REPORT ON INTERCEPTION

OF

PRIVATE COMMUNICATIONS

By JUSTICE YVONNE MOKGORO

Joint Standing Committee on Intelligence: Parliament

September 2012 – September 2014

STRUCTURE

1. INTRODUCTION

2. INTERCEPTION

3. INTERNATIONAL LAW

4. SOUTH AFRICAN LEGISLATIVE FRAMEWORK

4.1 Prohibition of Interception of Communication

4.2 Interception in case of Emergency

4.3 Application for issuing of directions and entry warrants

5. KEEPING OF RECORDS BY HEADS OF INTERCEPTION

6. SUPPLEMENTARY DIRECTIVES REGARDING APPLICATIONS

7. THE ACT vs RIGHT TO PRIVACY

8. CHALLENGES

9. RICA AND THE FUTURE

10. FULL STATISTICAL INFORMATION OF APPLICATIONS

10.1 The National Intelligence

10.2 The South African Police Service

1. INTRODUCTION

The 2010/2011 South African Police Statistical Report has revealed that, approximately 2.1 million violent crimes were registered in the last financial year. Although this figure shows a decline in comparison with the previous financial year, the number remains high.

The escalating rate of crime where electronic technology is used has increased significantly and is becoming more sophisticated. The latter situation poses severe challenging to the law enforcement agencies to fulfil their duties optimally and efficiently. Criminals utilize these technologies successfully and with ease.

These methods are frequently utilised in the planning and perpetration of serious crimes ranging from:

- Human trafficking;
- drug dealing and drug trafficking;
- money laundering;
- corruption and fraud;
- kidnappings;
- assassinations;
- terrorism;
- heists; etc

This state of affairs, together with the escalating rate of technological crime and highly sophisticated criminal methods have made interception a popular method of investigation not only in the Republic of South Africa but in almost every country in

the world. Interception of communications is generally considered a necessary evil to protect law abiding citizens from criminal conduct.

2. INTERCEPTION

Lawful interception plays a crucial role in advancing the investigation process. It represents an indispensable means of gathering criminal intelligence. [1] The Regulation of Interception of Communications and Communication-related Information Act, 2002 (Act 70 of 2002), herein after referred to as the "RICA"), was designed to allow the State to intercept communications and provide communication-related information during the investigation of serious crimes. This process becomes legal and the information gathered becomes admissible in court, if it is done in accordance with the RICA.[2]

The RICA provides guidance and requires strict compliance with the procedure that should be undertaken when applying for an interception direction from the designated judge.[3] When doing so, the RICA demands thorough appreciation and application of section 14 of the Constitution, which relates to the right to Privacy.

Most importantly, the application process for an interception direction should be considered as a last resort, as the RICA seeks to guard against abuse of constitutionally protected rights.

---

[1] Notes on OECS Interception of Communications' Bill, page 6 found at: http://unpan1.un.org/inradoc/groups/public/documents/TASF/UNPAN024636.pdf

[2] S v Naidoo and Another 1998 (1) SACR 479 (N)-It was argued that the tape recordings were made in contravention of IM Act of 1992 and thus be declared inadmissible.

[3] Regulations of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002 RICA is the successor to the Interception and Monitoring Act 127 of 1992.

3. INTERNATIONAL LAW

To detect and investigate crimes that are committed through the use of electronic technology has been a global challenge for years. This resulted in the approval of the use of interception devises by the Council of Europe Convention, to which South Africa is a signatory. Almost all countries in the world, for example, the United Kingdom (Regulation of Investigatory Powers Act, 2000), the United States of America (, inter alia,Title III of the Omnibus Crime Control and Safe Streets Act of 1968 as amended), Australia (Telecommunications (Interception) Act 1979), New Zeeland (Crimes Act and Misuse of Drugs Act), various countries in Europe etc, have adopted legislation to regulate the lawfully intercepted communications in order to combat criminal activities. In general the interception and monitoring of communications in all these countries balance the subject's right to privacy with that of the need to investigate and detect crime. Interception of communications in these countries is only allowed if it is judicially sanctioned or approved by an independent higher authority.

4. SOUTH AFRICAN LEGISLATIVE FRAMEWORK

To deal with the question of finding better mechanisms in addressing this challenge, the South African Law Reform Commission (SALRC) felt it was important to undertake a review of the effectiveness of the then Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992). The investigation had shown that the Interception and Monitoring Prohibition Act, was outdated in that it did not adequately deal with new developments in the field of electronic technology and the use thereof in the commission of crimes.

As a result of the recommendations of the SALRC the Interception and Monitoring Prohibition Act, was replaced by the RICA. The aims of the RICA are, inter alia, to:

(a) Protect subjects of the Republic against the unlawful interception of communications;

(b) oblige all electronic communications service providers (ECSPS) to provide a service which is interceptable and which is able to store communication related information;

(c) provide for a structure which is responsible for the interception of communications;

(d) oblige ECSPS to record and store information which can be used to identify their customers;

(e) prohibit the possession and manufacturing of interception devises;

(f) provide for the interception of communications in emergency situations;

(g) provide that the interception of communications must, unless the RICA provides otherwise, be approved by a judge.

Some of these aspects are dealt with in more detail below:

4.1 Prohibition of interception of communication

The Regulations on Interception of Communications prohibit any person to intentionally intercept or attempt to intercept, or otherwise procure any other person to intercept or attempt to intercept, at any place in the Republic, any

communication in the course of its occurrence or transmission unless it is done in terms of the provisions of the RICA.[4]

4.2 Interception in cases of emergency

In a case of an emergency, where there are reasonable grounds to believe that an emergency exists by reason of the fact that the life of another person is being endangered, the applicant can orally request the ECSP concerned to intercept any communication to or from the sender in any other manner which the telecommunication deems appropriate or provide such assistance as may be necessary to determine the location of such a person (sections 7 and 8 of the RICA).[5]

These processes are however subject to judicial scrutiny in that the information obtained as well as affidavits from the ECSPS and law enforcement officers who requested the information must be submitted to the designated judge for scrutiny.

4.3 Application for issuing of directions and entry warrants

Under the RICA, a designated judge may authorise –

(a) the interception of direct or indirect communications by way of an interception direction in terms of section 16 of the RICA;(b) the interception of real-time communication-related information on an ongoing basis by means of a direction in terms of section 17 of the RICA;

[4] Section 2
[5] Section 8(1)(b) and (aa)

(b) the combined interception of of direct or indirect communications, real-time communication-related and provision of archived communication-related information by means of a direction in terms of section 18 of RICA;

(c) the decryption of intercepted information by means of a decryption direction in terms of section section 21 of RICA; and

(d) entry warrants for the purposes of entering a premises for the placing of interception devices in terms of section 22 of RICA.

The above-mentioned directions or entry warrant can only be granted after the law enforcement agencies make a formal application to the designated judge. In considering such an application, the RICA imposes various factors that must be considered by the designated judge before he or she may grant a direction or entry warrant.

With regard to an interception direction, the Act compels any person who is authorised to intercept communication, to complete an application and submit it to the designated judge for consideration. The application should clearly indicate, *inter alia,* the identity of the applicant, the identity of the law enforcement officer, the person whose communication is required and the telecommunication service provider to whom the direction must be addressed.[6]

To invoke the application of section 36 of the Constitution, the Act further requires the applicant, in his or her application, to include the basis for believing that evidence relating to the ground on which the application is made will be obtained

[6] Section 16

through the interception applied for.[7] Furthermore, the application must indicate, where applicable, whether other investigative procedures have been applied and failed to produce the required evidence and why other investigative means are unlikely to succeed or appear to be too dangerous.[8]

An interception direction may be granted if the designated judge is satisfied that:

- A serious offence has been or is being or will be committed or public health or safety is threatened etc;
- the interception will provide information regarding the offence or threat;
- the facilities from which the communications will be intercepted are usually used by the person; and
- other investigative methods had been unsuccessful or too dangerous.

5. KEEPING OF RECORDS BY HEADS OF INTERCEPTION

The head of an interception centre must on a quarterly basis submit a written report of the records kept, abuses in connection with execution of directions and any defect in any electronic communications system which has been discovered.[9]

This obligation is there to ensure that there is full compliance with the RICA.

6. SUPPLEMENTARY DIRECTIVES REGARDING APPLICATIONS

A designated judge or designated judges, jointly, after consultation with the respective Judges-President of the High Courts, may issue directives to

[7] Section 16(2)(d)(ii)
[8] Section 16(2)(e)
[9] Section 37(1)(2)(a)(i-iii)

supplement the procedure for making applications for the issuing of directions or entry warrants and the directive issued must be submitted to parliament.[10]

7. THE ACT *vs* THE RIGHT TO PRIVACY

Section 14 of the constitution protects everyone's right to privacy, which includes the right not to have "the privacy of their communications infringed". [11] Furthermore, Privacy is a fundamental human right recognised internationally in instruments like the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights, and regionally in the African Charter on Peoples' Rights, etc. It underpins human dignity and other key values such as freedom of association and freedom of speech.[12]

Article 8 of the Convention on Human Rights explicitly states that, "there shall be no interference by a public authority with the exercise of this right except in accordance with the law and to the extent that it is necessary in a democratic society and in the interests of national security, public safety or the economic well-being of the country. The right to privacy in this regard may also be limited in preventing disorder or crime, for the protection of health, or the rights and freedom of others".

The Article makes it clear that the information collected by enforcement agencies, must only relate to that which is identified by the warrant issued, such that, only persons or people who are suspected of committing serious offences or

[10] Section 58(1) and (3)
[11] The Constitution of the Republic of South Africa, 1996
[12] Privacy and Human Rights-An International Survey and Privacy Laws-http://gilc.org/privacy/survey/intro.html

participating in activities against the interests of national security, may lose their right to privacy.[13]

In our Constitution, no right is absolute. All rights, including the right to privacy are limited, but only in terms of a law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors.[14]

Indeed, "the shift in balance towards absolute individual privacy is in itself a threat to security and the consequence of this choice will [in the context of the state of crime rates in South Africa] affect our personal safety, our right to live in a society where lawlessness is not tolerated and the ability of law enforcement to prevent serious and other violent criminal activity".[15]

In the matter of *The Investigating Directorate and Others v Hyundai Motor Distributions,* Justice Langa DP held that

"It is a notorious fact that the rate of crime in South Africa is unacceptably high. There are frequent reports of violent crime and incessant disclosures of fraudulent activity. This has a serious effect not only on the security of citizens and morale of the community but also on the country's economy. This ultimately affects the government's ability to address the pressing social welfare problems in South Africa. The need to fight crime is thus an important objective in our society…"[16]*, then*

---

[13] European Convention on Human Rights for the Protection of Human Rights and Fundamental Freedom-www.hrcr.org/docs/Eur convention/euroconv3.html

[14] The Constitution of the Republic of South, section 36(1) 1996-Limitation Clause

[15] Lawful interception-Andres Rojab-centre for advanced Internet Architectures Swinburne University of Technology-Feb 9 2006- http://caia.swin.edu.au

[16] The Investigating Directorate and Others v Hyundai Motor Distributions (PTY) (LTD) 2001 (1) SA 545 (CC)

In *Califonia v Ciraolo* the court held,

> *"The right to privacy is not meant to shield criminal activities or to conceal evidence of crime from the criminal justice process, however, state officials are not entitled without good cause to invade the premises of persons for purposes of searching and seizing property..."*[17]

8. CHALLENGES

There is a general public perception that some law enforcement and other institutions use these intrusive methods to advance their own interests with no regard to the rights and values in the Constitution. The media, in particular the social networks, are inundated with reports, allegations and comments of manipulation and abuse of the interception system by officials and even individuals, ranging from-

- obtaining of information in less than 36 hours, without the Designated Judge's knowledge;
- acquisition of cell phone billing and ownership records through crime intelligence, without the Judge's knowledge or approval, in order to expedite the investigation;
- obtaining text messages and cell phone billing records needed for personal reasons, through a contact at crime intelligence;
- the popularity of interception method which is preferred over conventional method;
- the apparent lack of trust of the Designated Judge with regard to information gathered through crime intelligence;

[17] California v Ciraolo 476 US 207 (1985) at 213-4

- failure of applicants to provide fact-based justification for an application to the Judge;
- applicant's need to comprehend that suspicion of crime without any factual basis is not sufficient for application for interception;
- the tendency for vagueness of basis for an application, the cut and paste approach to an affidavit and the tendency to regard the authorisation for interception as a given and therefore the taking and
- wide allegations of bribery of contacts at banks and telecommunications service providers;[18] etc

Not all of these challenges may be resolved through legislative amendments. Some may only be resolved through the dedication, commitment, full understanding and appreciation of the role of investigation officers gathering crime intelligence in a democratic society based on the values of human dignity, freedom and equality. The need to sharpen and constantly improve the investigative skills and prowess of our law enforcement agencies comes to mind - no doubt on important aspect of contemporary policing.

9. RICA AND THE FUTURE

The RICA was assented to on 30 December 2002 and came into operation on 30 September 2005. From 2002 to date, there have been substantial developments that took place in the electronic communications field. The Electronic Communications Act, 2005 (Act 36 of 2005), introduced a new electronic communications dispensation in South Africa, moving away from the dispensation

[18] How the government spies on you-Mail and Guardian Online-http://mg.co.za/articles/2011-10-14

envisaged in the RICA, where there is a clear, based on the Telecommunications Act, 1996 (Act No. 103 of 1996), distinction based on fixed line, internet and mobile cellular communications. The RICA should be revamped to bring the terminology in line with the current electronic communications dispensation as is envisaged in the Electronic Communications Act, 2005.

New services are seeing the light, inter alia, Black Berry Messenger Services, BlackBerry Enterprise Services, Skype and a host of other services, which is mostly Internet based, which is clearly not interceptable, and even if it were interceptable, the encryption that is applied to such services makes it nearly impossible for the law enforcement agencies to obtain any information about the content of a communication. This aspect should be further investigated in order to find a solution.

RICA may need to be revised in light of the obligations which the Republic may incur if we accede to the African Union Convention on the establishment of a credible legal framework for cyber security in Africa in order to deal with cybercrime.

RICA should in so far as possible regularly be revised in order to ensure that it keeps pace with developments.

There is reliable information that an electronic process for the application of directions was previously discussed in this Committee. The Department of Justice and Constitutional Development, who is the State Department responsible for the administration of the RICA, will be approached in due course to consider proposals.

10. STATISTICAL INFORMATION OF APPLICATIONS FOR DIRECTIONS

10.1 State Security Agency (SSA)

Figures for the period are as follow:

• Applications (New)	28
• Re-applications	32
• Amendments	34
• Extensions	31
• Amendments and Extensions	13
• Entry Warrants	4
• Section (11)	66
• Oral intercepts	2
• Refused	5 (No RICA confirmation)
• **Total**	**215**

10.2 THE SOUTH AFRICAN POLICE SERVICES (SAPS)

Figures for the period are as follow:

• Applications (New)	150
• Re-applications	22
• Amendments	8
• Extensions	4
• Amendments and Extensions	18
• **Total**	**202**

10.3 THE SOUTH AFRICAN SECRET SERVICE(SASS)

Figures for the period are as follow:

- Applications (New) 2

Total **2**

10.4 FINANCIAL INTELLIGENCE CENTRE(FIC)

Figures for the period are as follow:

- Applications (New) 3

Total **3**

10.5 SOUTH AFRICAN NATIONAL DEFENCE FORCE(SANDF)

Figures for the period are as follow:

- Applications (New) 3
- Amendments 1

Total **4**

Combined figures for NIA , SAPS,SASS,FIC and SANDF are as follow:

• Applications (New)	185
• Re-applications	54
• Amendments	5
• Extensions	35
• Amendments and Extensions	31
• Entry Warrants	4
• Section(11)	66
• Oral intercepts	2
• Refused	5
• **Total**	**387**