International Journal of Social Science Research and Review

http://ijssrr.com
editor@ijssrr.com
Volume 7, Issue 1
January, 2024
Pages: 518-529

An Analysis of SAPS Partnership with Other Government Departments in Identifying First-Time Offenders Through Fingerprints

Ntombenhle Cecilia Dube; Angel Mabudusha

University of South Africa, South Africa

E-mail: 32646275@mylife.unisa.ac.za

http://dx.doi.org/10.47814/ijssrr.v7i1.1977

Abstract

The South African Police Service`s (SAPS) fingerprints system can only identify persons who had previously been charged of an offence, meaning it cannot identify latent prints of innocent people or first-time offender with no prior criminal charges. As a result, over 100 000 first-time offenders were unidentified even though there were positive latent prints collected from the crime scene. This is because the South African Police data capturing system does not have information of first-time offenders while other departments such as Home Affairs and Transport including Traffic department is in possession of such fingerprints. The only challenge is to access that particular information lawfully. Therefore, the purpose of this article is to explore the use of fingerprint systems to identify latent-prints of first-time offenders. This is to ensure that other government departments which collect fingerprints from their clients, are partnering with the South African Police Service in an effort to identify first-time offenders. The research approach used in this article is a qualitative approach with a purposive sampling of extracting rich data from identified experts who are working with the fingerprint system. The researchers interviewed 19 participants in this article due to the capacity of fingerprint experts. The findings of this article confirms that the SAPS 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 Identification Verification Application (PIVA) system which integrates the fingerprint systems from a few government departments cannot identify latent prints. The article recommended the implementation of a system that will allow LCRC to identify first-time offenders who are not on the Automated Fingerprint Investigation System (AFIS). It also recommended that the SAPS should have a database of fingerprint information from the citizens who are applying for security checks. This database can store information separately from that of the criminal records. To avoid poorly obtained fingerprints as it has been a concern of all participants, police stations should be issued with digital fingerprints scanners.

Keywords: *Fingerprints; Latent Prints; Undetected Case; First-Time Offender*

1. Introduction

The Locard' principle asserts that, every time a person makes physical contact with anything it results in an exchange of physical materials such as fingerprints (Newburn, Williamson and Wright, 2007: 320). It is therefore obvious that the access to and use of effective and efficient fingerprint identification systems by the police service is of significance. The case dockets with latent prints of first-time offenders are closed as undetected due to unavailability of information in the Local Criminal Record Centre (LCRC) database known as the Automated Fingerprints Identification System (AFIS). This database only keeps information of people who were criminally arrested, charged and convicted. It is for this reason that Criminal Law (Forensic Procedure) Act No. 6 of 2010 was enacted. Section 15D (4) (b) of Criminal Law (Forensic Procedure) Act No. 6 of 2010 provides 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 required databases and implement safety measures to protect the people' personal information. This partnership will enhance the investigation of crime by assisting the police to identify first-time offenders using latent prints found in crime scenes.

Therefore, it is the intention of this article to explore how the current fingerprints system can be used to enhance the investigation of latent prints found in crimes scene.

2. Problem Statement

The SAPS LCRC does not have access to other government departments` fingerprint systems where information of all South African citizens can be found. This is a problem because some cases where latent-prints of first-time offenders are involved remain undetected and unresolved because suspects are not recorded on the LCRC database. These include latent prints found at residential and business places during burglaries as well as on stolen and recovered cars.

The Criminal Law (Forensic Procedure) Act No. 6 of 2010 promotes the sharing of fingerprints information between government departments and it gives directives for such departments to develop a standard operating procedure that will assist the police in identifying latent prints of first-time offenders, which in turn will also assist other departments in resolving their problems where sharing of fingerprints information is concerned. Subsequent to this Act, the Integrated Justice System (IJS) under the Department of Justice and Correctional Development, implemented the Person Identification Verification Application (PIVA) which integrates information from different government departments. The Chairperson of IJSB explained to the police committee that PIVA solution entails instant verification of South African identities via the DHA HANIS/ABIS system using biometric devices (Lesiba, 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 undetected because there are no leads to suspects.

The White Paper on Remand Detention Management in South Africa (2014: 14) also pointed out the challenges which are faced by the DCS whereby if information of first-time offenders were accessible to them they would relieve them of these challenges. These include: the use of multiple identities by remand detainees; redundant information; the slow process of verification of identifications within 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 article intended to explore the use of fingerprints systems of latent prints for first time offenders.

Of concern, is that during 2020/2021 period several cases where suspect identification required fingerprint information were not taken to court because, only a few of the reported cases could be detected and taken to court (SAPS Annual Report, 2021: 201). 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.

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

The above table shows that out of 343 840 reported cases only 70 067 suspects were detected during 2020/2021 leaving 273 773 undetected. As a result, the opportunity of police having access to the fingerprint information of first-time offenders will enhance the quality of the investigation process, thus restoring the trust in the community as the number of undetected cases will be reduced.

3. Research Methodology

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, Strydom, Fouchè, and Delport, (2011: 91) explicated that the qualitative researcher is concerned with understanding through naturalisation observation rather than controlled measurement. De Vos *et al.* (2011: 320) explained that since qualitative researchers are primarily interested in the meaning which the subject gives 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.

The study followed a qualitative research approach with the intention to understand the topic under investigation through the experiences of officials working with the fingerprint system. Then through purposive sampling, the researchers purposefully selected participants who were directly involved in the identification, verification and comparison of fingerprints to get credible and accurate information. The researchers analysed data by means of thematic analysis where data codes were developed to represent identified themes which were linked to the research questions. Interviews were conducted with the following participants:

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

4. Closing of Case Dockets as Undetected

The National Instruction 325 as cited in the Consolidation Notice (2012), lists a number of reasons for closing case dockets, namely: no leads, when there were identifiable fingerprints but with no name or address that can guide the investigator to trace the suspect. This means that without sufficient evidence to prosecute offenders, a number of cases are closed as undetected leaving the investigating officer disappointment and helpless. As mentioned earlier, the reason for closing dockets undetected may be that latent-prints uplifted from the crime scene are not identifiable by the LCRC because the person who left the fingerprints at the crime scene has never been charged. Such fingerprints are not destroyed but they are stored on the AFIS the LCRC database, the 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 should initiate 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 another crime, get arrested and charged, the LCRC draws out the stored fingerprints where the suspect was unknown and links them with the information of the arrested person. Paragraph 2 (j) of the National Instruction 325, issued by Consolidated Notice (2012: 6), states 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 disposed; and the commander closing the docket must endorse a "Brought forward date" in red ink and endorse it with "Do not dispose before the date endorsed. This can happen when the same fingerprints are found in different crime scenes, where the person has never been arrested, as he/she is not on the LCRC database.

5. Sharing of Fingerprints Information with Other Government Departments

The sharing of fingerprints information will not only assist law enforcement agencies but will assist other departments who do not work with criminal cases but also experiences crime. The DOJ & CD Annual Report 1998/1999 (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. This implies that the IJS has been in operation since 1999, and the intention was to fight crime by linking and putting together departments involved in criminal justice.

In this report, the IJS mentioned the individuality of four departments (DOJ, Safety and Security, Department of Social Development (DSD) and DCS) as one of the causes for the inadequate response of

the justice system to the problems related to crime. However not only these four departments are working in separation, but most of government departments are working in isolation, there is no collaboration between the departments. Nevertheless, the sharing of information as mentioned in the Criminal Law (Forensic Procedures) Amendment Act No. 6 of 2010 has not been successful or put into practice, since the statistics on the detection rate of property related crimes is still very low as indicated in the number of complaints reported above. The DOJ & CD Annual Report (1998/1999: 32) also saw the need for the integration of systems as it reported that some of the reasons for the inadequate response of the system to the problem of crime included:

- A lack of integration of the activities, systems, processes, and information within the core departments.
- 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) Act has been an issue since 1998/1999, as well as integrating activities, systems, processes and information. However, it has not been successful in other aspects. Government loses enormous amount of money on fraudulent social grants including non-existing children, and to fight this scourge, the sharing of fingerprint information between the DHA and the DSD can be a solution to this problem. The lack of integration and operating independently between government departments had cost the DSD millions and more during the COVID-19 Pandemic. The fraudsters managed to register deceased people and sentenced offenders 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 were not eligible for the relief fund, for instance, deceased, incarcerated people and people working in government. If the Department had access to the DCS and the DHA systems, such activities would have been prevented. 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. Department of Social Development also needs integration or sharing of information with other government departments. Currently few of the DCS correctional centres do not have fingerprints systems and few do have. Interviews were conducted at the facility with no system and from the facility which has the fingerprint system. During interviews, it emerged that offenders were admitted at the facilities without the requirement of an official Identity document (ID), it is possible that offenders can use false names making it impossible to be traced. If the offenders were admitted with their ID numbers in correctional centres, such information would have been available to other departments, the DSD would have detected that such people were incarcerated in correctional centres. The information technology systems across government carry data on almost everyone in the country, but this rich data is not integrated or shared across government departments (Makwethu, 2020: 4). Wyllie (2017) emphasised the importance of replacing manual operations with technology by indicating that the large number of offenders in correctional centres makes it difficult to manage identification records securely, therefore many correctional centres in the USA were moving away from collecting fingerprints manually and are adopting biometric fingerprint identification technology.

Wyllie (2017) explained 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 (J7) with prints obtained manually by them may result in wrongly admitting an offender with particulars of another offender. The use of multiple identities by Remand Detainees who are clients of the Criminal Justice System (CJS) leads to the creation of aliases within the CJS system and redundant information (The White Paper for Remand Detention Management in South Africa, 2014: 51). These are the challenges faced by the DCS when dealing with offenders manually with no fingerprints database.

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. 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 subject of the fingerprint appearing in the J7, as this verification is done by physically comparing the prints.

6. Fingerprints Information and People's Privacy

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. 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 and 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. A person divulging people`s information for personal gain or someone else`s benefit can be charged for unauthorised use or sharing of information in terms of POPI Act or in terms of the Bill of Rights. 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 (Government 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. EPIC (2018: Par 1) indicated that in the USA, the FBI launched a system called Next Generation Identification (NGI), a database that contained the biometric data of millions of Americans to enhance background 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. Though the Electronic Privacy Information Center (EPIC) opposed the program, saying the program raised privacy issues, the point in this case is that the FBI made drastic measures to access information in order to enhance their investigations.

In order to protect people`s information, the officials working with such information should be sensitized and trained about the consequences of illegally sharing and accessing such information. Extensive protection measures like the use of thumbprints or face recognition security features must be installed. This security feature will also reduce sharing of passwords. ABIS already has the face recognition feature for the wanted suspects and people required for verification as reported by the DHA Annual Report, 2017/2018 (2018: 10) that ABIS allows the identification and verification by fingerprint, facial, iris recognition and other means.

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 (for verification purposes) 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 fingerprints information will not violate people`s privacy and that government does have control when privacy of people is concerned.

7. The Challenges Faced by The LCRC in Identifying First-Time Offenders

The former Justice Minister Jeff Hadebe (as cited in News24, 2010) mentioned that the Criminal Law (Forensic Procedure) Amendment Act 6 of 2010 was intended to deal with two pivotal aspects of forensic crime fighting namely the fingerprint and DNA evidence. The Minister pointed out that SAPS had access only to the fingerprints stored on the SAPS AFIS system and had no direct access to the DHA system where the fingerprints of 41 million citizens and 2.5 million foreigners were kept. The Minister further quoted statistics by mentioning that, the criminal justice system review office, had found that 52% perpetrators remained undetected in 2006/07 and 46% perpetrators also remained undetected in 2007/08 suggesting that the new Act was going to reduce a number of undetected perpetrators. However to this date with this Act in place, property related cases as mentioned above in section 2 are still closed undetected and unresolved as the detection rate is still low.

The SAPS Annual Report (2015/2016: 149) reported that the DHA do assist the police with identification but they assist in identifying fingerprints of circulated persons and stolen vehicles. The DHA system is indeed assisting the police in cases where a warrant of arrest had been issued, the person is missing, or an unknown person is found dead. 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.

However 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 a missing person where the family had provided the police with such information.

SAPS Annual Report (2020/2021: 202) explained that a wanted person can also be a suspect who is sought, but not arrested and whose particulars were known and used to circulate him/her as a wanted. The reports are not clear about the identification of first-time offenders` latent prints. The LCRC uses the AFIS system to record a criminal offence on an individual by means of fingerprints. Criminal records are also obtained from the AFIS for investigation purposes, court purposes, and security clearance. Security clearance is conducted to check whether a person has a criminal record or not. They also conduct security clearances for employment purposes or for application of firearm licenses or travelling visas and or drivers permits etc. Storing these fingerprints information for future use like DNA database will be of great assistance in identifying first time offenders. The article revealed that people can apply for expungement of criminal records on certain conditions if they qualify. People who were charged for minor offences can be cleared and those who were convicted and spent ten years clean can apply to be removed from the criminal record database. Section 36B 6 (iii) of the Criminal Procedure Act 57 of 1977 stated that any person arrested but found not guilty by court should be cleared from the criminal record register. This article proposed 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.

If LCRC was to create a database with these fingerprints information most first time offenders not found on the criminal record could be found in the database created from the security clearance applications. This fingerprint information should be stored in the database separate from the criminal record database and be utilised whenever a first-time offender is not found on criminal database. A challenge faced by the LCRC is the unavailability of a system that can identify the latent prints of first-time offenders. The available system, with integrated information from other departments the PIVA system is not available at the LCRC. Another challenge faced by the LCRC is the poor quality of obtained fingerprints, since the LCRC deals with fingerprint forms where fingerprints are often unclear as they obtained manually using ink and paper. The LCRC experts find it difficult to record those prints in their system, and those prints are sent back to the police station for a retake and by the time the prints get back for a retake, the offender is already released on bail or moved to the correctional centre. This is the concern mentioned by Wyllie (2017) as mentioned earlier that it is important to collect readable fingerprints because if collected incorrectly the offender could go through the entire criminal justice process even to incarceration without having had fingerprints properly captured resulting to the offender having a clear criminal record.

8. Fingerprints Systems Used by Other Government Departments

Integrated Justice System (IJS) from the Department of Justice and Correctional Development (DOJ & CD) developed a system called the Person Identification Verification Application (PIVA). PIVA provides a platform for the identity of an individual to be verified against the Department of Home Affairs records using their fingerprints. Identity verification is a common requirement across all IJS member departments, and the development of the application was a combined effort from a number of departments. PIVA system has been implemented and is fully operational in police stations. SAPS are the criminal justice system entry point, and they are the first department to implement PIVA (IJS Report, 2017:12).

The implementation is still in progress not all departments are having this system and not all police officers know about the system. At the time of interviews, some of the LCRC and DCS officials who are working with fingerprints identification did not know about PIVA system. Only participants from LCRC Head Office confirmed hearing about the PIVA system but not using 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 SAPS CAS (Case Administration system) 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. 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) report 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, when a child is apprehended by the SAPS, the arrest information recorded by SAPS sends notification to the 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 PIVA also retrieves information by means of ID numbers, this can assist departments like the DSD, DCS and others who need to verify information before processing certain applications. PIVA also requires the subject of fingerprints to be present during the verification. Whilst LCRC verifies and compares fingerprints in the absence of the subject they do not need permission from the subject of fingerprints to access his or her information. However, for security clearance, LCRC uses signed fingerprint forms where the subject of fingerprints gave consent or permission for processing of such fingerprint's information.

The PIVA system is available at police stations because it assists criminal justice system departments with integration and sharing of case information. 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. Department of Transport requires security clearance when issuing Professional Driving Permits (PRDPs) the information provided by drivers or applicants can also be shared with other departments via the PIVA system or a developed integrated system.

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. Some participants at the LCRC confirmed that in most cases fingerprints are readable but with identification information unavailable. Whilst some participants indicated that they were not aware of the fact that when fingerprints were positive but with no details of the offender, the dockets get closed. Participants confirmed that in serious cases where the latent prints are not found on their local database, the prints are sent to the National LCRC. 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) stressed in his burglary study 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 offenders are very slim.

This is because those cases are dealt with by the LCRC using the database that does not have particulars of first-time offenders and cannot get assistance from the DHA. The detection tools in burglary cases is 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 offenders use fingerprints barriers like gloves to prevent identification whilst others are smudged and contaminated and cannot be read. Nevertheless, as indicated earlier, there are dockets which are closed with positive fingerprints because the fingerprints picked up from the crime scene have not been found on AFIS. In such cases access to the integrated fingerprint system will assist the police.

9. Findings and Recommendations

The findings revealed that the LCRC cannot identify latent prints of first-time offenders as their database only stores information of people who were criminally charged. The case dockets where people committed a crime for the first time are still closed with positive fingerprints because of the lack of identification information. The implemented PIVA system which integrates the fingerprint information from a few government departments cannot identify latent prints, it cannot assist LCRC. The researchers also found that LCRC does security clearance of people for many purposes including travelling, job

application, firearm applications, public driving permits and for people who were charged and later cleared, but they do not keep these fingerprints on any database. If fingerprints of all citizens coming into contact with SAPS are stored in another database, some of first-time offenders can be discovered in that database. The researchers further found that not all fingerprints obtained manually are readable as some are poorly obtained. This causes the officers to either request a retake or overlook the process which may cause an offender to have a clear record whilst being incarcerated. This can be avoided by the use of digital fingerprint scanners in police stations, courts and in correctional centres instead of inked paper. Wyllie (2017) stated 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 the biometric fingerprint identification technology. Therefore, this article recommends that there is a dire need for a partnership between SAPS and other government departments in identifying latent fingerprints of first-time offends. To ensure that this partnership is effective, the following should be in place:

- **New fingerprint database for daily contact with the police**- where fingerprint information is not available in the criminal record system, the fingerprint expert, must be able to search the database which contains fingerprints information of people who were in contact with the police for matters such as the security clearance and so on.
- **Inter-department fingerprints services-** when the fingerprint information is not available on LCRC database, the LCRC fingerprint expert should proceed to ask for assistance from officials working with the Inter-department fingerprints system to check if their system contains the information of the fingerprints in question. This service department should be established at the 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.
- **Enhanced protection of people`s personal information-** to ensure that people`s personal information is respected, the access to people`s information on inter-departmental system 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. Government departments are already sharing sensitive information which is contained in the Persal system and payments information contained in the BAS system where all government payments are processed. All these systems are a confirmation that sharing of information between government departments is possible and if fingerprint information is shared with LCRC, people`s privacy will still be protected. To avoid poorly obtained fingerprints as it has been a concern of all participants, police stations, the courts and correctional centres should be issued with digital fingerprints scanners to avoid the manual obtaining of fingerprints.

Conclusion

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 SAPS LCRC has property related 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. The PIVA system does not assist police with latent prints searches. 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. If the DHA has been sharing information with other departments, the DSD 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 their fingerprint information with other departments, DSD 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 be reduced by the sharing of information, but government departments will also benefit whilst victims of crime will find justice and have trust in police investigations.

List of References

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

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

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.

Electronic Privacy Information (EPIC). 2019. *EPIC Urges FBI to Limit Fingerprint-Based Background Checks: 09 January 2018).* Retrieved from https://archive.epic.org/2017/08/fbi-issues-final-rule-on-biome.html. (Accessed on February 2019).

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

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

IJS. (Integrated Justice System). 2017. Progress Report. Integrated Justice System (IJS) 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).

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.

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).

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).

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).

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

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

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.

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

South Africa. 1996. *Constitution of South Africa. Act 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. *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. 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).
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).
Van Rooyen, H.J.N., 2008. *The Practitioner`s Guide to Forensic Investigation South Africa.* Pretoria. Henmar Publications.
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 fromhttps://www.correctionsone.com/products/police-technology/investigation/biometrics-identification/articles/how-biometric-technologies-will-help-correctional-facilities-HAjTzVlupizKxEVV/. (Accessed on 12 February 2020).