

# REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT 70 OF 2002

[ASSENTED TO 30 DECEMBER 2002] [DATE OF COMMENCEMENT: 30 SEPTEMBER 2005]  
(Unless otherwise indicated)

*(English text signed by the President)*

## **as amended by**

Prevention and Combating of Corrupt Activities Act 12 of 2004  
Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of  
2004  
Electronic Communications Act 36 of 2005  
Regulation of Interception of Communications and Provision of Communication-related  
Information Amendment Act 48 of 2008

## **Regulations under this Act**

NOTICE IN TERMS OF SECTION 31: FIXED LINE OPERATORS (GN R92 in GG 31844 of 6 February 2009)

NOTICE IN TERMS OF SECTION : MOBILE CELLULAR OPERATORS (GN R93 in GG 31844 of 6 February 2009)

## **ACT**

**To regulate the interception of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information; to regulate the making of applications for, and the issuing of, directions authorising the interception of communications and the provision of communication-related information under certain circumstances; to regulate the execution of directions and entry warrants by law enforcement officers and the assistance to be given by postal service providers, telecommunication service providers and decryption key holders in the execution of such directions and entry warrants; to prohibit the provision of telecommunication services which do not have the capability to be intercepted; to provide for certain costs to be borne by certain telecommunication service providers; to provide for the establishment of interception centres, the Office for Interception Centres and the Internet Service Providers Assistance Fund; to prohibit the manufacturing, assembling, possessing, selling, purchasing or advertising of certain equipment; to create offences and to prescribe penalties for such offences; and to provide for matters connected therewith.**

### ARRANGEMENT OF SECTIONS

#### *Section*

#### CHAPTER 1 INTRODUCTORY PROVISIONS

- 1 Definitions and interpretation

#### CHAPTER 2 PROHIBITION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF REAL-TIME OR ARCHIVED COMMUNICATION-RELATED INFORMATION AND EXCEPTIONS

##### *Part 1*

##### *Prohibition of interception of communications and exceptions*

- 2 Prohibition of interception of communication
- 3 Interception of communication under interception direction

- 4 Interception of communication by party to communication
- 5 Interception of communication with consent of party to communication
- 6 Interception of indirect communication in connection with carrying on of business
- 7 Interception of communication to prevent serious bodily harm
- 8 Interception of communication for purposes of determining location in case of emergency
- 9 Interception of communications authorised by certain other Acts
- 10 Monitoring of signal for purposes of installation or maintenance of equipment, facilities or devices
- 11 Monitoring of signal and radio frequency spectrum for purposes of managing radio frequency spectrum

[S. 11 substituted by s. 97 of Act 36 of 2005.]

#### *Part 2*

#### *Prohibition of provision of real-time or archived communication-related information and exceptions*

- 12 Prohibition of provision of real-time or archived communication-related information
- 13 Provision of real-time or archived communication-related information under real-time communication-related direction or archived communication-related direction
- 14 Provision of real-time or archived communication-related information upon authorisation by customer
- 15 Availability of other procedures for obtaining real-time or archived communication-related information

#### CHAPTER 3

#### APPLICATIONS FOR, AND ISSUING OF, DIRECTIONS AND ENTRY WARRANTS

- 16 Application for, and issuing of, interception direction
- 17 Application for, and issuing of, real-time communication-related direction
- 18 Combined application for, and issuing of, interception direction, real-time communication-related direction and archived communication-related direction or interception direction supplemented by real-time communication-related direction
- 19 Application for, and issuing of, archived communication-related direction
- 20 Amendment or extension of existing direction
- 21 Application for, and issuing of, decryption direction
- 22 Application for, and issuing of, entry warrant
- 23 Oral application for, and issuing of, direction, entry warrant, oral direction or oral entry warrant
- 24 Reports on progress
- 25 Cancellation of direction, entry warrant, oral direction or oral entry warrant

#### CHAPTER 4

#### EXECUTION OF DIRECTIONS AND ENTRY WARRANTS

- 26 Execution of direction

- 27 Execution of entry warrant
- 28 Assistance by postal service provider and telecommunication service provider
- 29 Assistance by decryption key holder

CHAPTER 5  
INTERCEPTION CAPABILITY AND COMPENSATION

- 30 Interception capability of telecommunication services and storing of communication-related information
- 31 Compensation payable to postal service provider, telecommunication service provider and decryption key holder

CHAPTER 6  
INTERCEPTION CENTRES, OFFICE FOR INTERCEPTION CENTRES AND INTERNET SERVICE PROVIDERS ASSISTANCE FUND

- 32 Establishment of interception centres
- 33 Establishment of Office for Interception Centres
- 34 Director and staff of Office
- 35 Powers, functions and duties of Director
- 36 Head and staff of interception centres
- 37 Keeping of records by heads of interception centres and submission of reports to Director
- 38 Establishment and control of Internet Service Providers Assistance Fund

CHAPTER 7  
DUTIES OF TELECOMMUNICATION SERVICE PROVIDER AND CUSTOMER

- 39 Information to be obtained and kept by certain telecommunication service providers
- 40 Information to be obtained and kept by electronic communication service provider who provides a mobile cellular electronic communications service  
[S. 40 substituted by s. 2 of Act 48 of 2008.]
- 41 Loss, theft or destruction of cellular phone or SIM-card to be reported

CHAPTER 8  
GENERAL PROHIBITIONS AND EXEMPTIONS

- 42 Prohibition on disclosure of information
- 43 Disclosure of information by authorised person for performance of official duties
- 44 Listed equipment
- 45 Prohibition on manufacture, possession and advertising of listed equipment
- 46 Exemptions

CHAPTER 9  
CRIMINAL PROCEEDINGS, OFFENCES AND PENALTIES

- 47 Use of information in criminal proceedings
- 48 Proof of certain facts by certificate
- 49 Unlawful interception of communication
- 50 Unlawful provision of real-time or archived communication-related information

- 51 Offences and penalties
- 52 Failure to give satisfactory account of possession of cellular phone or SIM-card
- 53 Absence of reasonable cause for believing cellular phone or SIM-card properly acquired
- 54 Unlawful acts in respect of telecommunication and other equipment
- 55 Failure to report loss, theft or destruction of cellular phone or SIM-card and presumption
- 56 Revoking of licence to provide electronic communication service

[S. 56 substituted by s. 97 of Act 36 of 2005.]

- 57 Forfeiture of listed or other equipment

#### CHAPTER 10 GENERAL PROVISIONS

- 58 Supplementary directives regarding applications
- 59 Amendment of section 205 of Act 51 of 1977 , as substituted by section 11 of Act 204 of 1993
- 60 Amendment of section 11 of Act 140 of 1992
- 61 Amendment of section 3 of Act 40 of 1994 , as amended by section 3 of Act 31 of 1995 and section 3 of Act 42 of 1999
- 62 Repeal of law and transitional arrangements
- 62A Determination of tariffs

[S. 62A inserted by s. 5 of Act 48 of 2008.]

- 62B Information to be provided to customers

[S. 62B inserted by s. 5 of Act 48 of 2008.]

- 62C Keeping of information by juristic persons and persons who lease SIM-cards

[S. 62C inserted by s. 5 of Act 48 of 2008.]

- 63 Short title and commencement

[S. 63 substituted by s. 6 of Act 48 of 2008.]

Schedule

### CHAPTER 1 INTRODUCTORY PROVISIONS (s 1)

#### 1 Definitions and interpretation

(1) In this Act, unless the context otherwise indicates-

**'activate'** means to allow access to the electronic communication system of the electronic communication service provider who provides a mobile cellular electronic communications service and **'activated'** has a corresponding meaning;

[Definition of 'activate' inserted by s. 1 (a) of Act 48 of 2008.]

**'address'** means-

(a) in the case of a natural person-

(i) the address where the person usually resides, or where such

residential address is not available-

- (aa) the address where the person is employed;
- (bb) the address where the business of the person is situated;  
or
- (ii) where such a person resides in an informal settlement and cannot provide an address contemplated in subparagraph (i), any other address, including that of a school, church or retail store, where a person usually receives his or her post; or
- (b) in the case of a juristic person, the registered address or the address where the business is situated;

[Definition of 'address' inserted by s. 1 (a) of Act 48 of 2008.]

**'Agency'** means the Agency as defined in section 1 of the Intelligence Services Act;

**'applicant'** means-

- (a) an officer referred to in section 33 of the South African Police Service Act, if the officer concerned obtained in writing the approval in advance of another officer in the Police Service with at least the rank of assistant-commissioner and who has been authorised in writing by the National Commissioner to grant such approval;
- (b) an officer as defined in section 1 of the Defence Act, if the officer concerned obtained in writing the approval in advance of another officer in the Defence Force with at least the rank of major-general and who has been authorised in writing by the Chief of the Defence Force to grant such approval;
- (c) a member as defined in section 1 of the Intelligence Services Act, if the member concerned obtained in writing the approval in advance of another member of the Agency or the Service, as the case may be, holding a post of at least general manager;
- (d) the head of the Directorate or an Investigating Director authorised thereto in writing by the head of the Directorate;
- (e) a member of a component referred to in paragraph (e) of the definition of 'law enforcement agency', authorised thereto in writing by the National Director; or
- (f) a member of the Independent Complaints Directorate, if the member concerned obtained in writing the approval in advance of the Executive Director;

**'archived communication-related direction'** means a direction issued under section 18 (3) (a) or 19 (3) in terms of which a telecommunication service provider is directed to provide archived communication-related information in respect of a customer;

**'archived communication-related information'** means any communication-related information in the possession of a telecommunication service provider and which is being stored by that telecommunication service provider in terms of section 30 (1) (b) for the period determined in a directive referred to in section 30 (2) (a), beginning on the first day immediately following the expiration of a period of 90 days after the date of the transmission of the indirect communication to which that communication-related information relates;

**'authorised person'** means any-

- (a) law enforcement officer who may, in terms of section 26 (1) (a) (i), execute a direction; or

- (b) law enforcement officer or other person who may, in terms of section 26 (1) (a) (ii), assist with the execution of a direction;

**'Authority'** means the Independent Communications Authority of South Africa established by section 3 of the Independent Communications Authority of South Africa Act, 2000 ( Act 13 of 2000 );

**'business'** means any business activity conducted by any person, including activities of any private or public body;

**'cellular phone'** means any fixed or mobile cellular apparatus or terminal which is capable of connection to a cellular telecommunication system and which is used by a customer to transmit or receive indirect communications over such telecommunication system;

**'communication'** includes both a direct communication and an indirect communication;

**'communication-related information'** means any information relating to an indirect communication which is available in the records of a telecommunication service provider, and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system;

**'Constitution'** means the Constitution of the Republic of South Africa, 1996 ( Act 108 of 1996 );

**'contents'** , when used with respect to any communication, includes any information concerning the substance, purport or meaning of that communication;

**'customer'** means any person-

- (a) to whom an electronic communication service provider provides an electronic communications service, including an employee of the electronic communication service provider or any person who receives or received such service as a gift, reward, favour, benefit or donation;
- (b) who has entered into a contract with an electronic communication service provider for the provision of an electronic communications service, including a pre-paid electronic communications service; or
- (c) where applicable-
  - (i) to whom an electronic communication service provider in the past has provided an electronic communications service; or
  - (ii) who has, in the past, entered into a contract with an electronic communication service provider for the provision of an electronic communications service, including a pre-paid electronic communications service;

[Definition of 'customer' substituted by s. 1 (b) of Act 48 of 2008.]

**'decryption assistance'** means to-

- (a) allow access, to the extent possible, to encrypted information; or
- (b) facilitate the putting of encrypted information into an intelligible form;

**'decryption direction'** means a direction issued under section 21 (3) in terms of which a decryption key holder is directed to-

- (a) disclose a decryption key; or
- (b) provide decryption assistance in respect of encrypted information, and includes an oral decryption direction issued under section 23 (7);

**'decryption key'** means any key, mathematical formula, code, password, algorithm or any other data which is used to-

- (a) allow access to encrypted information; or
- (b) facilitate the putting of encrypted information into an intelligible form;

**'decryption key holder'** means any person who is in possession of a decryption key for purposes of subsequent decryption of encrypted information relating to indirect communications;

**'Defence Act'** means the Defence Act, 1957 ( Act 44 of 1957 );

**'Defence Force'** means the defence force referred to in section 199 (2) of the Constitution;

**'designated judge'** means any judge of a High Court discharged from active service under section 3 (2) of the Judges' Remuneration and Conditions of Employment Act, 2001 ( Act 47 of 2001 ), or any retired judge, who is designated by the Minister to perform the functions of a designated judge for purposes of this Act;

**'direct communication'** means an-

- (a) oral communication, other than an indirect communication, between two or more persons which occurs in the immediate presence of all the persons participating in that communication; or
- (b) utterance by a person who is participating in an indirect communication, if the utterance is audible to another person who, at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication;

**'direction'** means any interception direction, real-time communication-related direction, archived communication-related direction or decryption direction issued under this Act, and includes an oral direction issued under section 23 (7), but, for purposes of section 20, excludes an archived communication-related direction;

**'Director'** means the Director: Office for Interception Centres, seconded in terms of section 34 (1);

**'Directorate'** means the Directorate of Special Operations referred to in section 1 of the National Prosecuting Authority Act;

**'electronic communication service provider'** means any-

- (a) person who provides an electronic communication service under and in accordance with a electronic communication service licence issued to such person under Chapter 3 of the Electronic Communications Act, and includes any person who provides-
  - (i) a local access communication service, public pay-telephone service, value-added network service or private electronic communication network as defined in the Electronic Communications Act; or

- (ii) any other electronic communication service licensed or deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act; and

(b) Internet service provider;

[Definition of 'electronic communication service provider' substituted for definition of 'telecommunication service provider' by s. 97 of Act 36 of 2005.]

**'electronic communication system'** means any system or series of electronic communication facilities or radio, optical or other electromagnetic apparatus or any similar technical system used for the purpose of electronic communication, whether or not such electronic communication is subject to re-arrangement, composition or other processes by any means in the course of their transmission or emission or reception;

[Definition of 'electronic communication system', previously definition of 'telecommunication system', substituted by s. 97 of Act 36 of 2005.]

**'Electronic Communications Act'** means the Electronic Communications Act, 2005.

[Definition of 'Electronic Communications Act' inserted by s. 97 of Act 36 of 2005.]

**'electronic communications service'** means electronic communications service as defined in the Electronic Communications Act;

[Definition of 'electronic communications service', previously definition of 'telecommunication service', substituted by s. 97 of Act 36 of 2005.]

**'encrypted information'** means any electronic data which, without the decryption key to that data-

- (a) cannot, or cannot readily, be accessed; or
- (b) cannot, or cannot readily, be put into an intelligible form;

**'entry warrant'** means a warrant issued under section 22 (3) and which authorises entry upon any premises for purposes of-

- (a) intercepting a postal article or communication on the premises; or
- (b) installing and maintaining an interception device on, and removing an interception device from, the premises, and includes an oral entry warrant issued under section 23 (7);

**'Executive Director'** means the Executive Director appointed in terms of section 51 of the South African Police Service Act;

**'family member'** means-

- (a) a person who is related to another person-
  - (i) biologically; or
  - (ii) by statutory, customary or religious law, including affinity by marriage, adoption or foster care;
- (b) a person's permanent life partner; or
- (c) in the case of an orphan, a care-giver as defined in the Children's Act, 2005 ( Act 38 of 2005 );

[Definition of 'family member' inserted by s. 1 (c) of Act 48 of 2008.]



**'fixed date'** means the date of commencement of this Act;

**'Fund'** means the Internet Service Providers Assistance Fund established by section 38 (1);

**'Identification Act'** means the Identification Act, 1997 ( Act 68 of 1997 );

**'identification document'** means, in the case of a person-

- (a) who is a South African citizen or is lawfully and permanently resident in the Republic-
  - (i) a green, bar-coded identity document issued in terms of section 8 of the Identification Act, 1986 (Act 72 of 1986), until such identity document is replaced by an identity card as contemplated in section 25 of the Identification Act;
  - (ii) an identity card issued in terms of section 14 of the Identification Act;
  - (iii) a temporary identity certificate issued in terms of section 16 of the Identification Act; or
  - (iv) a South African passport issued in terms of the South African Passports and Travel Documents Act, 1994 ( Act 4 of 1994 ); or
- (b) who is not a South African citizen or not permanently resident in the Republic, excluding a refugee, a valid passport or travel document as contemplated in paragraphs (b) and (c) of the definition of 'passport' in the Immigration Act, 2002 ( Act 13 of 2002 ); or
- (c) who is a refugee, a valid identity document issued in terms of section 30 of the Refugees Act, 1998 ( Act 130 of 1998 );

[Definition of 'identification document' substituted by s. 1 (d) of Act 48 of 2008.]

**'identity number'** means-

- (a) in the case of a person who is a South African citizen or who is lawfully and permanently resident in the Republic, the number referred to as the identity number in the document contemplated in paragraph (a) (i), (ii) or (iii) of the definition of 'identification document' or the number referred to as the passport number in the document contemplated in paragraph (a) (iv) of the definition of 'identification document';
- (b) in the case of a person who is not a South African citizen or who is not permanently resident in the Republic, excluding a refugee, the number referred to as the passport number in the document contemplated in paragraph (b) of the definition of 'identification document'; or
- (c) in the case of a refugee, the number referred to as the identity number in the document contemplated in paragraph (c) of the definition of 'identification document';

[Definition of 'identity number' inserted by s. 1 (e) of Act 48 of 2008.]

**'Independent Complaints Directorate'** means the Independent Complaints Directorate established by section 50 (1) of the South African Police Service Act;

**'indirect communication'** means the transfer of information, including a message or any part of a message, whether-

- (a) in the form of-
  - (i) speech, music or other sounds;
  - (ii) data;
  - (iii) text;
  - (iv) visual images, whether animated or not;
  - (v) signals; or
  - (vi) radio frequency spectrum; or
- (b) in any other form or in any combination of forms,

that is transmitted in whole or in part by means of a postal service or a telecommunication system;

**'informal settlement'** means a place in an urban or rural setting used for residential purposes and in respect of which no physical addresses or street particulars are officially assigned;

[Definition of 'informal settlement' inserted by s. 1 (f) of Act 48 of 2008.]

**'Intelligence Services Act'** means the Intelligence Services Act, 1994 (Act 38 of 1994);

**'intelligible form'** means the form in which electronic data was before an encryption or similar process was applied to it;

**'intercept'** means the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the-

- (a) monitoring of any such communication by means of a monitoring device;
- (b) viewing, examination or inspection of the contents of any indirect communication; and
- (c) diversion of any indirect communication from its intended destination to any other destination,

and **'interception'** has a corresponding meaning;

**'interception centre'** means an interception centre established by section 32 (1) (a) ;

**'interception device'** means any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to intercept any communication, but does not include-

- (a) any instrument, device, equipment or apparatus, or any component thereof-
  - (i) furnished to the customer by a telecommunication service provider in the ordinary course of his or her business and being used by the customer in the ordinary course of his or her business;
  - (ii) furnished by such customer for connection to the facilities of such telecommunication service and used in the ordinary course

of his or her business; or

- (iii) being used by a telecommunication service provider in the ordinary course of his or her business; or
- (b) a hearing aid or similar device being used to correct below normal hearing to not better than normal,

and a reference to an **'interception device'** includes, where applicable, a reference to a **'monitoring device'** ;

**'interception direction'** means a direction issued under section 16 (4) or 18 (3) (a) and which authorises the interception, at any place in the Republic, of any communication in the course of its occurrence or transmission, and includes an oral interception direction issued under section 23 (7);

**'Internet'** means the international computer network known by that name;

**'internet service provider'** means any person who provides access to, or any other service related to, the Internet to another person, whether or not such access or service is provided under and in accordance with an electronic communication service licence issued to the first-mentioned person under Chapter 3 of the Electronic Communications Act;

[Definition of 'internet service provider' substituted by s. 97 of Act 36 of 2005.]

**'law enforcement agency'** means-

- (a) the Police Service;
- (b) the Defence Force;
- (c) the Agency or the Service;
- (d) the Directorate; or
- (e) any component of the prosecuting authority, designated by the National Director to specialise in the application of Chapter 6 of the Prevention of Organised Crime Act;

**'law enforcement officer'** means any member of-

- (a) the Police Service;
- (b) the Defence Force, excluding a member of a visiting force;
- (c) the Agency or the Service;
- (d) the Directorate; or
- (e) any component referred to in paragraph (e) of the definition of 'law enforcement agency';

**'listed equipment'** means any equipment declared to be listed equipment under section 44 (1) (a) , and includes any component of such equipment;

**'Minister'** means the Cabinet member responsible for the administration of justice, except in Chapter 6 where it means the Cabinet member responsible for intelligence services;

**'monitor'** includes to listen to or record communications by means of a monitoring device, and **'monitoring'** has a corresponding meaning;

**'monitoring device'** means any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to or record any communication;

**'National Commissioner'** means the National Commissioner referred to in section 6 (1) of the South African Police Service Act;

**'National Director'** means the National Director of Public Prosecutions contemplated in section 179 (1) (a) of the Constitution;

**'National Prosecuting Authority Act'** means the National Prosecuting Authority Act, 1998 ( Act 32 of 1998 );

**'Office'** means the Office for Interception Centres established by section 33;

**'oral direction'** means any direction issued under section 23 (7);

**'oral entry warrant'** means an entry warrant issued under section 23 (7);

**'party to the communication'** , for purposes of-

- (a) section 4, means, in the case of-
  - (i) a direct communication, any person-
    - (aa) participating in such direct communication or to whom such direct communication is directed; or
    - (bb) in whose immediate presence such direct communication occurs and is audible to the person concerned, regardless of whether or not the direct communication is specifically directed to him or her; or
  - (ii) an indirect communication-
    - (aa) the sender or the recipient or intended recipient of such indirect communication;
    - (bb) if it is intended by the sender of an indirect communication that such indirect communication be received by more than one person, any of those recipients; or
    - (cc) any other person who, at the time of the occurrence of the indirect communication, is in the immediate presence of the sender or the recipient or intended recipient of that indirect communication; and
- (b) section 5, means, in the case of-
  - (i) a direct communication, any person participating in such direct communication or to whom such direct communication is directed; or
  - (ii) an indirect communication-
    - (aa) the sender or the recipient or intended recipient of such indirect communication; or
    - (bb) if it is intended by the sender of an indirect communication that such indirect communication be received by more than one person, any of those recipients;

**'Police Service'** means the South African Police Service established by section 5 (1) of the South African Police Service Act;

**'postal article'** means any postal article as defined in the Postal Services Act;

**'postal service'** means a postal service as defined in the Postal Services Act, and includes any-

- (a) private postal service; and
- (b) service which is offered or provided as a service of which the main purpose, or one of the main purposes, is to make available, or to facilitate, a means of transmission from one place to another place of postal articles containing indirect communications;

**'Postal Services Act'** means the Postal Services Act, 1998 ( Act 124 of 1998 );

**'postal service provider'** means any person who provides a postal service;

**'premises'** includes any land, building, structure, vehicle, ship, boat, vessel, aircraft or container;

**'Prevention of Organised Crime Act'** means the Prevention of Organised Crime Act, 1998 ( Act 121 of 1998 );

**'private body'** means-

- (a) a natural person who carries on any trade, business or profession, but only in such capacity;
- (b) a partnership which carries on any trade, business or profession; or
- (c) any juristic person,

but excludes a public body;

**'prosecuting authority'** means the national prosecuting authority established by section 179 of the Constitution;

**'public body'** means any-

- (a) department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
- (b) other functionary or institution when-
  - (i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or
  - (ii) exercising a public power or performing a public function in terms of any legislation;

**'real-time communication-related direction'** means a direction issued under section 17 (3) or 18 (3) in terms of which a telecommunication service provider is directed to provide real-time communication-related information in respect of a customer, on an ongoing basis, as it becomes available, and includes an oral real-time communication-related direction issued under section 23 (7);

**'real-time communication-related information'** means communication-related information which is immediately available to a telecommunication service provider-

- (a) before, during, or for a period of 90 days after, the transmission of an indirect communication; and
- (b) in a manner that allows the communication-related information to be

associated with the indirect communication to which it relates;

**'relevant Ministers'** means the Cabinet members responsible for-

- (a) communications;
- (b) defence;
- (c) intelligence services; and
- (d) policing,

except in Chapter 6 where it means the Cabinet members referred to in paragraphs (a) , (b) and (d) and the Cabinet member responsible for the administration of justice;

**'serious offence'** means any-

- (a) offence mentioned in the Schedule; or
- (b) offence that is allegedly being or has allegedly been or will probably be committed by a person, group of persons or syndicate-
  - (i) acting in an organised fashion which includes the planned, ongoing, continuous or repeated participation, involvement or engagement in at least two incidents of criminal or unlawful conduct that has the same or similar intents, results, accomplices, victims or methods of commission, or otherwise are related by distinguishing characteristics;
  - (ii) acting in the execution or furtherance of a common purpose or conspiracy; or
  - (iii) which could result in substantial financial gain for the person, group of persons or syndicate committing the offence,

including any conspiracy, incitement or attempt to commit any of the above-mentioned offences;

**'Service'** means the Service as defined in section 1 of the Intelligence Services Act;

**'SIM-card'** means the Subscriber Identity Module which is an independent, electronically activated device designed for use in conjunction with a cellular phone to enable the user of the cellular phone to transmit and receive indirect communications by providing access to telecommunication systems and enabling such telecommunication systems to identify the particular Subscriber Identity Module and its installed information;

**'South African Police Service Act'** means the South African Police Service Act, 1995 ( Act 68 of 1995 );

**'system controller'** of, or in relation to-

- (a) a private body, means, in the case of a-
  - (i) natural person, that natural person or any person duly authorised by that natural person;
  - (ii) partnership, any partner of the partnership or any person duly authorised by the partnership; or
  - (iii) juristic person, the-
    - (aa) chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or
    - (bb) person who is acting as such or any person duly

- authorised by such acting person; and
- (b) a public body, means, in the case of-
- (i) a national department, provincial administration or organisational component-
    - (aa) mentioned in Column 1 of Schedule 1 or 3 to the Public Service Act, 1994 ( Proclamation 103 of 1994 ), the officer who is the incumbent of the post bearing the designation mentioned in Column 2 of the said Schedule 1 or 3 opposite the name of the relevant national department, provincial administration or organisational component or the person who is acting as such; or
    - (bb) not so mentioned, the Director-General, head, executive director or equivalent officer, respectively, of that national department, provincial administration or organisational component, respectively, or the person who is acting as such;
  - (ii) a municipality, the municipal manager appointed in terms of section 82 of the Local Government: Municipal Structures Act, 1998 ( Act 117 of 1998 ), or the person who is acting as such; or
  - (iii) any other public body, the chief executive officer, or equivalent officer, of that public body or the person who is acting as such;

'Telecommunications Act' means the Telecommunications Act, 1996 ( Act 103 of 1996 ).

(2) For purposes of this Act-

- (a) the interception of a communication takes place in the Republic if, and only if, the interception is effected by conduct within the Republic and the communication is either intercepted, in the case of-
  - (i) a direct communication, in the course of its occurrence; or
  - (ii) an indirect communication, in the course of its transmission by means of a postal service or telecommunication system, as the case may be; and
- (b) the time during which an indirect communication is being transmitted by means of a telecommunication system includes any time when the telecommunication system by means of which such indirect communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it.

(3) A reference in this Act to the interception of a communication does not include a reference to the interception of any indirect communication which is broadcast or transmitted for general reception.

## CHAPTER 2

### PROHIBITION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF REAL-TIME OR ARCHIVED COMMUNICATION-RELATED INFORMATION AND EXCEPTIONS (ss 2-15)

#### *Part 1*

#### *Prohibition of interception of communications and exceptions (ss 2-11)*

## 2 Prohibition of interception of communication

Subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or 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.

### **3 Interception of communication under interception direction**

Subject to this Act, any-

- (a) authorised person who executes an interception direction or assists with the execution thereof, may intercept any communication; and
- (b) postal service provider to whom an interception direction is addressed, may intercept any indirect communication,

to which that interception direction relates.

### **4 Interception of communication by party to communication**

(1) Any person, other than a law enforcement officer, may intercept any communication if he or she is a party to the communication, unless such communication is intercepted by such person for purposes of committing an offence.

(2) Any law enforcement officer may intercept any communication if he or she is-

- (a) a party to the communication; and
- (b) satisfied that there are reasonable grounds to believe that the interception of a communication of another party to the communication is necessary on a ground referred to in section 16 (5) (a) ,

unless such communication is intercepted by such law enforcement officer for purposes of committing an offence.

### **5 Interception of communication with consent of party to communication**

(1) Any person, other than a law enforcement officer, may intercept any communication if one of the parties to the communication has given prior consent in writing to such interception, unless such communication is intercepted by such person for purposes of committing an offence.

(2) Any law enforcement officer may intercept any communication if-

- (a) one of the parties to the communication has given prior consent in writing to such interception;
- (b) he or she is satisfied that there are reasonable grounds to believe that the party who has given consent as contemplated in paragraph (a) will-
  - (i) participate in a direct communication or that a direct communication will be directed to him or her; or
  - (ii) send or receive an indirect communication; and
- (c) the interception of such direct or indirect communication is necessary on a ground referred to in section 16 (5) (a) ,

unless such communication is intercepted by such law enforcement officer for purposes of committing an offence.

### **6 Interception of indirect communication in connection with carrying on of business**



(1) Any person may, in the course of the carrying on of any business, intercept any indirect communication-

- (a) by means of which a transaction is entered into in the course of that business;
- (b) which otherwise relates to that business; or
- (c) which otherwise takes place in the course of the carrying on of that business,

in the course of its transmission over a telecommunication system.

(2) A person may only intercept an indirect communication in terms of subsection (1)-

- (a) if such interception is effected by, or with the express or implied consent of, the system controller;
- (b) for purposes of-
  - (i) monitoring or keeping a record of indirect communications-
    - (aa) in order to establish the existence of facts;
    - (bb) for purposes of investigating or detecting the unauthorised use of that telecommunication system; or
    - (cc) where that is undertaken in order to secure, or as an inherent part of, the effective operation of the system; or
  - (ii) monitoring indirect communications made to a confidential voice-telephony counselling or support service which is free of charge, other than the cost, if any, of making a telephone call, and operated in such a way that users thereof may remain anonymous if they so choose;
- (c) if the telecommunication system concerned is provided for use wholly or partly in connection with that business; and
- (d) if the system controller has made all reasonable efforts to inform in advance a person, who intends to use the telecommunication system concerned, that indirect communications transmitted by means thereof may be intercepted or if such indirect communication is intercepted with the express or implied consent of the person who uses that telecommunication system.

## **7 Interception of communication to prevent serious bodily harm**

(1) Any law enforcement officer may, if-

- (a) he or she is satisfied that there are reasonable grounds to believe that a party to the communication has-
  - (i) caused, or may cause, the infliction of serious bodily harm to another person;
  - (ii) threatens, or has threatened, to cause the infliction of serious bodily harm to another person; or
  - (iii) threatens, or has threatened, to take his or her own life or to perform an act which would or may endanger his or her own life or would or may cause the infliction of serious bodily harm to himself or herself;
- (b) he or she is of the opinion that because of the urgency of the need to intercept the communication, it is not reasonably practicable to make an application in terms of section 16 (1) or 23 (1) for the issuing of an

interception direction or an oral interception direction; and

- (c) the sole purpose of the interception is to prevent such bodily harm,

intercept any communication or may orally request a telecommunication service provider to route duplicate signals of indirect communications specified in that request to the interception centre designated therein.

(2) A telecommunication service provider must, upon receipt of a request made to him or her in terms of subsection (1), route the duplicate signals of the indirect communications concerned to the designated interception centre.

(3) The law enforcement officer who made a request under subsection (1) must as soon as practicable after making that request, furnish the telecommunication service provider concerned with a written confirmation of the request which sets out the information given by that law enforcement officer to that telecommunication service provider in connection with the request.

(4) The law enforcement officer who intercepts a communication under subsection (1) or (2) must, as soon as practicable after the interception of the communication concerned, submit to a designated judge-

- (a) a copy of the written confirmation referred to in subsection (3);
- (b) an affidavit setting forth the results and information obtained from that interception; and
- (c) any recording of the communication that has been obtained by means of that interception, any full or partial transcript of the recording and any notes made by that law enforcement officer of the communication if nothing in the communication suggests that bodily harm, attempted bodily harm or threatened bodily harm has been caused or is likely to be caused.

(5) A telecommunication service provider who, in terms of subsection (2), has routed duplicate signals of indirect communications to the designated interception centre must, as soon as practicable thereafter, submit an affidavit to a designated judge setting forth the steps taken by that telecommunication service provider in giving effect to the request concerned and the results obtained from such steps.

(6) A designated judge must keep all written confirmations and affidavits and any recordings, transcripts or notes submitted to him or her in terms of subsections (4) and (5), or cause it to be kept, for a period of at least five years.

## **8 Interception of communication for purposes of determining location in case of emergency**

(1) In circumstances where-

- (a) a person is a party to a communication;
- (b) that person, as a result of information received from another party to the communication (in this section referred to as the 'sender'), has reasonable grounds to believe that an emergency exists by reason of the fact that the life of another person, whether or not the sender, is being endangered or that he or she is dying or is being or has been seriously injured or that his or her life is likely to be endangered or that he or she is likely to die or to be seriously injured; and
- (c) the location of the sender is unknown to that person,

the person referred to in paragraph (a) may, if he or she is-

- (i) a law enforcement officer, and if he or she is of the opinion that determining the location of the sender is likely to be of assistance in dealing with the emergency, orally request, or cause another law enforcement officer to orally request, the telecommunication service provider concerned to-
  - (aa) intercept any communication to or from the sender for purposes of determining his or her location; or
  - (bb) determine the location of the sender in any other manner which the telecommunication service provider deems appropriate; or
- (ii) not a law enforcement officer, inform, or cause another person to inform, any law enforcement officer of the matters referred to in paragraphs (a) , (b) and (c) .

(2) A law enforcement officer who has been informed as contemplated in subsection (1) (ii), may, if he or she is of the opinion that determining the location of the sender is likely to be of assistance in dealing with the emergency, orally request, or cause another law enforcement officer to orally request, the telecommunication service provider concerned to act as contemplated in subsection (1) (i) (aa) or (bb) .

(3) A telecommunication service provider must, upon receipt of a request made to him or her in terms of subsection (1) (i) or (2)-

- (a) intercept any communication to or from the sender for purposes of determining his or her location; or
- (b) determine the location of the sender in any other manner which the telecommunication service provider deems appropriate,

and if the location of the sender has been so determined, the telecommunication service provider concerned must, as soon as practicable after determining that location, provide the law enforcement officer who made the request with the location of the sender and any other information obtained from that interception which, in the opinion of the telecommunication service provider concerned, is likely to be of assistance in dealing with the emergency.

(4) The law enforcement officer who made a request under subsection (1) (i) or (2) must-

- (a) as soon as practicable after making that request, furnish the telecommunication service provider concerned with a written confirmation of the request which sets out the information given by that law enforcement officer to that telecommunication service provider in connection with the request;
- (b) as soon as practicable after making that request, furnish a designated judge with a copy of such written confirmation; and
- (c) if the location of the sender and any other information has been provided to him or her in terms of subsection (3), as soon as possible after receipt thereof, submit to a designated judge an affidavit setting forth the results and information obtained from that interception.

(5) A telecommunication service provider who has taken any of the steps contemplated in subsection (3), must, as soon as practicable thereafter, submit to a designated judge-

- (a) an affidavit setting forth the steps taken by that telecommunication service provider in giving effect to the request concerned and the results and information obtained from such steps; and

- (b) if such steps included the interception of an indirect communication, any recording of that indirect communication that has been obtained by means of that interception, any full or partial transcript of the recording and any notes made by that telecommunication service provider of that indirect communication.

(6) A designated judge must keep all written confirmations and affidavits and any recordings, transcripts or notes submitted to him or her in terms of subsections (4) (b) and (c) and (5), or cause it to be kept, for a period of at least five years.

## 9 Interception of communications authorised by certain other Acts

(1) Any communication may, in the course of its occurrence or transmission, be intercepted in any prison as defined in section 1 of the Correctional Services Act, 1998 ( Act 111 of 1998 ), if such interception takes place in the exercise of any power conferred by or under, and in accordance with, any regulations made under that Act.

(2) If any regulations referred to in subsection (1)-

- (a) were made prior to the fixed date, the Cabinet member responsible for correctional services must within one month after the fixed date, if Parliament is then in ordinary session, or, if Parliament is not then in ordinary session, within one month after the commencement of its next ensuing ordinary session, submit a copy of those regulations to Parliament; or
- (b) are made after the fixed date, the Cabinet member responsible for correctional services must, before the publication thereof in the *Gazette* , submit those regulations to Parliament.

## 10 Monitoring of signal for purposes of installation or maintenance of equipment, facilities or devices

Any person who is lawfully engaged in duties relating to the-

- (a) installation or connection of any equipment, facility or device used, or intended to be used, in connection with a telecommunication service;
- (b) operation or maintenance of a telecommunication system; or
- (c) installation, connection or maintenance of any interception device used, or intended to be used, for the interception of a communication under an interception direction,

may, in the ordinary course of the performance of those duties, monitor a signal relating to an indirect communication where it is reasonably necessary for that person to monitor that signal for purposes of performing those duties effectively.

## 11 Monitoring of signal and radio frequency spectrum for purposes of managing radio frequency spectrum

Any person appointed as an inspector in terms of section 17F of the Independent Communications Authority of South Africa Act and who is lawfully engaged in performing the functions of the Authority relating to the management of the radio frequency spectrum, as contemplated in section 30 (1) of the Electronic Communications Act, may, in the ordinary course of the performance of those functions, monitor a signal or radio frequency spectrum relating to an indirect communication which is transmitted over radio, where it is reasonably necessary for that employee to monitor that signal or radio frequency spectrum for purposes of identifying, isolating or preventing an unauthorised or interfering use of such a signal or frequency or of a transmission.

[S. 11 substituted by s. 97 of Act 36 of 2005.]

*Prohibition of provision of real-time or archived communication-related information and exceptions (ss 12-15)*

**12 Prohibition of provision of real-time or archived communication-related information**

Subject to this Act, no telecommunication service provider or employee of a telecommunication service provider may intentionally provide or attempt to provide any real-time or archived communication-related information to any person other than the customer of the telecommunication service provider concerned to whom such real-time or archived communication-related information relates.

**13 Provision of real-time or archived communication-related information under real-time communication-related direction or archived communication-related direction**

Subject to this Act, any telecommunication service provider to whom a real-time communication-related direction or an archived communication-related direction is addressed, may provide any real-time or archived communication-related information to which that real-time communication-related direction or archived communication-related direction relates.

**14 Provision of real-time or archived communication-related information upon authorisation by customer**

Any telecommunication service provider may, upon the written authorisation given by his or her customer on each occasion, and subject to the conditions determined by the customer concerned, provide to any person specified by that customer, real-time or archived communication-related information which relates to the customer concerned.

**15 Availability of other procedures for obtaining real-time or archived communication-related information**

(1) Subject to subsection (2), the availability of the procedures in respect of the provision of real-time or archived communication-related information provided for in sections 17 and 19 does not preclude obtaining such information in respect of any person in accordance with a procedure prescribed in any other Act.

(2) Any real-time or archived communication-related information which is obtained in terms of such other Act may not be obtained on an ongoing basis.

**CHAPTER 3  
APPLICATIONS FOR, AND ISSUING OF, DIRECTIONS AND ENTRY  
WARRANTS (ss 16-25)**

**16 Application for, and issuing of, interception direction**

(1) An applicant may apply to a designated judge for the issuing of an interception direction.

(2) Subject to section 23 (1), an application referred to in subsection (1) must be in writing and must-

- (a) indicate the identity of the-
  - (i) applicant and, if known and appropriate, the identity of the law enforcement officer who will execute the interception direction;
  - (ii) person or customer, if known, whose communication is required to be intercepted; and
  - (iii) postal service provider or telecommunication service provider to whom the direction must be addressed, if applicable;

- (b) specify the ground referred to in subsection (5) (a) on which the application is made;
- (c) contain full particulars of all the facts and circumstances alleged by the applicant in support of his or her application;
- (d) include-
  - (i) subject to subsection (8), a description of the-
    - (aa) nature and location of the facilities from which, or the place at which, the communication is to be intercepted, if known; and
    - (bb) type of communication which is required to be intercepted; and
  - (ii) the basis for believing that evidence relating to the ground on which the application is made will be obtained through the interception;
- (e) if applicable, indicate whether other investigative procedures have been applied and have failed to produce the required evidence or must indicate the reason why other investigative procedures reasonably appear to be unlikely to succeed if applied or are likely to be too dangerous to apply in order to obtain the required evidence: Provided that this paragraph does not apply to an application for the issuing of a direction in respect of the ground referred to in subsection (5) (a) (i) or (v) if the-
  - (i) serious offence has been or is being or will probably be committed for the benefit of, at the direction of, or in association with, a person, group of persons or syndicate involved in organised crime; or
  - (ii) property is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities;
- (f) indicate the period for which the interception direction is required to be issued;
- (g) indicate whether any previous application has been made for the issuing of an interception direction in respect of the same person or customer, facility or place specified in the application and, if such previous application exists, must indicate the current status of that application; and
- (h) comply with any supplementary directives relating to applications for interception directions issued under section 58.

(3) An application on a ground referred to in-

- (a) subsection (5) (a) (i), must be made by an applicant referred to in paragraph (a) , (d) or (f) of the definition of 'applicant';
- (b) subsection (5) (a) (ii) or (iii), must be made by an applicant referred to in paragraph (b) or (c) of the definition of 'applicant';
- (c) subsection (5) (a) (iv), must, in the case of-
  - (i) the investigation of a serious offence, be made by an applicant referred to in paragraph (a) or (d) of the definition of 'applicant'; and
  - (ii) the gathering of information, be made by an applicant referred

to in paragraph (c) of the definition of 'applicant'; and

- (d) subsection (5) (a) (v), must be made by an applicant referred to in paragraph (e) of the definition of 'applicant':

Provided that an applicant referred to in paragraph (f) of the definition of 'applicant' may only make an application on the ground referred to in subsection (5) (a) (i)-

- (i) if the offence allegedly has been or is being or will be committed by a member of the Police Service; or
- (ii) in respect of a death in police custody or as a result of police action.

(4) Notwithstanding section 2 or anything to the contrary in any other law contained, a designated judge may, upon an application made to him or her in terms of subsection (1), issue an interception direction.

(5) An interception direction may only be issued if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that-

- (a) there are reasonable grounds to believe that-
- (i) a serious offence has been or is being or will probably be committed;
- (ii) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;
- (iii) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;
- (iv) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in-
- (aa) accordance with an international mutual assistance agreement; or
- (bb) the interests of the Republic's international relations or obligations; or
- (v) the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities is necessary;
- (b) there are reasonable grounds to believe that-
- (i) the interception of particular communications concerning the relevant ground referred to in paragraph (a) will be obtained by means of such an interception direction; and
- (ii) subject to subsection (8), the facilities from which, or the place at which, the communications are to be intercepted are being used, or are about to be used, in connection with the relevant ground referred to in paragraph (a) are commonly used by the person or customer in respect of whom the application for the issuing of an interception direction is made; and
- (c) in respect of the grounds referred to in paragraph (a) (i), (iii), (iv) or

(v), other investigative procedures have been applied and have failed to produce the required evidence or reasonably appear to be unlikely to succeed if applied or are likely to be too dangerous to apply in order to obtain the required evidence and that the offence therefore cannot adequately be investigated, or the information therefore cannot adequately be obtained, in another appropriate manner: Provided that this paragraph does not apply to an application for the issuing of a direction in respect of the ground referred to in paragraph (a) (i) or (v) if the-

- (i) serious offence has been or is being or will probably be committed for the benefit of, at the direction of, or in association with, a person, group of persons or syndicate involved in organised crime; or
- (ii) property is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities.

(6) An interception direction-

- (a) must be in writing;
- (b) must contain the information referred to in subsection (2) (a) (ii) and (iii) and (d) (i);
- (c) may specify conditions or restrictions relating to the interception of communications authorised therein; and
- (d) may be issued for a period not exceeding three months at a time, and the period for which it has been issued must be specified therein.

(7) (a) An application must be considered and an interception direction issued without any notice to the person or customer to whom the application applies and without hearing such person or customer.

(b) A designated judge considering an application may require the applicant to furnish such further information as he or she deems necessary.

(8) The requirements of subsections (2) (d) (i) (aa) and (5) (b) (ii) relating to the description of the facilities from which, or the place at which, the communication is to be intercepted do not apply if, in the case of an application for the issuing of an interception direction which authorises the interception of-

- (a) a direct communication-
  - (i) the application contains full particulars of all the facts and circumstances as to why such description is not practical;
  - (ii) the application indicates the identity of the person whose communication is required to be intercepted; and
  - (iii) the designated judge is satisfied, on the facts alleged in the application, that such description is not practical; and
- (b) an indirect communication, the-
  - (i) application indicates the identity of the customer whose communication is required to be intercepted;
  - (ii) applicant submits proof that there are reasonable grounds to believe that the actions of the customer concerned could have the effect of preventing interception from a specified facility;



- (iii) designated judge is satisfied that sufficient proof has been submitted; and
- (iv) interception direction authorises the interception only for such time as it is reasonable to presume that the customer identified in the application is or was reasonably close to the instrument through which such communication will be or was transmitted.

(9) The interception of a communication under an interception direction to which the requirements of subsections (2) (d) (i) (aa) and (5) (b) (ii) do not apply by reason of subsection (8) (a) may not take place until the place at which the communication is to be intercepted is determined by the authorised person who executes the interception direction concerned or assists with the execution thereof.

(10) (a) A telecommunication service provider to whom an interception direction referred to in subsection (8) (b) is addressed, may in writing apply to a designated judge for an amendment or the cancellation of the interception direction concerned on the ground that his or her assistance with respect to the interception of the indirect communication cannot be performed in a timely or reasonable fashion.

(b) A designated judge to whom an application is made in terms of paragraph (a) must, as soon as possible after receipt thereof-

- (i) inform the applicant concerned of that application; and
- (ii) consider and give a decision in respect of the application.

## **17 Application for, and issuing of, real-time communication-related direction**

(1) If no interception direction has been issued and only real-time communication-related information on an ongoing basis is required, an applicant may apply to a designated judge for the issuing of a real-time communication-related direction.

(2) Subject to section 23 (1), an application referred to in subsection (1) must be in writing and must-

- (a) indicate the identity of the-
  - (i) applicant;
  - (ii) customer, if known, in respect of whom the real-time communication-related information is required; and
  - (iii) telecommunication service provider to whom the real-time communication-related direction must be addressed;
- (b) specify the ground referred to in subsection (4) on which the application is made;
- (c) contain full particulars of all the facts and circumstances alleged by the applicant in support of his or her application;
- (d) include-
  - (i) a description of the type of real-time communication-related information that is required; and
  - (ii) the basis for believing that evidence relating to the ground on which the application is made will be obtained through the provision of the real-time communication-related information;
- (e) indicate whether the real-time communication-related information must be-

- (i) routed to a designated interception centre specified in the application; or
- (ii) provided to the law enforcement agency concerned;
- (f) indicate the period for which, and the manner in which, the real-time communication-related information is required to be provided;
- (g) indicate whether any previous application has been made for the issuing of a real-time communication-related direction in respect of the same customer or real-time communication-related information specified in the application and, if such previous application exists, must indicate the current status of that application; and
- (h) comply with any supplementary directives relating to applications for real-time communication-related directions issued under section 58.

(3) Notwithstanding section 12 or anything to the contrary in any other law contained, a designated judge may, upon an application made to him or her in terms of subsection (1), issue a real-time communication-related direction.

(4) A real-time communication-related direction may only be issued if it appears to the designated judge concerned, on the facts alleged in the application concerned, that there are reasonable grounds to believe that-

- (a) a serious offence has been or is being or will probably be committed;
- (b) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;
- (c) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;
- (d) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in-
  - (i) accordance with an international mutual assistance agreement; or
  - (ii) the interests of the Republic's international relations or obligations; or
- (e) the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities is necessary,

and that the provision of real-time communication-related information is necessary for purposes of investigating such offence or gathering such information.

(5) A real-time communication-related direction-

- (a) must be in writing;
- (b) must contain the information referred to in subsection (2) (a) (ii) and (iii), (d) (i) and (e) ;
- (c) may specify conditions or restrictions relating to the provision of real-time communication-related information authorised therein; and

- (d) may be issued for a period not exceeding three months at a time, and the period for which it has been issued must be specified therein.

(6) Section 16 (3) and (7) applies, with the necessary changes, in respect of an application for, and the issuing of, a real-time communication-related direction.

**18 Combined application for, and issuing of, interception direction, real-time communication-related direction and archived communication-related direction or interception direction supplemented by real-time communication-related direction**

(1) If the-

- (a) interception of an indirect communication and the provision of communication-related information, whether real-time or archived or both; or
- (b) provision of real-time and archived communication-related information,

are required, an applicant may, subject to sections 16 (2) and (3), 17 (1) and (2) and 19 (1) and (2), in a combined application, apply to a designated judge for the simultaneous issuing of any combination of directions referred to in those sections.

(2) (a) If an interception direction has been issued under section 16, the applicant who made the application in respect of the interception direction concerned or, if he or she is not available, any other applicant who would have been entitled to make that application, may, subject to section 17 (1) and (2), apply to a designated judge for the issuing of a real-time communication-related direction to supplement that interception direction.

(b) An application referred to in paragraph (a) must-

- (i) contain an affidavit setting forth the results obtained from the interception direction concerned from the date of its issuance up to the date on which that application is made, or a reasonable explanation of the failure to obtain such results;
- (ii) contain proof that an interception direction has been issued; and
- (iii) be made at any stage after the issuing of the interception direction concerned, but before the expiry of the period or extended period for which it has been issued.

(3) Notwithstanding sections 2 and 12 or anything to the contrary in any other law contained, a designated judge may, upon an application made to him or her in terms of-

- (a) subsection (1) and subject to sections 16 (5), (6) and (7), 17 (4), (5) and (6) and 19 (4), (5) and (6), issue the combination of directions applied for; or
- (b) subsection (2) and subject to section 17 (4), (5) and (6), issue a real-time communication-related direction to supplement that interception direction: Provided that a real-time communication-related direction issued under this paragraph expires when the period or extended period for which the interception direction concerned has been issued, lapses.

(4) Notwithstanding section 19 (1), (3) and (4)-

- (a) an application in terms of subsection (1) for the issuing of an archived communication-related direction may only be made to a designated judge; and

- (b) only a designated judge may issue an archived communication-related direction under subsection (3) (a) .

## 19 Application for, and issuing of, archived communication-related direction

(1) If only archived communication-related information is required, an applicant may apply to a judge of a High Court, a regional court magistrate or a magistrate for the issuing of an archived communication-related direction.

- (2) An application referred to in subsection (1) must be in writing and must-
  - (a) contain, with the necessary changes, the information referred to in section 17 (2); and
  - (b) comply with any supplementary directives relating to applications for archived communication-related directions issued under section 58.

(3) Notwithstanding section 12 or anything to the contrary in any other law contained, a judge of a High Court, a regional court magistrate or a magistrate may, upon an application made to him or her in terms of subsection (1), issue an archived communication-related direction.

(4) An archived communication-related direction may only be issued if it appears to the judge of a High Court, regional court magistrate or magistrate concerned, on the facts alleged in the application concerned, that there are reasonable grounds to believe that-

- (a) a serious offence has been or is being or will probably be committed;
- (b) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;
- (c) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;
- (d) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in-
  - (i) accordance with an international mutual assistance agreement; or
  - (ii) the interests of the Republic's international relations or obligations; or
- (e) the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities is necessary,

and that the provision of archived communication-related information is necessary for purposes of investigating such offence or gathering such information.

- (5) An archived communication-related direction-
  - (a) must be in writing;
  - (b) must contain the information referred to in section 17 (2) (a) (ii) and (iii), (d) (i) and (e) ;

- (c) must state the period within which the archived communication-related information must be routed or provided; and
- (d) may specify conditions or restrictions relating to the provision of archived communication-related information authorised therein.

(6) Section 16 (3) and (7) applies, with the necessary changes, in respect of an application for, and the issuing of, an archived communication-related direction.

(7) If a judge of a High Court, regional court magistrate or magistrate issues an archive communication-related direction, he or she must, as soon as practicable thereafter, submit a copy of the application and archived communication-related direction concerned to a designated judge.

(8) A designated judge must keep all copies of applications and archived communication-related directions submitted to him or her in terms of subsection (7), or cause it to be kept, for a period of at least five years.

## **20 Amendment or extension of existing direction**

(1) The applicant who made the application in respect of an existing direction or, if he or she is not available, any other applicant who would have been entitled to make that application, may, at any stage after the issuing of the existing direction concerned, but before the expiry of the period for which it has been issued, apply to a designated judge for an amendment thereof or the extension of the period for which it has been issued.

- (2) An application referred to in subsection (1) must be in writing and must-
- (a) contain full particulars of the reasons and circumstances alleged by the applicant in support of his or her application;
  - (b) in the case of an application for the-
    - (i) amendment of an existing direction, indicate the amendment which is required; or
    - (ii) extension of the period for which an existing direction has been issued, indicate the period for which the extension is required;
  - (c) contain an affidavit setting forth the results obtained from the direction concerned from the date of its issuance up to the date on which that application is made, or a reasonable explanation of the failure to obtain such results; and
  - (d) comply with any supplementary directives relating to applications for the amendment or extension of directions issued under section 58.

(3) A designated judge may, upon an application made to him or her in terms of subsection (1)-

- (a) amend an existing direction; or
- (b) extend the period for which an existing direction has been issued.

(4) An existing direction may only be amended or the period for which it has been issued may only be extended if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that the amendment or extension is necessary for purposes of achieving the objectives of the direction concerned: Provided that the period for which an existing direction has been issued may only be extended for a further period not exceeding three months at a time.

(5) Any amendment of an existing direction or extension of the period for which it has

been issued, must be in writing.

(6) Section 16 (7) applies, with the necessary changes, in respect of the amendment of an existing direction or the extension of the period for which an existing direction has been issued.

## 21 Application for, and issuing of, decryption direction

(1) An applicant who-

- (a) makes an application referred to in section 16 (1) may in his or her application also apply for the issuing of a decryption direction; or
- (b) made an application referred to in section 16 (1) or, if he or she is not available, any other applicant who would have been entitled to make that application, may, at any stage after the issuing of the interception direction in respect of which such an application was made, but before the expiry of the period or extended period for which it has been issued, apply to a designated judge for the issuing of a decryption direction.

(2) Subject to section 23 (1), an application referred to in subsection (1) must be in writing and must-

- (a) indicate the identity of the-
  - (i) applicant;
  - (ii) customer, if known, in respect of whom the decryption of encrypted information is required; and
  - (iii) decryption key holder to whom the decryption direction must be addressed;
- (b) describe the encrypted information which is required to be decrypted;
- (c) specify the-
  - (i) decryption key, if known, which must be disclosed; or
  - (ii) decryption assistance which must be provided, and the form and manner in which it must be provided;
- (d) indicate the period for which the decryption direction is required to be issued;
- (e) indicate whether any previous application has been made for the issuing of a decryption direction in respect of the same customer or encrypted information specified in the application and, if such previous application exists, must indicate the current status of that application;
- (f) if the application is made in terms of subsection (1) (b) , also contain-
  - (i) proof that an interception direction has been issued; and
  - (ii) an affidavit setting forth the results obtained from the interception direction concerned from the date of its issuance up to the date on which that application is made, or a reasonable explanation of the failure to obtain such results; and
- (g) comply with any supplementary directives relating to applications for decryption directions issued under section 58.

(3) A designated judge may, upon an application made to him or her in terms of

subsection (1), issue a decryption direction.

(4) A decryption direction may only be issued-

- (a) if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that there are reasonable grounds to believe that-
  - (i) any indirect communication to which the interception direction concerned applies, or any part of such an indirect communication, consists of encrypted information;
  - (ii) the decryption key holder specified in the application is in possession of the encrypted information and the decryption key thereto;
  - (iii) the purpose for which the interception direction concerned was issued would be defeated, in whole or in part, if the decryption direction was not issued; and
  - (iv) it is not reasonably practicable for the authorised person who executes the interception direction concerned or assists with the execution thereof, to obtain possession of the encrypted information in an intelligible form without the issuing of a decryption direction; and
- (b) after the designated judge concerned has considered-
  - (i) the extent and nature of any other encrypted information, in addition to the encrypted information in respect of which the decryption direction is to be issued, to which the decryption key concerned is also a decryption key; and
  - (ii) any adverse effect that the issuing of the decryption direction might have on the business carried on by the decryption key holder to whom the decryption direction is addressed.

(5) A decryption direction-

- (a) must be in writing;
- (b) must contain the information referred to in subsection (2) (a) (ii) and (iii), (b) and (c) ;
- (c) must state the period within which the decryption key must be disclosed or the decryption assistance must be provided, whichever is applicable;
- (d) may specify conditions or restrictions relating to decryption authorised therein; and
- (e) may be issued for a period not exceeding three months at a time, and the period for which it has been issued must be specified therein: Provided that a decryption direction expires when the period or extended period for which the interception direction concerned has been issued, lapses.

(6) Section 16 (7) applies, with the necessary changes, in respect of the issuing of a decryption direction.

## **22 Application for, and issuing of, entry warrant**

(1) An applicant who-

- (a) makes an application referred to in section 16 (1) may in his or her

application also apply for the issuing of an entry warrant; or

- (b) made an application referred to in section 16 (1) or, if he or she is not available, any other applicant who would have been entitled to make that application, may, at any stage after the issuing of the interception direction in respect of which such an application was made, but before the expiry of the period or extended period for which it has been issued, apply to a designated judge for the issuing of an entry warrant.

(2) Subject to section 23 (1), an application referred to in subsection (1) must be in writing and must-

- (a) indicate the-
  - (i) identity of the applicant;
  - (ii) premises in respect of which the entry warrant is required to be issued; and
  - (iii) specific purpose, referred to in the definition of 'entry warrant', for which the application is made;
- (b) if the application is made in terms of subsection (1) (b) , also contain-
  - (i) proof that an interception direction has been issued; and
  - (ii) an affidavit setting forth the results obtained from the interception direction concerned from the date of its issuance up to the date on which that application is made, or a reasonable explanation of the failure to obtain such results;
- (c) indicate whether any previous application has been made for the issuing of an entry warrant for the same purpose or in respect of the same premises specified in the application and, if such previous application exists, must indicate the current status of that application; and
- (d) comply with any supplementary directives relating to applications for entry warrants issued under section 58.

(3) A designated judge may, upon an application made to him or her in terms of subsection (1), issue an entry warrant.

(4) An entry warrant may only be issued if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that-

- (a) the entry of the premises concerned is necessary for a purpose referred to in the definition of 'entry warrant'; or
- (b) there are reasonable grounds to believe that it would be impracticable to intercept a communication under the interception direction concerned otherwise than by the use of an interception device installed on the premises.

(5) An entry warrant-

- (a) must be in writing;
- (b) must contain the information referred to in subsection (2) (a) (ii) and (iii); and
- (c) may contain conditions or restrictions relating to the entry upon the premises concerned as the designated judge deems necessary.



(6) An entry warrant expires when-

- (a) the period or extended period for which the interception direction concerned has been issued, lapses; or
- (b) it is cancelled in terms of section 23 (11) or 25 (1) or (2) by the designated judge who issued it or, if he or she is not available, by any other designated judge,

whichever occurs first.

(7) Section 16 (7) applies, with the necessary changes, in respect of the issuing of an entry warrant.

(8) If an entry warrant has expired as contemplated in subsection (6) (a), the applicant who made the application in respect of the entry warrant concerned or, if he or she is not available, any other applicant who would have been entitled to make that application, must, as soon as practicable after the date of expiry of the entry warrant concerned, and without applying to a judge for the issuing of a further entry warrant, remove, or cause to be removed, any interception device which has been installed thereunder and which, at the date of expiry of that entry warrant, has not yet been removed from the premises concerned.

### **23 Oral application for, and issuing of, direction, entry warrant, oral direction or oral entry warrant**

(1) An application referred to in section 16 (1), 17 (1), 18 (1), 21 (1) or 22 (1) may be made orally by an applicant who is entitled to make such an application if he or she is of the opinion that it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application.

(2) An oral application referred to in subsection (1) must-

- (a) contain the information referred to in section 16 (2), 17 (2), 21 (2) or 22 (2), whichever is applicable;
- (b) indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the applicant, justify the making of an oral application; and
- (c) comply with any supplementary directives relating to oral applications issued under section 58.

(3) Notwithstanding sections 2 and 12 or anything to the contrary in any other law contained, a designated judge may, upon an oral application made to him or her in terms of subsection (1), issue the direction or entry warrant applied for.

(4) A direction or an entry warrant may only be issued under subsection (3)-

- (a) if the designated judge concerned is satisfied, on the facts alleged in the oral application concerned, that-
  - (i) there are reasonable grounds to believe that the direction or entry warrant applied for could be issued;
  - (ii) a direction is immediately necessary on a ground referred to in section 16 (5) (a), 17 (4) or 21 (4) (a), whichever is applicable, or an entry warrant is immediately necessary on a ground referred to in section 22 (4); and
  - (iii) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make

a written application for the issuing of the direction or entry warrant applied for; and

- (b) on condition that the applicant concerned must submit a written application to the designated judge concerned within 48 hours after the issuing of the direction or entry warrant under subsection (3).

(5) A direction or entry warrant issued under subsection (3) must be in writing.

(6) Section 16 (5) (b) and (c) , (6) and (7), 17 (5) and (6), 21 (4) (b) , (5) and (6) or 22 (5), (6), (7) and (8), whichever is applicable, applies, with the necessary changes, in respect of the issuing of a direction or an entry warrant under subsection (3).

(7) Notwithstanding subsection (5), a designated judge may, upon an oral application made to him or her in terms of subsection (1), orally issue the direction or entry warrant applied for.

(8) An oral direction or oral entry warrant may only be issued under subsection (7)-

- (a) if the designated judge concerned is satisfied, on the facts alleged in the oral application concerned, that-
  - (i) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances to issue the direction or entry warrant applied for in writing; or
  - (ii) any other exceptional circumstances exist which justify the issuing of an oral direction or oral entry warrant; and
- (b) on condition that the applicant concerned must submit a written application to the designated judge concerned within 48 hours after the issuing of the oral direction or oral entry warrant under subsection (7).

(9) Section 16 (5) (b) and (c) , (6) (b) , (c) and (d) and (7), 17 (5) (b) , (c) and (d) and (6), 21 (4) (b) , (5) (b) , (c) , (d) and (e) and (6) or 22 (5) (b) and (c) , (6), (7) and (8), applies, with the necessary changes, in respect of the issuing of an oral direction or oral entry warrant under subsection (7).

(10) A designated judge who issues an oral direction or oral entry warrant under subsection (7) must-

- (a) immediately after the issuing thereof, inform the applicant and, if applicable, the postal service provider or telecommunication service provider to whom it is addressed, orally of such an oral direction or oral entry warrant, including the-
  - (i) contents thereof; and
  - (ii) period for which it has been issued; and
- (b) confirm that oral direction or oral entry warrant in writing within 12 hours after the issuing thereof.

(11) A designated judge who issued-

- (a) a direction or an entry warrant under subsection (3); or
- (b) an oral direction or oral entry warrant under subsection (7),

or, if he or she is not available, any other designated judge who would have been entitled to issue such direction, entry warrant, oral direction or oral entry warrant must, upon

receipt of a written application submitted to him or her in terms of subsection (4) (b) or (8) (b) , reconsider that application whereupon he or she may confirm, amend or cancel that direction, entry warrant, oral direction or oral entry warrant.

- (12) If a direction, entry warrant, oral direction or oral entry warrant is-
- (a) confirmed or amended in terms of subsection (11), the designated judge concerned must forthwith in writing inform-
    - (i) the applicant concerned; and
    - (ii) if applicable, the postal service provider, telecommunication service provider or decryption key holder concerned,
 of such confirmation or amendment; or
  - (b) cancelled in terms of subsection (11), section 25 (3), (4) and (5) applies with the necessary changes.

## 24 Reports on progress

The designated judge who issued a direction or an entry warrant may at the issuing thereof or at any stage before the date of expiry thereof, in writing require the applicant who made the application in respect of the direction or entry warrant concerned to report to him or her in writing-

- (a) at such intervals as he or she determines, on-
  - (i) the progress that has been made towards achieving the objectives of the direction or entry warrant concerned; and
  - (ii) any other matter which the designated judge deems necessary; or
- (b) on the date of expiry of the entry warrant concerned, on whether the interception device has been removed from the premises concerned and, if so, the date of such removal.

## 25 Cancellation of direction, entry warrant, oral direction or oral entry warrant

(1) The designated judge who issued a direction or an entry warrant or, if he or she is not available, any other designated judge who would have been entitled to issue such direction or entry warrant may cancel that direction or entry warrant if-

- (a) the applicant concerned fails to submit a report in terms of section 24, if applicable; or
- (b) he or she, upon receipt of a report submitted in terms of section 24, is satisfied that the-
  - (i) objectives of the direction or entry warrant concerned have been achieved; or
  - (ii) ground on which the direction or the purpose for which the entry warrant concerned was issued, has ceased to exist.

(2) The designated judge who issued-

- (a) a direction or an entry warrant under section 23 (3); or
- (b) an oral direction or oral entry warrant,

or, if he or she is not available, any other designated judge who would have been entitled to issue such a direction, entry warrant, oral direction or oral entry warrant, must cancel that direction, entry warrant, oral direction or oral entry warrant if the applicant

concerned fails to comply with section 23 (4) (b) or (8) (b) .

(3) If a designated judge cancels-

- (a) a direction or an entry warrant;
- (b) a direction or an entry warrant issued under section 23 (3); or
- (c) an oral direction or oral entry warrant,

in terms of subsection (1) or (2), he or she must forthwith in writing inform-

- (i) the applicant concerned; and
- (ii) if applicable, the postal service provider, telecommunication service provider or decryption key holder concerned,

of such cancellation.

(4) If an entry warrant or oral entry warrant is cancelled in terms of subsection (1) or (2), the applicant concerned must, as soon as practicable after having been informed of such cancellation, remove, or cause to be removed, any interception device which has been installed under the entry warrant or oral entry warrant concerned.

(5) If a direction issued under section 23 (3) or an oral direction is cancelled in terms of subsection (2)-

- (a) the contents of any communication intercepted under that direction or oral direction will be inadmissible as evidence in any criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, unless the court is of the opinion that the admission of such evidence would not render the trial unfair or otherwise be detrimental to the administration of justice; or
- (b) any postal article that was taken into possession under that direction or oral direction must be dealt with in accordance with section 26 (4).

## CHAPTER 4

### EXECUTION OF DIRECTIONS AND ENTRY WARRANTS (ss 26-29)

#### 26 Execution of direction

(1) (a) If a direction has been issued under this Act, any-

- (i) law enforcement officer may execute that direction; or
- (ii) law enforcement officer or other person may assist with the execution thereof,

if the law enforcement officer or person concerned has been authorised by the applicant who made the application for the issuing of the direction concerned to execute that direction or to assist with the execution thereof.

(b) A direction issued under this Act upon an application made by an applicant referred to in paragraph (f) of the definition of 'applicant' may only be executed by a law enforcement officer authorised thereto in writing by the applicant concerned, after consultation with the National Commissioner, if that law enforcement officer is a member of the Police Service, or the National Director, if that law enforcement officer is a member of the Directorate or of any component referred to in paragraph (e) of the definition of 'law enforcement agency'.

(2) The applicant concerned may authorise such number of authorised persons to assist with the execution of the direction as he or she deems necessary.

(3) An authorised person who executes a direction or assists with the execution thereof may intercept, at any place in the Republic, any communication in the course of its occurrence or transmission to which the direction applies.

(4) If any postal article has been taken in possession in terms of subsection (3), the authorised person who executes the direction concerned or assists with the execution thereof-

- (a) must take proper care of such postal article and may, if the postal article concerned is perishable, with due regard to the interests of the persons concerned and with the written approval of the applicant concerned, dispose of that postal article in such manner as the circumstances may require;
- (b) must, with the written approval of the applicant concerned, return such postal article, if it has not been disposed of in terms of paragraph (a), or cause it to be returned to the postal service provider concerned if, in the opinion of the applicant concerned-
  - (i) no criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, will be instituted in connection with such postal article; or
  - (ii) such postal article will not be required at any such criminal or civil proceedings for purposes of evidence or for purposes of an order of court; and
  - (iii) such postal article may be returned without prejudice to the public health or safety, national security or compelling national economic interests of the Republic, as the case may be; or
- (c) may, in circumstances other than those referred to in-
  - (i) paragraph (b), with the written approval of the applicant concerned, return such postal article or cause it to be returned to the postal service provider concerned if such postal article-
    - (aa) has not been disposed of in terms of paragraph (a); and
    - (bb) in the opinion of the applicant concerned, may be returned without prejudice to the public health or safety, national security or compelling national economic interests of the Republic, as the case may be; or
  - (ii) paragraph (a), on the written instructions of the applicant concerned dispose of such postal article in such manner as the public health or safety, national security or compelling national economic interests of the Republic, as the case may be, requires, if such postal article-
    - (aa) has not been disposed of in terms of paragraph (a); and
    - (bb) in the opinion of the applicant concerned, cannot be returned in terms of subparagraph (i) without prejudice to the public health or safety, national security or compelling national economic interests of the Republic, as the case may be.

## 27 Execution of entry warrant

If an entry warrant has been issued, any authorised person who executes the interception direction in respect of which that entry warrant has been issued or assists with the execution thereof may, at any time during which the entry warrant is of force, without prior notice enter the premises specified in the entry warrant and perform any act relating to the purpose, referred to in the definition of 'entry warrant', for which the entry warrant concerned has been issued.

## 28 Assistance by postal service provider and telecommunication service provider

(1) If an interception direction or a copy thereof is handed to the postal service provider or telecommunication service provider to whom the interception direction is addressed by the authorised person who executes that interception direction or assists with the execution thereof, the-

- (a) postal service provider concerned must intercept the postal article to which the interception direction applies and hand it to the authorised person concerned; or
- (b) telecommunication service provider concerned must immediately-
  - (i) route the duplicate signals of indirect communications to which that interception direction applies to the designated interception centre concerned; or
  - (ii) make available the necessary assistance and, subject to section 46 (7) (b) , the necessary facilities and devices to enable the authorised person concerned to effect the necessary connections in order to intercept any indirect communications to which the interception direction applies.

(2) If a real-time communication-related direction or an archived communication-related direction or a copy thereof is handed to the telecommunication service provider to whom the real-time communication-related direction or archived communication-related direction is addressed by the authorised person who executes that real-time communication-related direction or archived communication-related direction or assists with the execution thereof, the telecommunication service provider concerned must-

- (a) route the-
  - (i) real-time communication-related information specified in the real-time communication-related direction concerned immediately; or
  - (ii) archived communication-related information specified, and within the period stated, in the archived communication-related direction concerned,

to the designated interception centre concerned; or

- (b) provide the-
  - (i) real-time communication-related information specified in the real-time communication-related direction concerned immediately; or
  - (ii) archived communication-related information specified, and within the period stated, in the archived communication-related direction concerned,

to the law enforcement agency concerned, in the form as specified in that real-time communication-related direction or archived communication-related direction.

## 29 Assistance by decryption key holder

(1) If a decryption direction or a copy thereof is handed to the decryption key holder to whom the decryption direction is addressed by the authorised person who executes that decryption direction or assists with the execution thereof, the decryption key holder concerned must within the period stated in the decryption direction-

- (a) disclose the decryption key; or

- (b) provide the decryption assistance,

specified in the decryption direction concerned, to the authorised person concerned.

(2) In complying with a decryption direction, a decryption key holder-

- (a) must only disclose such decryption key or provide such decryption assistance which is necessary to obtain access to the encrypted information specified in that decryption direction or to put that encrypted information in an intelligible form;
- (b) may only disclose the decryption key or provide the decryption assistance to the authorised person who executes that decryption direction or assists with the execution thereof; and
- (c) may not disclose any other information, which is not specified in that decryption direction, relating to the customer in respect of whose encrypted information the decryption key has been disclosed or the decryption assistance has been provided.

(3) A decryption key holder to whom a decryption direction is addressed and who is in possession of both the encrypted information and the decryption key thereto-

- (a) may use any decryption key in his or her possession to provide decryption assistance; and
- (b) must, in providing such decryption assistance, make a disclosure of the encrypted information in an intelligible form.

(4) A decryption key holder who, in terms of a decryption direction, is required to provide decryption assistance in respect of any encrypted information, will be regarded as having complied with that requirement if he or she-

- (a) instead of providing such decryption assistance, discloses any decryption key to the encrypted information that is in his or her possession; and
- (b) makes such a disclosure, in accordance with the decryption direction concerned, to the authorised person to whom, and by the time by which, he or she was required to provide the decryption assistance.

(5) If a decryption key holder to whom a decryption direction is addressed, is-

- (a) not in possession of the encrypted information; or
- (b) incapable, without the use of a decryption key that is not in his or her possession, to comply fully with that decryption direction,

the decryption key holder concerned must endeavour to comply, to the best of his or her ability, with that decryption direction.

(6) If a decryption key holder to whom a decryption direction is addressed, is in possession of different decryption keys, or combinations of decryption keys, to the encrypted information-

- (a) it will not be necessary, for purposes of complying with the decryption direction concerned, for the decryption key holder to disclose any decryption keys in addition to those the disclosure of which, alone, is sufficient to enable the authorised person to whom they are disclosed to obtain access to the encrypted information and to put it into an intelligible form; or
- (b) the decryption key holder may select which of the decryption keys, or

combination of decryption keys, to disclose for purposes of complying with the decryption direction concerned.

- (7) If a decryption direction is addressed to a decryption key holder who-
- (a) has been in possession of the decryption key to the encrypted information, but is no longer in possession thereof;
  - (b) if he or she had continued to have the decryption key in his or her possession, he or she would have been required by virtue of the decryption direction to disclose it; and
  - (c) is in possession of any information that would facilitate the obtaining or discovery of the decryption key or the provision of decryption assistance,

he or she must disclose all such information as is in his or her possession to the authorised person who executes the decryption direction or assists with the execution thereof.

(8) An authorised person to whom a decryption key has been disclosed under this section-

- (a) may use the decryption key only in respect of the encrypted information, and in the manner and for the purposes, specified in the decryption direction concerned; and
- (b) must, on or before the expiry of the period or extended period for which the decryption direction concerned has been issued, with the written approval of the applicant who made the application for the issuing of a decryption direction, destroy all records of the disclosed decryption key if, in the opinion of the applicant concerned-
  - (i) no criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, will be instituted in connection with such records; or
  - (ii) such records will not be required at any such criminal or civil proceedings for purposes of evidence or for purposes of an order of court.

## CHAPTER 5

### INTERCEPTION CAPABILITY AND COMPENSATION (ss 30-31)

#### **30 Interception capability of telecommunication services and storing of communication-related information**

- (1) Notwithstanding any other law, a telecommunication service provider must-
- (a) provide a telecommunication service which has the capability to be intercepted; and
  - (b) store communication-related information.

(2) The Cabinet member responsible for communications, in consultation with the Minister and the other relevant Ministers and after consultation with the Authority and the telecommunication service provider or category of telecommunication service providers concerned, must, on the date of the issuing of a telecommunication service licence under the Electronic Communications Act, to such a telecommunication service provider or category of telecommunication service providers-

- (a) issue a directive in respect of that telecommunication service provider or category of telecommunication service providers, determining the-



- (i) manner in which effect is to be given to subsection (1) by the telecommunication service provider or category of telecommunication service providers concerned;
  - (ii) security, technical and functional requirements of the facilities and devices to be acquired by the telecommunication service provider or category of telecommunication service providers to enable the-
    - (aa) interception of indirect communications in terms of this Act; and
    - (bb) storing of communication-related information in terms of subsection (1) (b) ; and
  - (iii) type of communication-related information which must be stored in terms of subsection (1) (b) and the period for which such information must be stored, which period may, subject to subsection (8), not be less than three years and not more than five years from the date of the transmission of the indirect communication to which that communication-related information relates; and
- (b) determine a period, which may not be less than three months and not more than six months from the date on which a directive referred to in paragraph (a) is issued, for compliance with such a directive, and the period so determined must be mentioned in the directive concerned.

[Sub-s. (2) amended by s. 97 of Act 36 of 2005.]

(3) A directive referred to in subsection (2) (a) -

- (a) must, where applicable, prescribe the-
  - (i) capacity needed for interception purposes;
  - (ii) technical requirements of the systems to be used;
  - (iii) connectivity with interception centres;
  - (iv) manner of routing duplicate signals of indirect communications to designated interception centres in terms of section 28 (1) (b) (i); and
  - (v) manner of routing real-time or archived communication-related information to designated interception centres in terms of section 28 (2) (a) ; and
- (b) may prescribe any other matter which the Cabinet member responsible for communications, in consultation with the Minister and the other relevant Ministers and after consultation with the Authority, deems necessary or expedient.

(4) Notwithstanding any other law, agreement or licence, a telecommunication service provider must, subject to section 46 (1) (a) , at own cost acquire, whether by purchasing or leasing, the facilities and devices determined in a directive referred to in subsection (2) (a) .

(5) Any costs incurred by a telecommunication service provider under this Act in-

- (a) enabling-
  - (i) a telecommunication service to be intercepted; and
  - (ii) communication-related information to be stored,

- including the investment, technical, maintenance and operating costs; and
- (b) complying with section 28 (1) (b) (i) and (2) (a) ,

must be borne by that telecommunication service provider.

(6) A directive issued under subsection (2) (a) may in like manner be amended or withdrawn.

(7) The Cabinet member responsible for communications must, within two months after the fixed date and in consultation with the Minister and the other relevant Ministers and after consultation with the Authority and a telecommunication service provider or category of telecommunication service providers to whom, prior to the fixed date, a telecommunication service licence has been issued under the Electronic Communications Act-

- (a) issue a directive referred to in subsection (2) (a) in respect of such a telecommunication service provider or category of telecommunication service providers; and
- (b) determine a period, which may not be less than three months and not more than six months from the date on which a directive referred to in paragraph (a) is issued, for compliance with such a directive, and the period so determined must be mentioned in the directive concerned.

[Sub-s. (7) amended by s. 97 of Act 36 of 2005.]

(8) If a period of more than three years has been determined in terms of subsection (2) (a) (iii), the Cabinet member responsible for communications may, upon application by the telecommunication service provider concerned and in consultation with the relevant Ministers, reduce that period to a period which may not be less than three years by issuing an amended directive under subsection (2) (a) .

### **31 Compensation payable to postal service provider, telecommunication service provider and decryption key holder**

(1) (a) The Minister, after consultation with the Cabinet members responsible for communications and national financial matters and the postal service providers or telecommunication service providers concerned, as the case may be, must by notice in the *Gazette* prescribe-

- (i) the forms of assistance in the execution of a direction for which a postal service provider, telecommunication service provider or decryption key holder must be compensated; and
- (ii) reasonable tariffs of compensation payable to a postal service provider, telecommunication service provider or decryption key holder for providing such prescribed forms of assistance.

(b) The tariffs prescribed under paragraph (a) (ii)-

- (i) may differ in respect of different categories of postal service providers, telecommunication service providers or decryption key holders; and
- (ii) must be uniform in respect of each postal service provider, telecommunication service provider or decryption key holder falling within the same category.

(c) A notice issued under paragraph (a) may at any time in like manner be amended or withdrawn.

(d) The first notice to be issued under paragraph (a) must be published in the *Gazette* within three months after the fixed date.

(2) The forms of assistance referred to in subsection (1) (a) (i) must include, in the case of a-

- (a) telecommunication service provider, the making available of a facility, device or telecommunication system; and
- (b) decryption key holder, the-
  - (i) disclosure of a decryption key; and
  - (ii) provision of decryption assistance.

(3) The compensation payable to a postal service provider, telecommunication service provider or decryption key holder in terms of this section will only be for direct costs incurred in respect of personnel and administration which are required for purposes of providing any of the forms of assistance contemplated in subsection (1) (a) (i).

(4) Any notice issued under subsection (1) must, before publication thereof in the *Gazette*, be submitted to Parliament.

## CHAPTER 6

### INTERCEPTION CENTRES, OFFICE FOR INTERCEPTION CENTRES AND INTERNET SERVICE PROVIDERS ASSISTANCE FUND (ss 32-38)

#### 32 Establishment of interception centres

(1) The Minister, in consultation with the relevant Ministers and the Cabinet member responsible for national financial matters, must, at State expense-

- (a) establish one or more centres, to be known as interception centres, for the interception of communications in terms of this Act;
- (b) equip, operate and maintain such interception centres;
- (c) acquire, install and maintain connections between telecommunication systems and interception centres; and
- (d) administer the interception centres.

(2) The Minister must exercise final responsibility over the administration and functioning of interception centres.

(3) Notwithstanding the Electronic Communications Act, an interception centre will, for purposes of performing its functions in terms of this Act, be exempted from-

- (a) obtaining any kind of licence required by that Act; and
- (b) paying any fees payable in terms of that Act.

[Sub-s. (3) amended by s. 97 of Act 36 of 2005.]

(4) The Minister must enter into service level agreements with the relevant Ministers in respect of the provision of services by the interception centres to the law enforcement agencies.

(5) The Executive Director may enter into agreements with the National Commissioner and National Director to make use of the services of interception centres, including the cost thereof.

#### 33 Establishment of Office for Interception Centres

There is hereby established an office to be known as the Office for Interception Centres.

### **34 Director and staff of Office**

(1) The Minister and the relevant Ministers must, from among their respective Departments, second a member or an officer to the Office as the Director: Office for Interception Centres, who will be the head of the Office.

(2) The Director may exercise the powers and must perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Minister or under this Act, subject to the control and directions of the Minister.

(3) Whenever the Director is for any reason unable to exercise, perform and carry out his or her powers, functions and duties or when the secondment of a member or an officer as Director is pending, the Minister and the relevant Ministers may, from among their respective Departments, designate a member or an officer to the Office as Acting Director, to exercise the powers, perform the functions and carry out the duties of the Director.

(4) The Director will in the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Minister or under this Act, be assisted, subject to his or her control and directions, by-

- (a) members of the law enforcement agencies, seconded or designated to the Office for that purpose by the-
  - (i) National Commissioner;
  - (ii) Secretary for Defence;
  - (iii) Director-General: National Intelligence Agency;
  - (iv) Director-General: South African Secret Service; and
  - (v) National Director; and
- (b) officers of any other Department of State seconded to the Office, for a particular service.

(5) A member or an officer may only be seconded or designated as contemplated in this section and section 36-

- (a) in terms of the laws regulating such secondment;
- (b) with his or her consent; and
- (c) after a security clearance has been issued by the Agency in respect of that member or officer.

### **35 Powers, functions and duties of Director**

(1) In order to achieve the objects of this Act, the Director-

- (a) must carry out the administrative duties relating to the functioning of the Office;
- (b) must exercise control over heads of interception centres and staff of the Office;
- (c) must manage, and exercise administrative control over, interception centres;
- (d) must regulate the procedure and determine the manner in which the provisions of this Act must be carried out by interception centres;

- (e) must co-ordinate the activities of interception centres;
- (f) must prescribe the information to be kept by the head of an interception centre in terms of section 37, which must include particulars relating to-
  - (i) applications for the issuing of directions and the directions issued upon such applications which is relevant to the interception centre of which he or she is the head; and
  - (ii) the results obtained from every direction executed at that interception centre;
- (g) must prescribe the manner in, and the period for, which such information must be kept; and
- (h) is, for purposes of the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Minister or under this Act, accountable to the Minister.

(2) A member or an officer seconded or designated in terms of section 34 (4) may exercise the powers and must perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Director, subject to the control and directions of the Director.

(3) The law enforcement agencies and other Departments of State must render such assistance as may be reasonably required in the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon the Director by the Minister or under this Act.

### **36 Head and staff of interception centres**

(1) The Minister must in respect of every interception centre to be established by section 32 (1) (a) , request the persons referred to in section 34 (4) (a) (i) to (v) to second a member or an officer from among their respective Departments to such interception centre as head of the interception centre in terms of the laws regulating such secondment.

(2) The head of an interception centre may exercise the powers and must perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Director or under this Act, subject to the control and directions of the Director.

(3) Whenever the head of an interception centre is for any reason unable to exercise, perform and carry out his or her powers, functions and duties or when the secondment of a member or an officer as head of an interception centre is pending, the Minister may request the persons referred to in section 34 (4) (a) (i) to (v), to designate, from among their respective Departments, a member or an officer to that interception centre as acting head of the interception centre concerned, to exercise the powers, perform the functions and carry out the duties of the head of that interception centre.

(4) The head of an interception centre will in the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Director or under this Act, be assisted, subject to his or her control and directions, by-

- (a) members of the law enforcement agencies, seconded or designated to the interception centre concerned for that purpose by the persons referred to in section 34 (4) (a) (i) to (v); and
- (b) officers of any other Department of State seconded to the Office, for a particular service.

(5) A member or an officer seconded or designated in terms of subsection (4) may exercise the powers and must perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Director or the head of the interception centre concerned, subject to the control and directions of the head of the interception centre concerned.

(6) In order to achieve the objects of this Act, the head of an interception centre must exercise control over members and officers seconded or designated to the interception centre in terms of subsection (4).

### **37 Keeping of records by heads of interception centres and submission of reports to Director**

(1) The head of an interception centre must keep or cause to be kept proper records of such information as may be prescribed by the Director in terms of section 35 (1) (f) .

(2) (a) The head of an interception centre must on a quarterly basis, or as often as the Director requires, submit a written report to the Director on-

- (i) the records kept by him or her in terms of subsection (1);
- (ii) any abuses in connection with the execution of directions which he or she is aware of;
- (iii) any defects in any telecommunication system or in the operation of the interception centre which have been discovered; and
- (iv) such activities at the interception centre or on any other matter relating to this Act which the Director requests the head of the interception centre to deal with in such report.

(b) Notwithstanding paragraph (a) , a head of an interception centre may at any stage submit a report to the Director on any matter which, in the opinion of the head concerned, should urgently be brought to the attention of the Director.

(3) The Director must, upon receipt of a report contemplated in subsection (2) (a) , submit a copy of that report to the Minister and the Chairperson of the Joint Standing Committee on Intelligence established by section 2 of the Intelligence Services Control Act, 1994 ( Act 40 of 1994 ).

### **38 Establishment and control of Internet Service Providers Assistance Fund**

(1) There is hereby established a fund to be known as the Internet Service Providers Assistance Fund.

(2) The Fund will be credited with-

- (a) the contributions referred to in section 46 (1) (b) ;
- (b) interest derived from the investment of money in the Fund; and
- (c) money accruing to the Fund from any other source.

(3) The money in the Fund must be utilised for-

- (a) acquiring, whether by purchasing or leasing, facilities and devices for purposes of section 46 (7) (b) ; and
- (b) the expenses involved in the control and management of the Fund.

(4) The Director is the accounting officer of the Fund in terms of the Public Finance

Management Act, 1999 ( Act 1 of 1999 ).

(5) The Fund is, subject to the directions of the Minister, in consultation with the relevant Ministers, under the control and management of the Director, who-

- (a) must utilise the money in the Fund in accordance with subsection (3);
- (b) will be charged with the responsibility of accounting for money received in, and payments made from, the Fund; and
- (c) must cause the necessary accounting and other related records to be kept.

(6) The Minister, in consultation with the relevant Ministers, must make recommendations to the Director relating to the utilisation of the money in the Fund as contemplated in subsection (3) (a) .

(7) Any money in the Fund which is not required for immediate use must be invested by the Director with a banking institution approved by the Minister, in consultation with the Cabinet member responsible for national financial matters, and may be withdrawn when required.

(8) Any unexpended balance of the money in the Fund at the end of any financial year must be carried forward as a credit in the Fund to the next financial year.

(9) The Fund and the records referred to in subsection (5) (c) must be audited by the Auditor-General.

## **CHAPTER 7**

### **DUTIES OF TELECOMMUNICATION SERVICE PROVIDER AND CUSTOMER (ss 39-41)**

#### **39 Information to be obtained and kept by certain telecommunication service providers**

(1) Before a telecommunication service provider, other than a telecommunication service provider who provides a mobile cellular telecommunication service, enters into a contract with any person for the provision of a telecommunication service to that person, he or she-

- (a) must, if that person is a natural person-
  - (i) obtain from him or her-
    - (aa) his or her full names, identity number, residential and business or postal address, whichever is applicable; and
    - (bb) a certified photocopy of his or her identification document on which his or her photo, full names and identity number, whichever is applicable, appear;
  - (ii) retain the photocopy obtained in terms of subparagraph (i) (bb) ; and
  - (iii) verify the photo, full names and identity number, whichever is applicable, of that person with reference to his or her identification document; or
- (b) must, if that person is a juristic person-
  - (i) obtain from the person representing that juristic person-
    - (aa) his or her full names, identity number, residential and postal address, whichever is applicable;
    - (bb) the business name and address and, if registered as such in terms of any law, the registration number of that

juristic person;

- (cc) a certified photocopy of his or her identification document on which his or her photo, full names and identity number, whichever is applicable, appear; and
- (dd) a certified photocopy of the business letterhead of, or other similar document relating to, that juristic person;
- (ii) retain the photocopies obtained in terms of subparagraph (i) (cc) and (dd) ; and
- (iii) verify the-
  - (aa) photo, full names and identity number, whichever is applicable, of that person with reference to his or her identification document; and
  - (bb) name and registration number of that juristic person with reference to its business letterhead or other similar document; and
- (c) may obtain from such person any other information which the telecommunication service provider deems necessary for purposes of this Act.

(2) A telecommunication service provider referred to in subsection (1) must ensure that proper records are kept of-

- (a) the information, including the photocopies, referred to in subsection (1) and, where applicable, any change in such information which is brought to his or her attention;
- (b) the telephone number or any other number allocated to the person concerned; and
- (c) any other information in respect of the person concerned which the telecommunication service provider concerned may require in order to enable him or her to identify that person.

(3) An applicant may, for purposes of making an application for the issuing of a direction, in writing request a telecommunication service provider referred to in subsection (1) to-

- (a) confirm that the person specified in the request is a customer of that telecommunication service provider concerned;
- (b) provide the applicant with the telephone number or any other number allocated to that person by that telecommunication service provider; and
- (c) furnish the applicant with a photocopy of the identification document of that person which is retained by that telecommunication service provider in terms of subsection (1) (a) (ii).

(4) A telecommunication service provider who receives a request referred to in subsection (3) must immediately comply with that request if the person specified in the request is a customer of the telecommunication service provider concerned.

#### **40 Information to be obtained and kept by electronic communication service provider who provides a mobile cellular electronic communications service**

(1) (a) Subject to paragraph (b) , an electronic communication service provider who provides a mobile cellular electronic communications service shall not activate a SIM-card on its electronic communication system unless subsection (2) has been complied with.



(b) Paragraph (a) does not apply to a customer of an electronic communication service provider who provides a mobile cellular electronic communications service outside the Republic who enters the geographical coverage area of a mobile cellular electronic communication service provider in the Republic and uses the electronic communication system of such provider to make, receive and send voice calls or data or access other services.

(2) From the date of commencement of this section an electronic communication service provider must, subject to subsection (4), at own cost implement a process to record and store, and must record and store-

- (a) the Mobile Subscriber Integrated Service Digital Network number (MSISDN-number) of the SIM-card that is to be activated by an electronic communication service provider at the request of a person contemplated in paragraphs (b) and (c) ;
- (b) in the case of a person who-
  - (i) is a South African citizen or is lawfully and permanently resident in the Republic, the full names and surname, identity number and at least one address of such person who requests that a SIM-card referred to in subsection (1) be activated on the electronic communication system of an electronic communication service provider; or
  - (ii) is not a South African citizen or who is not permanently resident in the Republic, and who requests that a SIM-card referred to in subsection (1) be activated on the electronic communication system of an electronic communication service provider, the full names and surname, identity number and at least one address of such person and the country where the passport was issued; or
- (c) in the case of a juristic person-
  - (i) the full names, surname, identity number and an address of the authorised representative of the juristic person; and
  - (ii) the name and address of the juristic person and, where applicable, the registration number of the juristic person.

(3) (a) For the purposes of subsection (2), an electronic communication service provider must, in the manner provided for in paragraph (b) , verify-

- (i) the full names, surname, identity number and identity of the person contemplated in subsection (2) (b) and (c) and, where applicable, the country where the passport was issued;
- (ii) the name and, where applicable, the registration number of the juristic person;
- (iii) in the case of a person contemplated in subsection (2) (b) (i) and (c) , the address; and
- (iv) the authority of the representative of a juristic person.

(b) An electronic communication service provider must verify-

- (i) the information contemplated in paragraph (a) (i) by means of an identification document;
- (ii) the information contemplated in paragraph (a) (ii) by means of documentation, including a registration document, founding statement, document issued by the South African Revenue Service or

any other similar document;

- (iii) the address contemplated in paragraph (a) (iii) by means of documentation, including a bank statement, a municipal rates and taxes invoice, telephone or cellular phone account of not older than three months, or any other utility bill or an account of a retailer of not older than three months, or an existing lease, rental or credit sale agreement, insurance policy, a current television licence or a new motor vehicle licence document; and
- (iv) the authority of the representative of the juristic person by means of a letter of authority or an affidavit.

(4) (a) An electronic communication service provider must ensure that-

- (i) the process contemplated in subsection (2);
- (ii) the information recorded and stored in terms of that subsection; and
- (iii) the facility in or on which the information is recorded and stored,

are secure and only accessible to persons specifically designated by that electronic communication service provider.

(b) The Minister may, in consultation with the Cabinet member responsible for communications, by notice in the *Gazette*, determine security standards relating to the matters contemplated in paragraph (a).

(5) From the date of commencement of this section, any customer who sells or in any manner provides an activated SIM-card to a person, other than a family member, and the person who is to receive the SIM-card must, immediately upon the sale or provision of the SIM-card, provide the relevant electronic communication service provider with-

- (a) the full names, surname and identity number of the customer; and
- (b) all particulars as required in subsection (2) in respect of the person who is to receive the SIM-card.

(6) (a) An electronic communication service provider must, upon receipt of the information provided in terms of subsection (5)-

- (i) verify the full names, surname, identity number and identity of the persons with reference to the persons' identification documents;
- (ii) verify the address, contemplated in subsection (3) (a) (iii), of the person who is to receive the SIM-card by means of the documents contemplated in subsection (3) (b) (iii); and
- (iii) verify the particulars contemplated in subsection (2) (a).

(b) An electronic communication service provider must, upon receipt of the information provided in terms of paragraph (a), immediately record and store the information as contemplated in subsection (2).

(7) (a) An applicant may, for the purposes of making an application for the issuing of a direction, in writing, request an electronic communication service provider to-

- (i) confirm that the person specified in the request is or was a customer of that electronic communication service provider; and
- (ii) provide the applicant with the information recorded and stored in terms of subsection (2).

(b) An electronic communication service provider who receives a request referred to in paragraph (a) must immediately comply with that request if the person specified in the request is or was a customer of the electronic communication service provider concerned.

(8) If an employee or agent of an electronic communication service provider knows or suspects that an identification document submitted for verification as contemplated in subsection (3) is false, he or she must, within 24 hours, report the matter to a police official at any police station.

(9) An electronic communication service provider must, on its electronic communication system, record and store-

- (a) every MSISDN-number used with every IMEI-number; and
- (b) every IMEI-number used with every MSISDN-number,

which must, on production of a direction, be provided to an applicant within 12 hours.

(10) The information recorded and stored in terms of subsections (2), (6) and (9) must be stored by an electronic communication service provider for a period of five years after-

- (a) a customer has cancelled his or her contract with the electronic communication service provider; or
- (b) the electronic communication service provider has ended the electronic communications service provided to the customer.

[S. 40 substituted by s. 2 of Act 48 of 2008.]

[Date of commencement of s. 40: 1 July 2009.]

#### **41 Loss, theft or destruction of cellular phone or SIM-card to be reported**

(1) Whenever a cellular phone or SIM-card is lost, stolen or destroyed, the owner of that cellular phone or SIM-card, or any other person who was in possession, or had control, thereof when it was so lost, stolen or destroyed, must within a reasonable time after having reasonably become aware of the loss, theft or destruction of the cellular phone or SIM-card, report such loss, theft or destruction in person or through a person authorised thereto by him or her, to a police official at any police station.

(2) A police official who receives a report contemplated in subsection (1), must immediately provide the person who makes the report with written proof that the report has been made or, in the case of a telephonic report, with the official reference number of the report.

(3) A record of every report made in terms of subsection (1) must be kept at the police station where such a report has been made.

(4) (a) The Minister must, within three months after the fixed date and in consultation with the Cabinet member responsible for policing, issue directives prescribing the-

- (i) form and manner in which-
  - (aa) a report contemplated in subsection (1) must be made; and
  - (bb) records contemplated in subsection (3) must be kept; and
- (ii) information to be contained in such a report or record.

(b) Any directive issued under paragraph (a) may at any time in like manner be amended or withdrawn.

(c) Any directive issued under paragraph (a) must, before the implementation thereof,

be submitted to Parliament.

## CHAPTER 8 GENERAL PROHIBITIONS AND EXEMPTIONS (ss 42-46)

### 42 Prohibition on disclosure of information

(1) 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 this Act, except-

- (a) to any other person who of necessity requires it for the performance of his or her functions in terms of this Act;
- (b) if he or she is a person who of necessity supplies it in the performance of his or her functions in terms of this Act;
- (c) information which is required in terms of any law or as evidence in any court of law; or
- (d) to any competent authority which requires it for the institution, or an investigation with a view to the institution, of any criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act.

(2) No-

- (a) postal service provider, telecommunication service provider or decryption key holder 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 this Act; or
- (b) employee of a postal service provider, telecommunication service provider or decryption key holder may disclose any information which he or she obtained in the course of his or her employment and which is connected with the exercising of any power or the performance of any duty in terms of this Act, whether that employee is involved in the exercising of that power or the performance of that duty or not,

except for the purposes mentioned in subsection (1).

(3) The information contemplated in subsections (1) and (2) includes information relating to the fact that-

- (a) a direction has been issued under this Act;
- (b) a communication is being or has been or will probably be intercepted;
- (c) real-time or archived communication-related information is being or has been or will probably be provided;
- (d) a decryption key is being or has been or will probably be disclosed or that decryption assistance is being or has been or will probably be provided; and
- (e) an interception device is being or has been or will probably be installed.

### 43 Disclosure of information by authorised person for performance of official duties

Notwithstanding section 42 (1), any authorised person who executes a direction or assists with the execution thereof and who has obtained knowledge of-

- (a) the contents of any communication intercepted under that direction, or evidence derived therefrom; or

- (b) real-time or archived communication-related information provided under that direction,

may-

- (i) disclose such contents or evidence or real-time or archived communication-related information to another law enforcement officer, to the extent that such disclosure is necessary for the proper performance of the official duties of the authorised person making or the law enforcement officer receiving the disclosure; or
- (ii) use such contents or evidence or real-time or archived communication-related information to the extent that such use is necessary for the proper performance of his or her official duties.

#### 44 Listed equipment

(1) (a) The Minister must, by notice in the *Gazette*, declare any electronic, electro-magnetic, acoustic, mechanical or other instrument, device or equipment, the design of which renders it primarily useful for purposes of the interception of communications, under the conditions or circumstances specified in the notice, to be listed equipment.

(b) A notice issued under paragraph (a) may at any time in like manner be amended or withdrawn.

(c) The first notice to be issued under paragraph (a) must be published in the *Gazette* within three months after the fixed date.

(2) (a) Before the Minister exercises the powers conferred upon him or her by subsection (1), he or she must-

- (i) consult the relevant Ministers; and
- (ii) cause to be published in the *Gazette* a draft of the proposed notice, together with a notice inviting all interested parties to submit to him or her in writing and within a specified period, comments and representations in connection with the proposed notice.

(b) A period of not less than one month must elapse between the publication of the draft notice and the notice under subsection (1).

(3) Subsection (2) does not apply-

- (a) if the Minister, in pursuance of comments and representations received in terms of subsection (2) (a) (ii), decides to publish a notice referred to in subsection (1) in an amended form; and
- (b) to any declaration in terms of subsection (1) in respect of which the Minister is of the opinion that the public interest requires that it be made without delay.

(4) Any notice issued under subsection (1) must, before publication thereof in the *Gazette*, be submitted to Parliament.

#### 45 Prohibition on manufacture, possession and advertising of listed equipment

(1) Subject to subsection (2) and section 46, no person may manufacture, assemble, possess, sell, purchase or advertise any listed equipment.

(2) Subsection (1) does not apply to any telecommunication service provider or other person who, or law enforcement agency which, manufactures, assembles, possesses,

sells, purchases or advertises listed equipment under the authority of a certificate of exemption issued to him or her or it for that purpose by the Minister under section 46.

#### 46 Exemptions

(1) (a) The Minister may, upon application and in consultation with the relevant Ministers, exempt any-

- (i) Internet service provider from complying with section 30 (4) in respect of the facilities and devices referred to in section 30 (2) (a) (ii);
- (ii) telecommunication service provider or any other person from one or all of the prohibited acts referred to in section 45 (1); or
- (iii) law enforcement agency from the prohibited acts of possessing and purchasing referred to in section 45 (1),

for such period and on such conditions as the Minister determines.

(b) A condition referred to in paragraph (a) may include that an Internet service provider to whom an exemption has been granted under paragraph (a) (i) must pay as an annual contribution to the Fund such amount as the Minister determines in each case.

(2) The Minister may only grant an exemption under subsection (1) (a) if he or she is satisfied that-

- (a) in the case of an exemption under subsection (1) (a) (i), the Internet service provider concerned carries on such a small business that he or she cannot comply with section 30 (4); or
- (b) in the case of an exemption under subsection (1) (a) (ii), the purpose for which the listed equipment will be manufactured, assembled, possessed, sold, purchased or advertised is reasonably necessary; and
- (c) such exemption is in the public interest; or
- (d) special circumstances exist which justify such exemption.

(3) (a) An exemption under subsection (1) (a) must be granted by issuing to the-

- (i) Internet service provider;
- (ii) telecommunication service provider or other person; or
- (iii) law enforcement agency,

concerned, a certificate of exemption in which his or her or its name and the scope, period and conditions of the exemption are specified.

(b) A certificate of exemption issued under paragraph (a) -

- (i) must be published in the *Gazette* ; and
- (ii) becomes valid upon the date of such publication.

(4) (a) The Minister must, before he or she publishes a certificate of exemption in terms of subsection (3) (b) (i), table such certificate in the National Assembly for approval.

(b) The National Assembly may reject a certificate tabled in terms of paragraph (a) within two months after it has been tabled, if Parliament is then in ordinary session, or, if Parliament is not then in ordinary session, within 14 days after the commencement of its

next ensuing ordinary session.

(c) If the National Assembly rejects such a certificate, the Minister may table an amended certificate in the National Assembly.

(d) If the Minister tables an amended certificate and the National Assembly-

- (i) approves the amended certificate, the Minister must publish that certificate in terms of subsection (3) (b) (i) within one month of the National Assembly's approval; or
- (ii) rejects the amended certificate within two months after it has been tabled, if Parliament is then in ordinary session, or, if Parliament is not then in ordinary session, within 14 days after the commencement of its next ensuing ordinary session, paragraph (c) and this paragraph apply.

(e) If the National Assembly does not reject a certificate as contemplated in paragraph (b) or (d) (ii)-

- (i) such certificate will be deemed to have been approved by the National Assembly; and
- (ii) the Minister must publish that certificate in terms of subsection (3) (b) (i) within one month thereafter.

(5) A certificate of exemption contemplated in subsection (3) may at any time in like manner be amended or withdrawn by the Minister.

(6) An exemption under subsection (1) (a) lapses upon-

- (a) termination of the period for which it was granted; or
- (b) withdrawal of the relevant certificate under subsection (5).

(7) If an exemption has been granted to an Internet service provider under subsection (1) (a) (i)-

- (a) that Internet service provider will be subject to all the other applicable provisions of this Act; and
- (b) the law enforcement agency which made the application for the issuing of the direction which is addressed to such Internet service provider, must make available the necessary facilities and devices to execute that direction.

## CHAPTER 9

### CRIMINAL PROCEEDINGS, OFFENCES AND PENALTIES (ss 47-57)

#### 47 Use of information in criminal proceedings

(1) Information regarding the commission of any criminal offence, obtained by means of any interception, or the provision of any real-time or archived communication-related information, under this Act, or any similar Act in another country, may be admissible as evidence in criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act.

(2) Any information obtained by the application of this Act, or any similar Act in another country, may only be used as evidence in any criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, with the written authority of the National Director, or any member of the prosecuting authority authorised thereto in writing by the National Director.

#### 48 Proof of certain facts by certificate

Whenever in any criminal proceedings or civil proceedings in terms of Chapter 5 or 6 of the Prevention of Organised Crime Act, the question arises whether a designated judge, judge of a High Court, regional magistrate or magistrate has issued a direction under this Act, a certificate signed by a designated judge, judge of a High Court, regional magistrate or magistrate in which he or she-

- (a) alleges that he or she has received and considered an application made to him or her in terms of this Act;
- (b) alleges that he or she has issued a direction under this Act; and
- (c) specifies the contents of such direction,

shall, upon its mere production at such proceedings, be *prima facie* proof that the designated judge, judge of a High Court, regional magistrate or magistrate concerned received and considered such application, issued such direction and of the contents thereof.

#### **49 Unlawful interception of communication**

(1) Any person who intentionally intercepts or attempts to intercept, or authorises or procures 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, is guilty of an offence.

(2) Subsection (1) does not apply to the-

- (a) interception of a communication as contemplated in sections 3, 4, 5, 6, 7, 8 and 9; or
- (b) monitoring of a signal or radio frequency spectrum as contemplated in sections 10 and 11.

#### **50 Unlawful provision of real-time or archived communication-related information**

(1) Any telecommunication service provider or employee of a telecommunication service provider who intentionally provides or attempts to provide any real-time or archived communication-related information to any person other than the customer of the telecommunication service provider concerned to whom such real-time or archived communication-related information relates, is guilty of an offence.

(2) Subsection (1) does not apply to the provision of real-time or archived communication-related information as contemplated in sections 13, 14 and 15.

#### **51 Offences and penalties**

(1) (a) Any person who-

- (i) contravenes or fails to comply with section 6 (2), 7 (4), 8 (4), 29 (8), 42 (1) or 45 (1);

[Sub-para. (i) substituted by s. 3 (a) of Act 48 of 2008.]

- (ii) in any application made in terms of this Act, furnishes information or makes a statement, knowing such information or statement to be false, incorrect or misleading or not believing it to be correct;
- (iii) acts contrary to the authority of any direction issued under this Act or proceeds to act under any such direction knowing that it has expired;
- (iv) acts contrary to the authority of an entry warrant issued under this Act or, without being authorised thereto under an entry warrant, enters any premises for purposes of intercepting a postal article or communication, or installing and maintaining an interception device, on that premises;



- (v) forges or, with the intent to deceive, alters or tampers with any direction or entry warrant issued under this Act;
- (vi) furnishes particulars or information in any affidavit or report referred to in this Act, knowing such particulars or information to be false, incorrect or misleading or not believing it to be correct; or
- (vii) obstructs, hinders or interferes with an authorised person who executes any direction or entry warrant issued under this Act or assists with the execution thereof, in the exercising of his or her powers under that direction or entry warrant,

is guilty of an offence.

- (b) Any person who is convicted of an offence referred to in-
  - (i) paragraph (a) or in section 49 (1) or 54, is liable to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years; or
  - (ii) section 52, 53 (1) or 55 (1), is liable to a fine or to imprisonment for a period not exceeding two years.
- (2) (a) Any postal service provider or employee of a postal service provider who-
  - (i) contravenes or fails to comply with section 28 (1) (a) ;
  - (ii) contravenes or fails to comply with section 42 (2); or
  - (iii) performs an act contemplated in subsection (1) (a) (iii), (v) or (vii),

is guilty of an offence.

- (b) Any postal service provider or employee of a postal service provider who is convicted of an offence referred to in paragraph (a) is liable, in the case of-
  - (i) a postal service provider who is a-
    - (aa) natural person, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years; or
    - (bb) juristic person, to a fine not exceeding R5 000 000; or
  - (ii) an employee, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years.

- (3) (a) Any telecommunication service provider or employee of a telecommunication service provider who-
  - (i) contravenes or fails to comply with section 7 (2), 8 (3), 28 (1) (b) or (2), 30 (1) or 39 (4);
  - (ii) contravenes or fails to comply with section 30 (4);
  - (iii) contravenes or fails to comply with section 7 (5), 8 (5), 39 (1) or (2) or 42 (2); or
  - (iv) performs an act contemplated in subsection (1) (a) (iii), (v) or (vii),

is guilty of an offence.

- (b) Any telecommunication service provider or employee of a telecommunication service provider who is convicted of an offence referred to in paragraph (a) or in section 50 (1), is liable, in the case of-
  - (i) a telecommunication service provider who is a-

- (ii)
    - (aa) natural person, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years; or
    - (bb) juristic person, to a fine not exceeding R5 000 000; or
- an employee, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years.

- (3A) Any electronic communication service provider who fails to comply with-
- (a) the directives issued in terms of section 30 (2) (a) ;
  - (b) section 40 (1), (2), (3), (4) or any determination made thereunder, (6), (7), (9) or (10); or
  - (c) section 62 (6) (a) , (b) , (c) or (d) ,

is guilty of an offence and liable on conviction to a fine not exceeding R100 000 for each day on which such failure to comply continues.

[Sub-s. (3A) inserted by s. 3 (b) of Act 48 of 2008.]

(3B) Any customer or person who fails to comply with section 40 (5) is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding 12 months.

[Sub-s. (3B) inserted by s. 3 (b) of Act 48 of 2008.]

(3C) An employee or agent of an electronic communication service provider who fails to comply with section 40 (8), is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding 12 months.

[Sub-s. (3C) inserted by s. 3 (b) of Act 48 of 2008.]

- (3D) Any-
- (a) juristic person contemplated in section 62C (1); or
  - (b) person contemplated in section 62C (2),

who fails to comply with section 62C, is guilty of an offence and liable on conviction to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years.

[Sub-s. (3D) inserted by s. 3 (b) of Act 48 of 2008.]

- (4) (a) Any decryption key holder or any employee of a decryption key holder who-
- (i) contravenes or fails to comply with section 29 (1);
  - (ii) contravenes or fails to comply with section 29 (2), (3) (b) , (5) or (7) or 42 (2); or
  - (iii) performs an act contemplated in subsection (1) (a) (iii), (v) or (vii),

is guilty of an offence.

(b) Any decryption key holder or employee of a decryption key holder who is convicted of an offence referred to in paragraph (a) is liable, in the case of-

- (i) a decryption key holder who is a-
  - (aa) natural person, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years; or
  - (bb) juristic person, to a fine not exceeding R5 000 000; or
- (ii) an employee, to a fine not exceeding R2 000 000 or to imprisonment for a

period not exceeding 10 years.

(5) A conviction of an offence referred to in-

- (a) subsection (2) (a) (i) does not relieve any postal service provider or any employee of such a postal service provider of the obligation to comply with section 28 (1) (a) ;
- (b) subsection (3) (a) (i) or (ii) does not relieve any telecommunication service provider or any employee of such a telecommunication service provider of the obligation to comply with section 28 (1) (b) or (2), 30 (1) or (4) or 39 (4);
- (b A ) subsection (3A) does not relieve any electronic communication service provider of the obligation to comply with-
  - (i) the directives issued in terms of section 30 (2) (a) ;
  - (ii) section 40 (1), (2), (3), (4) or any determination made thereunder, (6), (7), (9) or (10); or
  - (iii) section 62 (6) (a) , (b) , (c) or (d) ; or

[Para. (b A ) inserted by s. 3 (c) of Act 48 of 2008.]
- (c) subsection (4) (a) (i) does not relieve any decryption key holder or any employee of such a decryption key holder of the obligation to comply with section 29 (1).

(6) Notwithstanding anything to the contrary in any other law contained, a magistrate's court may impose any penalty provided for in this Act.

(7) No person who-

- (a) in good faith assists an authorised person with the execution of a direction; and
- (b) believes on reasonable grounds that such authorised person is acting in accordance with such a direction,

is liable to prosecution for a contravention of this Act.

## **52 Failure to give satisfactory account of possession of cellular phone or SIM-card**

Any person who is found in possession of any cellular phone or SIM-card in regard to which there is reasonable suspicion that it has been stolen and is unable to give a satisfactory account of such possession, is guilty of an offence.

## **53 Absence of reasonable cause for believing cellular phone or SIM-card properly acquired**

(1) Any person who in any manner acquires or receives into his or her possession from any other person a stolen cellular phone or SIM-card without having reasonable cause for believing at the time of such acquisition or receipt that such cellular phone or SIM-card is the property of the person from whom he or she acquires or receives it or that such person has been duly authorised by the owner thereof to deal with it or dispose of it, is guilty of an offence.

(2) In the absence of evidence to the contrary which raises a reasonable doubt, proof of such possession is sufficient evidence of the absence of reasonable cause.

## **54 Unlawful acts in respect of telecommunication and other equipment**

- (1) Any person who, intentionally and unlawfully, in any manner-
- (a) modifies, tampers with, alters, reconfigures or interferes with, any telecommunication equipment, including a cellular phone and a SIM-card, or any part thereof;
  - (b) reverse engineers, decompiles, disassembles or interferes with, the software installed on any telecommunication equipment, including a cellular phone and a SIM-card, by the manufacturer thereof; or
  - (c) allows any other person to perform any of the acts referred to in paragraph (a) or (b) ,

is guilty of an offence.

- (2) Any person who, intentionally and unlawfully, in any manner-
- (a) modifies, tampers with or interferes with, any interception or monitoring equipment, device or apparatus installed or utilised in terms of this Act; or
  - (b) allows any other person to perform any of the acts referred to in paragraph (a) ,

is guilty of an offence.

### **55 Failure to report loss, theft or destruction of cellular phone or SIM-card and presumption**

(1) Any person who fails to report the loss, theft or destruction of a cellular phone or SIM-card in terms of section 41 (1), is guilty of an offence.

(2) Whenever a person is charged with an offence referred to in subsection (1) and it is proved that such person was, at the time, the owner or authorised possessor of the cellular phone or SIM-card alleged to have been lost, stolen or destroyed, proof that the person has failed to produce such cellular phone or SIM-card within seven days of a written request by a police official to do so, will, in the absence of evidence to the contrary which raises reasonable doubt, be sufficient evidence that the cellular phone or SIM-card has been lost, stolen or destroyed.

### **56 Revoking of licence to provide electronic communication service**

The Cabinet member responsible for communications, after consultation with the Authority, may, in the case of a second or subsequent conviction of an electronic communication service provider of an offence referred to in section 51 (3) (a) (ii) and notwithstanding the imposition of any penalty prescribed by section 51 (3) (b) , revoke the licence issued to the electronic communication service provider concerned under Chapter 3 of the Electronic Communications Act, to provide an electronic communications service.

[S. 56 substituted by s. 97 of Act 36 of 2005.]

### **57 Forfeiture of listed or other equipment**

(1) A court convicting a person of an offence referred to in section 51 must, in addition to any penalty which it may impose in respect of that offence, declare any listed equipment-

- (a) by means of which the offence was committed;
- (b) which was used in connection with the commission of the offence;
- (c) which was found in the possession of the convicted person; or

- (d) the possession of which constituted the offence,

to be forfeited to the State.

(2) A court convicting a person of an offence referred to in section 51 may, in addition to any penalty which it may impose in respect of that offence, declare any equipment, other than listed equipment-

- (a) by means of which the offence was committed;
- (b) which was used in connection with the commission of the offence;
- (c) which was found in the possession of the convicted person; or
- (d) the possession of which constituted the offence,

to be forfeited to the State.

(3) Any listed equipment or other equipment declared forfeited under subsection (1) or (2) must, as soon as practicable after the date of declaration of forfeiture, be delivered to the Police Service.

(4) Any listed equipment or other equipment delivered to the Police Service in terms of subsection (3) must, in the case of-

- (a) listed equipment declared forfeited under subsection (1), be kept by the Police Service-
  - (i) for a period of four months with effect from the date of declaration of forfeiture;
  - (ii) if an application referred to in subsection (6) (a) is made, until a final decision in respect of any such application has been given; or
  - (iii) if an application referred to in subsection (7) (a) is made, until a final decision in respect of any such application has been given,

and must-

- (aa) as soon as practicable after the expiry of the period referred to in subparagraph (i);
- (bb) if the decision referred to in subparagraph (ii) has been given against the telecommunication service provider or other person concerned, as soon as practicable after that decision has been given; or
- (cc) if an application referred to in subparagraph (iii) has been refused, as soon as practicable after such refusal; or
- (b) equipment declared forfeited under subsection (2), be kept by the Police Service-
  - (i) for a period of 30 days with effect from the date of declaration of forfeiture; and
  - (ii) must as soon as practicable after the expiry of the period referred to in subparagraph (i),

be destroyed by the Police Service.

(5) A declaration of forfeiture under subsection (1) does not affect any right which any telecommunication service provider or other person, other than the convicted person, may have to such listed equipment, if it is proved that such telecommunication service

provider or other person-

- (a) has been exempted, under section 46 (1) (a) , from the relevant prohibited act referred to in section 45 (1) in respect of such listed equipment;
- (b) could not reasonably be expected to have known or had no reason to suspect that the listed equipment concerned was being or would be used in connection with the offence; and
- (c) had taken all reasonable steps to prevent the use thereof in connection with the offence.

(6) (a) The court in question or, if the judge or judicial officer concerned is not available, any other judge or judicial officer of the court in question, may upon an application made at any time within a period of three months with effect from the date of declaration of forfeiture under subsection (1), by any telecommunication service provider or other person, other than the convicted person, who claims that-

- (i) the listed equipment declared forfeited under subsection (1) is his or her property; and
- (ii) he or she is a person referred to in subsection (5),

inquire into and determine those matters.

(b) If the court referred to in paragraph (a) is satisfied that the-

- (i) listed equipment concerned is the property of the telecommunication service provider or other person concerned; and
- (ii) telecommunication service provider or other person concerned is a person referred to in subsection (5),

the court must set aside the declaration of forfeiture and direct that the listed equipment concerned be returned to such telecommunication service provider or other person.

(c) If a determination by the court under paragraph (b) is adverse to the applicant, he or she may appeal therefrom as if it were a conviction by the court making the determination, and such appeal may be heard either separately or jointly with an appeal against the conviction as a result whereof the declaration of forfeiture under subsection (1) was made, or against a sentence imposed as a result of such conviction.

(d) When determining the matters referred to in paragraph (a) (i) and (ii), the record of the criminal proceedings in which the declaration of forfeiture under subsection (1) was made, must form part of the relevant proceedings, and the court making the determination may hear such additional evidence, whether by affidavit or orally, as it deems fit.

(7) (a) The Minister may, if an application referred to in subsection (6) (a) -

- (i) has not been made, upon an application made at any time after a period of three months with effect from the date of declaration of forfeiture under subsection (1) but before the expiry of a period of four months from that date; or
- (ii) has been made and the declaration of forfeiture has not been set aside, upon an application made at any time within a period of one month with effect from the date on which a final decision in respect of that application has been given,

in terms of section 46 (1) (a) (iii) exempt the law enforcement agency which made the

application from possessing the listed equipment declared forfeited under subsection (1).

(b) Section 46 applies with the necessary changes in respect of an application referred to in paragraph (a) .

## CHAPTER 10 GENERAL PROVISIONS (ss 58-63)

### 58 Supplementary directives regarding applications

(1) A designated judge or, if there is more than one designated judge, all the designated judges jointly, may, after consultation with the respective Judges-President of the High Courts, issue directives to supplement the procedure for making applications for the issuing of directions or entry warrants in terms of this Act.

(2) Any directive issued under subsection (1) may at any time in like manner be amended or withdrawn.

(3) Any directive issued under subsection (1) must be submitted to Parliament.

**59** Amends section 205 of the Criminal Procedure Act 51 of 1977 by substituting subsection (1).

**60** Amends section 11 of the Drugs and Drug Trafficking Act 140 of 1992 by substituting paragraph (e) .

**61** Amends section 3 (a) of the Intelligence Services Act 40 of 1994 by substituting subparagraph (iii).

### 62 Repeal of law and transitional arrangements

(1) Subject to subsections (2) and (3), the Interception and Monitoring Prohibition Act, 1992 ( Act 127 of 1992 ), is hereby repealed.

[Date of commencement of sub-s. (1): 30 June 2008.]

(2) Any judge whose designation in terms of the Interception and Monitoring Prohibition Act, 1992, to perform the functions of a judge for purposes of that Act is still in force on the fixed date, must be regarded as having been so designated in terms of this Act.

[Date of commencement of sub-s. (2): 30 June 2008.]

(3) A direction issued under section 3 of the Interception and Monitoring Prohibition Act, 1992, and which is still in force on the fixed date, must be regarded as having been issued under this Act and remains in force until the period or extended period for which that direction has been issued, lapses.

[Date of commencement of sub-s. (3): 30 June 2008.]

(4) The directives issued under section 6 of the Interception and Monitoring Prohibition Act, 1992, and which are still in force immediately before the fixed date, cease to be of force and effect from the fixed date.

[Date of commencement of sub-s. (4): 30 June 2008.]

(5) (a) Any place which, immediately before the fixed date, has been used by the Police Service, Defence Force, Agency, Service or Directorate for the interception and monitoring of communications in terms of the Interception and Monitoring Prohibition Act, 1992, will, as from a date specified by the Cabinet member responsible for intelligence services, cease to exist unless such place is established as an interception centre as contemplated in section 32 (1) (a) .

- (b) If any place referred to in paragraph (a) -
- (i) is established as an interception centre as contemplated in that paragraph, all assets, liabilities, rights and obligations of that place will vest in the interception centre so established; or
  - (ii) ceases to exist as contemplated in that paragraph, all-
    - (aa) assets, including liabilities and obligations relating thereto, and rights of that place will, as from the date on which it ceases to exist, vest in interception centres established by section 32 (1) (a) and specified by the Cabinet member responsible for intelligence services for that purpose, without formal transfer and without payment of any fees, duties, taxes or other charges; and
    - (bb) other liabilities and obligations of that place remain with the Police Service, Defence Force, Agency, Service or Directorate, whichever used that place for purposes referred to in paragraph (a) .

[Date of commencement of sub-s. (5): 30 June 2008.]

(6) (a) Notwithstanding section 40 (1), an electronic communication service provider who, prior to the date of commencement of this section, provides a mobile cellular electronic communications service must, within 18 months from the said date, record and store the information contemplated in section 40 (2) in respect of all customers whose SIM-cards are activated on its system, if the information in question has not already been recorded and stored in terms of section 40.

(b) Section 40 (2), (3), (4), (9) and (10) applies with the necessary changes in respect of the information recorded and stored in terms of paragraph (a) .

(c) The obligations and rights conferred upon a person and an applicant in terms of section 40 (7) and (8) apply with the necessary changes.

(d) An electronic communication service provider shall not allow service continuation on its electronic communication system in respect of any activated SIM-card if the information referred to in paragraph (b) has not been recorded and stored at the expiry of the 18-month period contemplated in paragraph (a) .

[Sub-s. (6) substituted by s. 4 of Act 48 of 2008.]

[Date of commencement of sub-s. (6): 1 July 2009.]

## **62A Determination of tariffs**

The Minister may, in consultation with the Cabinet member responsible for communications, at the request of any electronic communication service provider who provides a mobile cellular electronic communications service, determine uniform tariffs of compensation payable by the electronic communication service providers who provide a mobile cellular electronic communications service, to persons employed to record and store the information contemplated in sections 40 and 62 (6) of the Act.

[S. 62A inserted by s. 5 of Act 48 of 2008.]

## **62B Information to be provided to customers**

An electronic communication service provider who provides a mobile cellular electronic communications service must, from the date of commencement of this section, inform-

- (a) a customer of his or her obligations in terms of sections 40, 41 and 62 (6) and 62C of the Act;
- (b) a customer of the manner in which the obligations must be complied with; and



- (c) a customer of the consequences of non-compliance with the obligations.

[S. 62B inserted by s. 5 of Act 48 of 2008.]

### **62C Keeping of information by juristic persons and persons who lease SIM-cards**

(1) Any juristic person, having complied with section 40 (2) or 62 (6), and who provides a SIM-card to a person in its employment must, before handing over the SIM-card to the other person-

- (a) record the particulars as required in section 40 (2) and the date on and period for which the SIM-card is provided; and
- (b) verify-
- (i) the full names, surname, identity number and identity of the person to whom the SIM-card is provided; and
- (ii) the address contemplated in section 40 (3) (a) (iii),

by means of documentation contemplated in section 40 (3) (b) .

(2) Any person, having complied with section 40 (2) or 62 (6), and who rents a SIM-card to another person must, before handing over the SIM-card to the other person-

- (a) record the particulars as required in section 40 (2) and the date on and period for which the SIM-card is rented; and
- (b) verify-
- (i) the full names and surname, identity number and identity of the person to whom the SIM-card is rented;
- (ii) the name and, where applicable, the registration number of the juristic person; and
- (iii) the address contemplated in section 40 (3) (a) (iii),

by means of documentation contemplated in section 40 (3) (b) .

(3) The information referred to in subsections (1) and (2) must be stored for a period of five years.

(4) (a) An applicant may, for the purposes of making an application for the issuing of a direction, in writing request a person contemplated in subsection (1) or (2) to provide the applicant with the information recorded and stored in terms of subsection (1) or (2), respectively.

(b) A person contemplated in subsection (1) or (2) who receives a request referred to in paragraph (a) must immediately comply with that request if the request relates to any SIM-card in its, his or her possession or to any person to whom the SIM-card was provided or rented.

(5) If a person contemplated in subsection (1) or (2) knows or suspects that an identification document submitted for verification as contemplated in section 40 (3) is false, it, he or she must, within 24 hours, report the matter to a police official at any police station.

[S. 62C inserted by s. 5 of Act 48 of 2008.]

### **63 Short title and commencement**

(1) This Act is called the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, and comes into operation on a date fixed by the President by proclamation in the *Gazette* .

(2) Notwithstanding subsection (1), sections 40 and 62 (6) come into operation on the date on which the Regulation of Interception of Communications and Provision of Communication-related Information Amendment Act, 2008, takes effect.

[S. 63 substituted by s. 6 of Act 48 of 2008.]

## Schedule

(Section 1)

[Schedule amended by s. 36 (1) of Act 12 of 2004 and by s. 27 (1) of Act 33 of 2004.]

- 1 High treason;
- 2 any offence referred to in paragraph (a) of the definition of 'specified offence' of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004;  
[Item 2 substituted by s. 27 (1) of Act 33 of 2004.]
- 3 .....  
[Item 3 deleted by s. 27 (1) of Act 33 of 2004.]
- 4 sedition;
- 5 any offence which could result in the loss of a person's life or serious risk of loss of a person's life;
- 6 any offence referred to in Schedule 1 to the Implementation of the Rome Statute of the International Criminal Court Act, 2002 ( Act 27 of 2002 );
- 7 any specified offence as defined in section 1 of the National Prosecuting Authority Act;
- 8 any offence referred to in Chapters 2, 3 and 4 of the Prevention of Organised Crime Act;
- 9 any offence referred to in section 13 (f) of the Drugs and Drug Trafficking Act, 1992 ( Act 140 of 1992 );
- 10 any offence relating to the dealing in or smuggling of ammunition, firearms, explosives or armament and the unlawful possession of such firearms, explosives or armament;
- 11 any offence under any law relating to the illicit dealing in or possession of precious metals or precious stones;
- 12 any offence contemplated in Part 1 to 4, or section 17, 20 or 21 (in so far as it relates to the aforementioned offences) of Chapter 2 of the Prevention and Combating of Corrupt Activities Act, 2004;  
[Item 12 substituted by s. 36 (1) of Act 12 of 2004.]
- 13 dealing in, being in possession of or conveying endangered, scarce and protected game or plants or parts or remains thereof in contravention of any legislation;
- 14 any offence the punishment wherefor may be imprisonment for life or a period of imprisonment prescribed by section 51 of the Criminal Law Amendment Act, 1997 ( Act 105 of 1997 ), or a period of imprisonment exceeding five years without the option of a fine.

**REGULATION OF INTERCEPTION OF COMMUNICATIONS AND  
PROVISION OF COMMUNICATION-RELATED INFORMATION  
AMENDMENT ACT 48 OF 2008**

[ASSENTED TO 6 JANUARY 2009] [DATE OF COMMENCEMENT: 1 JULY 2009]  
(Unless otherwise indicated)

*(English text signed by the President)*

**ACT**

**To amend the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, so as to insert certain new definitions and to amend certain definitions; to provide afresh for information to be obtained and kept in respect of cellular phones and SIM-cards; to further regulate offences and penalties; and to provide for matters connected therewith.**

BE IT ENACTED by the Parliament of the Republic of South Africa, as follows:-

**1** Amends section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 , as follows: paragraph (a) inserts the definitions of 'activate' and 'address'; paragraph (b) substitutes the definition of 'customer'; paragraph (c) inserts the definition of 'family member'; paragraph (d) substitutes the definition of 'identification document'; paragraph (e) inserts the definition of 'identity number'; and paragraph (f) inserts the definition of 'informal settlement'.

**2** Substitutes section 40 of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 .

**3** Amends section 51 of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 , as follows: paragraph (a) substitutes subsection (1) (a) (i); paragraph (b) inserts subsections (3A), (3B), (3C) and (3D); and paragraph (c) deletes the word 'or' at the end of subsection (5) (b) and inserts paragraph (b A) .

[Date of commencement of s. 3: 1 August 2009.]

**4** Amends section 62 of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 by substituting subsection (6).

**5** Inserts sections 62A, 62B and 62C in the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 .

**6** Substitutes section 63 of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 .

**7 Short title and commencement**

This Act is called the Regulation of Interception of Communications and Provision of Communication-related Information Amendment Act, 2008, and comes into operation on a date determined by the President by proclamation in the *Gazette* .