

**Act No. 70, 2002** REGULATION OF INTERCEPTION OF COMMUNICATIONS  
AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT, 2002

- (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. 5
- (e) If the National Assembly does not reject a certificate as contemplated in paragraph (b) or (d)(ii)— 10
- (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- (5) A certificate of exemption contemplated in subsection (3) may at any time in like manner be amended or withdrawn by the Minister. 15
- (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)— 20
- (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. 25

## CHAPTER 9

### CRIMINAL PROCEEDINGS, OFFENCES AND PENALTIES

#### Use of information in criminal proceedings

47. (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. 30

(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. 35

#### Proof of certain facts by certificate

40

48. 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— 45

- (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. 50

**Act No. 70, 2002 REGULATION OF INTERCEPTION OF COMMUNICATIONS  
AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT, 2002**

**Unlawful interception of communication**

**49.** (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. 5

(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. 10

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

**50.** (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. 15

(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.

**Offences and penalties**

**51.** (1) (a) Any person who— 20

- (i) contravenes or fails to comply with section 6(2), 7(4), 8(4), 29(8), 40(1), (2) or (3), 42(1) or 45(1);
- (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; 25
- (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; 30
- (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 35
- (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, 40

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. 45

(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), 50

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—

**Act No. 70, 2002** REGULATION OF INTERCEPTION OF COMMUNICATIONS  
AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT, 2002

- (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
- (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); 10
- (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— 15
- (i) a telecommunication 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 20
- (ii) an employee, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years.
- (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); 25  
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— 30
- (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 35  
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); 40
- (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); or
- (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 45  
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; 50  
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.

**Act No. 70, 2002 REGULATION OF INTERCEPTION OF COMMUNICATIONS  
AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT, 2002**

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

52. 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.

**Absence of reasonable cause for believing cellular phone or SIM-card properly acquired 5**

53. (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. 10

(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.

**Unlawful acts in respect of telecommunication and other equipment 15**

54. (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 20

(c) allows any other person to perform any of the acts referred to in paragraph (a) or (b),

is guilty of an offence. 25

(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. 30

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

55. (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. 40

**Revoking of licence to provide telecommunication service**

56. The Cabinet member responsible for communications, after consultation with the Authority, may, in the case of a second or subsequent conviction of a telecommunication 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 telecommunication service provider concerned under Chapter V of the Telecommunications Act, to provide a telecommunication service. 45

**Act No. 70, 2002** REGULATION OF INTERCEPTION OF COMMUNICATIONS  
AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT, 2002

**Forfeiture of listed or other equipment**

**57.** (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; 5
- (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; 10
- (b) which was used in connection with the commission of the offence;
- (c) which was found in the possession of the convicted person; or 15
- (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. 20

(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; 25
  - (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. 30

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 35
- (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— 40
  - (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. 45

(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; 50
- (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. 55

(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— 60

**Act No. 70, 2002 REGULATION OF INTERCEPTION OF COMMUNICATIONS  
AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT, 2002**

- (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— 5  
(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 10  
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 15  
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 20  
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; 25  
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 30  
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** 35

**GENERAL PROVISIONS**

**Supplementary directives regarding applications**

**58.** (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 40  
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.

**Amendment of section 205 of Act 51 of 1977, as substituted by section 11 of Act 204 45  
of 1993**

**59.** Section 205 of the Criminal Procedure Act, 1977, is hereby amended by the substitution for subsection (1) of the following subsection:

“(1) A judge of [the supreme court] a High Court, a regional court magistrate or a magistrate may, subject to the provisions of subsection (4) and section 15 of the 50  
Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, upon the request of [an attorney-general] a Director of Public Prosecutions or a public prosecutor authorized thereto in writing by the [attorney-general] Director of Public Prosecutions, require the attendance before him or her or any other judge, regional court magistrate or magistrate, for 55  
examination by the [attorney-general] Director of Public Prosecutions or the public prosecutor authorized thereto in writing by the [attorney-general] Director

**Act No. 70, 2002** REGULATION OF INTERCEPTION OF COMMUNICATIONS  
AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT, 2002

of Public Prosecutions, of any person who is likely to give material or relevant information as to any alleged offence, whether or not it is known by whom the offence was committed: Provided that if such person furnishes that information to the satisfaction of the [attorney-general] Director of Public Prosecutions or public prosecutor concerned prior to the date on which he or she is required to appear before a judge, regional court magistrate or magistrate, he or she shall be under no further obligation to appear before a judge, regional court magistrate or magistrate.”.

**Amendment of section 11 of Act 140 of 1992**

**60.** Section 11 of the Drugs and Drug Trafficking Act, 1992, is hereby amended by the substitution in subsection (1) for paragraph (e) of the following paragraph: 10

“(e) subject to section 15 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, require from any person who has in his or her possession or custody or under his or her control any register, record or other document which in the opinion of the police official may have a bearing on any offence or alleged offence under this Act, to deliver to him or her then and there, or to submit to him or her at such time and place as may be determined by the police official, any such register, record or document.”.

**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** 20

**61.** Section 3 of the Intelligence Services Control Act, 1994, is hereby amended by the substitution in paragraph (a) for subparagraph (iii) of the following subparagraph:

“(iii) any designated judge as defined in section 1 of the Regulation of Interception [and Monitoring Prohibition] of Communications and Provision of Communication-related Information Act, [1992 (Act No. 127 of 1992)] 2002, a report regarding the functions performed by him or her in terms of that Act, including statistics regarding such functions, together with any comments or recommendations which such designated judge may deem appropriate: Provided that such report shall not disclose any information contained in an application or direction [contemplated in section 3 of] referred to in that Act.”.

**Repeal of law and transitional arrangements**

**62.** (1) Subject to subsections (2) and (3), the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), is hereby repealed. 35

(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.

(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. 40

(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. 45

(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). 50

**Act No. 70, 2002** REGULATION OF INTERCEPTION OF COMMUNICATIONS  
AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT, 2002

- (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).
- (6) (a) Any person who, at the fixed date, is the owner of a cellular phone or a SIM-card must, in the manner and within the period determined by the Minister by notice in the *Gazette*, provide the information referred to in section 40(1) to the person who sold, or in any other manner provided, the cellular phone or SIM-card to him or her, or to the telecommunication service provider or other person mentioned in such notice.
- (b) Different periods may be determined in terms of paragraph (a) in respect of—
- (i) owners whose surnames start with different letters of the alphabet, or whose dates of birth fall in different months; or
  - (ii) categories of numbers of cellular phones or SIM-cards.
- (c) Before the Minister exercises the powers conferred on him or her by paragraph (a), he or she must consult the telecommunication service providers concerned.
- (d) Any notice issued under paragraph (a) must, before publication thereof in the *Gazette*, be submitted to Parliament.
- (e) Section 40(2) and (3) applies, with the necessary changes, in respect of a telecommunication service provider or other person to whom information has been provided in terms of paragraph (a).

**Short title and commencement**

**63.** 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*.

**Act No. 70, 2002** REGULATION OF INTERCEPTION OF COMMUNICATIONS  
AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT, 2002

**SCHEDULE**

(Section 1)

1. high treason;
2. any offence relating to terrorism;
3. any offence involving sabotage;
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 No. 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 No. 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 section 1(1) of the Corruption Act, 1992 (Act No. 94 of 1992);
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 No. 105 of 1997), or a period of imprisonment exceeding five years without the option of a fine.