often label the criminal justice system as lenient to offenders. It is therefore imperative that strategies of sharing information with those who possess information should not be overlooked.

Olckers (2007: 1) supports the views of the participants by indicating that many citizens believe that when they experience a burglary or house robbery, the chances of cases getting solved are slim, since such crimes are not given priority attention and must wait in line for attention behind more prioritised violent crimes. People who report housebreaking, or when a vehicle has been broken into, do not touch anything, waiting for the police and fingerprint expert to come and take latent prints and they expect that there will be a possible arrest and/or recovery of stolen goods. In paragraph 95 of S v Mbatha 2018 (170) ZAGPJHC, a judge described housebreaking as a crime that is difficult to trace. The Judge, upon reading his judgement stated the following:

> *"In housebreakings, perpetrators target time when property owners are absent or fast asleep and are difficult to trace."*

The SAPS have latent prints uplifted from crime scenes and which are stored on their database. With the involvement of DHA or the Department of Transport (DOT) those perpetrators can be identified. Until such perpetrators are arrested and charged, they are still on the loose.

The participants at the LCRC emphasised that they still have latent fingerprints which are identified but cannot be linked with any of the fingerprint information on their database. They pointed out that the reason for not being able to link or compare fingerprints on their database is that the person, who left the prints at the crime scene, has not been arrested and the relevant information is not on the LCRC database.

Participant 17 from the LCRC was very keen and looking forward to the integration of criminal justice system departments. She indicated that to this date, the SAPS does not have access to DHA fingerprint information unless it is a high- profile case. She even raised a concern that all people`s cases should be prioritised equally. This confirms the frustration the community experiences because they feel that their cases are not getting prioritised.

This perception has also been raised by Olckers (2007: 1) who stressed that by not listing burglary crime as a priority crime, burglary gets 'side-lined' or 'marginalised' in terms of the allocation of police time, resources, investigations, etc. This opinion is confirmed by the fact that police officers are also not excited by housebreaking cases because it is a known fact that fingerprints will be picked up, but the chances of identifying the suspect are very slim. Although fingerprint officers who uplift fingerprints do not mention this, their turnout time also does not indicate any enthusiasm, as they take long to respond to if not the following day.

Participant 5 from the LCRC did not agree with the integration and the searching of latent prints by utilizing the Department of Home Affairs. This participant raised a concern of identifying the wrong people, as the DHA has information of all people. The answer to such a concern lies in the skills of the investigator. Not all fingerprints found on the crime scene belong to the offender. Kriel (2011) pointed out that by examining the evidence submitted, the laboratory may be able to compare and identify latent prints for elimination purposes. It has been mentioned previously that the identification of fingerprints does not mean that the suspect has been found, but simply means that there may be a lead to the suspect.

Participants confirmed that at the provincial and local criminal record centres they do not assist investigators with identifying unidentified bodies, but such information is retrieved by the National Criminal Record Centre which liaises with the DHA. The process for such identification is that the investigator obtains fingerprints from the deceased and personally sends them to the National Criminal Record Centre. The LCRC needs a system that will identify latent prints of a first-time offender who is not on SAPS system and whose identity is unknown, but his latent prints are readable.

Such system must have access to the DHA and the Department of Transport as well as any other government department databases. The following case presents proof that minor crimes can turn into serious crimes. In the case S v Mbatha 2018 (170) ZAGPJHC, suspects were linked with fingerprint information. Count 1 was Housebreaking with the intent to steal and theft. This is confirmation that a suspect can turn himself from a minor crime offender to a serious crime offender. The case is as follows:

> *"Count1: Housebreaking occurred on 18 June 2006: Five (5) years imprisonment.*
>
> *Count 2: Robbery occurred on 16 July 2006: Fifteen (15) years imprisonment*
>
> *Count 3: Attempted Murder Occurred on 16 July 2006: Seven (7) years imprisonment.*
>
> *Count 4: Murder Occurred on 16 July 2006: Life imprisonment Crime committed.*

> *Count 5: Robbery occurred on 18 August 2006: Fifteen (15) years imprisonment”*

The accused in this case committed a crime in June 2006 and he was not caught, he believed that it was possible to commit a crime and still walk free, few weeks later he returned to the same house and killed one victim. In June 2017 he was arrested for a Housebreaking having been caught red-handed. In the 2017 Housebreaking he was not traced by means of fingerprints, but he was caught in action by witnesses. His fingerprints were obtained and LCRC managed to link him with latent fingerprints uplifted from 2006 crime scene.

According to the interview conducted with the IJS participants, the integrated system PIVA is available in 753 SAPS police stations across all nine provinces. However, the interview conducted with officials from the LCRC clearly indicated that they had very little to no knowledge about the PIVA. Only participant 7 confirmed some knowledge of the PIVA system, but also confirmed that he does not use it to verify information. It is therefore evident that the PIVA system is at a police station level not in criminal record centres where latent prints and fingerprints are investigated, since LCRCs are not situated in police stations centralised.

Participant 18 stated that the system is effective as it has checked a number of persons; for instance, at April 2020 to January 2021, the system verified the identity of 112,076 persons, of which 58,574 had previous SAPS records, and 3,084 were identified as wanted persons. Although the participant was dissatisfied by the number of checks conducted on this system, saying it could be better, a number of factors could have caused the low statistics. The country was in lockdown due to the COVID 19 pandemic, and not many people required these services as some other government offices were not fully operational and others were closed at some stage.

This also could be because some police stations were still using their LCRC instead of the PIVA for the verification of fingerprint information due to lack of training, lack of information or even ignorance. The DCS participants were also unaware of the system as the participants with the fingerprints system only knew about their system, the IIMS, which is not linked to any of the government department but only to the DCS.

The DCS has a shortage of fingerprint systems, since not all DCS Correctional centres have the required software. Mngcungusa (2005) indicated that the Department of Correctional Services deployed biometric technology in correctional centres that was piloted in June 2005 in three provinces, namely Gauteng, Eastern Cape and KwaZulu-Natal. After the system had crashed in Durban Westville it was not replaced and no other fingerprints system was implemented.

The centres that have the fingerprint system use the IIMS which is effective, but not linked with any of the other departments. However, the study revealed that there are a number of correctional centres which are still using the manual system to manage offenders or inmates, and that very few centres use the IIMS.

The manual filing of inmates is outdated, and the use of technology is essential to avoid neglect of duties where the staff might overlook other responsibilities and to avoid inmates from taking advantage of the system. This already happens in some correctional centres and in the SAPS where offenders supply wrong particulars or false identities knowing that they will not be recognised. The facilities with large number of inmates like the Westville Correctional Centre and other correctional centres in KwaZulu Natal still use manual admission and release of inmates.

There is no sharing of information and there is no integration of information between the departments. Departments operate independently, regardless of the fact that the implementation of integration had already been discussed before 2001. The process started thereafter, and it was further regulated in 2010 with the Criminal Law (Forensic Procedures) Amendment Act, No. 6 of 2010. According to the briefing held by the Department of Correctional Services in March 2001, the Committee was told that the automated fingerprint system would be used in the integrated justice system consisting of the Department of Correctional Services, Department of Social Development, Safety and Security, and the Department of Justice (PMG, 2001).

Participants emphasised that the biometric system that was used in their facilities was very useful and indicated that it should be reinstated. The participants called the system the Inmate Tracking System (ITS). ITS system had devices that were installed on inmates` wrists, to track the movement of the inmates, but they were not accurate. Participant 19 mentioned that if an inmate was on the third floor of the building the device would point out the building without pointing out the floor.

However, on other functions, the system was perfect and is still commended by members. Members were not sure why the system stopped working, because some other equipment was not removed and was still operative, some members indicated that the, service providers were no longer paid while others said the service crashed because it was not big enough to handle the collected data. Another reason given by some members was that the effectiveness of the device was tested in a pilot study.

The importance of an effective fingerprint system in the correctional centre has been stressed by the participants, it is essential that information is shared with other departments. Commissioner Motseki the former Chief Deputy Commissioner in the Department of Correctional DCS, explained the objectives of the inmate tracking system, stating that it was intended to decrease the detention cycle time of awaiting trial detainees, and indicated that there were two pilot sites where the system was tested, namely the Durban-Westville and the Johannesburg Correctional Centres (PMG, 2008).

Wyllie (2017) states that the large number of offenders in correctional centres makes it difficult to manage identification records, therefore many correctional centres are moving away from collecting fingerprints manually and adopting biometric fingerprint identification technology. Wyllie (2017) explained that once a fingerprint has been scanned, it will be attached to that inmate’s records so that the inmate`s identity and all other information are available in the facility database.

Participant 9 indicated that the use of a fingerprint system would be very helpful as the manual recording of inmates is time consuming in itself, apart from searching for the hard copy of the inmate`s file in the filing cabinets.

Participant 16 indicated that:

> “M*odernization and reform of the criminal justice system is overdue, and the program has been working closely with SITA to address issues related to poor project delivery progress. Resource constraints are often cited for under performance, and the program is working closely with SITA to establish a team of dedicated ICT professionals to support the Integrated Justice System program and the prioritized member department projects.”*

The involvement of SITA (State Information Technology Agency) in this process shows the gravity and importance of this implementation. SITA is the service provider for government departments and consolidates and coordinates the State`s information technology. For SITA to get involved in the implementation of the PIVA system in all government departments would be ideal as they are already on the ground and work closely with all departments. SITA will also provide the best advice for government departments regarding the protection of people`s information.

Participant 9 suggested that the fingerprint system should be integrated with the courts to ensure that the person appearing in front of the magistrate is the correct person charged on a specific case. The White Paper for the Management of Remand Detainees (2014:51) also indicated that detainees do have the tendency of exchanging identities where the remand detainee intimidates or conspires with another remand detainee to exchange identities or to defeat the ends of justice.

6.3. The challenges faced by the LCRC in identifying first-time offender on fingerprints found at the crime scene.

A serious challenge faced by the LCRC is the unavailability of a system that can identify the latent prints of first-time offenders. The available system, the PIVA, is not implemented in the LCRC, and the LCRC participants did not know the system. Another challenge faced by the LCRC is the poor quality of obtained fingerprints, since the LCRC deals with fingerprints forms where the fingerprints are often unclear as they were obtained manually by careless who did not check them before sending them off to the LCRC. The LCRC experts find it difficult to record those prints in their database. The study found that the Department of Home Affairs had agreed to assist the SAPS with information under certain conditions. As indicated earlier.

Thomas (2009: 4) explained that the DHA has been able to provide information to the SAPS under certain conditions and in return the DHA will be able to carry on supporting requests, provided that the requests do not unduly burden their current personnel capacity. This is understandable in cases of staff shortages and backlog, but it allows the selection of cases where serious cases receive undivided attention whilst minor burglary cases are put aside. Therefore, a call is made to the DHA and the SAPS to prioritise each and every case where fingerprints are involved to prevent criminals from serious crimes.

The study also found that not all persons who had been arrested and charged are captured in the LCRC database. According to Section 36B 6 (iii) of Criminal Procedure Act, No. 57 of 1977, any fingerprints of a person not found guilty in court must be removed from the criminal record register. The clearing of criminal records is a respectable idea, since some people learn from their mistakes and move forward, and a criminal record may prevent them from progressing. However, that information should be kept in a separate database, where if those fingerprints are picked up at another crime scene, they can be identified. Participant 5 indicated that if the person is a first-time offender, the AFIS will not have their fingerprints any more, as their fingerprints records will have been destroyed. This implies that this person will go free because the LCRC no longer has his information.

This study discovered that some correctional centres do not have the biometric or fingerprint system, such as Westville, Kokstad, Umzinto and Pietermaritzburg. As a matter of fact, the DCS relies on the DHA when verification of offenders` information is required, and SAPS with SAP 69 for previous convictions, and that is the current procedure which is manually conducted. Participants from institutions where there is no fingerprint system, indicated that it is even worse when thumbprints are compared manually by the naked eye, as the fingerprint they obtain need to be the same as the fingerprint appearing in the warrant, but if the one on the J7 is not clear, they end up admitting the person.

This study also found that it is possible for offenders to use different names during admission and that sometimes two or three inmates share the same names. This is possible to happen coincidently; but participants pointed out that inmates do this deliberately. An inmate can go through the whole process of the criminal justice system with his criminal record not recorded at all, or incorrectly recorded. This happens when fingerprints are not obtained correctly. The use of fingerprints in all departments is very important, so that if the police failed to obtain fingerprints correctly, the DCS may have a fingerprint system and the fingerprint will be available on the system. In so doing, the fingerprint information captured by the DCS will automatically be available in the integrated system, in this case the PIVA system.

6.4. The role that can be played by other government departments to assist SAPS in identifying first-time offenders

The Minister for the Department of Home Affairs, Gigaba (2018), during his speech on the launching of the ABIS, indicated that the Department of Home Affairs has rolled out the ABIS project which will be implemented in phases over a five-year period. The Minister indicated that implementation would entail migration of the current HANIS data (fingerprints and facial recognition) to the new ABIS, with improved functionality, installation, and configuration of the ABIS infrastructure (hardware), and building of system functionalities. The HANIS system, as discussed above is the system which was used to assist the police with information at border posts.

The Minister mentioned a number of benefits that could be expected when the ABIS goes live, including the following:

- The SAPS will be able to search for suspects by matching latent prints against records on the ABIS,

The Minister of Home Affairs listed these expectations after the implementation of the PIVA system, as mentioned earlier that the DHA also included in the PIVA system. However, this is not working because the dockets are still closed as undetected with positive latent prints found but there is no information available to assist the police. The PIVA is available in several police stations, but it still does not identify fingerprints picked up from a crime scene because those prints are not uplifted by a police station; they are uplifted by a fingerprint expert who does not have access to the PIVA system. As discussed earlier, the PIVA in police stations is used to check if the arrested person is a repeat offender or not.

SAPS Annual Report 2021/2022 (2022: 62) confirmed implementation of PIVA system in police stations as of 2022 and there is no mention of PIVA in the identification of latent prints or any other fingerprints.

> *“In terms of the utilisation of digital systems for multi-modal biometric person identification and verification, the current identification and verification of accused persons is implemented at 908 police stations.”*

In police stations PIVA system assists investigators in establishing the criminal record of the accused before appearing in court and to inform other role players that such a person has been arrested. The PIVA also assists the investigators and the court to determine whether to decline bail or to allow the accused to be released on bail. One of the members who work with PIVA and who attended the PIVA course indicated the following:

> *“PIVA in police stations is used to identify repeat offenders and it is now called PVIS (Personal Verification Identification System) and its purpose is the same as PIVA but only configuration changed. This system is only used on live fingerprints of the person.”*

The DHA describes the ABIS as a modern IT system which will integrate with other relevant systems, inside and outside Home Affairs, to allow for one holistic view of the status of clients; it will serve as a single source for biometric authentication of citizens and non-citizens across state institutions and private sector entities. Another difference between ABIS and PIVA is that the ABIS will also assist the private sector whereas the PIVA system only works with government departments. Some commercial banks already collaborate with the DHA. By means of a thumbprint, the bank verifies and links the client`s thumbprint with information on the identity book. Participant 16, who knows the processing of the PIVA system explained the process as follows,

> *“A government official will enter or scan a person’s identity document number into the PIVA application, and will scan two of his/her fingerprints, using an approved fingerprint scanner. The PIVA application will then communicate with DHA to verify if the data is valid for the specified identity document number.*

This implies that the PIVA system requires the physical thumb print or identity number to be available; unlike in the case with latent prints, where none of these will be available. Latent prints will not have the owner of fingerprints nor the identity number available. Therefore, the PIVA is not suitable for comparison and verification of latent prints, and it requires more features to accommodate the LCRC.

The table below presents a summary of the differences between the ABIS and the PIVA system. These differences are according to the researcher's analyses by means of annual reports and comments as discussed above:

Figure 6: Difference between PIVA system and ABIS

PIVA	**ABIS**
Searches criminal record	Searches criminal record
Limited to public sector departments	Can be accessed by a private sector e.g., commercial banks
Cannot search latent prints	Can search latent prints with limited access
Requires physical fingerprints	Physical fingerprints and/or thumb print
Searches ID number	Searches ID number
System is in different department	Located in the DHA offices

The Minister of Home Affairs reported that the ABIS would be for identification and security solution in support of the national government's drive towards modernisation of all departments. The advantage of having access to the ABIS is that SAPS will be able to search latent prints against records on ABIS, whereas the PIVA cannot search latent prints.

The difference between the two systems is that PIVA is or will be available in other government departments whilst the ABIS is found in the DHA offices only and police access is limited to unidentified deceased and priority cases. The PIVA integrates and the ABIS allows access, although the ABIS is available at the DHA office and can be used by the DHA personnel. The PIVA system will be implemented in government departments and will be easily accessed by the departments. Having the ABIS accessible at the DHA only, will make it impossible to assist the LCRC with all their property crime cases, as emphasized by Thomas (2009: 4) that the DHA will carry on supporting requests provided that the requests do not overburden the DHA personnel capacity.

In this study, some of the participants at the LCRC confirmed that some fingerprints are readable but with identification information unavailable. Though they confirmed this but they were not aware of the fact that when fingerprints were readable and given the status “P” (Positive), the detectives close the docket. They indicated that they were not sure what happens to the docket. Participant 17 confirmed knowledge that the docket gets closed with the brought forward date but was also not happy with the fact that the investigation does not go further than that. She asked why there is no link or collaboration with the DHA, as DHA has all citizens` fingerprints.

Some participants at the LCRC confirmed knowing that in serious cases where the latent prints are not found on their local database, those prints are sent to the National CRC; however, they were also concerned about the practice of prioritising certain cases and neglecting the so-called minor cases, indicating that it is unfair to those who reported cases. Olckers (2007: 1) pointed out that residents who were interviewed felt that their burglary cases were not prioritised, they wait in line for attention behind higher prioritised violent crimes cases. This is because those cases are dealt with by the local Criminal Record Centre by means of the database that does not have the particulars of first-time offenders and cannot get assistance from the DHA.

2020/2021 to 2021/2022 (SAPS Annual Report, 2022: 213) pointed out that the detection rate for property related crimes is still a challenge. The detection rate during these two years shows that from the 441 135 cases that were reported only 82 222 cases were detected. The Annual Report pointed out that these were case dockets in which suspects were known or could be identified by means of forensic leads, such as fingerprints and were apprehended.

This implies that detection tools are still a challenge, since the number of reported cases in property crimes (which may be detected by latent prints found from the crime scene) is still too high. The word may be detected means that not all fingerprint related cases can be detected, as it is noted that some suspects use fingerprints barriers like gloves to prevent identification. Nevertheless, as indicated in Chapter 1, there are dockets which are closed with positive fingerprints because the fingerprints picked up from the crime scene have not been found on the AFIS. In such cases access to the integrated system the PIVA will assist the LCRC.

Sharing of information between government departments is crucial to reduce or avoid fraud. In the departments which do not have the technology systems to record information, there manipulation and dishonesty are rife, aspects which attract and encourage criminals. For instance, some government hospitals and clinics do not use technology to register the birth of children, fraudsters then get birth cards, and register children with the DHA defraud SASSA and the Department of Social Development. Although the DHA is technologically advanced, there is no collaboration with the Department of Health to check if a specific child was really born in that hospital/clinic.

A system which will link the Department of Health and the Department of Home Affairs is essential as it will reduce or stop such activities. These fraudulent practices will slowly come to an end, as it has been reported that hospitals are now registering patients electronically which will be more effective if such system is linked with other department systems. The Police will also benefit from such a system, as people not found in other systems may then be found on hospital systems. The South African Government (2020) reported that the South African President during the 2020 State of the Nation Address, indicated that in preparation for the National Health Insurance (NHI), the government has already registered more than 44 million people at over 3 000 clinics in the electronic Health Patient Registration System, and is now implementing this system in hospitals. As discussed earlier, the Auditor General Makwethu (2020: 5) stressed the integration and sharing of information between government departments as such information would have been used by SASSA to check if the people applying for such grants were eligible or not.

A person who cannot be found in other departments might be found in the records of clinics and hospitals. Therefore, sharing information with the Department of Health will be useful. Also, during the Covid-19 pandemic, people were required to produce their latest identity information during vaccination, had every person registered for the vaccination, the DOH would have every citizen recorded in their database. The vaccination process proved that the Department of Health can also require identity information for health services; just like in private hospitals where patients have to produce full identity information.

The Identity information from a dying patient may be obtained by implementing a new, where the patient information is retrieved using fingerprints scanners for thumb prints. The Department of Health may have an issue with adhering to the POPI Act and protecting patient information. However, it is not the patient history that is needed but only the record of who was seen. This sounds impossible to govern, however, to fight crime and to deter crime, this can be made possible. Section 6 of the POPI Act as discussed in earlier chapters allows public bodies to process personal information. The Act states that the protection of personal information does not apply to the processing of information by the public bodies if it is required for criminal investigation.

6.5. The international best practices on the identification of first-time offender

6.5.1. Identification of persons not found on criminal record database

The POPI Act has restrictions regarding the in sharing of people`s private information. This should not involve law enforcements if there is proof that information is required for investigation purposes. Government departments have justifiable reasons to share information amongst themselves, especially for the prevention of crime and for investigation. The POPI Act should not be the reason why the departments do not expose the criminals because the same person they are protecting, might turn the department into a victim. Section 6 of Protection of Personal Information Act, No. 4 of 2013 authorizes departments to share information amongst themselves as it states that protection of personal information does not apply to the processing of information by the public body. All government departments are public bodies.

The Federal Bureau of Investigation (FBI) released a rule claiming several Privacy Act Exemptions. The FBI released this rule to enhance their investigations which emphasizes the commitment of the FBI to fight crimes. In addition, the FBI implemented a program known as the Next Generation Identification (NGI) to access the information of a certain percentage of the population. However, the Electronic Privacy Information Center (EPIC) opposed the program, indicating that the program raises privacy issues that implicate the rights of Americans all across the country (FBI, 2013).

South Africa has a Limitation Clause, Section 36 of the Constitution of the Republic of South Africa, No. 108 of 1996. Section 36 is used by law enforcements where people`s rights are infringed not that they are allowed to infringed people`s rights but Section 36 comes to their rescue as it justifies some acts for law enforcement which are infringing the Bill of Rights. As per the FBI and their Privacy Act Exemption, the South African Criminal Justice System is covered by Section 36 (limitation clause) which provides that such rights may be limited only in terms of the law on condition that the limitation is reasonable and justifiable. With Clause 36 and Section 6 of POPI Act departments should freely share information of suspected people.

6.5.2. National fingerprints Database created from security clearance.

The study found that the USA launched a database that will have biometric data of all Americans to enhance the background search of criminals and non-criminals (FBI, 2013). This will work for the FBI, since other departments might not provide them with information. In South Africa security clearance is done with the LCRC, as they are approached by applicants who give consent for the processing of information. Therefore, these must also be used to launch a system that will store information of all South African citizens.

6.5.3. The use of digital scanners in obtaining fingerprints

The use of fingerprints for information in correctional centres has been commended by Wyllie (2017) who indicates that the large number of offenders in correctional centres makes it difficult to manage identification records securely. Therefore, correctional centres in USA are moving away from collecting fingerprints manually and they are adopting biometric fingerprint identification technology. The responses of participants clearly indicated that South Africa should have such a system have such a system as well.

Wyllie (2017) believes that during the booking process, one of the most important things correctional centres must do is to establish the subject’s identity by collecting readable fingerprints because failure to do so can present a host of problems including having an offender go through the entire criminal justice process booking, sentencing, incarceration and release without having had his or her fingerprints properly captured. An offender may have submitted false and misleading information and appears to have no criminal record, whereas in reality he is a serious offender. This may happen because some correctional centres are not equipped with fingerprints systems.

Another reason might not be the failure to obtain readable prints, but some offenders are doing it deliberately to keep their real identity clean. This was confirmed by the participants who indicated that sometimes a wrong offender responds not willingly by being forced by other offenders to respond. An integrated fingerprint system in all correctional centres will be able to determine if the person who responded is not the one required. Additionally, the use of fingerprint scanners will enable the proper collecting of fingerprints rather that by means of fingerprint papers and ink.

6.6. Summary

This chapter focused on analysing the responses from the literature review and from the participants. The discussion on the research questions and/or the objectives of the study. The aim was to explore the fingerprint identification systems that can be used to enhance the investigation of first-time offenders. The study found that currently there is no integration or information sharing between the departments. A PIVA system is available in police stations and has fingerprint information from other departments, but it does not work with latent prints, and it does not assist fingerprints experts to verify fingerprints. First-time offenders remain undetected. All participants indicated that they are not using the PIVA system, in actual fact some did not know of the existence of the PIVA. The next chapter, chapter 7 discusses the recommendations to be considered for implementation in order to improve the service delivery within the SAPS and other government departments, the chapter also outlines what this study has found in the conclusion.

CHAPTER SEVEN: RECOMMENDATIONS AND CONCLUSION

7.1. Introduction

The aim of this research was to explore the use of fingerprints identification systems on latent prints of first-time offenders. Chapter 6 interpreted the findings thus unpacking what the study has found in the previous chapters, in this chapter the researcher provides recommendations to be considered for implementation. The recommendations are based on a number of factors, including the lack of collaboration between government departments which contributes to poor service delivery to the community. The lack of collaboration contributes to poor identification of latent prints of first-time offenders because the LCRC database has information of previously charged people, but they do not have information of previously innocent first-time offenders.

The research approach used in this study is a qualitative approach with case study research design to understand the topic under investigation through the experiences of officials working with the fingerprint system. The researcher used semi-structured interviews and non-probability sampling as it does not implement randomisation. Through purposive sampling, the researcher purposefully selected participants who were directly involved in the identification, verification and comparison of fingerprints to get credible and accurate information.

The researcher analysed data by means of thematic analysis where data codes were developed to represent identified themes which were linked to the research questions and the objectives. The researcher developed the following objectives which were used to collect data.

7.2. The process followed by the LCRC in identifying unknown suspects when latent prints are found at the crime scene.

The LCRC uses the AFIS system for comparison, identification, verification and recording of criminal records, but the system is not linked with any of the Criminal Justice System departments. Verification is done manually by going to DHA, there is no standard operating procedure.

Recommendations:

- Latent prints of first-time offenders which are sent to local Criminal Record Centre are not detected, and only serious crimes are sent to the National Criminal Record Centre for identification. The SAPS and the DHA must consider another operating procedure which will accommodate latent prints of first-time offenders not found in Local CRC database. For instance, when a local expert examined/investigate fingerprints and could find any information available on the database, further steps should be taken to locate fingerprint information.

- Those fingerprints must be searched/investigated on the DHA database, no matter how small the crime, is or searched through the PIVA system. This situation is a compelling reason to empower the PIVA to search latent prints and then be deployed at the LCRC rather than at police stations. Criminals who got away with minor crimes like housebreaking (as it is called) can be dangerous as those can turn into serious crimes. If criminals are not apprehended, they made continue with their criminal activities as it becomes more difficult to bring them to justice, or by the time they are brought to justice even more crimes may have been committed.

- It is recommended that all government departments be equipped with a system that will allow record keeping and sharing of information. The use of technology is imperative, since working manually can cost the government billions of money. Technology replaced paper, therefore advancing to technology is crucial to beat the criminal mind. Criminals are also technologically advancing themselves to latest technology every time a new system is introduced. The risk of not staying abreast of the latest technology developments, costs departments a lot of money.

Departments with dated/ old systems experience filing challenges and information retrieving challenges. Offenders begin with minor crimes and if they are not caught, their confidence grows, and they escalate to serious crimes. A minor housebreaking can grow to a house robbery and may escalate to murder if the perpetrator is not apprehended after committing the first minor offence. It is impossible to have a crime-free country but reducing crime with effective mechanisms is possible if fingerprint information can be shared.

- When sharing of information, stricter access to information is vital complicate for those intending to divulge information. Punishment for members who contravene laws and policies protecting people`s privacy must be communicated to other employees to act as deterrent to similar acts.

- The implementation of the PIVA in correctional centres is important since the PIVA uses fingerprints to identify persons. The system will not only be used for admission and releasing but, it will also be useful in sharing of information between departments.

7.3. The challenges faced by the SAPS LCRC in identifying first-time offender on fingerprints found at the crime scene.

The LCRC can only identify fingerprints of previously charged persons and cannot identify first-time offenders. During interviews all participants complained of poorly obtained fingerprints with the results that fingerprint forms are not clear and cannot be scanned on fingerprint system. Some correctional centres do not have fingerprint system and are admitting and releasing offenders manually. Therefore, the following is recommended:

Recommendations:

- It is recommended that the SAPS implement or create a database of all South African citizens they come into contact with. The SAPS should store fingerprint information of all security clearances; not on a criminal record database, but a database that will be used to identify fingerprints of people not found on the AFIS or criminal record database. For example, police take people`s fingerprints for security clearance purposes, for firearm applications, employment clearance, travelling visa clearance, vetting purposes and for Professional Driving Permits (PRDPs), but the police do not store those fingerprints in their database, or they do not use those fingerprints in first-time offenders' searches.

- This database should also include fingerprint information of people who have been cleared of criminal records. The study revealed that people can apply for expulsion of criminal records on certain conditions if they qualify. People who were charged for minor offences and people convicted for 10 years and beyond can be removed from the LCRC database. This study proposes that those fingerprints should remain in the database of innocent people who have applied for security clearances, so that if a set of fingerprints is not found in the criminal record, the search should be extended to this database before other searches are attempted. As mentioned in Chapter 1, the Purpose of Criminal Law (Forensic Procedure) Act 6 of 2010 was to amend SAPS Act 1995 to regulate the storing and the use of fingerprints. The fingerprints that must be stored, that require this regulation should include those fingerprints obtained during the non-criminal checks such as security clearances.

- The LCRC experts are trained for comparison and verification of fingerprints, and police station officers do not have such expertise. The LCRC must be equipped with a system that contains information of all citizens e.g., the PIVA system to identify latent prints of first-time offenders positively. This will enable the police detectives to perform their jobs effectively. This will enable the local fingerprint experts (LCRC) to identify suspects in minor cases or in serious cases, without travelling to the National CRC for verification.

- Not all investigators will use information for infringement purposes, but only a fraction compared to the number of undetected cases. All means to detect fingerprints cases must be exhausted before it can be decided that the suspect was indeed undetected. Mofokeng and de Vries (2012: 28) were of the view that many cases go undetected because of the police`s weak criminal investigation capabilities especially in respect of forensic investigation. Therefore, in order to fight this belief the SAPS must work hard to gain access to these databases.

7.4. The role that can be played by departments such as the DHA and the DCS to assist the SAPS in identifying latent prints of first-time offenders.

There is no relationship between the departments, as all departments are working independently. The obligation and emphasis to protect people`s information in terms of POPI Act hampers the sharing of information.

Recommendations:

- It is recommended that all government departments be equipped with systems that will allow record keeping and sharing of information. Technology has become very important, as there is worldwide movement to become paperless. Those systems will save the government money and time. Criminals manage to keep abreast of the latest technological systems and therefore government must become technologically advanced. In the departments where systems are dated, there are filing challenges and information retrieval challenges.

- Further stringent access to information is necessary to complicate accessibility for those who are intending to divulge information. Training and workshops on confidential information, and sensitisation on illegal use of people` information in terms of POPI Act must be conducted continuously. Members who are caught contravening the laws and policies on people`s privacy as per the POPI Act, must be punished and the punishment must be published as a form of deterrence to prevent similar acts.

Department of Correctional Services

- The DCS to have a system that will store information of all inmates admitted and released and the same system must be shared amongst other facilities, this will assist the correctional centres to recognize the repeat offenders.

- It is recommended that fingerprints scanners be implemented in court as the participants raised concerns that sometimes there are challenges during admission, where fingerprints taken on the warrant (J7) are of poor quality and not visible enough for a positive verification. Wyllie (2017) indicates that the large number of offenders in correctional centres makes it difficult to manage identification records, therefore correctional centres in USA are moving away from manually obtaining of fingerprints and they are adopting fingerprints identification systems. Komarinski (2005: 85) saw that the use of AFIS technology was appreciated by agencies involved in fingerprinting. Komarinski (2005: 85) indicated that the clerical work that was performed by the FBI Criminal Justice Information Services (CJIS), such as retrieving and classifying fingerprint cards, storing them in file cabinets, and looking for a misplaced or misfiled card was either reduced or was eliminated totally. In this study, this was an issue at the correctional centre where there was no fingerprint system, and the manual filing of fingerprints was said to be an inconvenience when it comes to searching for files.

- The DCS should require identity numbers (ID numbers) from offenders and inmates. An ID number must be a prerequisite during admissions. The use of a fingerprint system linked to DHA system should be used to retrieve the identity number of the person admitted preventing false identities. This will require fingerprint scanners where offenders` fingerprints will be scanned to get their ID numbers so that the correct information is recorded at the centre. This will assist even families, who are looking for their loved ones or police looking for missing persons. If the offender used a wrong identity during admission, enquiries will be done at the correctional centre to locate a person, and often to no avail since the police or the family will have another name whilst the correctional centre has another name.

Department of Home Affairs

- It is recommended that the Department of Home Affairs should consider cooperating with other departments. They should consider the amount of crime the country is facing when they (DHA) can reduce such crimes by allowing the police to bring the wrongdoers to justice. When there is a proof that information is required for investigation purposes, DHA should not be concerned by the privacy of information; Section 6 of Protection of Personal Information Act No. 4 of 2013 stated that protection of personal information does not apply to the processing of information by a public body if it is for the purpose of prevention, detection, of investigation or to prove an offence. POPI Act defines a public body as any department of state in the national or provincial sphere of government. Therefore, DHA is one of the public bodies, it does not have to be a criminal justice department.

7.5. The highlight of international best practices on the identification of first-time offender using fingerprints systems.

Interpol suggested the sharing of information with other member states via integration. The United States of America (USA) has implemented a database containing non-criminals using information obtained during security clearances and the USA is working towards obtaining fingerprints by means of fingerprint scanners to avoid poorly obtained fingerprints.

Recommendations:

- To avoid poorly obtained fingerprints as it has been a concern of all participants, police stations and correctional centres should be provided with digital fingerprint scanners to create the fingerprints forms known as the SAP 76. Komarinski (2005: 15) indicated that since the rolling of inked fingers onto a tenprint card has been replaced with the digital capture devices (livescans); the turnaround time for identification is much quicker, as the speed of technology to confirm or deny identifications is within minutes. Komarinski (2005: 15) further stated that these livescan images can be sent to the state identification bureau electronically. Similarly, as mentioned earlier Wyllie (2017) states that correctional centres are stopping the use of manual collecting of fingerprints and turning to biometric fingerprint identification technology. Therefore, fingerprint information obtained digitally during that process can be processed to the LCRC and the previous convictions (SAP 69s) may be available immediately for court.

- Most organisations are now technologically advanced, and SAPS should do the same. The use of fingerprints papers should be phased out. This will also save departments a lot of travelling to and from the LCRC, submitting SAP 76s and collecting SAP 69s (previous convictions). Interpol (2022) also confirmed that fingerprints from charged persons can be obtained digitally by means of scanners, therefore SAPS should do away with fingerprint forms namely the SAP 76 forms used on to obtain fingerprints of an arrested persons, and SAP 91 (a) used for enquiry or security checks and any other fingerprint forms. This will save the state from purchasing ink, paper for forms, and other costs involved in using manual and paper fingerprinting. There will be no need to retake fingerprints from charged persons where poor fingerprints had been obtained.

- Interpol (2022) indicated that fingerprints can be taken with an electronic scanning device, and a scanner is then used to save the data electronically in the appropriate format. These digital devices can be used even for security clearance where applicants' fingerprints will be scanned and stored in LCRC database for the record to be used for a latent prints search at a later stage. According to Komarinski (2005: 15), the FBI CJIS uses livescans for fingerprints instead of paper and ink, the livescan takes a picture of the finger in a similar way as the rolling of the finger in the paper. He further explained that in the livescan the picture of each finger on both hands is taken, then the four fingers and then the thumbs. This is how fingerprints are taken using the ink and the fingerprint form SAP 76 or SAP 91a and other fingerprint obtaining forms. It is now confirmed that the full set of fingerprints can be obtained using digital devices, in this case livescans.

- Police training in technology is also important. Police detectives are trained to use computers but only to use certain functions of computers like commonly known acknowledgement receipt of the docket (4.8) and charging an accused (5.3) status of the docket (4.5.1). More computer training is important to equip them with up-to-date knowledge to beat the criminal mind. Detective courses should include computer training or computer literacy should become a prerequisite.

- According to Fedotov (2022) the UNODC Executive Director, technology enables criminals to work across regions, increasing their reach, their crimes and their profits. Just as the Internet has transformed every aspect of life, it has also become a foundation of crime. This calls for the police to be technologically advanced too, as untrained first responders can contaminate evidence. The more criminals equip themselves with technology, the more challenging it becomes for the police to possess the latest technology knowledge and skills. Deloitte (2022) suggested that the innovation that is shaping the future of law enforcement begin with the emerging technology that supports new concepts of operations.

Community taking the initiative (proactive response)

- Burglaries, theft from motor vehicles and theft of motor vehicles are crimes mostly planned for houses or businesses which are unattended. The SAPS should encourage neighbourhood watches and Community Police Forums (CPF) where residents work together and take turns in patrolling areas. Section 18 (1) of the South African Police Service Act No. 68 of 1995 states that the police service shall, to achieve the objects contemplated in Section 215 of the Constitution, liaise with the community through community police forums and area and provincial community police boards. According to Neighbourhood Watch SA (2022) the neighbourhood watch assists in protecting property, reducing car break-ins and house burglary effectively. In the earlier mentioned case the S v Mbatha 2018 (170) ZAGPJHC, the accused in this case was arrested by CPF members. An Armed Response Security company was alerted about a housebreaking in progress, they contacted CPF members, who then proceeded to the address given and they caught the suspects. Upon their arrest one was linked by means of his fingerprints to crimes committed in 2006.

- During the festive season the police presence in malls and coast line areas is very high and this reduces criminalities effectively. This, kind of police presence is necessary to prevent crime effectively. The SAPS should recruit more reservists as they are a community who is willing to work for free and SAPS has made it very difficult for the applicants to get these opportunities. Increased police visibility discourages criminality, and police visibility includes that of the SAPS, Metro police, Traffic Police, and any other law enforcement agencies.

- Intensive training is recommended for police reservists, neighbourhood watch and CPF members to be more cautious when dealing with criminals. Such sensitization is very important to alert the community against vigilantism where community members take matters into their own hands, such as the Phoenix tragedy during the July 2021 unrest. This is where the community members protected their area and the businesses around Phoenix area, but which resulted in tragedy (as the researcher is a Phoenix resident). Community policing is very effective because their members are closer to incidents and can respond quickly. Their quick response, deter crime, and criminals fear the community where the community is active.

- Police reservists should be sensitized about cases that will put the police organisation into disrepute. Placing too much emphasis on the protection of the police image can result in such recruitments being overlooked, since some misconducts are committed in uniforms and some investigations points to police reservists. Therefore, to continue using recruiting reservists, the police have a task to caution them and train them properly.

- The growth of private security companies doing patrols also reduces burglaries even though security companies are doing it for financial gain, SAPS should have some kind of regular meetings with these companies encouraging them. Not relying on them but getting them involved in patrols and visibilities. Security companies play a measure role in such crimes as they are meant to prevent burglaries, however not all residents can afford such services like CCTVs alarms systems. Therefore, collaboration between security companies, community policing forums and SAPS will help even those families who cannot afford, hence reducing the number of reported burglaries.

7.6. Contribution of the study

The contribution of this study into the body of knowledge is a proposed Fingerprints system that can be used to enhance the investigation of latent prints of first-time offenders that are found in crime scenes in South Africa. The proposed fingerprints system should enable the sharing of fingerprints information between government departments and should function as follows:

Step 1: Where fingerprint information is not available in the criminal record system, the fingerprint expert, must search the database which contains fingerprints information of cleared people, e.g., the security clearance database.

Step 2: If the fingerprint information is not available on LCRC database the LCRC fingerprint expert must proceed to the system which contains other departments` fingerprint information. In this case, it should be the proposed upgraded PIVA system (that searches latent prints) or the proposed new fingerprint system where fingerprint information will be shared with LCRC. This system should be installed in LCRC and other government departments to avoid the delay of information.

Other government departments who need verification of information like DCS and DSD should access the shared fingerprint systems in their respective departments. The shared fingerprint systems must be installed in their offices, as this will save travelling time from one department to another.

When none of the departments has information for a certain individual (i.e. suspect, DCS inmate or DHA client), the department seeking the verification of information must record that person in their system as the custodian of that information; this will enable other departments to detect the person through verification and avoid numerous identities for that one individual.

**To protect people`s information:** access to people`s information should be limited to a few authorised people. Intense security features must be installed on the system like the use of thumbprints, individual password creation or face recognition this will limit the sharing of credentials.

As discussed in chapter 3, currently, government departments are sharing certain information contained in the Persal system for Human Resources Management and payment information contained in BAS system where all government payments are processed. Government departments also have access to a Central Suppliers Database (CSD) where all private companies` information is stored for bidding purposes. All these systems are protected with security features which makes it impossible for an unauthorised person to gain access. This confirms that sharing of information between government departments is possible and if fingerprint information is shared with LCRC, people`s privacy will still be protected by the creation of intense security features like the individual password creation accompanied by thumbprints security feature as mentioned above.

Departmental policies must be updated to govern the unauthorised access to the system to add on available legislations. Officials authorised to access the system must be sensitized about the unauthorised and illegal sharing of people`s information. As indicated in chapter 3, security policies are the framework that ensures that informational assets are secured (Wells *et al.,* 2012: 1.1351). The system must be able to store information of authorised officials who had access to people`s profiles, in order to know who had access to a particular profile. This will enable the detection of an official who committed the illegal act and be dealt with accordingly.

7.7. Summary

This chapter provided recommendations to be considered for implementation in order to enhance the investigation of latent prints of first-time offenders and a proposed model to be considered in order to better the situation. The recommendations if implemented will improve service delivery not only for the LCRC but also for other government departments who will benefit from the sharing of fingerprints information. If implemented, government departments will be able to resolve crimes which are committed using false identities and protect the citizens of this country.

7.8. Conclusion

The aim in this study was to explore the fingerprints identification systems that can be used to enhance the investigations of first-time offenders and the main objective was to explore on the sharing of fingerprints systems between government departments to enhance the investigation of latent prints of first-time offenders.

Currently there is no cooperation between departments as derived the literature; and the participants confirmed that there is no co-operation between government departments. The recent case of fraud; as indicated by Makwethu the Auditor General (2020: 5) is an indication that there is no sharing of information between government departments as mentioned in Section 15D (4) of Criminal Law (Forensic Procedure) No. Act 6 of 2010. The SAPS LCRC has property cases where latent prints of first-time offenders were not detected because the person who left fingerprints at the crime scene is not on their database. Instead of the LCRC going to the Department of Home Affairs for the name of the person who left the fingerprints. The LCRC just keep the fingerprints and wait for that person to be arrested on another case and then appear on their database. This is not fair for the victim of the case, the country at large and for the economy. As discussed earlier, when criminals are not caught, they do not stop until they commit serious crimes, making the country unsafe.

As indicated earlier about burglaries in South Africa, burglar guards and any other security measures are mandatary because burglary in some areas is rife, for both residences and businesses. Olckers (2007: 89), in his study on Residential Burglaries in Johannesburg, pointed that there are a number of security measures which one should have to prevent burglary including electric fencing, electronic gate, CCTV (closed circuit television) cameras, remote panic button, etc. To fight this scourge, detection of suspects should be taken serious as the Criminal Law (Forensic Procedure) Act No. 6 of 2010 saw the need for sharing of information in order to detect criminals who are not found in the LCRC database. Burglaries in South Africa are rife, even vehicle insurance companies are cheaper when the vehicle is parked in secured properties with boundary walls/fences and lockable gates.

The study found that there is a system in place working towards integration, namely the PIVA which is newly implemented and the ABIS which is an upgrade of the HANIS, with slow to a bit faster progress. The PIVA is fully implemented in the SAPS police stations and other criminal justice system departments like the Department of Correctional Service is still waiting to be included in the implementation. The PIVA will be very useful in sharing information between the departments and the DCS and in this case the inclusion of the LCRC to detect latent prints of first-time offenders. The PIVA does not assist police with latent fingerprints. Cases where latent prints are involved are still closed with identifiable or readable fingerprints, but particulars of those fingerprints are not available on the SAPS local criminal record database. Such cases where fingerprints have not been identified accumulate the number of cases reported but with a low detection rate. If latent prints are identified and arrests made, the detection rate percentage will improve.

The Department of Home Affairs has the ABIS which is meant to enhance the investigation and for other departments to be able to access information. The Integrated Justice System has the PIVA which integrates information from different departments to access information for different departments but currently there is no sharing of information or integration. The ABIS will interface online with other systems of criminal justice institutions and entities, which will enhance cooperation and information sharing between the law enforcement agencies, but this is not the case at the moment. If the Department of Home Affairs has been sharing information with other departments, the Department of Social Development would not have lost so much money through fraud and corruption where people claimed Covid-19 social relief grants for deceased people. Additionally, as mentioned by the Auditor General, had the DCS been sharing fingerprint information with other departments, Department of Social Development would not have lost so much money through fraud and corruption with people claiming Covid-19 social relief grant for incarcerated people. Therefore, not only the number of property crimes will decrease from the sharing of information, but the victims of crimes will find justice and have trust in police investigations.

List of References

Anfara, V.A. & Mertz, N.T. 2006. *Theoretical Frameworks in Qualitative Research.* California. Sage Publications.

Assiri, W. 2016. Risk or Loss of Productivity in Workplaces*. International Journal of Scientific & Technology Research,* Vol 5 (5): 119.

Babbie, E. & Mouton, J. 2012. *The Practice of Social Research.* 14th edition. United Kingdom. Oxford University Press.

Bless, C., Higson-Smith, C. & Sithole, S. L. 2013. *Fundamentals of Social Research Methods. An African Perspective.* 5th edition. Cape Town. Juta & Company.

Caulfield, J. 2019. *Thematic Analysis. How to Do Thematic Analysis. Step by Step Guide & Examples.* Retrieved from https://www.scribbr.com/methodology/thematic-analysis/ (Accessed on 28 September2022).

Change.Org. 2019. *Bring Back the Death Sentence in SA For Crimes Against Women.* Retrieved from https://www.change.org/p/south-african-government-bring-back-the-death-sentence-in-sa-for-crimes-against-women. (Accessed on 23 November 2021).

Christen, P. 2012. *Data Matching. Concepts and Technologies for Record Linkage, Entity Resolution, and Duplicate Detection.* Canberra. Springer.

Creswell, J. W. 2013. *Qualitative Inquiry & Research Design: Choosing Among Five Approaches.* 3rd edition. Thousand oaks. Sage Publications.

Constitution. S*ee* South Africa. 1996.

Criminal Procedure Act. S*ee* South Africa. 1977.

Criminal Law (Forensic Procedure) Amendment Act *see* South Africa. 2010.

Criminal Law (Forensic Procedure) Amendment Act *see* South Africa. 2013.

Cross, N. 2010. *Criminal Law and Criminal Justice. An Introduction.* London. Sage Publications.

Daigle, L.E. 2012. *Victimology. The essentials. Los Angeles*. Sage Publications.

Daluz, H.M. 2015. *Fingerprint Analysis. Laboratory Workbook.* USA. CRC Press.

Davies, M., Croall, H. & Tyrer, J. 2010. *Criminal Justice*. 4th edition. United Kingdom. Pearson.

Department of Correctional Services. 2018*. Annual Performance Plan 2017/2018 Financial Year*. Retrieved from www.dcs.gov.za (Accessed on 10 September 2019).

Department of Correctional Services. 2019. *Volume 5. Revised Procedure Manual Supervision (Unit 1-8).* Retrieved from www.dcs.gov.za. (Accessed on 15 May 2020).

Department of Home Affairs. *Annual Report. 2017/2018. Vote No.05. 2017/2018 financial year.* Retrieved from http://www.dha.gov.za/index.php/about-us/annual-reports. (Accessed on 10 September 2019).

Department of Home Affairs. 2019. *ABIS. Automated Biometric Identification System.* http://www.dha.gov.za/index.php/civic-services/abis. (Accessed on 20 November 2019).

Department of National Treasury. Central Supplier Database for Government. Retrieved from https://secure.csd.gov.za/ (Accessed on 05 November 2019).

Department of National Treasury. Basic Accounting System. Retrieved from http://bas.pwv.gov.za/funcArea.aspx **(**Accessed on 05 November 2019).

Department of Transport. *Annual Report. 2017/2018. Vote 35.* Retrieved from https://www.transport.gov.za/publications (Accessed on 18 November 2019).

De Vos, A. S., Strydom, H., Fouchè, C.B. & Delport, C.S.L. 2002. 2nd edition. *Research at Grass Roots. For the social sciences and human services professions*. Pretoria. Van Schaik Publishers.

De Vos, A. S., Strydom, H., Fouchè, C.B. & Delport, C.S.L. 2011. 4th edition. *Research at Grass Roots. For the social sciences and human service professions*. Pretoria. Van Schaik Publishers.

DOJ & CD. Department of Justice and Constitutional Development. Annual Report. 1998/1999. Chapter 1. Preface. Retrieved from https://www.justice.gov.za/reportfiles/report_list.html.

Evert, L. 2011. *Unidentified bodies in Forensic Pathology Practice in South Africa.* Unpublished MSc in Health Sciences Dissertation. University of Pretoria. Pretoria.

Electronic Privacy Information (EPIC). *EPIC Urges FBI to Limit Fingerprint-Based Background Checks: 09 January 2018).* Retrieved from https://www.epic.org/foia/fbi/ngi/ (Accessed on: 18 February 2019).

FBI. 2013. Federal Bureau of *Investigation. Next Generation Identification (NGI). Bigger, Better, Faster. NGI. Overview for Strategic Planning July 2013.* Retrieved from Public Intelligence. http://info.publicintelligence.net. (Accessed on 02 February 2019).

Firearms Control Act 60 of 2000, S*ee* South Africa.

Gibbons, J.H. 1991. *The FBI Fingerprint identification Automation Program: Issues and Options. Background Paper.* Retrieved from: https://books.google.co.za/books?id=OO-67enEAxUC&pg=PA7&dq= fingerprints+to+identify+suspect+in+government+system&hl=en&sa=X&ved= 0ahUKEwiP8d7rivSAhWpJsAKHRa-CBAQ6AEIHzAB#v=onepage&q =fingerprints%20to%20identify%20suspect%20in%20government%20system &f=false. (Accessed on 25 July 2017).

Giordano, A.D. 2011. *Data Integration Blueprint and Modelling. Techniques for a Scalable and Sustainable Architecture.* USA. Pearson.

Government Communications and information System (GCIS). 2016. South Africa Yearbook 2015/2016. Justice and Correctional Services. Available at https://www.gcis.gov.za/content/resourcecentre/sa-info/yearbook2015-16. (Accessed on: 03 November 2017).

Guest, G., MacQueen, K.M. & Namey, E.E. 2012. *Applied Thematic Analysis.* Los Angeles. Sage Publications Inc.

Gygi, C. DeCarlo, N. & Williams, B. 2005. *Six Sigma for Dummies.* Indiana. Wiley Publishing.

Hagan, F.E. 2014. *Research Methods in Criminal Justice and Criminology.* 9th edition. USA. Pearson Education.

Harber, L & Harber, R.N. 2009. *Challenges to fingerprints.* Tucson, Arizona. Lawyers & Judges Inc.

Henry, S. & Lanier, M.M. 2001. What *Is A Crime. Controversies over the Nature of Crime and What to Do about It.* Florida. Rowman & Littlefield Publishers.

Holtzhausen, L. 2012. *Criminal Justice Social Work.* A South African Practice Framework. Cape Town. Juta.

IJS. Integrated Justice System. 2017. Progress Report. Integrated Justice System Programme. Select Committee on Security and Justice. 31 May 2017. Department of Justice and Constitutional Development. Retrieved from pmg-assets.s3-website-eu-west-1.amazonaws.com › 170531IJSReport. (Accessed on 18 November 2019).

IJS. Integrated Justice System. 2020. Integrating the Criminal Justice Information Systems. November 2020. (Accessed on 27 December 2020).

INTERPOL. 2012. Guidelines Concerning fingerprints transmission. INTERPOL OS/FTD/IDFP. Retrieved from https://www.interpol.int/en/How-we-work/Forensics/Fingerprints. (Accessed on 13 November 2019).

INTERPOL. 2018. Interpol Fact Sheet. Fingerprints. Retrieved from https://www.interpol.int/en/How-we-work/Forensics/Fingerprints. (Accessed on 13 November 2019).

James, S. H., Nordby, J. J. & Bell, S. 2014. *Forensic Science*. CRC Press. Florida.

Jali, M. 2015. *The impact of pay on productivity and motivation on general workers in South Africa.* Unpublished Master` s of Business Administration. University of Pretoria.

Komarinski, P. 2005. Automated Fingerprint Identification System (AFIS). Retrieved from https://books.google.co.za/books?id=kSfYd2Pj9V4C&pg=PA13&dq=paperless+fingerprinting. (Accessed on 21 June 2022).

Kriel, L. 2011. Latent Print Overview. Impression Manager. 404-270-8181. Retrieved from https://dofs-gbi.georgia.gov/document/publication/180850381gbi-latentprintspdf/download. (Accessed on 10 July 2017).

Krimsky, S. & Simoncelli, T. 2012. *DNA Data Banks, Criminal Investigations and Civil Liberties. Genetic Justice.* New York. Columbia University Press.

Lapan, S.D., Quartaroli, M.T. & Riemer, F.J. 2012. *Qualitative Research. An Introduction to Methods and Designs.* San Francisco. Josey-Bass.

Leedy, P.D. & Ormrod, J.E. 2015. *Practical Research. Planning and Design*. Global Edition. 11th Edition. USA. Pearson.

Leseba, G. 2015. Integrated Justice System (IJS). Presentation Portfolio Committee on Police. Theme: the deterrence of Crime in South Africa through CJS modernization: 10 June 2015. *Retrieved from* https://pmg.org.za › files › 150610IJS. (Accessed on 18 November 2019).

Linneberg, S. M. & Korsgaard, S. 2019. *Coding qualitative data. A synthesis guiding the novice.* Qualitative Research Journal. Vol. 19 No. 3, pp. 259-270. Retrieved from http://www.researchgate.net/publication/332957319_coding_qualitative_data_a_synthesis_guiding_the_novice. (Accessed on 23 October 2022).

Linthicum, D.S. 2000. *Enterprise Application Integration. Addison Wesley Information Technology Series*. New York. Library or Congress.

Lutz, W. & Knox, S. 2014. *Quantitative and Qualitative Methods in Psychotherapy Research.* New York. Routledge.

Lyle, D.P. 2012. *Forensic Science*. USA. Library of Congress.

Makwethu, K. 2020. Auditor General South Africa. Media Release. Auditor-General says the multi-billion rand Covid-19 relief package landed in an environment with many control weaknesses. Retrieved from https://www.agsa.co.za. (Accessed on 20 October 2020).

Mamoojee, I. A. 2001. Department of National Treasury. Office of the Accountant General Practice Notice 12 of 2001. Implementation of Basic Accounting System. Retrieved from www.treasury.gov.za › legislation › pfma › oag. **(**Accessed on 05 November 2019).

Mele, C. Pels, J. & Polese, F. 2010. A Brief Review of Systems Theories and Their Managerial Applications. Service Science 2(1/2), pp. 126 – 135. Retrieved from https://pubsonline.informs.org/doi/pdf/10.1287/serv.2.1_2.126. (Accessed on 10 October 2022).

Melville, S. & Goddard, W. 2007. *Research Methodology. An introduction.* 2nd Edition. Lansdowne. Juta & Company Limited.

Minister of Home Affairs Malusi Gigaba. Statement by Home Affairs Minister Malusi Gigaba *on the meeting with representatives of the Banking and Insurance Industries, SABRIC and Astute, 19 January 2016, Pretoria.* Retrieved from http://www.home-affairs.gov.za/index.php/statements-speeches/732-statement-by-home-affairs-minister-malusi-gigaba-on-the-meeting-with-representatives-of-the-banking-and-insurance-industries-sabric-and-astute-19-january-2016-pretoria. (Accessed on: 17 July 2017).

Minister of Home Affairs Malusi Gigaba. Statement by Home Affairs Minister Malusi Gigaba at *the Media Launch of the Automated Biometric Identification System (ABIS) Project, Taj Hotel, Cape Town: 16 May 2018.* Retrieved from http://www.dha.gov.za/index.php/statements-speeches/1123-opening-speech-by-home-affairs-director-general-mkuseli-apleni-at-the-media-launch-of-the-automated-biometric-identification-system-abis-project-taj-hotel-cape-town-16-may-2018 (Accessed on: 15 July 2020).

Mngcungusa, N. 2005. *Biometrics deployed in prisons.* Retrieved from https://www.itweb.co.za/content/dgp45vaY8DjvX9l8. (Accessed on 12 February 2020).

Mofokeng, J.T. & De Vries, I. D. 2012. Marriage Convenience (expert perspectives on General Detective-Public Prosecutor Relations in South Africa). *OIDA International Journal Sustainable Development Journal.* 4(4): 27-34.

Mokwele, M.E. 2015. *The Value of the Automated Fingerprint Identification System as a Technique in the Identification of Suspects.* (Dissertation Magister Technologiae in Forensic Investigation. Unpublished Dissertation. University of South Africa.

Muvoni Technology Group. 2013. *Fingerprint clearances no longer a headache for professional drivers.* Retrieved from: https://www.itweb.co.za/content/JKjlyrvw6kEqk6am. (Accessed on 21 June 2022).

Nath, S. 2010. *Fingerprint Identification.* New Delhi. Shiv Shakti Book Traders.

Newburn, T. Williamson, T. & Wright, A. 2007. *Handbook of Criminal Investigation.* New York. Willian Publishing.

Newburn, T. Williamson, T. & Wright, A. 2011. *Handbook of Criminal Investigation.* New York. Willian Publishing.

News24 Archives. 2010. Police get access to fingerprint. 2 June 2010. Retrieved from http://www.news24.com/SouthAfrica/Politics/Police-get-access-to-fingerprints-20100602 (Accessed on: 25 October 2017).

News24. 2022. Credit bureau TransUnion hacked for ransom - hundreds of companies under threat. 18 March 2022. Retrieved from https://www.news24.com/fin24/companies/credit-bureau-transunion-hacked-for-ransom-hundreds-of-companies-under-threat-20220318. (Accessed on 10 May 2021).

Office of the Premier. 2017. Province of KwaZulu Natal. Persal Introduction Manual, December 2017. KwaZulu Natal. Government printers.

Ogle, R.R. & Plotkin, S. 2018. *Crime Scene Investigation & Reconstruction.* 4th edition. Hoboken. Pearson.

Olckers. C. 2007. *An examination of the impact of residential security measures on the incidence of residential burglary in two selected northern suburbs of Johannesburg.* Unpublished Magister Technologiae. University of South Africa. Pretoria.

Orthmann, C.H. & Hess, K.M. 2013. *Criminal Investigation.* 10th edition. Boston. Cengage.

Phahlane. P.J. 2017. Acting National Commissioner. South African Police Service. *Opening of 4th Forensic Services Conference*. Retrieved from www.saps.gov.za. (Accessed on 07 November 2017).

PMG. Parliamentary Monitoring Group. 2001. *The Portfolio Committee on Correctional Services on Rehabilitation and the Automated Finger Printing System.* Cape Town, 25 October 2001. Retrieved from https://pmg.org.za/committee-meeting/962/. (Accessed on: 02 November 2017).

PMG. Parliamentary Monitoring Group. 2008. *Electronic Monitoring and Inmate Tracking Systems: DCS briefing. Department of Correctional Services, 03 March 2008.* Retrieved from https://pmg.org.za/committee-meeting/8872/. (Accessed on 03 March 2020).

Porte, G.K. 2010. *Appraising Research in Second Language Learning. A Practical approach to critical analysis of quantitative research.* 2nd edition. Amsterdam. John Benjamins Publishing Company.

Protection of Information Act. *See* South Africa

Protection of Personal Information Act. 2013. *See* South Africa

Saferstein, R. 2011. *Forensic Science. An Introduction. 2nd edition.* New Jersey. Pearson.

Shaler, R.C. 2012. *Crime Scene Forensics. A Scientific Method Approach.* Florida. CRC Press Taylor & Francis Group.

Shu Chang, Y. D. 2022. *Multiparty Computations, Co-operations, and Communications for Privacy and Network Security*. *Application of Face Recognition in E-commerce Security Authentication in the Era of Big Data.* Volume 2022. Article ID 4246750. Retrieved from https://www.hindawi.com/journals/scn/2022/4246750/. (Accessed on 23 May 2023).

Siegel, J.A., Knupfer, G.C. & Saukko, P.J. 2000. *Encyclopedia of Forensic Sciences*. New York. Academy.

Smit, J., Minaar, A. & Schnetler, J. 2004. *Smart Policing for Law Enforcement Officials.* Claremont. New Africa Education.

South Africa. 1977. *Criminal Procedure Act. Act 51 of 1977.* Pretoria. Government Printers.

South Africa. 1996. *Constitution of South Africa No. 108 of 1996.* Pretoria. Government Printers.

South Africa. 2010. *Criminal Law (Forensic Procedures) Amendment Act No 6 of 2010*. Pretoria. Government Printers.

South Africa. 2013. *Criminal Law (Forensic Procedures) Amendment Act No 37 of 2010.* Pretoria. Government Printers.

South Africa. 2000. *Firearms Control Act. Act 60 of 2000.* Pretoria. Government Printers.

South Africa. 1982. *Protection of Information Act. Act 84 of 1982.* Pretoria. Government Printers.

South Africa. 2013. *Protection of Personal Information Act 4 of 2013.* Cape Town. Government Printers.

South Africa. 2014. *Department of Correctional Services. March 2014*. The use of Integrated Systems. White Paper on Remand Detention Management in South Africa. Pretoria. Government Printers.

South African Police Service (SAPS). 2012. *National Instruction/Standing Order 325. Closing of Case Dockets. Division: Detective Services. V0.02.* Issued by Consolidation Notice 2012.

South African Police Service. 2016. *Annual Report. 2015/2016. Vote 23. Retrieved from* https://www.saps.gov.za/about/.../annual_ report/.../saps_annual_report_2015_2016.pd. (Accessed on 23 June 2017).

South African Police Service. 2021. *Annual Report. 2020/2021. Vote 28.* Retrieved from https://www.gov.za/sites/default/files/gcis_document/202201/saps-annual-report-202021.pdf. (Accessed on 22 February 2022).

South African Police Service. 2022. *Annual Report. 2021/2022. Vote 28.* Retrieved from https://www.gov.za/sites/default/files/gcis_document/202211/saps-2021-22.pdf. (Accessed on 10 February 2023).

South African Police Service. 2010. *Strategic Management. Strategic Plan 2010 to 2014.* Obtained from http://www.saps.gov.za/about/stratframework/strategic_plan.php. (Accessed on 12 September 2016). Pretoria. SAPS *Strategic Management.*

South African Police Service. 2019. *SAPS Crime Situation in Republic of South Africa Twelve (12) Months (April 2018 to March 2019.* Retrieved from https://www.saps.gov.za/services/april_to_march2018_19_presentation.pdf. (Accessed on 29 May 2020).

South African Police Service. 2022. *SAPS Crime Situation in Republic of South Africa Twelve (12) Months (April 2021 to March 2022.* Retrieved from https://www.saps.gov.za/services/downloads/Annual-Crime-2021_2022-web.pdf. (Accessed on 06 February 2023).

South African Police Service Criminal Record Centre Training Committee. 1999. Grounds for the 7-point Criterium for the Individualizing of Fingerprints. *Training on 2011 Intake*. Pretoria. Government Printers.

South African Government. 2020. *Health. 2020 State of the Nation Address President Cyril Ramaphosa.* Retrieved from https://www.gov.za/issues/health. (Accessed on 21 June 2022).

Stuart, H.J., Nordby, J.J. & Suzanne, B. 2014. *Forensic Science. An Introduction to Scientific and Investigative Techniques.* 4th edition. Florida. CRC Press.

S v Mbatha (170/2018) [2018] ZAGPJHC 502 (13 August 2018). Republic Of South Africa. In The High Court of South Africa. Gauteng Local Division, Johannesburg. Retrieved from http://www.saflii.org/za/cases/ZAGPJHC/2018/502 (Accessed on 26 October 2022).

Terre Blanche, M.J., Durreihm, K. & Painter, D. 2011. *Research in Practice. Applied methods for the Social sciences*. Cape Town. University of Cape Town Press.

Timeslive. 2023. Department of Justice breaches Popi Act and Compromises security files. 11 May 2023. Retrieved from https://www.timeslive.co.za/news/south-africa/2023-05-11-department-of-justice-breaches-popi-act-and-compromises-security-files/. (Accessed on 11 May 2023).

Thomas, S. 2009. Department of Justice and Constitutional Development. Integrated Justice System. Criminal Law Forensic Procedure Amendment Bill. Retrieved from pmg-assets.s3-website-eu-west-1.amazonaws.com › docs. (Accessed on 13 November 2019).

UNISA. 2016. *UNISA Policy on Research Ethics.* University of South Africa. Pretoria.

Van Rooyen, H.J.N., 2008. *The Practitioner`s Guide to Forensic Investigation South Africa.* Pretoria. Henmar Publications.

Van Rooyen, H.J.N. 2013. *Investigate Corruption.* Pretoria. HJN Training. Henmar Publications.

Van Rooyen, J.H. 2016. *Pre-Employment Vetting. Director Execu Enterprises Ltd t/a ExecuConsult & Director at Cornerstone Mineral Corporation Ltd.* Retrieved from https://www.Linkedin.com. (Accessed on 27 March 2022).

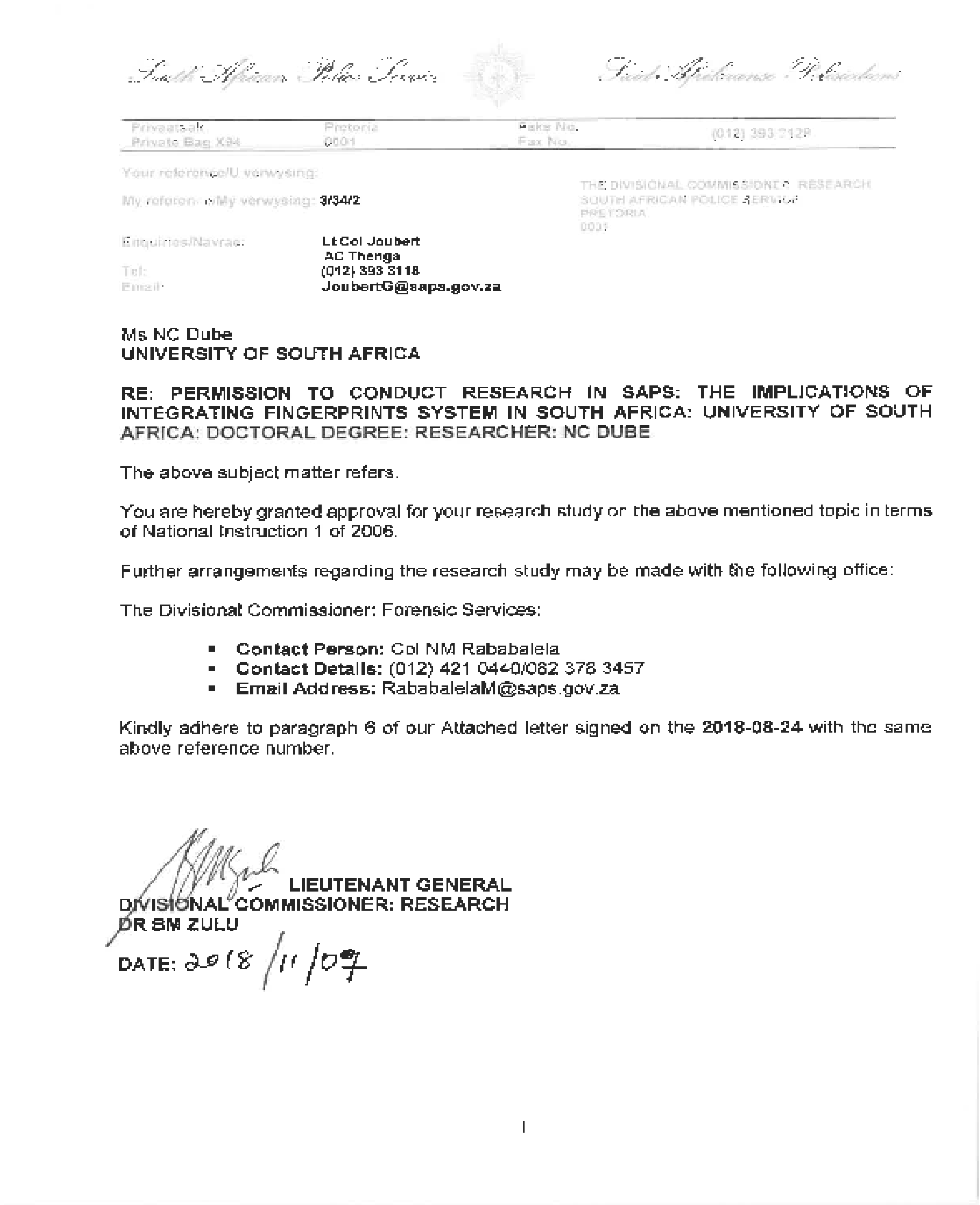
Wells, J.T., Bradford, N.S., Gilbert, G., John, D., Kramer, W.M., Ratley, J.D. & Robertson, J. 2012. *Fraud Examiners Manual. 2012 International Edition.* Texas. ACFE.

Welman, C., Kruger, F. & Mitchell, B. 2012. *Research Methodology.* 3rd edition. Cape Town. Oxford University press.

White Paper on Remand Detention Management in South Africa. *See* South Africa. 2014.

Wyllie, D. 2017. *How biometric technologies will help correctional facilities, May 16, 2017.* Retrieved from https://www.correctionsone.com/products/police-technology/investigation/biometrics-identification/articles/how-biometric-technologies-will-help-correctional-facilities-HAjTzVlupizKxEVV/. (Accessed on 12 February 2020).

Appendix 1: South African Police Service Consent Letter



South African Police Service   Suid-Afrikaanse Polisiediens

Privaatsak
Private Bag X94   Pretoria
0001   Faks No.
Fax No.   (012) 393 2128

Your reference/U verwysing:

My reference/My verwysing: 3/34/2

THE DIVISIONAL COMMISSIONER: RESEARCH
SOUTH AFRICAN POLICE SERVICE
PRETORIA
0001

Enquiries/Navrae: Lt Col Joubert
AC Thenga
Tel: (012) 393 3118
Email: JoubertG@saps.gov.za

Ms NC Dube
UNIVERSITY OF SOUTH AFRICA

RE: PERMISSION TO CONDUCT RESEARCH IN SAPS: THE IMPLICATIONS OF INTEGRATING FINGERPRINTS SYSTEM IN SOUTH AFRICA: UNIVERSITY OF SOUTH AFRICA: DOCTORAL DEGREE: RESEARCHER: NC DUBE

The above subject matter refers.

You are hereby granted approval for your research study or the above mentioned topic in terms of National Instruction 1 of 2006.

Further arrangements regarding the research study may be made with the following office:

The Divisional Commissioner: Forensic Services:

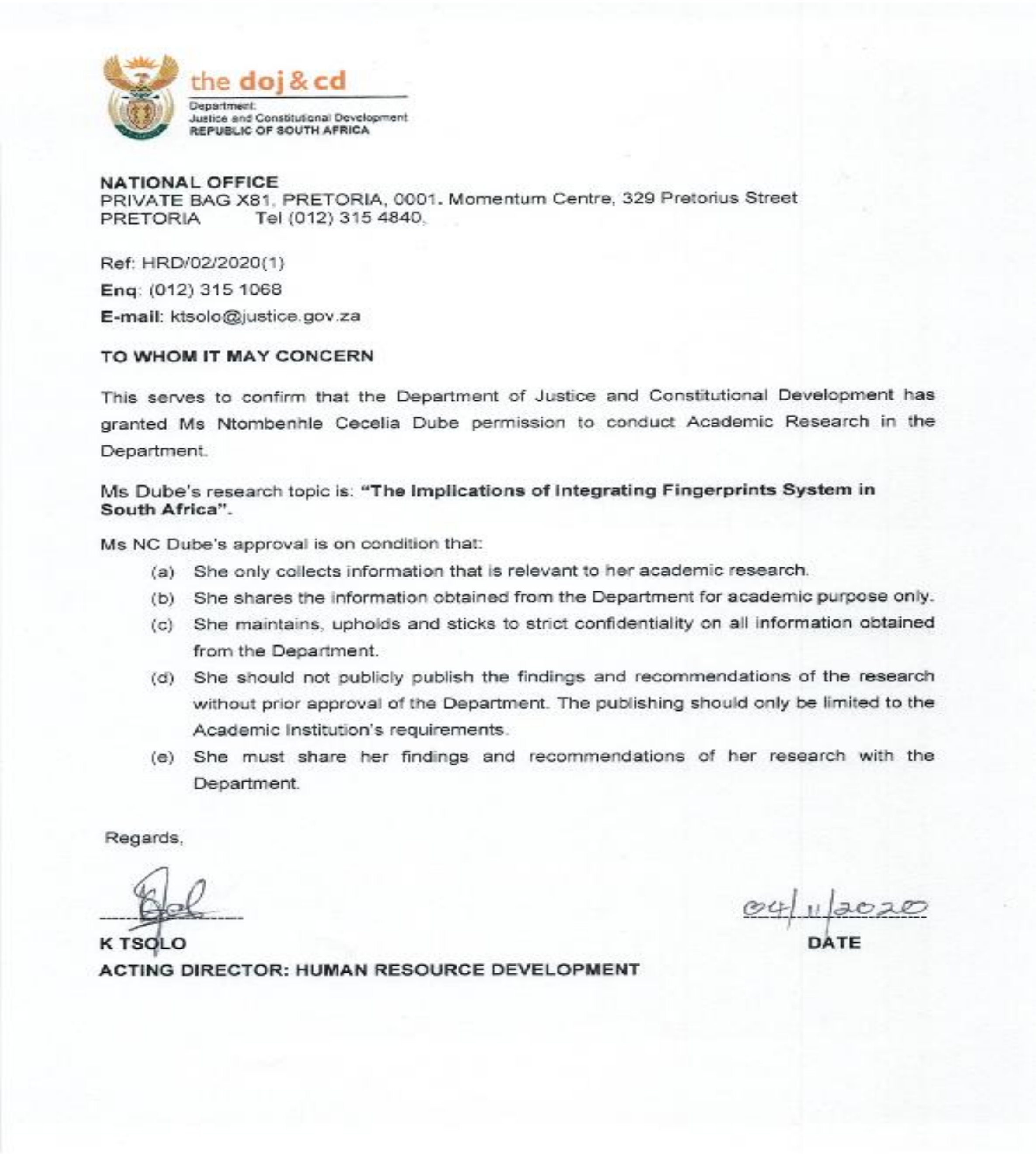
- **Contact Person:** Col NM Rababalela
- **Contact Details:** (012) 421 0440/082 378 3457
- **Email Address:** RababalelaM@saps.gov.za

Kindly adhere to paragraph 6 of our Attached letter signed on the **2018-08-24** with the same above reference number.

LIEUTENANT GENERAL
DIVISIONAL COMMISSIONER: RESEARCH
DR SM ZULU

DATE: 2018/11/07

Appendix 2: Department of Justice and Constitutional Development Consent Letter



the doj & cd
Department:
Justice and Constitutional Development
REPUBLIC OF SOUTH AFRICA

NATIONAL OFFICE
PRIVATE BAG X81, PRETORIA, 0001. Momentum Centre, 329 Pretorius Street
PRETORIA Tel (012) 315 4840,

Ref: HRD/02/2020(1)
Enq: (012) 315 1068
E-mail: ktsolo@justice.gov.za

TO WHOM IT MAY CONCERN

This serves to confirm that the Department of Justice and Constitutional Development has granted Ms Ntombenhle Cecelia Dube permission to conduct Academic Research in the Department.

Ms Dube's research topic is: **"The Implications of Integrating Fingerprints System in South Africa".**

Ms NC Dube's approval is on condition that:

(a) She only collects information that is relevant to her academic research.

(b) She shares the information obtained from the Department for academic purpose only.

(c) She maintains, upholds and sticks to strict confidentiality on all information obtained from the Department.

(d) She should not publicly publish the findings and recommendations of the research without prior approval of the Department. The publishing should only be limited to the Academic Institution's requirements.

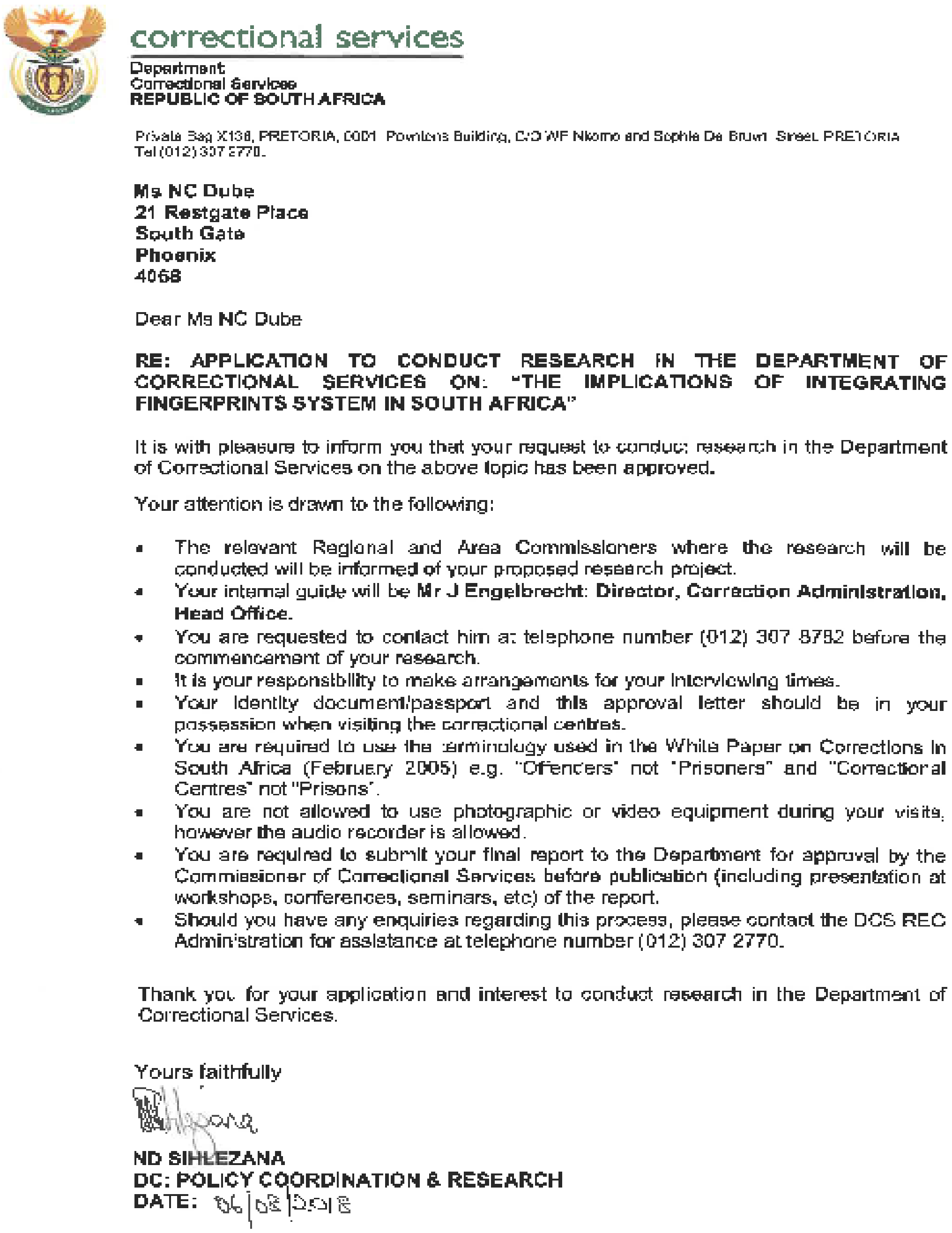
(e) She must share her findings and recommendations of her research with the Department.

Regards,

K TSOLO
ACTING DIRECTOR: HUMAN RESOURCE DEVELOPMENT

04/11/2020
DATE

Appendix 3: Department of Correctional Services Consent Letter for KZN



correctional services

Department:
Correctional Services
REPUBLIC OF SOUTH AFRICA

Private Bag X136, PRETORIA, 0001 Poyntons Building, C/O WF Nkomo and Sophie De Bruyn Street, PRETORIA
Tel (012) 307 2770.

Ms NC Dube
21 Restgate Place
South Gate
Phoenix
4068

Dear Ms NC Dube

RE: APPLICATION TO CONDUCT RESEARCH IN THE DEPARTMENT OF CORRECTIONAL SERVICES ON: "THE IMPLICATIONS OF INTEGRATING FINGERPRINTS SYSTEM IN SOUTH AFRICA"

It is with pleasure to inform you that your request to conduct research in the Department of Correctional Services on the above topic has been approved.

Your attention is drawn to the following:

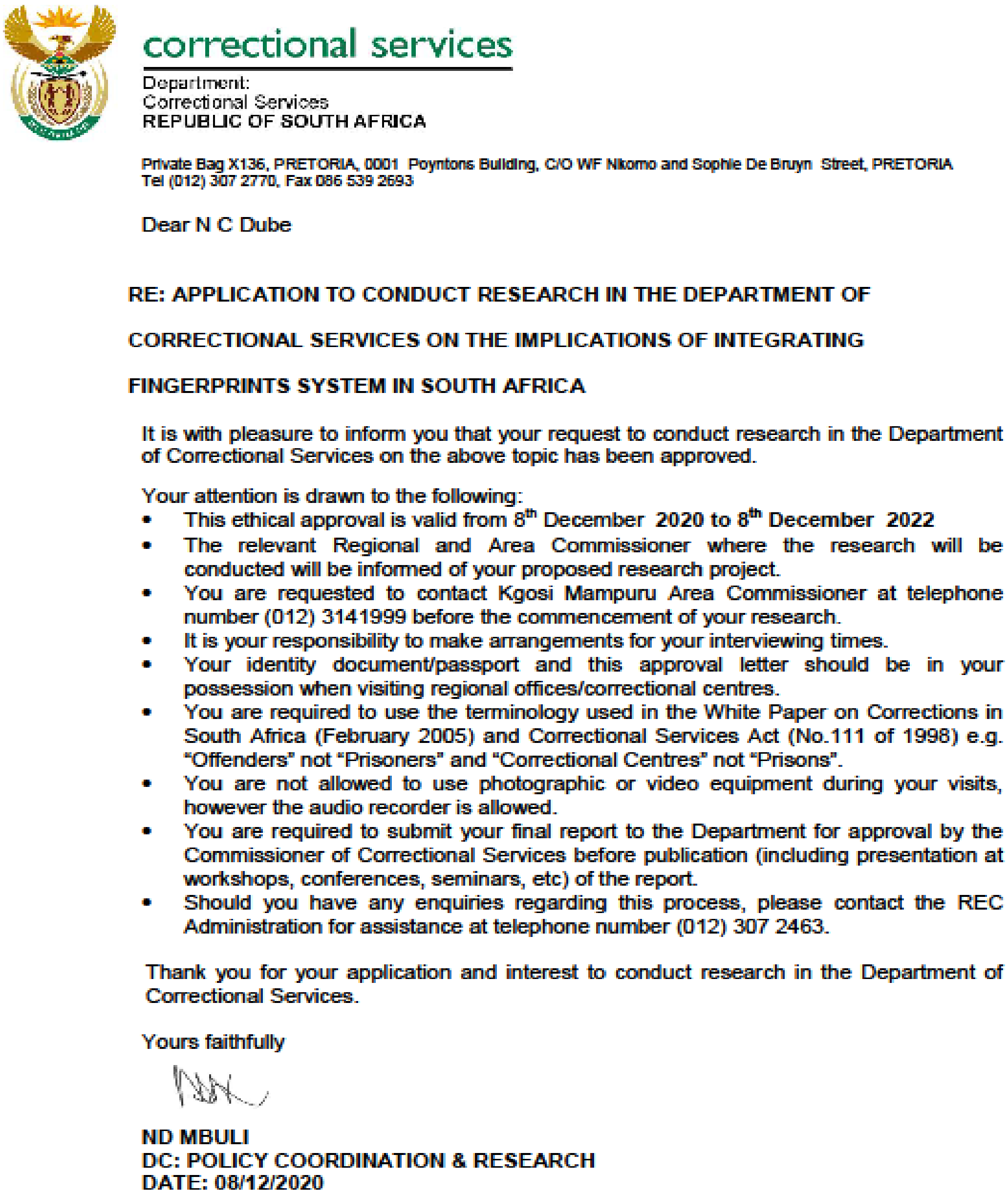
- The relevant Regional and Area Commissioners where the research will be conducted will be informed of your proposed research project.
- Your internal guide will be **Mr J Engelbrecht: Director, Correction Administration, Head Office.**
- You are requested to contact him at telephone number (012) 307 8782 before the commencement of your research.
- It is your responsibility to make arrangements for your interviewing times.
- Your identity document/passport and this approval letter should be in your possession when visiting the correctional centres.
- You are required to use the terminology used in the White Paper on Corrections in South Africa (February 2005) e.g. "Offenders" not "Prisoners" and "Correctional Centres" not "Prisons".
- You are not allowed to use photographic or video equipment during your visits, however the audio recorder is allowed.
- You are required to submit your final report to the Department for approval by the Commissioner of Correctional Services before publication (including presentation at workshops, conferences, seminars, etc) of the report.
- Should you have any enquiries regarding this process, please contact the DCS REC Administration for assistance at telephone number (012) 307 2770.

Thank you for your application and interest to conduct research in the Department of Correctional Services.

Yours faithfully

ND SIHLEZANA
DC: POLICY COORDINATION & RESEARCH
DATE: 06|08|2018

Appendix 4: Department of Correctional Services Consent Letter for Pretoria



correctional services

Department:
Correctional Services
REPUBLIC OF SOUTH AFRICA

Private Bag X136, PRETORIA, 0001 Poyntons Building, C/O WF Nkomo and Sophie De Bruyn Street, PRETORIA
Tel (012) 307 2770, Fax 086 539 2693

Dear N C Dube

RE: APPLICATION TO CONDUCT RESEARCH IN THE DEPARTMENT OF

CORRECTIONAL SERVICES ON THE IMPLICATIONS OF INTEGRATING

FINGERPRINTS SYSTEM IN SOUTH AFRICA

It is with pleasure to inform you that your request to conduct research in the Department of Correctional Services on the above topic has been approved.

Your attention is drawn to the following:

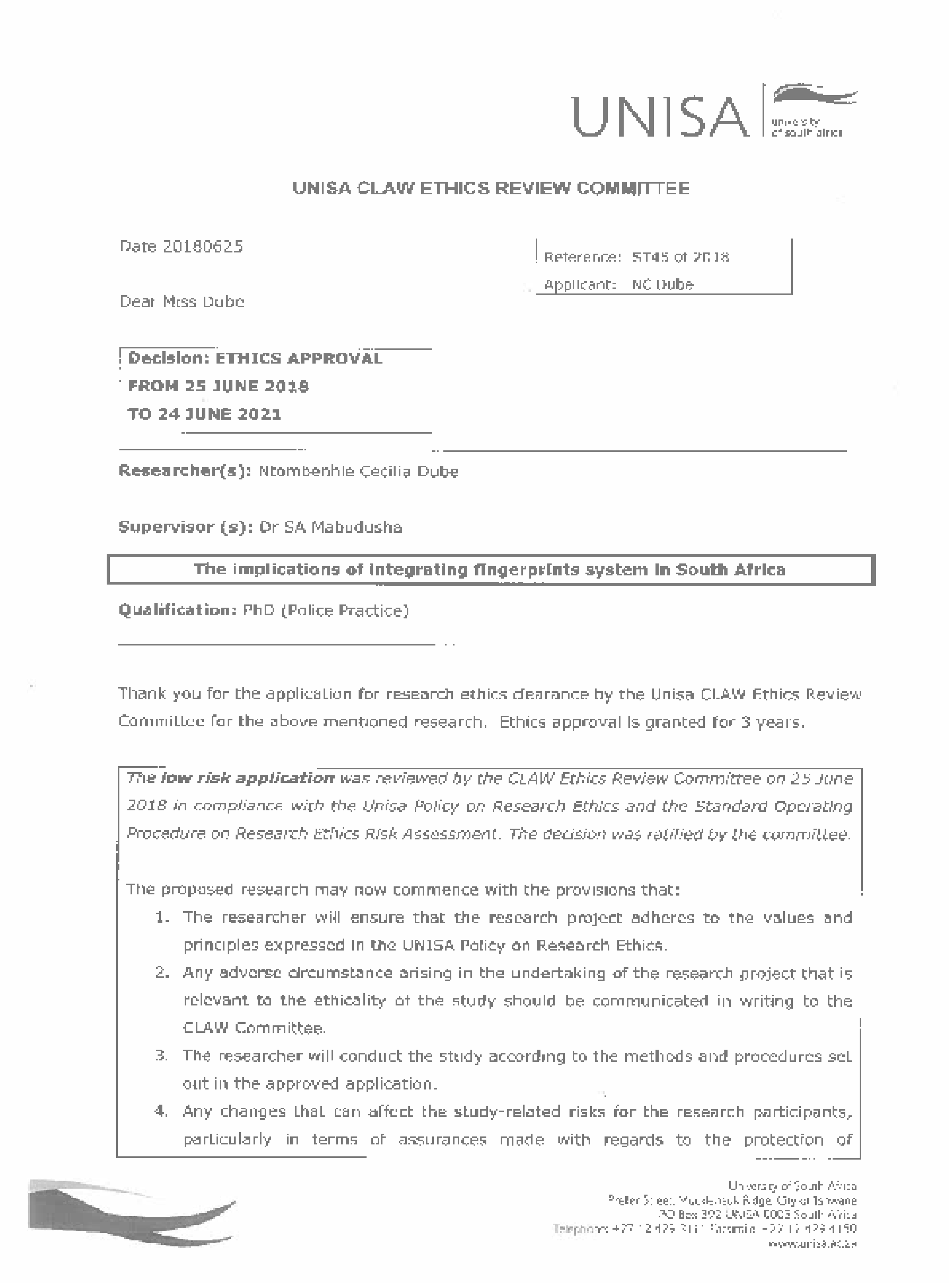
- This ethical approval is valid from 8th December **2020 to 8th December 2022**
- The relevant Regional and Area Commissioner where the research will be conducted will be informed of your proposed research project.
- You are requested to contact Kgosi Mampuru Area Commissioner at telephone number (012) 3141999 before the commencement of your research.
- It is your responsibility to make arrangements for your interviewing times.
- Your identity document/passport and this approval letter should be in your possession when visiting regional offices/correctional centres.
- You are required to use the terminology used in the White Paper on Corrections in South Africa (February 2005) and Correctional Services Act (No.111 of 1998) e.g. "Offenders" not "Prisoners" and "Correctional Centres" not "Prisons".
- You are not allowed to use photographic or video equipment during your visits, however the audio recorder is allowed.
- You are required to submit your final report to the Department for approval by the Commissioner of Correctional Services before publication (including presentation at workshops, conferences, seminars, etc) of the report.
- Should you have any enquiries regarding this process, please contact the REC Administration for assistance at telephone number (012) 307 2463.

Thank you for your application and interest to conduct research in the Department of Correctional Services.

Yours faithfully

ND MBULI
DC: POLICY COORDINATION & RESEARCH
DATE: 08/12/2020

Appendix 5: Unisa Clearance Certificate 2018



UNISA university of south africa

UNISA CLAW ETHICS REVIEW COMMITTEE

Date 20180625

Reference: ST45 of 2018
Applicant: NC Dube

Dear Miss Dube

Decision: ETHICS APPROVAL
FROM 25 JUNE 2018
TO 24 JUNE 2021

Researcher(s): Ntombenhle Cecilia Dube

Supervisor (s): Dr SA Mabudusha

The implications of integrating fingerprints system in South Africa

Qualification: PhD (Police Practice)

Thank you for the application for research ethics clearance by the Unisa CLAW Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years.

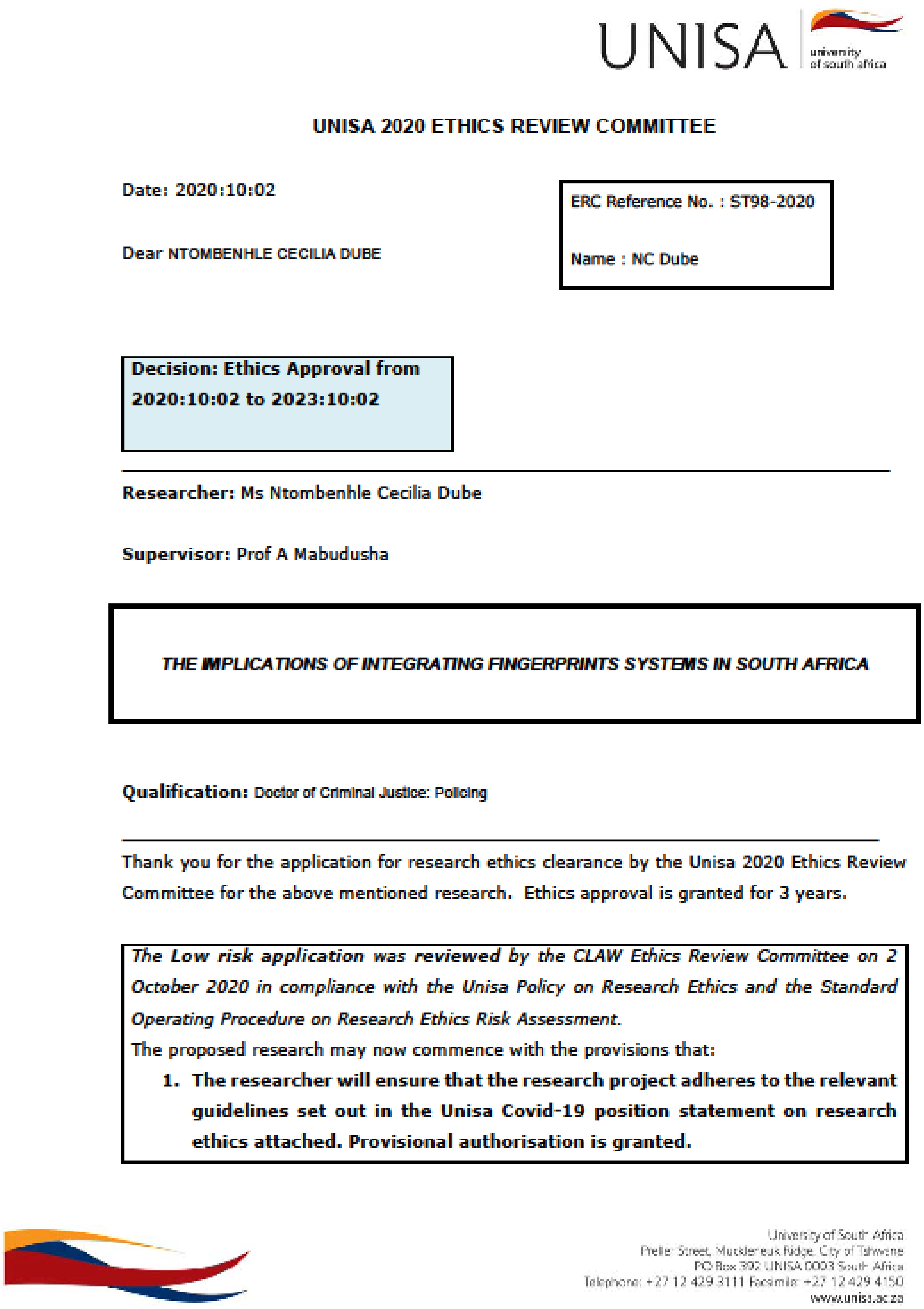
*The **low risk application** was reviewed by the CLAW Ethics Review Committee on 25 June 2018 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment. The decision was ratified by the committee.*

The proposed research may now commence with the provisions that:

1. The researcher will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
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 CLAW Committee.
3. The researcher will conduct the study according to the methods and procedures set out in the approved application.
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

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix 6: Unisa Clearance Certificate 2020



UNISA university of south africa

UNISA 2020 ETHICS REVIEW COMMITTEE

Date: 2020:10:02

Dear NTOMBENHLE CECILIA DUBE

ERC Reference No. : ST98-2020

Name : NC Dube

Decision: Ethics Approval from 2020:10:02 to 2023:10:02

Researcher: Ms Ntombenhle Cecilia Dube

Supervisor: Prof A Mabudusha

THE IMPLICATIONS OF INTEGRATING FINGERPRINTS SYSTEMS IN SOUTH AFRICA

Qualification: Doctor of Criminal Justice: Policing

Thank you for the application for research ethics clearance by the Unisa 2020 Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years.

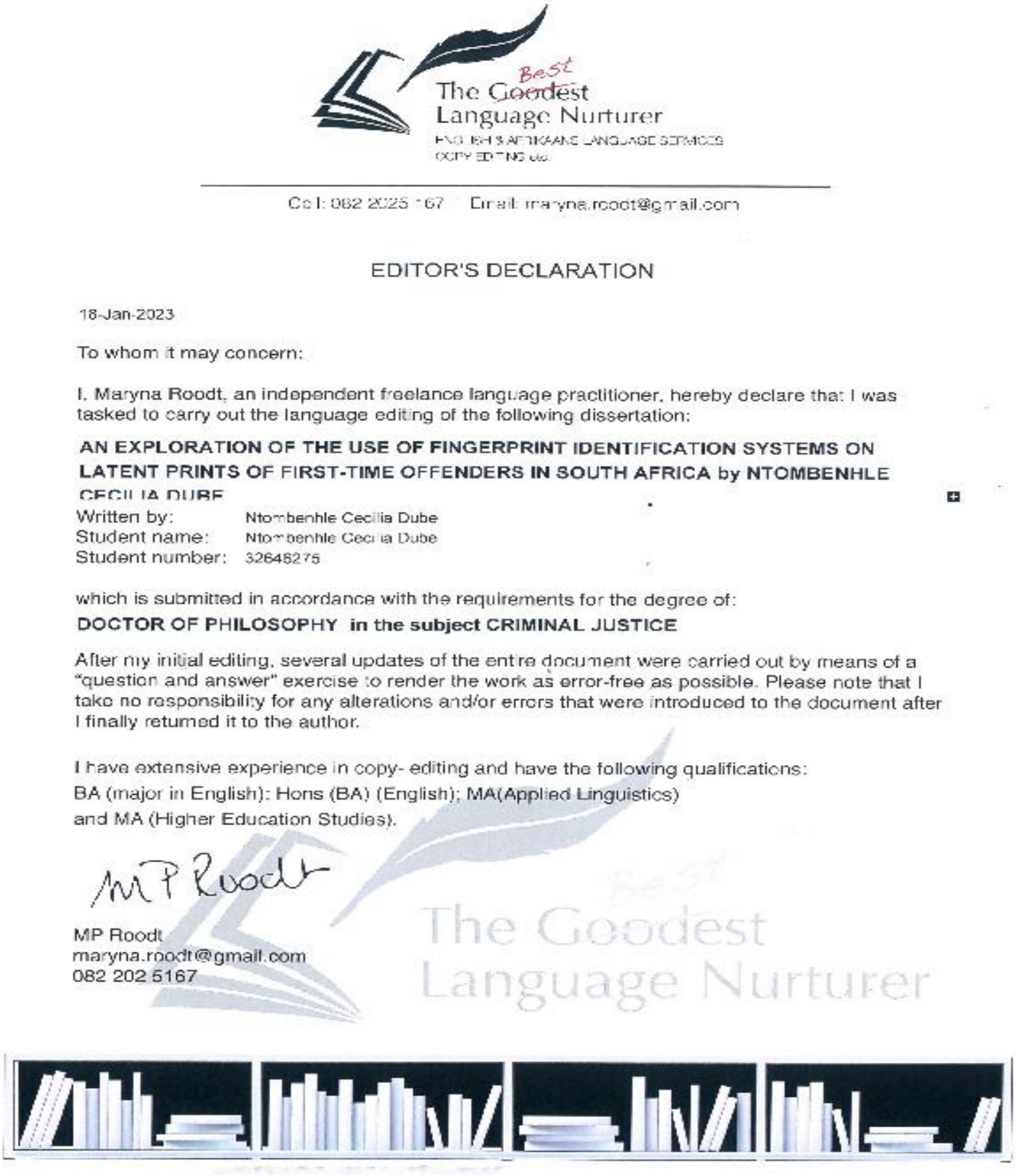
*The **Low risk application was reviewed** by the CLAW Ethics Review Committee on 2 October 2020 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.*

The proposed research may now commence with the provisions that:

1. **The researcher will ensure that the research project adheres to the relevant guidelines set out in the Unisa Covid-19 position statement on research ethics attached. Provisional authorisation is granted.**

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix 7: Editing Certificate



Best
The ~~Good~~est
Language Nurturer
ENGLISH & AFRIKAANS LANGUAGE SERVICES
COPY EDITING etc.

Cell: 082 2025 167 Email: maryna.roodt@gmail.com

EDITOR'S DECLARATION

18-Jan-2023

To whom it may concern:

I, Maryna Roodt, an independent freelance language practitioner, hereby declare that I was tasked to carry out the language editing of the following dissertation:

AN EXPLORATION OF THE USE OF FINGERPRINT IDENTIFICATION SYSTEMS ON LATENT PRINTS OF FIRST-TIME OFFENDERS IN SOUTH AFRICA by NTOMBENHLE CECILIA DUBE

Written by:	Ntombenhle Cecilia Dube
Student name:	Ntombenhle Cecilia Dube
Student number:	32645275

which is submitted in accordance with the requirements for the degree of:

DOCTOR OF PHILOSOPHY in the subject CRIMINAL JUSTICE

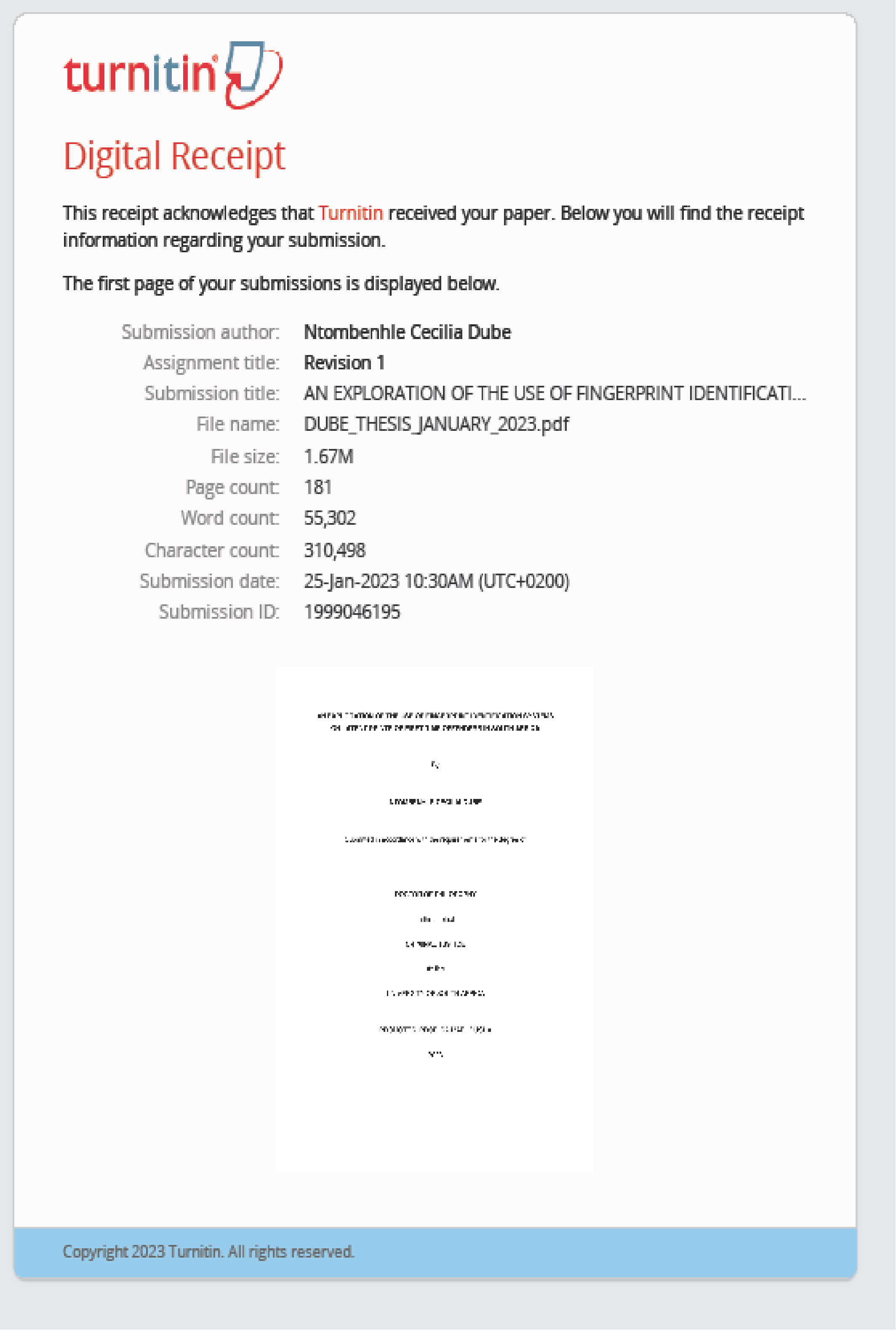
After my initial editing, several updates of the entire document were carried out by means of a "question and answer" exercise to render the work as error-free as possible. Please note that I take no responsibility for any alterations and/or errors that were introduced to the document after I finally returned it to the author.

I have extensive experience in copy- editing and have the following qualifications:
BA (major in English): Hons (BA) (English); MA(Applied Linguistics)
and MA (Higher Education Studies).

MP Roodt

MP Roodt
maryna.roodt@gmail.com
082 202 5167

Appendix 8: Turnitin Receipt



turnitin

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:	Ntombenhle Cecilia Dube
Assignment title:	Revision 1
Submission title:	AN EXPLORATION OF THE USE OF FINGERPRINT IDENTIFICATI...
File name:	DUBE_THESIS_JANUARY_2023.pdf
File size:	1.67M
Page count:	181
Word count:	55,302
Character count:	310,498
Submission date:	25-Jan-2023 10:30AM (UTC+0200)
Submission ID:	1999046195