[Last checked: 30 January 2026.*]
*The last time this Act was reviewed for updates.

# CYBERCRIMES ACT 19 OF 2020

[Updated to 11 October 2024.**]
**Date of last changes incorporated in this Act.

---

*(English text signed by President.)*

*Published: G. 44651, 1 June 2021*

---

*Published:* G. 44651, 1 June 2021

*Commencement:* **1 December 2021;**

Ss 20-23; 38 (1) (d), 38 (1) (e), 38 (1) (f), 40 (3), 40 (4), 41-44; Chapter 5, Chapter 6, s 54: **To be proclaimed;**

In the Schedule, Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007, ss 11B, 11C, 11D , 56A (3) (c), 56A (3) (d), 56A (3) (e): **To be proclaimed.**

ProcR 42, G. 45562, 23 November 2021

[Administration and the powers or functions entrusted by legislation transferred to the Minister of Justice and Constitutional Development - Proc 199, G. 51368, 11 October 2024.]

**ACT**

**To create offences which have a bearing on cybercrime; to criminalise the disclosure of data messages which are harmful and to provide for interim protection orders; to further regulate jurisdiction in respect of cybercrimes; to further regulate the powers to investigate cybercrimes; to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrimes; to provide for the establishment of a designated Point of Contact; to further provide for the proof of certain facts by affidavit; to impose obligations to report cybercrimes; to provide for capacity building; to provide that the Executive may enter into agreements with foreign States to promote measures aimed at the detection, prevention, mitigation and investigation of cybercrimes; to delete and amend provisions of certain laws; and to provide for matters connected therewith.**

PARLIAMENT of the Republic of South Africa enacts, as follows:—

## ARRANGEMENT OF SECTIONS

**CHAPTER 1**
**DEFINITIONS AND INTERPRETATION**

1. Definitions and interpretation

## CHAPTER 2
## CYBERCRIMES, MALICIOUS COMMUNICATIONS, SENTENCING AND ORDERS TO PROTECT COMPLAINANTS FROM HARMFUL EFFECT OF MALICIOUS COMMUNICATIONS

### *Part I*
### *Cybercrimes*


2. Unlawful access
3. Unlawful interception of data
4. Unlawful acts in respect of software or hardware tool
5. Unlawful interference with data or computer program
6. Unlawful interference with computer data storage medium or computer system
7. Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device
8. Cyber fraud
9. Cyber forgery and uttering
10. Cyber extortion
11. Aggravated offences
12. Theft of incorporeal property


### *Part II*
### *Malicious communications*


13. Definitions
14. Data message which incites damage to property or violence
15. Data message which threatens persons with damage to property or violence
16. Disclosure of data message of intimate image


### *Part III*
### *Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit offence*


17. Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit offence


### *Part IV*
### *Competent verdicts*


18. Competent verdicts

***Part V***

***Sentencing***

19. Sentencing

***Part VI***

***Orders to protect complainants from harmful effect of malicious communications***

20. Order to protect complainant pending finalisation of criminal proceedings
21. Electronic communications service provider to furnish particulars to court
22. Orders on finalisation of criminal proceedings
23. Penalties

**CHAPTER 3**

**JURISDICTION**

24. Jurisdiction

**CHAPTER 4**

**POWERS TO INVESTIGATE, SEARCH, ACCESS OR SEIZE**

25. Definitions
26. Standard Operating Procedures
27. Application of Criminal Procedure Act, 1977
28. Search for, access to, or seizure of certain articles
29. Article to be searched for, accessed or seized under search warrant
30. Oral application for search warrant or amendment of warrant
31. Search for, access to, or seizure of article without search warrant with consent of person who has lawful authority to consent
32. Search for, access to, or seizure of article involved in the commission of an offence without search warrant
33. Search for, access to, or seizure of article on arrest of person
34. Assisting police official or investigator
35. Obstructing or hindering police official or investigator and authority to overcome resistance
36. Powers conferred upon police official or investigator to be conducted in decent and orderly manner with due regard to rights of other persons
37. Wrongful search, access or seizure and restriction on use of instrument, device, password or decryption key or information to gain access
38. False information under oath or by way of affirmation
39. Prohibition on disclosure of information

40. Interception of indirect communication and obtaining of real-time communication-related information
41. Expedited preservation of data direction
42. Preservation of evidence direction
43. Oral application for preservation of evidence direction
44. Disclosure of data direction and search for, access to, and seizure of articles subject to preservation
45. Obtaining and using publicly available data or receiving data from person who is in possession of data

**CHAPTER 5**
**MUTUAL ASSISTANCE**

46. Application of provisions of Chapter
47. Spontaneous information
48. Foreign requests for assistance and cooperation
49. Complying with order of designated judge
50. Informing foreign State of outcome of request for mutual assistance and expedited disclosure of traffic data
51. Issuing of direction requesting assistance from foreign State

**CHAPTER 6**
**DESIGNATED POINT OF CONTACT**

52. Establishment and functions of designated Point of Contact

**CHAPTER 7**
**EVIDENCE**

53. Proof of certain facts by affidavit

**CHAPTER 8**
**REPORTING OBLIGATIONS AND CAPACITY BUILDING**

54. Obligations of electronic communications service providers and financial institutions
55. Capacity to detect, prevent and investigate cybercrimes
56. National Director of Public Prosecutions must keep statistics of prosecutions

**CHAPTER 9**
**GENERAL PROVISIONS**

57. National Executive may enter into agreements
58. Repeal or amendment of laws
59. Regulations
60. Short title and commencement
Schedule: Repeal or amendment of laws

## CHAPTER 1
## DEFINITIONS AND INTERPRETATION

### 1. Definitions and interpretation

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

**"article"** means any—

(a) data;

(b) computer program;

(c) computer data storage medium; or

(d) computer system,

which—

(i) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission;

(ii) may afford evidence of the commission or suspected commission; or

(iii) is intended to be used or is, on reasonable grounds believed to be intended to be used in the commission or intended commission, of—

(aa) an offence in terms of Part I and Part II of Chapter 2;

(bb) any other offence in terms of the law of the Republic; or

(cc) an offence in a foreign State that is substantially similar to an offence contemplated in Part I or Part II of Chapter 2 or another offence recognised in the Republic;

**"computer"** means any electronic programmable device used, whether by itself or as part of a computer system or any other device or equipment, or any part thereof, to perform predetermined arithmetic, logical, routing, processing or storage operations in accordance with set instructions and includes any data, computer program or computer data storage medium that are related to, connected with or used with such a device;

**"computer data storage medium"** means any device from which data or a computer program is capable of being reproduced or on which data or a computer program is capable of being stored, by a computer system, irrespective of whether the device is physically attached to or connected with a computer system;

**"computer program"** means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

**"computer system"** means—

(a) one computer; or

(b) two or more inter-connected or related computers, which allow these inter-connected or related computers to—

(i) exchange data or any other function with each other; or

(ii) exchange data or any other function with another computer or a computer system;

**"Constitution"** means the Constitution of the Republic of South Africa, 1996;

**"Criminal Procedure Act, 1977"** means the Criminal Procedure Act, 1977 (Act 51 of 1977);

**"Customs and Excise Act, 1964"** means the Customs and Excise Act, 1964 (Act 91 of 1964);

**"Customs Control Act, 2014"** means the Customs Control Act, 2014 (Act 31 of 2014);

**"data"** means electronic representations of information in any form;

**"data message"** means data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form;

**"designated judge"** means a designated judge as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002;

**"designated Point of Contact"** means the office established or designated in terms of section 52;

**"Electronic Communications Act, 2005"** means the Electronic Communications Act, 2005 (Act 36 of 2005);

**"electronic communications network"** means an electronic communications network as defined in section 1 of the Electronic Communications Act, 2005, and includes a computer system;

**"electronic communications service"** means any service which consists wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services as defined in section 1 of the Electronic Communications Act, 2005;

**"electronic communications service provider"** means—

(a) any person who provides an electronic communications service to the public, sections of the public, the State, or the subscribers to such service, under and in accordance with an electronic communications service licence issued to that person in terms of the Electronic Communications Act, 2005, or who is deemed to be licenced or exempted from being licenced as such in terms of that Act; and

(b) a person who has lawful authority to control the operation or use of a private electronic communications network used primarily for providing electronic communications services for the owner's own use and which is exempted from being licensed in terms of the Electronic Communications Act, 2005;

**"financial institution"** means a financial institution as defined in section 1 of the Financial Sector Regulation Act, 2017 (Act 9 of 2017);

**"foreign State"** means any State other than the Republic;

**"Intelligence Services Oversight Act, 1994"** means the Intelligence Services Oversight Act, 1994 (Act 40 of 1994);

**"International Co-operation in Criminal Matters Act, 1996"** means the International Co-operation in Criminal Matters Act, 1996 (Act 75 of 1996);

**"Justices of the Peace and Commissioners of Oaths Act, 1963"** means the Justices of the Peace and Commissioners of Oaths Act, 1963 (Act 16 of 1963);

**"magistrate"** includes a regional court magistrate;

**"Magistrates' Courts Act, 1944"** means the Magistrates' Courts Act, 1944 (Act 32 of 1944);

**"National Commissioner"** means the National Commissioner of the South African Police Service, appointed by the President under section 207 (1) of the Constitution;

**"National Director of Public Prosecutions"** means the person contemplated in section 179 (1) (a) of the Constitution and appointed in terms of section 10 of the National Prosecuting Authority Act, 1998;

**"National Head of the Directorate"** means a person appointed in terms of section 17CA (1) of the South African Police Service Act, 1995;

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

**"National Strategic Intelligence Act, 1994"** means the National Strategic Intelligence Act, 1994 (Act 39 of 1994);

**"output of a computer program"** means any—

(a) data or output of the data;

(b) computer program; or

(c) instructions,

generated by a computer program;

**"output of data"** means by having data displayed or in any other manner;

**"person"** means a natural or a juristic person;

**"police official"** means a member of the South African Police Service as defined in section 1 of the South African Police Service Act, 1995;

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

**"Protection from Harassment Act, 2011"** means the Protection from Harassment Act, 2011 (Act 17 of 2011);

**"Protection of Personal Information Act, 2013"** means the Protection of Personal Information Act, 2013 (Act 4 of 2013);

**"publicly available data"** means data which is accessible in the public domain without restriction;

**"Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002"** means the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act 70 of 2002);

**"responsible party"** means a responsible party as defined in section 1 of the Protection of Personal Information Act, 2013;

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

**"South African Reserve Bank"** means the South African Reserve Bank, referred to in section 223 of the Constitution, read with the South African Reserve Bank Act, 1989;

**"South African Reserve Bank Act, 1989"** means the South African Reserve Bank Act, 1989 (Act 90 of 1989);

**"specifically designated police official"** means a police official of the rank of captain or above referred to in section 33 of the South African Police Service Act, 1995, who has been designated in writing by the National Commissioner and the National Head of the Directorate, respectively, to—

(a) make oral applications for a search warrant or an amendment of a warrant contemplated in section 30;

(b) issue expedited preservation of data directions contemplated in section 41; or

(c) serve or execute an order of the designated judge as contemplated in section 48 (10);

**"Superior Courts Act, 2013"** means the Superior Courts Act, 2013 (Act 10 of 2013);

**"Tax Administration Act, 2011"** means the Tax Administration Act, 2011 (Act 28 of 2011); and

**"traffic data"** means data relating to a communication indicating the communication's origin, destination, route, format, time, date, size, duration or type, of the underlying service.

(2) For the purposes of section 2, 3 (2) or (3), or 7 (1) or (2) of this Act, any failure by a responsible party to comply with—

(a) the conditions for lawful processing of personal information referred to in Chapter 3;

(b) section 72; or

(c) the provisions of a code of conduct issued in terms of section 60,

of the Protection of Personal Information Act, 2013, must be dealt with in terms of Chapter 10 of that Act.

## CHAPTER 2
## CYBERCRIMES, MALICIOUS COMMUNICATIONS, SENTENCING AND ORDERS TO PROTECT COMPLAINANTS FROM HARMFUL EFFECT OF MALICIOUS COMMUNICATIONS

### *Part I*
### *Cybercrimes*

**2. Unlawful access**

(1) Any person who unlawfully and intentionally performs an act in respect of—

(a) a computer system; or

(b) a computer data storage medium,

which places the person who performed the act or any other person in a position to commit an offence contemplated in subsection (2), section 3 (1), 5 (1) or 6 (1), is guilty of an offence.

(2)

(a) Any person who unlawfully and intentionally accesses a computer system or a computer data storage medium, is guilty of an offence.

(b) For purposes of paragraph (a)—

(i) a person accesses a computer data storage medium, if the person—

(aa) uses data or a computer program stored on a computer data storage medium; or

(bb) stores data or a computer program on a computer data storage medium; and

(ii) a person accesses a computer system, if the person—

(aa) uses data or a computer program held in a computer system;

(bb) stores data or a computer program on a computer data storage medium forming part of the computer system; or

(cc) instructs, communicates with, or otherwise uses, the computer system.

(c) For purposes of paragraph (b)—

(i) a person uses a computer program, if the person—

(aa) copies or moves the computer program to a different location in the computer system or computer data storage medium in which it is held or to any other computer data storage medium;

(bb) causes a computer program to perform any function; or

(cc) obtains the output of a computer program; and

(ii) a person uses data, if the person—

(aa) copies or moves the data to a different location in the computer system or computer data storage medium in which it is held or to any other computer data storage medium; or

(bb) obtains the output of data.

**3. Unlawful interception of data**

(1) Any person who unlawfully and intentionally intercepts data, including electromagnetic emissions from a computer system carrying such data, within or which is transmitted to or from a computer system, is guilty of an offence.

(2) Any person who unlawfully and intentionally possesses data or the output of data, with the knowledge that such data was intercepted unlawfully as contemplated in subsection (1), is guilty of an offence.

(3) Any person who is found in possession of data or the output of data, in regard to which there is a reasonable suspicion that such data was intercepted unlawfully as contemplated in subsection (1) and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

(4) For purposes of this section **"interception of data"** means the acquisition, viewing, capturing or copying of data of a non-public nature through the use of a hardware or software tool contemplated in section 4 (2) or any other means, so as to make some or all of the data available to a person, other than the lawful owner or holder of the data, the sender or the recipient or the intended recipient of that data, and includes the—

(a) examination or inspection of the contents of the data; and

(b) diversion of the data or any part thereof from its intended destination to any other destination.

**4. Unlawful acts in respect of software or hardware tool**

(1) Any person who unlawfully and intentionally—

(a) uses; or

(b) possesses,

any software or hardware tool for purposes of contravening the provisions of section 2 (1) or (2), 3 (1), 5 (1), 6 (1) or 7 (1) (a) or (d), is guilty of an offence.

(2) For purposes of this section **"software or hardware tool"** means any electronic, mechanical or other instrument, device, equipment, apparatus or a substantial component thereof or a computer program, which is designed or adapted primarily for the purpose to—

(a) access as contemplated in section 2 (1) or (2);

(b) intercept data as contemplated in section 3 (1);

(c) interfere with data or a computer program as contemplated in section 5 (1);

(d) interfere with a computer data storage medium or a computer system as contemplated in section 6 (1); or

(e) acquire, make available or use a password, access code or similar data or device as defined in section 7 (3).

**5. Unlawful interference with data or computer program**

(1) Any person who unlawfully and intentionally interferes with—

(a) data; or

(b) a computer program,

is guilty of an offence.

(2) For purposes of this section **"interfere with data or a computer program"** means to permanently or temporarily—

(a) delete data or a computer program;

(b) alter data or a computer program;

(c) render vulnerable, damage or deteriorate data or a computer program;

(d) render data or a computer program meaningless, useless or ineffective;

(e) obstruct, interrupt or interfere with the lawful use of, data or a computer program; or

(f) deny access to data or a computer program,

held in a computer data storage medium or a computer system.

**6. Unlawful interference with computer data storage medium or computer system**

(1) Any person who unlawfully and intentionally interferes with a computer data storage medium or a computer system, is guilty of an offence.

(2) For purposes of this section **"interfere with a computer data storage medium or a computer system"** means to permanently or temporarily—

(a) alter any resource; or

(b) interrupt or impair—

(i) the functioning;

(ii) the confidentiality;

(iii) the integrity; or

(iv) the availability,

of a computer data storage medium or a computer system.

**7. Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device**

(1) Any person who unlawfully and intentionally—

(a) acquires;

(b) possesses;

(c) provides to another person; or

(d) uses,

a password, an access code or similar data or device for purposes of contravening the provisions of section 2 (1) or (2), 3 (1), 5 (1), 6 (1), 8 or 9 (1), is guilty of an offence.

(2) Any person who is found in possession of a password, an access code or similar data or device in regard to which there is a reasonable suspicion that such password, access code or similar data or device—

(a) was acquired;

(b) is possessed;

(c) is to be provided to another person; or

(d) was used or may be used,

for purposes of contravening the provisions of section 2 (1) or (2), 3 (1), 5 (1), 6 (1), 8 or 9 (1), and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

(3) For purposes of this section **"password, access code or similar data or device"** includes—

(a) a secret code or pin;

(b) an image;

(c) a security token;

(d) an access card;

(e) any device;

(f) biometric data; or

(g) a word or a string of characters or numbers,

used for financial transactions or user-authentication in order to access or use data, a computer program, a computer data storage medium or a computer system.

**8. Cyber fraud**

Any person who unlawfully and with the intention to defraud makes a misrepresentation—

(a) by means of data or a computer program; or

(b) through any interference with data or a computer program as contemplated in section 5 (2) (a), (b) or (e) or interference with a computer data storage medium or a computer system as contemplated in section 6 (2) (a),

which causes actual or potential prejudice to another person, is guilty of the offence of cyber fraud.

**9. Cyber forgery and uttering**

(1) Any person who unlawfully and with the intention to defraud makes—

(a) false data; or

(b) a false computer program,

to the actual or potential prejudice of another person, is guilty of the offence of cyber forgery.

(2) Any person who unlawfully and with the intention to defraud, passes off—

(a) false data; or

(b) a false computer program,

to the actual or potential prejudice of another person, is guilty of the offence of cyber uttering.

**10. Cyber extortion**

Any person who unlawfully and intentionally commits or threatens to commit any offence contemplated in section 3 (1), 5 (1), 6 (1) or 7 (1) (a) or (d), for the purpose of—

(a) obtaining any advantage from another person; or

(b) compelling another person to perform or to abstain from performing any act,

is guilty of the offence of cyber extortion.

**11. Aggravated offences**

(1)

(a) Any person who commits an offence referred to in—

(i) section 3 (1), 5 (1) or 6 (1), in respect of; or

(ii) section 7 (1), in so far as the passwords, access codes or similar data and devices relate to,

a restricted computer system, and who knows or ought reasonably to have known or suspected that it is a restricted computer system, is guilty of an aggravated offence.

(b) For purposes of paragraph (a), a **"restricted computer system"** means any data, computer program, computer data storage medium or computer system—

(i) under the control of, or exclusively used by—

(aa) a financial institution; or

(bb) an organ of state as set out in section 239 of the Constitution, including a court; and

(ii) which is protected by security measures against unauthorised access or use.

(2) Any person who commits an offence referred to in section 5 (1), 6 (1) or 10, and who knows or ought reasonably to have known or suspected that the offence in question will—

(a) endanger the life or cause serious bodily injury to, or the death of, any person, or any number or group of persons;

(b) cause serious risk to the health or safety of the public or any segment of the public; or

(c) create a serious public emergency situation,

is guilty of an aggravated offence.

(3) The Director of Public Prosecutions having jurisdiction must authorise in writing a prosecution in terms of subsection (1) or (2).

**12. Theft of incorporeal property**

The common law offence of theft must be interpreted so as not to exclude the theft of incorporeal property.

## *Part II*

## *Malicious communications*

### 13. Definitions

In Part II, unless the context indicates otherwise—

**"damage to property"** means damage to any corporeal or incorporeal property;

**"disclose"** in respect of a data message referred to in sections 14, 15 and 16, means to—

(a) send the data message to a person who is the intended recipient of the electronic communication or any other person;

(b) store the data message on an electronic communications network, where the data message can be viewed, copied or downloaded; or

(c) send or otherwise make available to a person, a link to the data message that has been stored on an electronic communication network, where the data message can be viewed, copied or downloaded;

**"group of persons"** means characteristics that identify an individual as a member of a group, which characteristics include without limitation, race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language, birth or nationality;

**"related person"** means any member of the family or household of a person or any other person in a close relationship with that person; and

**"violence"** means bodily harm.

### 14. Data message which incites damage to property or violence

Any person who discloses, by means of an electronic communications service, a data message to a person, group of persons or the general public with the intention to incite—

(a) the causing of any damage to property belonging to; or

(b) violence against,

a person or a group of persons, is guilty of an offence.

**15. Data message which threatens persons with damage to property or violence**

A person commits an offence if they, by means of an electronic communications service, unlawfully and intentionally discloses a data message, which—

(a) threatens a person with—

(i) damage to property belonging to that person or a related person; or

(ii) violence against that person or a related person; or

(b) threatens a group of persons or any person forming part of, or associated with, that group of persons with—

(i) damage to property belonging to that group of persons or any person forming part of, or associated with, that group of persons; or

(ii) violence against the group of persons or any person forming part of, or associated with, that group of persons,

and a reasonable person in possession of the same information, with due regard to all the circumstances, would perceive the data message, either by itself or in conjunction with any other data message or information, as a threat of damage to property or violence to a person or category of persons contemplated in paragraph (a) or (b), respectively.

**16. Disclosure of data message of intimate image**

(1) Any person (**"A"**) who unlawfully and intentionally discloses, by means of an electronic communications service, a data message of an intimate image of a person (**"B"**), without the consent of B, is guilty of an offence.

(2) For purposes of subsection (1)—

(a) **"B"** means—

(i) the person who can be identified as being displayed in the data message;

(ii) any person who is described as being displayed in the data message, irrespective of the fact that the person cannot be identified as being displayed in the data message; or

(iii) any person who can be identified from other information as being displayed in the data message; and

(b) **"intimate image"** means a depiction of a person—

(i) real or simulated, and made by any means in which—

(aa) B is nude, or the genital organs or anal region of B is displayed, or if B is a female person, transgender person or intersex person, their breasts, are displayed; or

(bb) the covered genital or anal region of B, or if B is a female person, transgender person or intersex person, their covered breasts, are displayed; and

(ii) in respect of which B so displayed retains a reasonable expectation of privacy at the time that the data message was made in a manner that—

(aa) violates or offends the sexual integrity or dignity of B; or

(bb) amounts to sexual exploitation.

## *Part III*
## *Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit offence*

### 17. Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit offence

Any person who unlawfully and intentionally—

(a) attempts;

(b) conspires with any other person; or

(c) aids, abets, induces, incites, instigates, instructs, commands or procures another person,

to commit an offence in terms of Part I or Part II of this Chapter, is guilty of an offence and is liable on conviction to the punishment to which a person convicted of actually committing that offence would be liable.

## *Part IV*
## *Competent verdicts*

### 18. Competent verdicts

(1) If the evidence in criminal proceedings does not prove the commission of the offence charged but proves a contravention of section 17—

(a) in respect of the offence charged; or

(b) in respect of any other offence of which an accused may be convicted on the offence charged,

the accused may be found guilty of the offence so proved.

(2) If the evidence on a charge of a contravention of section 3 (1), does not prove the offence or a contravention of section 17 in respect of that offence, but proves a contravention of—

(a) section 2 (1) or (2);

(b) section 3 (2) or (3); or

(c) section 4 (1), in so far as it relates to the use or possession of a software or hardware tool, for purposes of contravening section 3 (1),

the accused may be found guilty of the offence so proved.

(3) If the evidence on a charge of a contravention of section 5 (1), does not prove the offence or a contravention of section 17 in respect of that offence, but proves—

(a) a contravention of section 2 (1) or (2);

(b) a contravention of section 4 (1), in so far as it relates to the use or possession of a software or hardware tool, for purposes of contravening section 5 (1); or

(c) the offence of malicious injury to property,

the accused may be found guilty of the offence so proved.

(4) If the evidence on a charge of a contravention of section 6 (1), does not prove the offence or a contravention of section 17 in respect of that offence, but proves—

(a) a contravention of section 2 (1) or (2);

(b) a contravention of section 4 (1), in so far as it relates to the use or possession of a software or hardware tool, for purposes of contravening section 6 (1); or

(c) the offence of malicious injury to property,

the accused may be found guilty of the offence so proved.

(5)

(a) If the evidence on a charge of a contravention of section 7 (1) (a) or (d) does not prove the offence or a contravention of section 17 in respect of that offence, but proves a contravention of—

(i) section 2 (1) or (2);

(ii) section 7 (1) (b) or (c) or (2); or

(iii) section 4 (1), in so far as it relates to the use or possession of a software or hardware tool, to acquire or use a password, access code or similar data or device,

the accused may be found guilty of the offence so proved.

(b) If the evidence on a charge of a contravention of section 7 (1) (b) or (c) does not prove the offence or a contravention of section 17 in respect of that offence, but proves a contravention of section 7 (2), the accused may be found guilty of an offence so proved.

(6) If the evidence on a charge of a contravention of section 8, does not prove the offence or a contravention of section 17 in respect of the offence, but proves—

(a) a contravention of section 2 (1) or (2);

(b) a contravention of section 4 (1), in so far as it relates to the use or possession of a software or hardware tool, for the purposes of—

(i) interfering with data or a computer program as contemplated in section 5 (1); or

(ii) interfering with a computer data storage medium or a computer system as contemplated in section 6 (1);

(c) a contravention of section 7 (1) or (2), in so far as the password, access code or similar data or device was acquired, possessed, provided to another person or used for purposes of contravening the provisions of section 8;

(d) a contravention of section 9 (1) or (2);

(e) the common law offence of fraud or attempt to commit that offence;

(f) the common law offence of forgery or uttering or attempt to commit that offence; or

(g) the common law offence of theft or attempt to commit that offence,

the accused may be found guilty of the offence so proved.

(7)

(a) If the evidence on a charge of a contravention of section 9 (1), does not prove the offence or a contravention of section 17 in respect of the offence, but proves—

(i) the common law offence of forgery;

(ii) a contravention of section 9 (2); or

(iii) the common law offence of uttering,

the accused may be found guilty of the offence so proved.

(b) If the evidence on a charge of a contravention of section 9 (2), does not prove the offence, but proves the common law offence of uttering, the accused may be found guilty of the offence so proved.

(8) If an accused is charged with a contravention of section 11 (1), and the evidence on the charge does not prove a contravention of section 11 (1) or a contravention of section 17 in respect of that offence, but proves a contravention of—

(a) section 2 (1) or (2);

(b) section 3 (1) or any competent verdict provided for in subsection (2);

(c) section 5 (1) or any competent verdict provided for in subsection (3);

(d) section 6 (1) or any competent verdict provided for in subsection (4); or

(e) section 7 (1) or any competent verdict provided for in subsection (5),

the accused may be found guilty of the offence so proved.

(9) If an accused is charged with a contravention of section 11 (2), and the evidence on the charge does not prove the offence or a contravention of section 17 in respect of the offence, but proves a contravention of—

(a) section 2 (1) or (2);

(b) section 5 (1) or any competent verdict provided for in subsection (3); or

(c) section 6 (1) or any competent verdict provided for in subsection (4),

the accused may be found guilty of the offence so proved.

(10) If the evidence on a charge for any offence referred to in the preceding subsections does not prove the commission of the offence so charged or any competent verdict in respect of the offence, but proves the commission of an offence which by reason of the essential elements of that offence is included in the offence so charged, the accused may be found guilty of the offence so proved.

(11) If an accused is charged with a contravention of section 14, 15 or 16, and the evidence on the charge does not prove the offence in question or a contravention of section 17 in respect of the offence, but proves the commission of an offence which by reason of the essential elements of that offence is included in the offence so charged, the accused may be found guilty of the offence so proved.

## *Part V*
## *Sentencing*

### 19. Sentencing

(1) Any person who contravenes the provisions of section 2 (1) or (2), 3 (3) or 7 (2) is liable on conviction to a fine or to imprisonment for a period not exceeding five years or to both a fine and such imprisonment.

(2) Any person who contravenes the provisions of section 3 (1) or (2), 4 (1), 5 (1), 6 (1) or 7 (1) is liable on conviction to a fine or to imprisonment for a period not exceeding 10 years or to both a fine and such imprisonment.

(3) Any person who contravenes the provisions of section 11 (1) is liable on conviction to a fine or to imprisonment for a period not exceeding 15 years or to both a fine and such imprisonment.

(4) A court which convicts a person of an offence in terms of section 8, 9 (1) or (2), 10 or 11 (2) may, where a penalty is not prescribed in respect of that offence by any other law, impose a sentence, as provided for in section 276 of the Criminal Procedure Act, 1977, which that court considers appropriate and which is within that court's penal jurisdiction.

(5) A court which imposes any sentence in terms of this section, or where a person is convicted of the offence of theft that was committed or facilitated by electronic means, must, without excluding other relevant factors, consider as aggravating factors—

(a) the fact that the offence was committed by electronic means;

(b) the extent of the prejudice and loss suffered by the complainant or any other person as a result of the commission of such an offence;

(c) the extent to which the person gained financially, or received any favour, benefit, reward, compensation or any other advantage from the commission of the offence; or

(d) the fact that the offence was committed in concert with one or more persons.

(6)

(a) If a person is convicted of any offence provided for in section 2 (1) or (2), 3 (1), 5 (1), 6 (1), 7 (1), 8, 9 (1) or (2), 10 or 11 (1) or (2), a court imposing any sentence in terms of those sections must, unless substantial and compelling circumstances justify the

imposition of another sentence, impose a period of direct imprisonment, with or without a fine, if the offence was committed—

(i) by the person; or

(ii) with the collusion or assistance of another person,

who as part of their duties, functions or lawful authority were in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system belonging to another person in respect of which the offence in question was committed.

(b) A sentence imposed in terms of paragraph (a) may not be suspended as contemplated in section 297 (4) of the Criminal Procedure Act, 1977.

(7) Any person who contravenes the provisions of section 14, 15 or 16 is liable on conviction to a fine or to imprisonment for a period not exceeding three years or to both a fine and such imprisonment.

## *Part VI*

## *Orders to protect complainants from the harmful effect of malicious communications*

[Part IV commencement: To be proclaimed.]

### 20. Order to protect complainant pending finalisation of criminal proceedings

(1) A complainant (hereinafter referred to as the applicant) who lays a charge with the South African Police Service that an offence contemplated in section 14, 15 or 16 has allegedly been committed against them, may on an *ex parte* basis in the prescribed form and manner, apply to a magistrate's court for a protection order pending the finalisation of the criminal proceedings to—

(a) prohibit any person to disclose or further disclose the data message which relates to the charge; or

(b) order an electronic communications service provider whose electronic communications service is used to host or disclose the data message which relates to the charge, to remove or disable access to the data message.

(2) The court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (1) and may, for that purpose, consider any additional evidence it deems fit,

including oral evidence or evidence by affidavit, which must form part of the record of the proceedings.

(3) If the court is satisfied that there—

(a) is prima facie evidence that an offence referred to in section 14, 15 or 16, has allegedly been committed against the applicant; and

(b) are reasonable grounds to believe that a person referred to in subsection (1) (a) disclosed the data message in question; or

(c) are reasonable grounds to believe that the electronic communications service of the electronic communications service provider referred to in subsection (1) (b), is used to host or was or is used to disclose the data message in question,

the court may, subject to such conditions as the court may deem fit, issue the order referred to in subsection (1), in the prescribed form.

(4) The order, referred to in subsection (3), must be served on the person referred to in subsection (1) (a) or electronic communications service provider referred to in subsection (1) (b), in the prescribed manner: Provided, that if the court is satisfied that the order cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form or manner specified in that order.

(5) An order referred to in subsection (3) is of force and effect from the time it is issued by the court and the existence thereof has been brought to the attention of the person referred to in subsection (1) (a) or electronic communications service provider referred to in subsection (1) (b).

(6) A person referred to in subsection (1) (a), other than the person who is accused of having committed the offence in question, or an electronic communications service provider referred to in subsection (1) (b), may, within 14 days after the order has been served on them in terms of subsection (4) or within such further period as the court may allow, upon notice to the magistrate's court concerned, in the prescribed form and manner, apply to the court for the setting aside or amendment of the order referred to in subsection (3).

(7)

(a) The court must as soon as reasonably possible consider an application submitted to it in terms of subsection (6) and may, for that purpose, consider such additional evidence as it

deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings.

(b) The court may, if good cause is shown for the variation or setting aside of the protection order, issue an order to this effect.

(8) The court may, for purposes of subsections (2) and (7), in the prescribed form and manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case.

(9) Any person referred to in subsection (1) (a) or an electronic communications service provider, referred to in subsection (1) (b), that fails to comply with an order referred to in subsection (3) or any variations thereof, is guilty of an offence.

(10) Any person who is subpoenaed in terms of subsection (8) to attend proceedings and who fails to—

(a) attend or to remain in attendance;

(b) appear at the place and on the date and at the time to which the proceedings in question may be adjourned;

(c) remain in attendance at those proceedings as so adjourned; or

(d) produce any book, document or object specified in the subpoena,

is guilty of an offence.

(11) The provisions in respect of appeal and review as provided for in the Magistrates' Courts Act, 1944, and the Superior Courts Act, 2013, apply to proceedings in terms of this section.

(12) For purposes of this section and sections 21 and 22 **"to host a data message"** means to store the data message on an electronic communications network that is used to provide an electronic communications service, where it can be viewed, copied or downloaded.

[S 20 commencement: To be proclaimed.]

**21. Electronic communications service provider to furnish particulars to court**

(1) If an application for a protection order is made in terms of section 20 (1) and the court is satisfied in terms of section 20 (3) that a protection order must be issued and the particulars of the person referred to in section 20 (1) (a), who discloses the data message, or the electronic communications service provider referred to in section 20 (1) (b), whose service is used to host or was or is used to disclose the data message, is not known, the court may—

(a) adjourn the proceedings to any time and date on the terms and conditions which the court deems appropriate; and

(b) issue a direction in the prescribed form, directing an electronic communications service provider, that is believed to be able to furnish such particulars, to furnish the court in the prescribed manner by means of an affidavit in the prescribed form with—

(i) the electronic communications identity number from where the data message originated;

(ii) the name, surname, identity number and address of the person to whom the electronic communications identity number has been assigned;

(iii) any information which indicates that the data message was or was not sent from the electronic communications identity number of the person to the electronic communications identity number of the applicant;

(iv) any information that is available to an electronic communications service provider that may be of assistance to the court to identify the person referred to in section 20 (1) (a) or the electronic communications service provider referred to in section 20 (1) (b), which provides a service to that person;

(v) any information that is available to an electronic communications service provider which—

(aa) confirms whether or not its electronic communications service is used to host or was or is used to disclose the data message in question; or

(bb) may be of assistance to the court to identify the electronic communications service provider whose service is used to host or was or is used to disclose the data message in questions; or

(vi) an assessment whether or not the electronic communications service provider is in a position to—

(aa) remove the data message or a link to such data message; or

(bb) disable access to the data message or a link to such data message.

(2) If the court issues a direction in terms of subsection (1) (b), the court must direct that the direction be served on the electronic communications service provider in the prescribed manner: Provided, that if the court is satisfied that the direction cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form or manner specified in that order.

(3)

(a) The information referred to in subsection (1) (b) must be provided to the court within five ordinary court days from the time that the direction is served on an electronic communications service provider.

(b) An electronic communications service provider on which a direction is served, may in the prescribed manner by means of an affidavit in the prescribed form apply to the court for—

(i) an extension of the period of five ordinary court days referred to in paragraph (a) for a further period of five ordinary court days on the grounds that the information cannot be provided timeously; or

(ii) the cancellation of the direction on the grounds that—

(aa) it does not provide an electronic communications service to the applicant or the person referred to in section 20 (1) (a);

(bb) the requested information is not available in the records of the electronic communications service provider; or

(cc) its service is not used to host or was or is not used to disclose the data message in question.

(4) After receipt of an application in terms of subsection (3) (b), the court—

(a) must consider the application;

(b) may, in the prescribed manner, request such additional evidence by way of an affidavit from the electronic communications service provider as it deems fit;

(c) must give a decision in respect thereof; and

(d) must inform the electronic communications service provider in the prescribed form and manner of the outcome of the application.

(5)

(a) The court may, on receipt of an affidavit from an electronic communications service provider which contains the information referred to in subsection (1) (b), consider the issuing of a protection order in terms of section 20 (3) against the person or electronic communications service provider on the date to which the proceedings have been adjourned.

(b) Any information furnished to the court in terms of subsection (1) (b) forms part of the evidence that a court may consider in terms of section 20 (3).

(6) The Cabinet member responsible for the administration of justice may, by notice in the Gazette, prescribe reasonable tariffs of compensation payable to electronic communications service providers for providing the information referred to in subsection (1) (b).

(7) Any electronic communications service provider or employee of an electronic communications service provider who—

(a) fails to furnish the required information within five ordinary court days from the time that the direction is served on such electronic communications service provider to a court in terms of subsection (3) (a) or such extended period allowed by the court in terms of subsection (3) (b); or

(b) makes a false statement in an affidavit referred to in subsection (1) (b) or (3) (b) in a material respect,

is guilty of an offence.

(8) For purposes of this section **"electronic communications identity number"** means a technical identification label which represents the origin or destination of electronic communications traffic.

[S 21 commencement: To be proclaimed.]

**22. Orders on finalisation of criminal proceedings**

(1) Whenever a person is—

(a) convicted of an offence in terms of section 14, 15 or 16; or

(b) acquitted of an offence in terms of section 14, 15 or 16,

but evidence proves that the person engaged in, or attempted to engage in, harassment as contemplated in the Protection from Harassment Act, 2011, the trial court may, after holding an enquiry, issue a protection order contemplated in section 9 (4) of the Protection from Harassment Act, 2011, against the person, whereafter the provision of that Act must apply with the necessary changes as required by the context.

(2) The trial court which convicts a person of an offence contemplated in section 14, 15 or 16, must order—

(a) that person to refrain from further making available, disclosing or distributing the data message contemplated in section 14, 15 or 16, which relates to the charge on which that person is convicted;

(b) that person or any other person to destroy the data message in question, any copy of the data message or any output of the data message and to submit an affidavit in the prescribed form to the prosecutor identified in the order that the data message has been so destroyed; or

(c) an electronic communications service provider to remove or disable access to the data message in question.

(3) The order referred to in subsection (2) (b), in so far as it relates to a person other than the person who has been convicted of the offence, and subsection (2) (c), must be in the prescribed form and must be served on the person or electronic communications service provider in the prescribed manner: Provided, that if the trial court is satisfied that the order cannot be served in the prescribed form and manner, the court may make an order allowing service to be effected in the form or manner specified in that order.

(4) Any person contemplated in subsection (2) (a) or (b) or electronic communications service provider contemplated in subsection (2) (c), that fails to comply with an order referred to in subsection (2), is guilty of an offence.

(5) An electronic communications service provider that is ordered to remove or disable access to the data message may, within 14 days after the order has been served on it in terms of subsection (3), upon notice to the trial court concerned, in the prescribed form and manner, apply to the court for the setting aside or amendment of the order referred to in subsection (2) (c).

(6)

(a) The trial court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (5) and may for that purpose, consider such additional evidence as it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings.

(b) The trial court may, if good cause has been shown for the variation or setting aside of the order, issue an order to this effect.

(7) The court may, for purposes of subsection (6) (a), in the prescribed form and manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case.

(8) Any person who is subpoenaed in terms of subsection (7) to attend proceedings and who fails to—

(a) attend or to remain in attendance;

(b) appear at the place and on the date and at the time to which the proceedings in question may be adjourned;

(c) remain in attendance at those proceedings as so adjourned; or

(d) produce any book, document or object specified in the subpoena,

is guilty of an offence.

(9) For purposes of this section **"trial court"** means—

(a) a magistrate's court established under section 2 (1) (f) (i) of the Magistrates' Courts Act, 1944;

(b) a court for a regional division established under section 2 (1) (g) (i) of the Magistrates' Courts Act, 1944; or

(c) a High Court referred to in section 6 (1) of the Superior Courts Act, 2013.

(10) Whenever a person is convicted of an offence in terms of section 14, 15 or 16, the trial court must issue an order that the person must reimburse all expenses reasonably incurred by—

(a) a complainant as a result of any direction issued in terms of section 21 (1) (b); or

(b) an electronic communications service provider to remove or disable access to the data message in question,

whereupon the provisions of section 300 of the Criminal Procedure Act, 1977, shall apply with the necessary changes required by the context, to such order.

[S 22 commencement: To be proclaimed.]

**23. Penalties**

Any person or electronic communications service provider that is convicted of an offence referred in section 20 (9) or (10), 21 (7) or 22 (4) or (8), is liable on conviction to a fine or to imprisonment for a period not exceeding two years or to both a fine and such imprisonment.

[S 23 commencement: To be proclaimed.]

## CHAPTER 3
## JURISDICTION

**24. Jurisdiction**

(1) A court in the Republic has jurisdiction to try any offence referred to in Part I or Part II of Chapter 2, if—

(a) the accused was arrested in the territory of the Republic, on board a vessel, a ship, an off-shore installation or fixed platform, or an aircraft registered or required to be registered in the Republic;

(b) the person to be charged is—

(i) a citizen of the Republic or ordinary resident in the Republic;

(ii) a company, incorporated or registered as such under any law, in the Republic; or

(iii) any body of persons, corporate or unincorporated, in the Republic;

(c) the offence was committed—

(i) in the territory of the Republic; or

(ii) on board a vessel, a ship, an off-shore installation, or a fixed platform, or an aircraft registered or required to be registered in the Republic at the time that the offence was committed;

(d) any act in preparation of the offence or any action necessary to commit the offence or any part of the offence took place—

(i) in the territory of the Republic; or

(ii) on board a vessel, a ship, an off-shore installation or fixed platform, or an aircraft registered or required to be registered in the Republic at the time when the act, action or part of the offence took place;

(e) the offence affects any person, a restricted computer system contemplated in section 11 (1) (b), a public body or any business, in the Republic;

(f) the offence was committed outside of the Republic against—

(i) any person who is a citizen of the Republic or ordinarily resident in the Republic;

(ii) a restricted computer system contemplated in section 11 (1) (b);

(iii) a company, incorporated or registered as such under any law, in the Republic;

(iv) any body of persons, corporate or unincorporated, in the Republic; or

(v) a government facility of the Republic, including an embassy or other diplomatic or consular premises, or any other property of the Republic; or

(g) the evidence reveals any other basis recognised by law in terms of which the court may assert jurisdiction to try the offence.

(2) Any act alleged to constitute an offence referred to in Part I or Part II of Chapter 2 and which is committed outside the Republic by a person other than a person contemplated in subsection (1), must, regardless of whether or not the act constitutes an offence at the place of its commission, be deemed to have been committed in the Republic if—

(a) that person is extradited to the Republic; or

(b) that person—

(i) is found to be in the Republic; and

(ii) is for one or other reason not extradited by the Republic or if there is no application to extradite the person.

(3) Where a person is charged with attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence or as an accessory after the offence, the offence is deemed to have been committed not only at the place where the act was committed, but also at every place where the person so acted.

(4)

(a) A prosecution of an offence referred to in Part I or Part II of Chapter 2, which was committed outside the Republic—

(i) may only be instituted against a person with the written permission of the National Director of Public Prosecutions; and

(ii) must commence before a court designated by the National Director of Public Prosecutions.

(b) The accused must be served with a copy of the written permission and designation and the original thereof must be handed in at the court in which the proceedings are to commence.

(5) The National Commissioner and the National Head of the Directorate, in consultation with the National Director of Public Prosecutions, must issue directives, with which all police officials must comply in the execution of their functions in terms of this Act, regarding the investigation of offences that were committed outside the Republic.

## CHAPTER 4
## POWERS TO INVESTIGATE, SEARCH, ACCESS OR SEIZE

### 25. Definitions

In this Chapter, unless the context indicates otherwise—

**"access"** includes without limitation to make use of—

(a) a computer data storage medium, or a computer system, or their accessories and components or any part thereof or any ancillary device or component thereto; and

(b) data or a computer program held in a computer data storage medium or a computer system,

to the extent necessary to search for and seize an article;

**"investigator"** means any fit and proper person, who is not a member of the South African Police Service and who is—

(a) identified and authorised in terms of a search warrant as contemplated in section 29 (3); or

(b) requested by a police official in terms of section 31 (2), 32 (3) or 33 (4),

to, subject to the direction and control of a police official, assist the police official with the search for, access or seizure of an article; and

**"seize"** includes to—

(a) remove a computer data storage medium or any part of a computer system;

(b) render inaccessible, data, a computer program, a computer data storage medium or any part of a computer system in order to preserve evidence;

(c) make and retain a copy of data or a computer program; or

(d) make and retain a printout of the output of data or a computer program.

**26.* Standard Operating Procedures**

(1) The Cabinet member responsible for policing, in consultation with the National Commissioner, the National Head of the Directorate, the National Director of Public Prosecutions and the Cabinet member responsible for the administration of justice must, after following a process of public consultation, within 12 months of the commencement of this Chapter, issue Standard Operating Procedures which must be observed by—

(a) the South African Police Service; or

(b) any other person or agency who or which is authorised in terms of the provisions of any other law to investigate any offence in terms of any law,

in the investigation of any offence or suspected offence in terms of Part I or Part II of Chapter 2 or any other offence or suspected offence which may be committed by means of, or facilitated through the use of, an article.

(2) The Standard Operating Procedures referred to in subsection (1) and any amendment thereto must be published in the *Gazette*.

*Standard Operating Procedures for the investigation, search, access or seizure of articles – GN 3950, G. 49447, 6 October 2023.

**27. Application of Criminal Procedure Act, 1977**

The Criminal Procedure Act, 1977, applies in addition to the provisions of this Chapter in so far that it is not inconsistent with the provisions of this Chapter.

**28. Search for, access to, or seizure of certain articles**

A police official may, in accordance with the provisions of this Chapter, search for, access or seize any article, within the Republic.

**29. Article to be searched for, accessed or seized under search warrant**

(1) Subject to the provisions of sections 31, 32, 33 and 40 (1) and (2) of this Act, section 4 (3) of the Customs and Excise Act, 1964, sections 69 (2) (b) and 71 of the Tax Administration Act, 2011, and section 21 (e) and (f) of the Customs Control Act, 2014, an article can only be searched for, accessed or seized by virtue of a search warrant issued—

(a) by a magistrate or judge of the High Court, on written application by a police official, if it appears to the magistrate or judge, from information on oath or by way of affirmation, as set out in the application, that there are reasonable grounds for believing that an article—

(i) is within their area of jurisdiction; or

(ii) is being used or is involved or has been used or was involved in the commission of an offence—

(aa) within their area of jurisdiction; or

(bb) within the Republic, if it is unsure within which area of jurisdiction the article is being used or is involved or has been used or was involved in the commission of an offence; or

(b) by a magistrate or judge of the High Court presiding at criminal proceedings, if it appears to such magistrate or judge that an article is required in evidence at such proceedings.

(2) A search warrant issued under subsection (1) must require a police official identified in the warrant to search for, access or seize the article in question and, to that end, must authorise the police official to—

(a) search any person identified in the warrant;

(b) enter and search any container, premises, vehicle, facility, ship or aircraft identified in the warrant;

(c) search any person who is believed, on reasonable grounds, to be able to furnish any information of material importance concerning the matter under investigation and who is found near such container, on or at such premises, vehicle, facility, ship or aircraft;

(d) search any person who is believed, on reasonable grounds, to be able to furnish any information of material importance concerning the matter under investigation and who—

(i) is nearby;

(ii) uses; or

(iii) is in possession or in direct control of,

any data, computer program, computer data storage medium or computer system identified in the warrant to the extent set out in the warrant;

(e) search for any article identified in the warrant to the extent set out in the warrant;

(f) access an article identified in the warrant to the extent set out in the warrant;

(g) seize an article identified in the warrant to the extent set out in the warrant; or

(h) use or obtain and use any instrument, device, equipment, password, decryption key, data, computer program, computer data storage medium or computer system or other information that is believed, on reasonable grounds, to be necessary to search for, access or seize an article identified in the warrant to the extent set out in the warrant.

(3) A search warrant issued under subsection (1) may require an investigator or other person identified in the warrant to assist the police official identified in the warrant, with the search for, access or seizure of the article in question, to the extent set out in the warrant.

(4)

(a) A search warrant may be executed at any time, unless the person issuing the warrant in writing specifies otherwise.

(b) A search warrant may be issued on any day and is of force until it is executed or is cancelled by the person who issued it or, if such person is not available, by a person with like authority.

(5) A police official who executes a warrant under this section must hand to any person whose rights in respect of any search, or article accessed or seized under the warrant have been affected, a copy of the warrant and the written application of the police official contemplated in subsection (1) (a).

(6) The provisions of subsections (1) to (5) apply with the changes required by the context to an amendment of a warrant issued in terms of subsection (1).

**30. Oral application for search warrant or amendment of warrant**

(1) An application referred to in section 29 (1) (a), or an application for the amendment of a warrant issued in terms of section 29 (1) (a), may be made orally by a specifically designated police official, if 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) indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the police official, justify the making of an oral application; and

(b) comply with any supplementary directives relating to oral applications which may be issued by the Chief Justice in terms of section 8 (3) of the Superior Courts Act, 2013.

(3) A magistrate or judge of the High Court may, upon an oral application made to them in terms of subsection (1) and subject to subsection (4), issue a warrant or amend a warrant as contemplated in section 29 (1) (a).

(4) A warrant or any amendment to a warrant may only be issued under subsection (3)—

(a) if the magistrate or judge of the High Court concerned is satisfied, on the facts alleged in the oral application concerned, that—

(i) there are reasonable grounds to believe that a warrant or any amendment to a warrant applied for could be issued;

(ii) a warrant or an amendment to a warrant is necessary immediately in order to search for, access or seize an article—

(aa) within their area of jurisdiction; or

(bb) within the Republic, if it is unsure within which area of jurisdiction the article is being used or is involved or has been used or was involved in the commission of an offence; 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 a warrant or to amend a warrant; and

(b) on condition that the police official concerned must submit a written application to the magistrate or judge of the High Court concerned within 48 hours after the issuing of the warrant or amended warrant under subsection (3).

(5) warrant or any amendment to a warrant issued under subsection (3) must—

(a) be in writing;

(b) be transmitted electronically to the police official or be provided to the specifically designated police official; and

(c) contain a summary of the facts which were considered and the grounds upon which the warrant was issued.

(6) A magistrate or judge of the High Court who has issued a warrant or amended a warrant under subsection (3) or, if unavailable, any other magistrate or judge of the High Court must, upon receipt of a written application in terms of subsection (4) (b), reconsider that application whereupon they may confirm, amend or cancel that warrant.

(7) A magistrate or judge of the High Court contemplated in subsection (6), who amends or cancels the warrant, must make an order they deem fit on how any article which is affected by their decision is to be dealt with.

**31. Search for, access to, or seizure of article without search warrant with consent of person who has lawful authority to consent**

(1) Any police official may, without a search warrant, execute the powers referred to in section 29 (2), subject to any other law, if the person who has the lawful authority to consent to the search for, access to, or seizure of the article in question, consents, in writing, to such search, access or seizure.

(2) A police official acting in terms of subsection (1), may, subject to the lawful consent, in writing, of the person who has the lawful authority to consent, in writing authorise an investigator to assist them with the search for, access to, or seizure of the article in question.

**32. Search for, access to, or seizure of article involved in the commission of an offence without search warrant**

(1) A police official may without a search warrant referred to in section 29 (1) (a) search any person, container, premises, vehicle, facility, ship or aircraft for the purposes of performing the

powers referred to in paragraphs (a) and (b) of the definition of “seize” in respect of a computer data storage medium or any part of a computer system referred to in paragraph (c) or (d) of the definition of “article”, if the police official on reasonable grounds believes—

(a) that a search warrant will be issued to them under section 29 (1) (a) if they apply for such warrant; and

(b) that the delay in obtaining such warrant would defeat the object of the search and seizure.

(2) A police official may only access or perform the powers referred to in paragraphs (c) or (d) of the definition of “seize”, in respect of the computer data storage medium or a computer system referred to in subsection (1), in accordance with a search warrant issued in terms of section 29 (1) (a): Provided that a police official may, if they on reasonable grounds believe—

(a) that a search warrant will be issued to them under section 29 (1) (a) if they apply for such warrant; and

(b) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written or oral application for a search warrant,

access and perform the powers referred to in paragraph (c) or (d) of the definition of “seize” without a search warrant.

(3) An investigator authorised in writing by a police official may assist the police official to seize an article as contemplated subsections (1) and (2) and to access the article as contemplated in subsection (2).

**33. Search for, access to, or seizure of article on arrest of person**

(1) police official may without a warrant, as contemplated in section 40 of the Criminal Procedure Act, 1977, arrest any person—

(a) who commits any offence in terms of Part I or Part II of Chapter 2 in their presence;

(b) whom they reasonably suspect of having committed any offence in terms of Part I and part II of Chapter 2; or

(c) who is concerned with or against whom a reasonable complaint has been made or credible information has been received or a reasonable suspicion exists that they have been concerned with an offence—

(i) similar to those contemplated in Part I or Part II of Chapter 2; or

(ii) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article,

in a foreign State, and for which they are, under any law relating to extradition or fugitive offenders, liable to be arrested or detained in custody in the Republic.

(2) On the arrest of a person contemplated in subsection (1) or in terms of section 40 or 43 of the Criminal Procedure Act, 1977, a police official may search for and perform the powers referred to in paragraphs (a) and (b) of the definition of “seize” in respect of a computer data storage medium or any part of a computer system referred to in paragraph (c) or (d) of the definition of “article”, which is found in the possession of or in the custody or under the control of the person.

(3) A police official may only access or perform the powers referred to in paragraph (c) or (d) of the definition of “seize”, in respect of a computer data storage medium or a computer system referred to in subsection (2), in accordance with a search warrant issued in terms of section 29 (1) (a): Provided that a police official may, if they on reasonable grounds believe—

(a) that a search warrant will be issued to them under section 29 (1) (a), if they apply for such warrant; and

(b) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written or oral application for a search warrant,

access and perform the powers referred to in paragraph (c) and (d) of the definition of “seize” without a search warrant.

(4) An investigator authorised in writing by a police official may assist the police official to seize an article as contemplated subsections (2) and (3) and to access the article as contemplated in subsection (3).

**34. Assisting police official or investigator**

(1) An electronic communications service provider, financial institution or person, other than the person who is suspected of having committed the offence which is being investigated, who is in control of any container, premises, vehicle, facility, ship, aircraft, data, computer program, computer data storage medium or computer system that is subject to a search authorised in terms of section 29 (1) must, if required, provide—

(a) technical assistance; and

(b) such other assistance as may be reasonably necessary,

to a police official or investigator in order to search for, access or seize an article.

(2) An electronic communications service provider, financial institution or person who fails to comply with the provisions of subsection (1), is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment.

**35. Obstructing or hindering police official or investigator and authority to overcome resistance**

(1) Any person who unlawfully and intentionally obstructs or hinders a police official or an investigator in the exercise of their powers or the performance of their duties or functions in terms of this Chapter or who refuses or fails to comply with a search warrant issued in terms of section 29 (1), is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment.

(2)

(a) A police official who may lawfully execute any power conferred upon them in terms of section 29 (2), may use such force as may be—

(i) reasonably necessary; and

(ii) proportional to all the circumstances,

relating to the execution of such powers.

(b) No police official may enter upon or search any premises, vehicle, facility, ship or aircraft unless they have audibly demanded admission to the premises, vehicle, facility, ship or aircraft and have notified the purpose of their entry.

(c) The provisions of paragraph (b) do not apply where the police official is, on reasonable grounds, of the opinion that an article which is the subject of the search may be destroyed, disposed of or tampered with if the provisions of paragraph (b) are complied with.

**36. Powers conferred upon police official or investigator to be conducted in decent and orderly manner with due regard to rights of other persons**

(1) The powers conferred upon a police official or an investigator in terms of section 29 (2), 31, 32 or 33, must be conducted—

(a) with strict regard to decency and order; and

(b) with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence.

(2) If a female needs to be searched physically in terms of section 29 (2) (a), (c) or (d), 32 or 33, such search must be carried out by a police official who is also a female: Provided that if no female police official is available, the search must be carried out by any female designated for that purpose by a police official.

**37. Wrongful search, access or seizure and restriction on use of instrument, device, password or decryption key or information to gain access**

(1) A police official or an investigator who unlawfully and intentionally—

(a) acts contrary to the authority of—

(i) a search warrant issued under section 29 (1); or

(ii) consent granted in terms of section 31 (1); or

(b) without being authorised thereto under this Chapter or the provision of any other law which affords similar powers to a police official or an investigator—

(i) searches for, accesses or seizes data, a computer program, a computer data storage medium or any part of a computer system; or

(ii) obtains or uses any instrument, device, password, decryption key or other information that is necessary to access data, a computer program, a computer data storage medium or any part of a computer system,

is guilty of an offence.

(2)

(a) A police official or an investigator who obtains or uses any instrument, device, equipment, password, decryption key, data or other information contemplated in section 29 (2) (h)—

(i) must use the instrument, device, equipment, password, decryption key, data or information only in respect of and to the extent specified in the warrant to gain access to or use data, a computer program, a computer data storage medium or any part of a computer system in the manner and for the purposes specified in the search warrant concerned; and

(ii) must destroy all passwords, decryption keys, data or other information if—

(aa) it is not required by a person who may lawfully possess the passwords, decryption keys, data or other information;

(bb) it will not be required for purposes of any criminal proceedings or civil proceedings contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, 1998, or for purposes of evidence or for purposes of an order of court; or

(cc) no criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, 1998, are to be instituted in connection with such information.

(b) A police official or an investigator who unlawfully and intentionally—

(i) uses any instrument, device, equipment, password, decryption key, data or information outside the authorisation of a warrant as contemplated in paragraph (a) (i); or

(ii) fails to destroy all passwords, decryption keys, data or other information as contemplated in paragraph (a) (ii),

is guilty of an offence.

(3) A police official or an investigator who contravenes or fails to comply with subsection (1) or (2), is liable on conviction to a fine or imprisonment for a period not exceeding 2 years or to both a fine and such imprisonment.

(4) Where a police official or an investigator is convicted of an offence referred to in subsection (1) or (2), the court convicting such a person may, upon application of any person who has suffered damage or upon the application of the prosecutor acting on the instructions of that person, award compensation in respect of such damage, whereupon the provisions of section 300 of the Criminal Procedure Act, 1977, shall apply with the necessary changes required by the context to such award.

**38. False information under oath or by way of affirmation**

(1) Any person who unlawfully or intentionally gives false information under oath or by way of affirmation knowing it to be false or not knowing it to be true, with the result that—

(a) a search warrant is issued;

(b) a search contemplated in section 31 took place on the basis of such information;

(c) a person, container, premises, vehicle, facility, ship or aircraft is searched or a computer data storage medium or any part of a computer system is seized or accessed in terms of section 32;

(d) an expedited preservation of data direction contemplated in section 41 is issued;
[S 38 (1) (d) commencement: To be proclaimed.]

(e) a preservation of evidence direction contemplated in section 42 is issued; or
[S 38 (1) (e) commencement: To be proclaimed.]

(f) a disclosure of data direction contemplated in section 44 is issued,
[S 38 (1) (f) commencement: To be proclaimed.]

is guilty of an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding two years or to both such fine and imprisonment.

(2) Where a person is convicted of an offence referred to in subsection (1), the court convicting such a person may, upon application of any person who has suffered damage or upon the application of the prosecutor acting on the instructions of that person, award compensation in respect of such damage, whereupon the provisions of section 300 of the Criminal Procedure Act, 1977, shall apply with the necessary changes required by the context to such award.

**39. Prohibition on disclosure of information**

(1) No person, investigator, police official, electronic communications service provider, financial institution or an employee of an electronic communications service provider or financial institution may, subject to subsection (2), disclose any information which they have obtained in the exercise of their powers or the performance of their duties in terms of Chapter 4 or 5 of this Act, except—

(a) to any other person who of necessity requires it for the performance of their functions in terms of this Act;

(b) if they are a person who of necessity supplies such information in the performance of their duties or functions in terms of this Act;

(c) if it is information which is required in terms of any law or as evidence in any court of law;

(d) if it constitutes information-sharing between electronic communications service providers, financial institutions, the South African Police Service, competent authorities or any other person or entity which is aimed at preventing, detecting, investigating or mitigating cybercrime: Provided that such information-sharing may not prejudice any criminal investigation or criminal proceedings; or

(e) to any competent authority in a foreign State which requires it for the prevention, detection, or mitigation of cybercrime, or the institution of criminal proceedings or an investigation with a view to institute criminal proceedings.

(2) The prohibition on disclosure of information contemplated in subsection (1) does not apply where the disclosure—

(a) is authorised in terms of this Act or any other Act of Parliament; or

(b) reveals a criminal activity.

(3) A person, investigator, police official, electronic communications service provider, financial institution or an employee of an electronic communications service provider or financial institution who unlawfully and intentionally contravenes the provisions of subsection (1) is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding three years or to both a fine and such imprisonment.

**40. Interception of indirect communication and obtaining of real-time communication-related information**

(1) The interception of an indirect communication as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication related Information Act, 2002, must take place in terms of a direction issued in terms of section 16 (4) or 18 (3) of that Act and must, subject to subsection (4), be dealt with further in the manner provided for in that Act.

(2) The obtaining of real-time communication-related information as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, on an ongoing basis, as it becomes available, must take place in terms of a direction issued in terms of section 17 (3) or 18 (3) of that Act, and must, subject to subsection (4), be dealt with further in the manner provided for in that Act.

(3) An electronic communications service provider who is—

(a) in terms of section 30 (1) (b) of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, required to provide an electronic communications service which has the capability to store communication-related information; and

(b) not required to store communication-related information in terms of a directive issued in terms of section 30 (2) of that Act,

must, in addition to any other obligation imposed by any law, comply with—

(i) a real-time communication-related direction contemplated in subsection (2), in terms of which the electronic communications service provider is directed to provide real-time communication-related information in respect of a customer, on an ongoing basis, as it becomes available;

(ii) an expedited preservation of data direction contemplated in section 41, in terms of which the electronic communications service provider is directed to preserve real-time communication-related information in respect of a customer;

(iii) a preservation of evidence direction contemplated in section 42, in terms of which the electronic communications service provider is directed to preserve real-time communication-related information in respect of a customer;

(iv) a disclosure of data direction contemplated in section 44, in terms of which the electronic communications service provider is directed to provide real-time communication-related information in respect of a customer that was preserved or otherwise stored by the electronic communications service provider; or

(v) any order of the designated judge in terms of section 48 (6), in terms of which the electronic communications service provider is ordered to—

(aa) obtain and preserve any real-time communication-related information; or

(bb) obtain and furnish traffic data.

[S 40 (3) commencement: To be proclaimed.]

(4) Any indirect communication which is to be intercepted or any real-time communication-related information or traffic data which is to be obtained, at the request of an authority, court or tribunal exercising jurisdiction in a foreign State must further be dealt with in the manner provided for in an order referred to in section 48 (6), which is issued by the designated judge.

[S 40 (4) commencement: To be proclaimed.]

**41. Expedited preservation of data direction**

(1) A specifically designated police official may—

(a) if they believe on reasonable grounds that any person, an electronic communications service provider referred to in section 40 (3), or a financial institution is—

(i) in possession of;

(ii) to receive; or

(iii) in control of, data as contemplated in paragraph (a) of the definition of “article”; and

(b) with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence in question,

issue an expedited preservation of data direction to such a person, electronic communications service provider or financial institution.

(2) Subsection (1) also applies to—

(a) archived communication-related information which an electronic communications service provider is no longer required to store due to the fact that the period contemplated in section 30 (2) (a) (iii) of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, is due to come to an end; or

(b) any other data which—

(i) must be stored for a certain period in terms of any other law and that period is due to come to an end; or

(ii) is stored by an electronic communications service provider which is not real-time communication-related information or archived communication-related information as contemplated in section 1, read with section 30 (2) and any directive issued in terms of that section, of the Regulation of Interception of Communications and Provision of Communication related Information Act, 2002.

(3) An expedited preservation of data direction must be in the prescribed form and must be served on the person, electronic communications service provider or financial institution affected thereby, in the prescribed manner by a police official.

(4) An expedited preservation of data direction must direct the person, electronic communications service provider or financial institution affected thereby, from the time of service of the direction, and for a period of 21 days—

(a) to preserve the current status of;

(b) not to deal in any manner with; or

(c) to deal in a certain manner with,

the data referred to in the direction in order to preserve the availability and integrity of the data.

(5) No data may be disclosed to a police official on the strength of an expedited preservation of data direction, unless it is authorised in terms of section 44.

(6) The 21 day period referred to in subsection (4), may only be extended by way of a preservation of evidence direction contemplated in section 42, once, for an additional period which may not exceed 90 days.

(7) A person, electronic communications service provider or financial institution to whom an expedited preservation of data direction, referred to in subsection (1), is addressed may, in writing in the prescribed form and manner, apply to a magistrate in whose area of jurisdiction the person, electronic communications service provider or financial institution is situated, for an amendment or the cancellation of the direction concerned on the ground that they cannot timeously or in a reasonable fashion, comply with the direction.

(8) The magistrate to whom an application is made in terms of subsection (7) must, as soon as possible after receipt thereof—

(a) consider the application and may for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application;

(b) give a decision in respect of the application; and

(c) inform the applicant and specifically designated police official referred to in subsection (1) of the outcome of the application.

(9) A person, electronic communications service provider or financial institution referred to in subsection (1) who—

(a) fails to comply with an expedited preservation of data direction or contravenes the provisions of subsection (5); or

(b) makes a false statement in an application referred to in subsection (7),

is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment.

[S 41 commencement: To be proclaimed.]

**42. Preservation of evidence direction**

(1) A magistrate or judge of the High Court, may—

(a) upon written application by a police official;

(b) if it appears to the magistrate or judge upon consideration of the information provided under oath or by way of affirmation, as set out in the application, that there are reasonable grounds to believe that any person, electronic communications service provider or financial institution—

(i) may receive;

(ii) is in possession of; or

(iii) is in control of,

an article; and

(c) with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence in question,

issue a preservation of evidence direction.

(2) A preservation of evidence direction must be in the prescribed form and must be served on the person, electronic communications service provider or financial institution affected thereby, in the prescribed manner by a police official.

(3) The preservation of evidence direction must direct the person, electronic communications service provider or financial institution, from the time of service of the direction, and for the time period specified in the direction, which may not exceed 90 days—

(a) to preserve the current status of;

(b) not to deal in any manner with; or

(c) to deal in a certain manner with,

an article in order to preserve the availability or integrity of the article.

(4) Any person, electronic communications service provider or financial institution who fails to comply with a preservation of evidence direction is guilty of an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding three years or to both a fine and such imprisonment.

(5) A person, electronic communications service provider or financial institution to whom a preservation of evidence direction referred to in subsection (1) is addressed may, in writing in the prescribed form and manner, apply to a magistrate or judge of the High Court in whose area of jurisdiction the person, electronic communications service provider or financial institution is situated for an amendment or the cancellation of the direction concerned on the ground that they cannot timeously or in a reasonable fashion, comply with the direction.

(6) The magistrate or judge of the High Court to whom an application is made in terms of subsection (5) must, as soon as possible after receipt thereof—

(a) consider the application and may, for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application;

(b) give a decision in respect of the application; and

(c) inform the applicant and police official of the outcome of the application.

[S 42 commencement: To be proclaimed.]

**43. Oral application for preservation of evidence direction**

(1) A police official may orally make an application referred to in section 42 (1), if they are 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) indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the police official, justify the making of an oral application; and

(b) comply with any supplementary directives relating to oral applications which may be issued by the Chief Justice in terms of section 8 (3) of the Superior Courts Act, 2013.

(3) A magistrate or judge of the High Court may, upon receipt of an oral application made to them in terms of subsection (1), issue the preservation of evidence direction applied for.

(4) A preservation of evidence direction may only be issued under subsection (3)—

(a) if the magistrate or judge of the High Court concerned is satisfied, on the facts alleged in the oral application concerned, that—

(i) there are reasonable grounds to believe that a preservation of evidence direction applied for could be issued;

(ii) a preservation of evidence direction is necessary immediately in order to ensure the availability or integrity, of the article; 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 preservation of evidence direction applied for; and

(b) on condition that the police official concerned must submit a written application to the magistrate or judge of the High Court concerned within 48 hours after the issuing of the preservation of evidence direction under subsection (3).

(5) A preservation of evidence direction issued under subsection (3) must be in writing and must be transmitted electronically to the police official or be provided to a specifically designated police official.

(6) A magistrate or judge of the High Court who issued a direction under subsection (3) or, if they are not available, any other magistrate or judge of the High Court must, upon receipt of a written application in terms of subsection (4) (b), reconsider that application whereupon they may confirm, amend or cancel that preservation of evidence direction.

[S 43 commencement: To be proclaimed.]

**44. Disclosure of data direction and search for, access to, and seizure of articles subject to preservation**

(1)

(a) A police official may, where it is expedient, other than by way of a search and seizure in terms of a warrant contemplated in section 29 (1), to obtain—

(i) data which is subject to preservation in terms of an expedited preservation of data direction or a preservation of evidence direction; or

(ii) data as contemplated in paragraph (a) of the definition of “article”, which is—

(aa) held in a computer system or computer storage medium; or

(bb) available to a computer system,

apply to a magistrate or judge of the High Court for the issuing of a disclosure of data direction.

(b) An application referred to in paragraph (a) (i) must—

(i) indicate the identity of the police official who applies for the disclosure of data direction;

(ii) identify the person, electronic communications service provider or financial institution to whom the disclosure of data direction must be addressed;

(iii) be accompanied by a copy of the expedited preservation of data direction or preservation of evidence direction or any amendment thereof;

(iv) contain a description of the data which must be provided and the format in which it must be provided;

(v) specify the grounds for believing that the data is an article as contemplated in paragraph (a) of the definition of “article”; and

(vi) comply with any supplementary directives relating to applications for the disclosure of data, which may be issued by the Chief Justice in terms of section 8 (3) of the Superior Courts Act, 2013.

(c) An application referred to in paragraph (a) (ii) must—

(i) indicate the identity of the policy official who applies for the disclosure of data direction;

(ii) identify the person, electronic communications service provider or financial institution to whom the disclosure of data direction must be addressed;

(iii) contain a description of the data which must be provided and the format in which it must be provided;

(iv) specify the grounds for believing that the data is an article as contemplated in paragraph (a) of the definition of “article”;

(v) specify the grounds for believing that the data, in question, is held in a computer system or computer data storage medium or is available to a computer system that is under the control of the person, electronic communications service provider or financial institution, referred to in subparagraph (ii), within the area of jurisdiction of the court; and

(vi) comply with any supplementary directives relating to applications for the disclosure of data, which may be issued by the Chief Justice in terms of section 8 (3) of the Superior Courts Act, 2013.

(2) A magistrate or judge of the High Court may, subject to the provisions of section 4 (2) of the Customs and Excise Act, 1964, sections 69 (2) (b) and 71 of the Tax Administration Act, 2011, and section 21 (e) and (f) of the Customs Control Act, 2014, on the written application by a police official referred to in subsection (1), if it appears to the magistrate or judge from information on oath or by way of affirmation, as set out in the application that—

(a) there are reasonable grounds for believing that—

(i) data which is subject to preservation in terms of an expedited preservation of data direction or a preservation of evidence direction, is an article as contemplated in paragraph (a) of the definition of “article”; or

(ii) data, which is an article as contemplated in paragraph (a) of the definition of “article”, is—

(aa) held in a computer system or computer data storage medium; or

(bb) available to a computer system,

within their area of jurisdiction; and

(b) it will be in the interests of justice if a disclosure of data direction is issued,

issue the disclosure of data direction applied for.

(3) A disclosure of data direction must be in the prescribed form and must be served on the person, electronic communications service provider or financial institution affected thereby, in the prescribed manner by a police official.

(4) The disclosure of data direction—

(a) must direct the person, electronic communications service provider or financial institution to provide the data identified in the direction to the extent set out in the direction to an identified police official;

(b) must specify the format in which the data identified in paragraph (a) must be provided;

(c) must set out the period within which the data identified in paragraph (a) must be provided; and

(d) may specify conditions or restrictions relating to the provision of data authorised therein.

(5) A person, electronic communications service provider or financial institution on whom a disclosure of data direction referred to in subsection (3) is served may, in writing in the prescribed form and manner, apply to the magistrate or judge for an amendment or the cancellation of the direction concerned on the ground that they cannot timeously or in a reasonable fashion comply with the direction.

(6) The magistrate or judge to whom an application is made in terms of subsection (5) must, as soon as possible after receipt thereof—

(a) consider the application and may, for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application;

(b) give a decision in respect of the application; and

(c) if the application is successful, inform the police official and the applicant of the outcome of the application.

(7) Any data made available in terms of a disclosure of data direction, must be—

(a) provided to the police official identified in the direction; and

(b) accompanied by an affidavit in the prescribed form by the person or authorised representative of an electronic communications service provider or financial institution, verifying the authenticity, integrity and reliability of the data that is furnished.

(8) A person, electronic communications service provider or a financial institution who—

(a) fails to comply with a disclosure of data direction;

(b) makes a false statement in an application referred to in subsection (5); or

(c) fails to comply with subsection (7),

is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment.

(9)

(a) Any article subject to a preservation of evidence direction that is not "data" must be seized in terms of a warrant referred to in section 29 (1).

(b) A police official may, at any time, apply for a search warrant in terms of section 29 (1) to search for, access or seize an article (which includes "data") that is or was subject to an expedited preservation of data direction or a preservation of evidence direction.

[S 44 commencement: To be proclaimed.]

**45. Obtaining and using publicly available data or receiving data from person who is in possession of data**

A police official may, without being specifically authorised thereto in terms of this Chapter, for the purposes of investigating any offence or suspected offence in terms of Part I or Part II of Chapter 2 or any other offence or suspected offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article—

(a) receive, obtain or use publicly available data regardless of where the data is located geographically; or

(b) receive and use non-publicly available data, regardless of where the data is located geographically, if a person who is in control of, or possesses the data, voluntarily and on such conditions regarding confidentiality and limitation of use which they deem necessary, discloses the data to a police official.

## CHAPTER 5
## MUTUAL ASSISTANCE

[Chapter 5 commencement: To be proclaimed.]

**46. Application of provisions of Chapter**

The provisions of sections 48 to 51 apply in addition to Chapter 2 of the International Co-operation in Criminal Matters Act, 1996, and relate, unless specified otherwise, to the preservation of an article or other evidence in electronic format regarding the commission or suspected commission of—

(a) an offence in terms of Part I or Part II of Chapter 2;

(b) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or

(c) an offence—

(i) similar to those contemplated in Part I or Part II of Chapter 2; or

(ii) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article,

in a foreign State,

pending a request in terms of section 2 or 7 of the International Co-operation in Criminal Matters Act, 1996.

[S 46 commencement: To be proclaimed.]

**47. Spontaneous information**

(1) The National Commissioner or the National Head of the Directorate, may, on such conditions regarding confidentiality and limitation of use as they may determine, furnish any information obtained during any investigation, to a law enforcement agency of a foreign State when the National Commissioner or the National Head of the Directorate is of the opinion that the disclosure of such information may—

(a) assist the foreign State in the initiation or carrying out of investigations; or

(b) lead to further cooperation with a foreign State to carry out an investigation,

regarding the commission or suspected commission of—

(i) an offence contemplated in Part I or Part II of Chapter 2, in the Republic;

(ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or

(iii) an offence—

(aa) similar to those contemplated in Part I or Part II of Chapter 2; or

(bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article,

in that foreign State.

(2) The South African Police Service may receive any information from a foreign State, subject to such conditions regarding confidentiality and limitation of use as may be agreed upon, which may—

(a) assist the South African Police Service in the initiation or carrying out of investigations; or

(b) lead to further cooperation with a foreign State to carry out an investigation,

regarding the commission or suspected commission of—

(i) an offence contemplated in Part I or Part II of Chapter 2, in the Republic;

(ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or

(iii) an offence—

(aa) similar to those contemplated in Part I or Part II of Chapter 2; or

(bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article,

in that foreign State.

[S 47 commencement: To be proclaimed.]

**48. Foreign requests for assistance and cooperation**

(1) A request by an authority, court or tribunal exercising jurisdiction in a foreign State for the—

(a) preservation of data or other article;

(b) seizure of data or other article;

(c) expedited disclosure of traffic data;

(d) obtaining of real-time communication-related information or archived communication-related information; or

(e) interception of indirect communications,

must, subject to subsection (9), be submitted to the designated Point of Contact.

(2) The designated Point of Contact must submit the request to the National Director of Public Prosecutions for consideration.

(3)

(a) Upon receipt of a request referred to in subsection (2), the National Director of Public Prosecutions must satisfy himself or herself that—

(i) proceedings have been instituted in a court or tribunal exercising jurisdiction in the requesting foreign State; or

(ii) there are reasonable grounds for believing that an offence has been committed in the requesting foreign State or that it is necessary to determine whether an offence has been so committed and that an investigation in respect thereof is being conducted in the requesting foreign State; and

(iii) the offence in question is—

(aa) similar to those contemplated in Part I or Part II of Chapter 2; or

(bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article; and

(iv) the foreign State intends to submit a request in terms of section 7 of the International Co-operation in Criminal Matters Act, 1996, for obtaining the data, information, a communication or an article in the Republic for use in such proceedings or investigation in the foreign State.

Consolidated by SAFLII (Southern African Legal Information Institute)
https://www.saflii.org/ | info@saflii.org

(b) For purposes of paragraph (a), the National Director of Public Prosecutions may rely on a certificate purported to be issued by a competent authority in the foreign State concerned, stating the facts contemplated in subsection (3) (a).

(4)

(a) The National Director of Public Prosecutions must submit the request for assistance, together with their recommendations, to the Cabinet member responsible for the administration of justice, for the Cabinet member's approval.

(b) Upon being notified of the Cabinet member's approval the National Director of Public Prosecutions must forward the request contemplated in subsection (1) to the designated judge for consideration.

(5) Where the request relates to the expedited disclosure of traffic data, subsections (3) (a) (iv) and (4) do not apply, and the National Director of Public Prosecutions must submit the request for assistance, together with their recommendations, to the designated judge.

(6) Subject to subsections (7) and (8), the designated judge may on receipt of a request referred to in subsection (4) or (5), issue any order they deem appropriate to ensure that the requested—

(a) data or other article is preserved in accordance with section 42;

(b) data or other article is seized on an expedited basis in accordance with section 29 and preserved;

(c) traffic data is disclosed on an expedited basis in terms of a disclosure of data direction in accordance with section 44;

(d) real-time communication-related information or archived communication related information, is obtained and preserved; or

(e) indirect communications are intercepted and preserved,

as is specified in the request.

(7) The designated judge may only issue an order contemplated in subsection (6), if—

(a) on the facts alleged in the request, there are reasonable grounds to believe that—

(i) an offence substantially similar to the offences contemplated in Part I or Part II of Chapter 2 has been, is being, or will probably be committed; or

(ii) any other offence substantially similar to an offence recognised in the Republic, has been, is being, or will probably be committed by means of, or facilitated through the use of, an article; and

(iii) for purposes of the investigation it is necessary, in the interests of justice, to give an order contemplated in subsection (6);

(b) the request clearly identifies—

(i) the person, electronic communications service provider or financial institution—

(aa) who or which will receive, is in possession of, or is in control of, the data or other article that must be preserved; or

(bb) from whose facilities the data, real-time communication-related information, archived communication-related information, indirect communications or traffic data must be obtained or intercepted;

(ii) the data or other article which must be preserved;

(iii) the data or other article which must be seized on an expedited basis and be preserved;

(iv) the traffic data which must be disclosed on an expedited basis;

(v) the real-time communication-related information or archived communication-related information, which is to be obtained; or

(vi) the indirect communications, which are to be intercepted;

(c) the request is, where applicable, in accordance with—

(i) any treaty, convention or other agreement to which that foreign State and the Republic are parties or which can be used as a basis for mutual assistance; or

(ii) any agreement with any foreign State entered into in terms of section 57; and

(d) the order contemplated in subsection (6) is in accordance with any applicable law of the Republic.

(8) The designated judge may, where a request relates to the expedited disclosure of traffic data—

(a) specify conditions or restrictions relating to the disclosure of traffic data as they deem appropriate; or

(b) refuse to issue an order referred to in subsection (6) (c), if the disclosure of the traffic data may prejudice the sovereignty, security, public safety or other essential interests of the Republic.

(9)

(a) In the case of urgency, a request by any authority, court or tribunal exercising jurisdiction in a foreign State referred to in subsection (1), may be submitted directly to the designated judge.

(b) Upon receipt of a request in terms of paragraph (a), the designated judge may issue any order referred to in subsection (6).

(10)

(a) A specifically designated police official must serve or execute an order contemplated in subsection (6).

(b) The specifically designated police official referred to in paragraph (a), must inform—

(i) the designated judge; and

(ii) the National Director of Public Prosecutions,

in writing, of the fact that an order has been served or executed.

(11) The National Director of Public Prosecutions must, in writing, inform the applicable authority in a foreign State of the fact that an order was issued and executed or not issued.

[S 48 commencement: To be proclaimed.]

**49. Complying with order of designated judge**

(1) A person, electronic communications service provider or financial institution must comply with an order of the designated judge issued in terms of section 48 (6).

(2) A person, electronic communications service provider or financial institution to whom an order referred to in section 48 (6) is addressed may, in writing, apply to the designated judge for an amendment or the cancellation of the order concerned on the ground that they cannot timeously or in a reasonable fashion, comply with the order.

(3) The designated judge to whom an application is made in terms of subsection (2) must, as soon as possible after receipt thereof—

(a) consider the application and may, for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application;

(b) give a decision in respect of the application; and

(c) if the application is successful, inform the National Director of Public Prosecutions of the outcome of the application.

(4) A person, electronic communications service provider or financial institution who—

(a) fails to comply with an order referred to in section 48 (6); or

(b) makes a false statement in an application referred to in subsection (2),

is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment.

[S 49 commencement: To be proclaimed.]

**50. Informing foreign State of outcome of request for mutual assistance and expedited disclosure of traffic data**

(1) The National Director of Public Prosecutions must inform—

(a) the designated judge; and

(b) the applicable authority in a foreign State,

of the outcome of the request for assistance and cooperation.

(2) Any traffic data made available in terms of an order referred to in section 48 (6) (c), must be—

(a) provided to the designated Point of Contact, in the prescribed manner, for submission to the applicable authority in a foreign State; and

(b) accompanied by—

(i) a copy of the order referred to in section 48 (6); and

(ii) an affidavit in the prescribed form by the person or authorised representative of an electronic communications service provider or financial institution, verifying the authenticity, integrity and reliability of the information that is furnished.

(3) The traffic data together with the copy of the order and affidavit referred to in subsection (2), must be provided to the applicable authority in a foreign State which requested the assistance in terms of section 48 (1).

(4) A person, electronic communications service provider or financial institution who—

(a) fails to comply with subsection (2) or any regulations contemplated in section 59 (1) (a) (xxii); or

(b) makes a false statement in an affidavit referred to in subsection (2) (b) (ii),

is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment.

[S 50 commencement: To be proclaimed.]

**51. Issuing of direction requesting assistance from foreign State**

(1) If it appears to a magistrate from information on oath or by way of affirmation that there are reasonable grounds for believing that—

(a) an offence contemplated in Part I or Part II of Chapter 2; or

(b) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article,

has been committed or that it is necessary to determine whether the offence has been so committed and that it is necessary—

(i) pending the issuing of a letter of request in terms of section 2 (2) of the International Co-operation in Criminal Matters Act, 1996, to—

(aa) preserve data or other articles;

(bb) seize data or other articles on an expedited basis;

(cc) obtain real-time communication-related information or archived communication-related information; or

(dd) intercept indirect communications; or

(ii) to obtain traffic data,

within the area of jurisdiction of a foreign State, the magistrate may issue a direction in the prescribed form in which assistance from that foreign State is sought as is stated in the direction.

(2) A direction contemplated in subsection (1) must specify that—

(a) there are reasonable grounds for believing that an offence contemplated in subsection (1) (a) or (b) has been committed in the Republic or that it is necessary to determine whether such an offence has been committed;

(b) an investigation in respect thereof is being conducted; and

(c) for purposes of the investigation it is necessary, in the interests of justice, that—

(i) data or other articles specified in the direction, be preserved;

(ii) data or any other article specified in the direction is to be seized on an expedited basis and be preserved;

(iii) traffic data specified in the direction, be disclosed on an expedited basis;

(iv) real-time communication-related information or archived communication-related information specified in the direction, be obtained and be preserved; or

(v) indirect communications, specified in the direction, be intercepted and be preserved,

within the area of jurisdiction of a foreign State.

(3) The direction must be sent to the National Director of Public Prosecutions for transmission to—

(a) the appropriate authority in the foreign State; or

(b) a designated point of contact in the foreign State,

which is requested to provide assistance and cooperation.

[S 51 commencement: To be proclaimed.]

## CHAPTER 6
## DESIGNATED POINT OF CONTACT

[Chapter 6 commencement: To be proclaimed.]

### 52. Establishment and functions of designated Point of Contact

(1) The National Commissioner must—

(a) establish or designate an office within existing structures of the South African Police Service to be known as the designated Point of Contact for the Republic; and

(b) equip, operate and maintain the designated Point of Contact.

(2) The National Commissioner exercises final responsibility over the administration and functioning of the designated Point of Contact.

(3)

(a) The designated Point of Contact must ensure the provision of immediate assistance for the purpose of proceedings or investigations regarding the commission or intended commission of—

(i) an offence under Part I or Part II of Chapter 2;

(ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or

(iii) an offence—

(aa) similar to those contemplated in Part I or Part II of Chapter 2; or

(bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article,

in a foreign State.

(b) The assistance contemplated in subsection (3) (a), includes—

(i) the provision of technical advice and assistance;

(ii) the facilitation or provision of assistance regarding anything which is authorised under Chapters 4 and 5;

(iii) the provision of legal assistance;

(iv) the identification and location of an article;

(v) the identification and location of a suspect; and

(vi) cooperation with appropriate authorities of a foreign State.

(4) The Cabinet member responsible for policing may make regulations to further—

(a) regulate any aspect provided for in subsection (3);

(b) impose additional duties on the designated Point of Contact; and

(c) regulate any aspect which is necessary or expedient for the proper implementation of this section.

(5) The National Director of Public Prosecutions must make available members of the National Prosecuting Authority—

(a) who have particular knowledge and skills in respect of any aspect dealt with in this Act; and

(b) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994, to the satisfaction of the National Director of Public Prosecutions,

to provide legal assistance to the designated Point of Contact as may be necessary or expedient for the effective operation of the designated Point of Contact.

(6)

(a) The Cabinet member responsible for policing must, at the end of each financial year, submit a report to the Chairperson of the Joint Standing Committee on Intelligence established by section 2 of the Intelligence Services Oversight Act, 1994, on the functions and activities of the designated Point of Contact.

(b) The report contemplated in paragraph (a) must include—

(i) the number of matters in which assistance was provided in terms of subsection (3)(a); and

(ii) the number of matters in which assistance was received from a foreign State.

[S 52 commencement: To be proclaimed.]

## CHAPTER 7
## EVIDENCE

### 53. Proof of certain facts by affidavit

(1) Whenever any fact established by any examination or process requiring any skill in—

(a) the interpretation of data;

(b) the design or functioning of data, a computer program, a computer data storage medium or a computer system;

(c) computer science;

(d) electronic communications networks and technology;

(e) software engineering; or

(f) computer programming,

is or may become relevant to an issue at criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, 1998, a document purporting to be an affidavit or a solemn or attested declaration made by a person who, in that document, states that they—

(i)

(aa) fall within a category of persons within the Republic; or

(bb) are in the service of a body in the Republic or a foreign State,

designated by the Cabinet member responsible for the administration of justice, by notice in the Gazette;

(ii) possess relevant qualifications, expertise and experience which makes them competent to make the affidavit; and

(iii) have established such fact by means of an examination or process that is documented in the document,

is, upon its mere production at such proceedings, prima facie proof of such fact.

(2) Any person who makes an affidavit or a solemn or attested declaration under subsection (1) and who in such affidavit or solemn or attested declaration wilfully states anything which is false, is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment.

(3) The court before which an affidavit or solemn or attested declaration is produced as prima facie proof of the relevant contents thereof may, in its discretion, cause the person who made the affidavit or solemn or attested declaration to be subpoenaed to give oral evidence in the proceedings in question or may cause written interrogatories to be submitted to such person for reply and such interrogatories and any reply thereto purporting to be a reply from such person are likewise admissible in evidence at such proceedings.

(4) No provision of this section affects any other law under which any certificate or other document is admissible in evidence and the provisions of this section are deemed to be additional to and not in substitution of any such law.

(5)

(a) For the purposes of subsection (1), a document purporting to be an affidavit or a solemn or attested declaration made by a person who in that affidavit alleges that they are in the service of a body in the Republic or a foreign State designated by the Cabinet member responsible for the administration of justice, by notice in the Gazette, has no effect unless it is—

(i) obtained in terms of an order of a competent court or on the authority of a government institution of the foreign State concerned, as the case may be; and

(ii) authenticated—

(aa) in the manner prescribed in the rules of court for the authentication of documents executed outside the Republic; or

(bb) by a person and in the manner contemplated in section 7 or 8 of the Justices of the Peace and Commissioners of Oaths Act, 1963.

(b) The admissibility and evidentiary value of an affidavit contemplated in paragraph (a) are not affected by the fact that the form of the oath, confirmation or attestation thereof differs from the form of the oath, confirmation or attestation prescribed in the Republic.

(c) A court before which an affidavit or a solemn or attested declaration contemplated in paragraph (a) is placed may, in order to clarify any obscurities in the said affidavit, order that a supplementary affidavit or a solemn or attested declaration be submitted or that oral evidence be heard: Provided that oral evidence may only be heard if the court is of the opinion that it is in the interests of the administration of justice and that a party to the proceedings would be prejudiced materially if oral evidence is not heard.

## CHAPTER 8
## REPORTING OBLIGATIONS AND CAPACITY BUILDING

**54. Obligations of electronic communications service providers and financial institutions**

(1) An electronic communications service provider or financial institution that is aware or becomes aware that its electronic communications service or electronic communications network is involved in the commission of any category or class of offences provided for in Part I of Chapter 2 and which is determined in terms of subsection (2), must—

(a) without undue delay and, where feasible, not later than 72 hours after having become aware of the offence, report the offence in the prescribed form and manner to the South African Police Service; and

(b) preserve any information which may be of assistance to the South African Police Service in investigating the offence.

(2) The Cabinet member responsible for policing, in consultation with the Cabinet member responsible for the administration of justice, must by notice in the Gazette, prescribe—

(a) the category or class of offences which must be reported to the South African Police Service in terms of subsection (1); and

(b) the form and manner in which an electronic communications service provider or financial institution must report offences to the South African Police Service.

(3) An electronic communications service provider or financial institution that fails to comply with subsection (1), is guilty of an offence and is liable on conviction to a fine not exceeding R50 000.

(4) Subject to any other law or obligation, the provisions of subsection (1) must not be interpreted as to impose obligations on an electronic service provider or financial institution to—

(a) monitor the data which the electronic communications service provider or financial institution transmits or stores; or

(b) actively seek facts or circumstances indicating any unlawful activity.

(5) This section does not apply to a financial sector regulator or a function performed by the South African Reserve Bank in terms of section 10 of the South African Reserve Bank Act, 1989.

[S 54 commencement: To be proclaimed.]

**55. Capacity to detect, prevent and investigate cybercrimes**

(1) The Cabinet member responsible for policing must—

(a) establish and maintain sufficient human and operational capacity to detect, prevent and investigate cybercrimes;

(b) ensure that members of the South African Police Service receive basic training in aspects relating to the detection, prevention and investigation of cybercrimes; and

(c) in co-operation with any institution of higher learning, in the Republic or elsewhere, develop and implement accredited training programmes for members of the South African Police Service primarily involved with the detection, prevention and investigation of cybercrimes.

(2) The Cabinet member responsible for policing may make regulations to further regulate any aspect referred to in subsection (1).

(3) The Cabinet member responsible for policing must, at the end of each financial year, submit a report to Parliament regarding—

(a) progress made with the implementation of this section;

(b) the number of—

(i) offences provided for in Part I or Part II of Chapter 2, which were reported to the South African Police Service;

(ii) cases which were, in terms of subparagraph (i), reported to the South African Police Service which resulted in criminal prosecutions; and

(iii) cases where no criminal prosecutions were instituted after a period of 18 months after a case was, in terms of subparagraph (i), reported to the South African Police Service; and

(c) the number of members of the South African Police Service who received training as contemplated in subsection (1) (b) and (c).

**56. National Director of Public Prosecutions must keep statistics of prosecutions**

(1) The National Director of Public Prosecutions must keep statistics of the number of prosecutions instituted for offences in terms of Part I or Part II of Chapter 2, the outcome of such prosecutions and any other information relating to such prosecutions, which is determined by the Cabinet member responsible for the administration of justice.

(2) The statistics or information contemplated in subsection (1) must be included in the report of the National Director of Public Prosecutions referred to in section 22 (4) (g) of the National Prosecuting Authority Act, 1998.

## CHAPTER 9
## GENERAL PROVISIONS

**57. National Executive may enter into agreements**

(1) The National Executive may enter into any agreement with any foreign State regarding—

(a) the provision of mutual assistance and cooperation relating to the investigation and prosecution of—

(i) an offence under Part I or Part II of Chapter 2;

(ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or

(iii) an offence—

(aa) similar to those contemplated in Part I or Part II of Chapter 2; or

(bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article,

in that foreign State;

(b) the implementation of cybercrime response activities;

(c) training, research, information and technology-sharing and the exchange of information on the detection, prevention, mitigation and investigation of cybercrimes;

(d) the establishment or designation of points of contact to facilitate the provision of mutual assistance and cooperation as contemplated in paragraph (a);

(e) the implementation of emergency cross-border response mechanisms to mitigate the effect of cybercrimes; and

(f) the reciprocal implementation of measures to curb cybercrime.

(2) A member of the National Executive must, as soon as practicable after Parliament has agreed to the ratification of, accession to, amendment of, or revocation of, an agreement referred to in subsection (1), give notice thereof in the Gazette.

**58. Repeal or amendment of laws**

The laws mentioned in the Schedule are hereby repealed or amended to the extent reflected in the third column of the Schedule.

**59. Regulations**

(1) The Cabinet member responsible for the administration of justice—

(a) must make regulations to prescribe the—

(i) form and manner of the application as contemplated in section 20 (1);

(ii) form of the order as contemplated in section 20 (3);

(iii) manner of serving the order as contemplated in section 20 (4);

(iv) form and manner of the application as contemplated in section 20 (6);

(v) form and manner in which the court may subpoena a person as contemplated in section 20 (8);

(vi) form of the direction and affidavit and manner to furnish information to a court as contemplated in section 21 (1) (b);

(vii) manner of serving a direction as contemplated in section 21 (2);

(viii) manner and the form of the affidavit to apply for an extension of the time period or cancellation of the direction as contemplated in section 21 (3) (b);

(ix) manner for requesting additional information as contemplated in section 21 (4) (b);

(x) form and manner of informing an electronic communications service provider of the outcome of application as contemplated in section 21 (4) (d);

(xi) tariffs of compensation payable to an electronic communications service provider as contemplated in section 21 (6);

(xii) form of the order and manner of service of the order as contemplated in section 22 (3);

(xiii) form and manner of the application as contemplated in section 22 (5);

(xiv) form and manner in which the court may subpoena a person as contemplated in section 22 (7);

(xv) the form of the expedited preservation of data direction and manner of service as contemplated in section 41 (3);

(xvi) form and manner for the making of an application as contemplated in section 41 (7);

(xvii) form of the preservation of evidence direction and manner of service as contemplated in section 42 (2);

(xviii) form and manner of an application to set aside a preservation of evidence direction as contemplated in section 42 (5);

(xix) form of the disclosure of data direction and manner of service as contemplated in section 44 (3);

(xx) form and manner of an application for the amendment or setting aside of a disclosure of data direction as contemplated in section 44 (5);

(xxi) form of the affidavit as contemplated in section 44 (7) (b);

(xxii) manner in which traffic data must be provided to the designated Point of Contact as contemplated in section 50 (2);

(xxiii) form of the affidavit as contemplated in section 50 (2) (b) (ii); and

(xxiv) form of the direction as contemplated in section 51 (1); and

(b) may make regulations which are not inconsistent with this Act or any other law to prescribe any matter which in terms of this Act may be prescribed or which may be necessary or expedient to prescribe in order to achieve or promote the objects of this Act.

(2)

(a) The Cabinet member responsible for policing must make regulations in terms of section 54 (2), prescribing the—

(i) category or class of offences which must be reported to the South African Police Service in terms of section 54 (2) (a); and

(ii) form and manner in which an electronic communications service provider or financial institution must report offences to the South African Police Service as contemplated in section 54 (2) (b).

(b) The Cabinet member responsible for policing may make regulations to further regulate aspects contemplated in section 52 (4) and 55 (2).

**60. Short title and commencement**

(1) This Act is called the Cybercrimes Act, 2020, and comes into operation on a date fixed by the President by proclamation in the Gazette.

(2) Different dates may be fixed under subsection (1) in respect of different provisions of this Act.

**SCHEDULE**

**LAWS REPEALED OR AMENDED**

*(Section 58)*

[Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007; amendment relating to ss 11B, 11C, 11D, 56A (3) (c), 56A (3) (d), 56A (3) (e) commencement: To be proclaimed.]

| Number and year of law | Short title | Extent of repeal or amendment |
|---|---|---|
| Act 51 of 1977 | Criminal Procedure Act, 1977 | The addition of the following items to Schedule 5:<br>"A contravention of section 8, 9 or 10 of the Cybercrimes Act, 2020-<br>(a) involving amounts of more than R500 000,00;<br>(b) involving amounts of more than R100 000,00, if it is proven that the offence was committed-<br>(i) by a person, group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; or<br>(ii) by a person or with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offence in question was committed; or<br>(c) if it is proven that the offence was committed by any law enforcement officer-<br>(i) involving amounts of more than R10 000; or<br>(ii) as a member of a group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; or<br>(iii) with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offence in question was committed.<br>A contravention of section 11(2) of the Cybercrimes Act, 2020.". |

| | | |
|---|---|---|
| Act 68 of 1995 | South African Police Service Act, 1995 | The deletion of section 71. |
| Act 65 of 1996 | Films and Publications Act, 1996 | The deletion of section 24B. |
| Act 105 of 1997 | Criminal Law Amendment Act, 1997 | The addition of the following item to Part II of Schedule 2:<br>"A contravention of section 8, 9 or 10 of the Cybercrimes Act, 2020—<br>(a) involving amounts of more than R500 000,00;<br>(b) involving amounts of more than R100 000,00, if it is proven that the offence was committed—<br>(i) by a person, group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; or<br>(ii) by a person or with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offence in question was committed; or<br>(c) if it is proven that the offence was committed by any law enforcement officer-<br>(i) involving amounts of more than R10 000; or<br>(ii) as a member of a group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; or<br>(iii) with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offence in question was committed.". |
| Act 32 of 1998 | National Prosecuting Authority Act, 1998 | The deletion of sections 40A and 41(4). |
| Act 111 of 1998 | Correctional Services Act, 1998 | The deletion of section 128. |
| Act 38 of 2001 | Financial Intelligence Centre Act, 2001 | The deletion of sections 65, 66 and 67. |

| | | |
|---|---|---|
| Act 25 of 2002 | Electronic Communications and Transactions Act, 2002 | (a) The deletion of sections 85, 86, 87 and 88. |
| | | (b) The substitution for section 89 of the following section:<br>**"Penalties**<br>**89. [(1)]** A person convicted of an offence referred to in sections 37(3), 40(2), 58(2), 80(5)**[,]** or 82(2) **[or 86(1), (2) or (3)]** is liable to a fine or imprisonment for a period not exceeding 12 months.<br>**[(2) A person convicted of an offence referred to in section 86(4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years.]**". |
| Act 70 of 2002 | Regulation of Interception of Communications and Provision of Communication related Information Act, 2002 | (a) The amendment of section 1 by the substitution for paragraph (a) of the definition of "serious offence" of the following paragraph:<br>"(a) offence mentioned in **[the]** Schedule 1; or". |
| | | (b) The amendment of section 4 by the addition of the following subsection:<br>"(3) Notwithstanding subsection (2), a law enforcement officer or a person who is authorised in terms of the Criminal Procedure Act, 1977, the Cybercrimes Act, 2020, or any other law to engage or to apprehend a suspect or to enter premises in respect of the commission or suspected commission of any offence, may during the apprehension of the suspect or during the time that he or she is lawfully on the premises, record what he or she observes or hears if—<br>(a) the recording relates directly to the purpose for which the suspect was apprehended or the law enforcement officer or person entered the premises; and<br>(b) the law enforcement officer or person has-<br>(i) identified himself or herself as such; and<br>(ii) verbally informed any person concerned that his or her direct communications are to be recorded,<br>before such recording is made." |
| | | (c) The substitution for subsection (4) of section 17 of the following subsection:<br>"(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—<br>(a) a serious offence or an offence mentioned in Schedule II has been or is being or will probably be committed;<br>(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;<br>(c) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;<br>(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, an offence mentioned in Schedule II or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in—<br>(i) accordance with an international mutual assistance agreement; or<br>(ii) the interests of the Republic's international relations or obligations; or<br>(e) the gathering of information concerning an offence mentioned in Schedule II, or 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,<br>and that the provision of real-time communication-related information is necessary for purposes of investigating such offence or gathering such information.''. |
| | | (d) The substitution for subsection (4) of section 19 of the following subsection:<br>''(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—<br>(a) a serious offence or an offence mentioned in |

| | | |
|---|---|---|
| | | Schedule II has been or is being or will probably be committed;<br>(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;<br>(c) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;<br>(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, an offence mentioned in Schedule II or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in—<br>(i) accordance with an international mutual assistance agreement; or<br>(ii) the interests of the Republic's international relations or obligations; or<br>(e) the gathering of information concerning an offence mentioned in Schedule II, or 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,<br>and that the provision of archived communication-related information is necessary for purposes of investigating such offence or gathering such information.''. |
| | | (e) The renaming of the Schedule to the Act as ''Schedule I'' and the addition of the following items:<br>''15 Any offence contemplated in section 17, 18, 19A or 20 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act 32 of 2007).<br>16 Any offence contemplated in-<br>(a) section 8, 9(1) or (2) or 10, which involves an amount of R200 000, 00 or more; or<br>(b) section 11(1) or (2) or 17 (in so far as the section relates to the offences referred to in section 11(1) or |

| | | |
|---|---|---|
| | | (2)),<br>of the Cybercrimes Act, 2020.'' |
| | | (f) The addition of the following Schedule after Schedule I:<br>''**Schedule II**<br>1 Any offence referred to in-<br>(a) section 3(1), 5, 6, 7(1), 8, 9(1) or (2), or 10; or<br>(b) section 17 (in so far as the section relates to the offences referred to in paragraph (a)),<br>of the Cybercrimes Act, 2020, which involves an amount of R50 000, 00 or more.<br>2 Any offence which is substantially similar to an offence referred to in item 1 which is or was committed in a foreign State, which involves an amount of R50 000, 00 or more.''. |
| Act 32 of 2007 | Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 | (a) The Index to the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007, is hereby amended—<br>(i) by the insertion of the following Part and items after item 11:<br>''**Part 3A**<br>Persons 18 years or older: Harmful disclosure of pornography and orders to protect complainant against harmful effects of disclosure of pornography<br>11A Harmful disclosure of pornography<br>11B Orders to protect complainant against harmful disclosure of pornography pending finalisation of criminal proceedings<br>11C Electronic communications service provider to furnish particulars to court<br>11D Orders on finalisation of criminal proceedings'';<br>(ii) by the substitution for the heading to Part 2 of Chapter 3 of the following heading:<br>''Sexual exploitation and sexual grooming of children, exposure or display of or causing exposure or display of child pornography or pornography to children, child pornography and using children for pornographic purposes or benefiting from child pornography''; and<br>(iii) the insertion after item 19 of the following item:<br>''19A. Offences relating to child pornography''<br>(b) The amendment of section 1— |

| | | |
|---|---|---|
| | | (i) by the insertion, after the definition of "Director of Public Prosecutions", of the following definitions:<br>" **'disclose'** and **'disclosure'**, in relation to the harmful disclosure of pornography contemplated in section 11A, includes—<br>(a) to send the pornography to a person who is the intended recipient of the electronic communication or any other person;<br>(b) to store the pornography on an electronic communications network, where the pornography can be viewed, copied or downloaded; or<br>(c) to send or otherwise make available to a person, a link to the pornography that has been stored on an electronic communication network, where the pornography can be viewed, copied or downloaded;<br>**'Electronic Communications Act'** means the Electronic Communications Act, 2005 (Act 36 of 2005);<br>**'electronic communications identity number'** means a technical identification label which represents the origin or destination of electronic communications traffic;<br>**'electronic communications network'** means an 'electronic communications network' as defined in section 1 of the Electronic Communications Act, 2005, and includes a computer system;<br>**'electronic communications service'** means any service which consists wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services as defined in section 1 of the Electronic Communications Act, 2005;<br>**'electronic communications service provider'** means—<br>(a) any person who provides an electronic communications service to the public, sections of the public, the State, or the subscribers to such service, under and in accordance with an electronic communications service licence issued to that person |

| | | |
|---|---|---|
| | | in terms of the Electronic Communications Act, 2005, or who is deemed to be licensed or exempted from being licensed as such in terms of that Act; and<br>(b) a person who has lawful authority to control the operation or use of a private electronic communications network used primarily for providing electronic communications services for the owner's own use and which is exempted from being licensed in terms of the Electronic Communications Act, 2005;"; and |
| | | (ii) by the insertion, after the definition of "genital organs" of the following definitions:<br>"**'host'** means to store information on an electronic communications network that is used to provide an electronic communications service, where it can be viewed, copied or downloaded;<br>**'live performance involving child pornography'** means an event where a child is used to create, make or produce child pornography;". |
| | | (c) The following Part and sections are hereby inserted in Chapter 2 after section 11:<br>"Part 3A<br>Persons 18 years or older: Harmful disclosure of pornography and orders to protect complainant against harmful effects of disclosure of pornography<br>**Harmful disclosure of pornography**<br>**11A.** (1) A person ('A') who unlawfully and intentionally discloses or causes the disclosure of pornography in which a person ('B') appears or is described and such disclosure-<br>(a) takes place without the consent of B; and<br>(b) causes any harm, including mental, psychological, physical, social or economic harm, to B or any member of the family of B or any other person in a close relationship to B,<br>is guilty of the offence of harmful disclosure of pornography.<br>(2) A person ('A') who unlawfully and intentionally threatens to disclose or threatens to cause the disclosure of pornography referred to in subsection (1) and such threat |

| | | |
|---|---|---|
| | | causes, or such disclosure could reasonably be expected to cause, any harm referred to in subsection (1)(b), is guilty of the offence of threatening to disclose pornography that will cause harm.<br>(3) A person ('A') who unlawfully and intentionally threatens to disclose or threatens to cause the disclosure of pornography referred to in subsection (1), for the purposes of obtaining any advantage from B or any member of the family of B or any other person in a close relationship to B, is guilty of the offence of harmful disclosure of pornography related extortion.<br>**Orders to protect complainant against harmful disclosure of pornography pending finalisation of criminal proceedings**<br>**11B.** (1)A complainant (hereinafter referred to as the applicant) who lays a charge with the South African Police Service that an offence contemplated in section 11A(1), (2) or (3) has allegedly been committed against him or her, may on an *ex parte* basis in the prescribed form and manner, apply to a magistrate's court for a protection order pending the finalisation of the criminal proceedings to-<br>(a) prohibit any person to disclose, or cause the disclosure or threaten the applicant with the disclosure or causing the disclosure of pornography which relates to the charge; or<br>(b) order an electronic communications service provider whose electronic communications service is used to host or disclose the pornography which relates to the charge, to remove or disable access to such pornography.<br>(2) The court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (1) and may, for that purpose consider any additional evidence it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings.<br>(3) If the court is satisfied that there-<br>(a) is prima facie evidence that an offence referred to in section 11A(1), (2) or (3), has allegedly been committed against the applicant; and<br>(b) are reasonable grounds to believe that a person referred to in subsection (1)(a), disclosed or caused |

| | | |
|---|---|---|
| | | the disclosure or threatened the applicant with the disclosure or causing the disclosure of such pornography; or<br>(c) are reasonable grounds to believe that the electronic communications service of the electronic communications service provider referred to in subsection (1)(b), is used to host or disclose such pornography,<br>the court may, subject to such conditions as the court may deem fit, issue the order referred to in subsection (1), in the prescribed form.<br>(4) The order, referred to in subsection (3), must be served on the person referred to in subsection (1)(a) or electronic communications service provider referred to in subsection (1)(b), in the prescribed manner: Provided, that if the court is satisfied that the order cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form or manner specified in that order.<br>(5) An order referred to in subsection (3) is of force and effect from the time it is issued by the court and the existence thereof has been brought to the attention of the person referred to in subsection (1)(a) or electronic communications service provider referred to in subsection (1)(b).<br>(6) A person referred to in subsection (1)(a), other than the person who is accused of having committed the offence in question, or an electronic communications service provider, referred to in subsection (1)(b) may, within 14 days after the order has been served on him, her or it in terms of subsection (4) or within such further period as the court may allow, upon notice to the magistrate's court concerned, in the prescribed form and manner, apply to the court for the setting aside or amendment of the order referred to in subsection (3).<br>(7) (a) The court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (6) and may for that purpose, consider such additional evidence as it deems fit, including oral evidence or evidence by affidavit, which must form part of the record |

| | | |
|---|---|---|
| | | of the proceedings.<br>(b) The court may if good cause has been shown for the variation or setting aside of the protection order, issue an order to this effect.<br>(8) The court may, for purposes of subsections (2) and (7), in the prescribed form and manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case.<br>(9) A person referred to in subsection (1)(a) or electronic communications service provider referred to in subsection (1)(b), that fails to comply with an order referred to in subsection (3) or any variation thereof, is guilty of an offence.<br>(10) Any person who is subpoenaed in terms of subsection (8) to attend proceedings and who fails to-<br>(a) attend or to remain in attendance;<br>(b) appear at the place and on the date and at the time to which the proceedings in question may be adjourned;<br>(c) remain in attendance at those proceedings as so adjourned; or<br>(d) produce any book, document or object specified in the subpoena,<br>is guilty of an offence.<br>(11) The provisions in respect of appeal and review as provided for in the Magistrates' Courts Act, 1944, and the Superior Courts Act, 2013, apply to proceedings in terms of this section.<br>(12) Sections 8 and 9(3) of the Protection from Harassment Act, 2011 (Act 17 of 2011), apply with the necessary changes required by the context to proceedings contemplated in subsections (2) and (7).<br>**Electronic communications service provider to furnish particulars to court**<br>**11C.** (1) If an application for a protection order is made in terms of section 11B(1) and the court is satisfied in terms of section 11B(3) that a protection order must be issued and the particulars of the person referred to in section 11B(1)(a), |

| | | |
|---|---|---|
| | | or the electronic communications service provider referred to in section 11B(1)(b), whose service is used to host or disclose such pornography, is not known, the court may—<br>(a) adjourn the proceedings to any time and date on the terms and conditions which the court deems appropriate; and<br>(b) issue a direction in the prescribed form, directing an electronic communications service provider, that is believed to be able to furnish such particulars, to furnish the court in the prescribed manner by means of an affidavit in the prescribed form with—<br>(i) the electronic communications identity number from where such pornography originated;<br>(ii) the name, surname, identity number and address of the person to whom the electronic communications identity number has been assigned;<br>(iii) any information which indicates that such pornography was or was not sent from the electronic communications identity number of the person to the electronic communications identity number of the applicant;<br>(iv) any information that is available to an electronic communications service provider that may be of assistance to the court to identify the person referred to in section 11B(1)(a) or the electronic communications service provider referred to in section 11B(1)(b), which provides a service to that person;<br>(v) any information that is available to an electronic communications service provider which—<br>(aa) confirms whether or not its electronic communications service is used to host or was or is used to disclose such pornography; or<br>(bb) may be of assistance to the court to identify the electronic |

| | | |
|---|---|---|
| | | communications service provider whose service is used to host or was or is used disclose such pornography; and<br>(vi) an assessment whether or not the electronic communications service provider is in a position to-<br>(aa) remove such pornography or a link to such pornography; or<br>(bb) disable access to such pornography or a link to such pornography.<br>(2) If the court issues a direction in terms of subsection (1)(b) the court must direct that the direction be served on the electronic communications service provider in the prescribed manner: Provided, that if the court is satisfied that the direction cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form or manner specified in that order.<br>(3)(a) The information referred to in subsection (1)(b) must be provided to the court within five ordinary court days from the time that the direction is served on an electronic communications service provider.<br>(b) An electronic communications service provider on which a direction is served, may in the prescribed manner by means of an affidavit in the prescribed form apply to the court for—<br>(i) an extension of the period of five ordinary court days referred to in paragraph (a) for a further period of five ordinary court days on the grounds that the information cannot be provided timeously; or<br>(ii) the cancellation of the direction on the grounds that—<br>(aa) it does not provide an electronic communications service to the applicant or the person referred to in section 11B(1)(a);<br>(bb) the requested information is not available in the records of the electronic communications service provider; or |

| | | |
|---|---|---|
| | | (cc) its service is not used to host or was or is not used to disclose such pornography.<br>(4) After receipt of an application in terms of subsection (3)(b), the court—<br>(a) must consider the application;<br>(b) may, in the prescribed manner, request such additional evidence by way of affidavit from the electronic communications service provider as it deems fit;<br>(c) must give a decision in respect thereof; and<br>(d) must inform the electronic communications service provider in the prescribed form and manner of the outcome of the application.<br>(5)(a) The court may, on receipt of an affidavit from an electronic communications service provider which contains the information referred to in subsection (1)(b), consider the issuing of a protection order in terms of section 11B(3) against the person or electronic communications service provider on the date to which the proceedings have been adjourned.<br>(b) Any information furnished to the court in terms of subsection (1)(b) forms part of the evidence that a court may consider in terms of section 11B(3).<br>(6) The Cabinet member responsible for the administration of justice may, by notice in the Gazette, prescribe reasonable tariffs of compensation payable to electronic communications service providers for providing the information referred to in subsection (1)(b).<br>(7) Any electronic communications service provider or employee of an electronic communications service provider who—<br>(a) fails to furnish the required information within five ordinary court days from the time that the direction is served on such electronic communications service provider to a court in terms of subsection (3)(a) or such extended period allowed by the court in terms of subsection (3)(b); or<br>(b) makes a false statement in an affidavit referred to in subsection (1)(b) or (3)(b) in a material respect, |

| | | |
|---|---|---|
| | | is guilty of an offence.<br>**Orders on finalisation of criminal proceedings**<br>**11D.** (1) The trial court, on convicting a person of any offence referred to in section 11A(1), (2) or (3), must order—<br>(a) that person to destroy the pornography and to submit an affidavit in the prescribed form to the prosecutor identified in the order, that the pornography has been so destroyed; or<br>(b) an electronic communications service provider whose service is used to host or disclose such pornography to remove or disable access to such pornography.<br>(2) The order referred to in subsection (1)(b), must be in the prescribed form and must be served on the electronic communications service provider in the prescribed manner: Provided, that if the trial court is satisfied that the order cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form or manner specified in that order.<br>(3) Any person or electronic communications service provider who fails to comply with an order referred to in subsection (1), is guilty of an offence.<br>(4) An electronic communications service provider may, within 14 days after the order referred to in subsection (1)(b) has been served on it in terms of subsection (2), upon notice to the trial court concerned, in the prescribed form and manner, apply to the trial court for the setting aside or amendment of the order.<br>(5)(a) The trial court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (4) and may for that purpose, consider such additional evidence as it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings.<br>(b) The trial court may if good cause has been shown for the variation or setting aside of the order, issue an order to this effect.<br>(6) The trial court may, for purposes of subsections (5)(a), in the prescribed form and manner cause to be |

| | | |
|---|---|---|
| | | subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case.<br>(7) Any person who is subpoenaed in terms of subsection (6) to attend proceedings and who fails to—<br>(a) attend or to remain in attendance;<br>(b) appear at the place and on the date and at the time to which the proceedings in question may be adjourned;<br>(c) remain in attendance at those proceedings as so adjourned; or<br>(d) produce any book, document or object specified in the subpoena,<br>is guilty of an offence.<br>(8) For purposes of this section **"trial court"** means-<br>(a) a magistrate's court established under section 2(1)(f)(i) of the Magistrates' Courts Act, 1944;<br>(b) a court for a regional division established under section 2(1)(g)(i) of the Magistrates' Courts Act, 1944; or<br>(c) a High Court referred to in section 6(1) of the Superior Courts Act, 2013.<br>(9) Whenever a person is convicted of an offence referred to in section 11A(1), (2) or (3), the trial court must issue an order that the person so convicted must reimburse all expenses reasonably incurred by—<br>(a) a complainant as a result of any direction issued in terms of section 11C(1)(b); or<br>(b) an electronic communications service provider to remove or disable access to such pornography,<br>whereupon the provisions of section 300 of the Criminal Procedure Act, 1977, shall apply with the necessary changes required by the context, to such order.". |
| | | (d) Chapter 3 is hereby amended—<br>(i) by the substitution for the heading to Part 2 of Chapter 3 of the following heading:<br>"**Sexual exploitation and sexual grooming of children, exposure or display of or causing exposure or display** |

| | | |
|---|---|---|
| | | **of child pornography or pornography to children, offences relating to child pornography and using children for pornographic purposes or benefiting from child pornography**”; |
| | | (ii) by the addition to section 17 of the following subsection: “(7) Any person who unlawfully and intentionally in any manner advocates, advertises, encourages or promotes the sexual exploitation of a child, is guilty of an offence.”; |
| | | (iii) by the insertion of the following section after section 19: “**Offences relating to child pornography**<br>**19A.** (1) Any person who unlawfully and intentionally creates, makes or produces child pornography in any manner, other than by using a child for child pornography as contemplated in section 20(1), is guilty of an offence.<br>(2) Any person who unlawfully and intentionally, in any manner assists in, or facilitates the creation, making or production of child pornography, is guilty of an offence.<br>(3) Any person who unlawfully and intentionally possesses child pornography, is guilty of an offence.<br>(4) Any person who unlawfully and intentionally, in any manner-<br>(a) distributes;<br>(b) makes available;<br>(c) transmits;<br>(d) offers for sale;<br>(e) sells;<br>(f) offers to procure;<br>(g) procures;<br>(h) accesses;<br>(i) downloads; or<br>(j) views,<br>child pornography, is guilty of an offence.<br>(5) Any person who unlawfully and intentionally, in any manner assists in, or facilitates the—<br>(a) distribution;<br>(b) making available;<br>(c) transmission;<br>(d) offering for sale;<br>(e) selling; |

| | | |
|---|---|---|
| | | (f) offering to procure;<br>(g) procuring;<br>(h) accessing;<br>(i) downloading; or<br>(j) viewing,<br>of child pornography, is guilty of an offence.<br>(6) Any person who unlawfully and intentionally processes or facilitates a financial transaction, knowing that such transaction will facilitate a contravention of subsections (1) to (5), is guilty of an offence.''; and |
| | | (iv) by the addition to section 20 of the following subsections:<br>''(3) Any person who unlawfully and intentionally—<br>(a) attends;<br>(b) views; or<br>(c) participates in,<br>a live performance involving child pornography, is guilty of the offence of attending, viewing or participating in, a performance involving child pornography.<br>(4) Any person (''A'') who unlawfully and intentionally recruits a child complainant (''B''), with or without the consent of B, whether for financial or other reward, favour or compensation to B or a third person (''C'') or not, for purposes of—<br>(a) creating, making or producing of child pornography, is guilty of the offence of recruiting a child for child pornography; or<br>(b) participating in a live performance involving child pornography, as contemplated in subsection (3), is guilty of the offence of recruiting a child for participating in a live performance involving child pornography.''. |
| | | (e) Section 54 of the Act is amended by the addition of the following subsections:<br>''(3) Any person who, having knowledge of the commission of any offence referred to in section 19A, or having reason to suspect that such an offence has been or is being or will probably be committed and unlawfully and intentionally fails |

| | | |
|---|---|---|
| | | to—<br>(a) report such knowledge or suspicion as soon as possible to the South African Police Service; or<br>(b) furnish, at the request of the South African Police Service, all particulars of such knowledge or suspicion,<br>is guilty of an offence.<br>(4) An electronic communications service provider that is aware or becomes aware that its electronic communications service or electronic communications network is used or involved in the commission of any offence provided for in section 19A, must—<br>(a) immediately report the offence to the South African Police Service;<br>(b) preserve any information which may be of assistance to the South African Police Service in investigating the offence; and<br>(c) take all reasonable steps to prevent access to the child pornography by any person.''. |
| | | (f) Section 56A of the Act is amended by the addition of the following subsections:<br>''(3)(a) Any person who contravenes the provisions of section 11A(1) or (2), is liable on conviction to a fine or to imprisonment for a period not exceeding five years or to both such fine and imprisonment.<br>(b) Any person who contravenes the provisions of section 11A(3), is liable on conviction to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.<br>(c) Any person or electronic communications service provider that is convicted of an offence referred to in section 11B(9) or (10), is liable on conviction to a fine or to imprisonment for a period not exceeding two years or to both such fine and imprisonment.<br>(d) Any person or electronic communications service provider that is convicted of an offence referred to in section 11C(7), is liable, on conviction to a fine or to imprisonment for a period not exceeding two years or to both such fine and imprisonment.<br>(e) Any electronic communications service provider |

| | | |
|---|---|---|
| | | or person that is convicted of an offence referred to in section 11D(3) or (7), is liable on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.<br>(4) Any person who contravenes the provisions of section 19A(3), (4)(f), (g), (h), (i) or (j), or (5)(f), (g), (h), (i) or (j) is liable-<br>(a) in the case of a first conviction, to a fine or to imprisonment for a period not exceeding five years or to both such fine and imprisonment;<br>(b) in the case of a second conviction, to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment; or<br>(c) in the case of a third and subsequent conviction, to a fine or to imprisonment for a period not exceeding 15 years or to both such fine and imprisonment.<br>(5) Any person who contravenes the provisions of section 17(7), 19A(1), (2), (4)(a), (b), (c), (d), or (e), (5)(a), (b), (c), (d) or (e) or 20(3) or (4), is liable—<br>(a) in the case of a first conviction, to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment; or<br>(b) in the case of a second and subsequent conviction, to a fine or to imprisonment for a period not exceeding 15 years or to both such fine and imprisonment.<br>(6) Any person who contravenes the provisions of section 19A(6), is liable—<br>(a) in the case of a first conviction, to a fine of R1 000 000 or to imprisonment for a period not exceeding 5 years, or to both such fine and imprisonment; or<br>(b) in the case of a second or subsequent conviction, to a fine of R2 000 000 or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.<br>(7) Any person who contravenes the provisions of section 54(3), is liable, on conviction to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment. |

| | | |
|---|---|---|
| | | (8) Any electronic communications service provider who contravenes the provisions of section 54(4), is liable, on conviction to a fine not exceeding R1 000 000 or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.''. |
| Act 75 of 2008 | Child Justice Act, 2008 | (a) The addition of the following item to Schedule 2:<br>''26. Any offence contemplated in-<br>(a) section 2, 3 or 4 of the Cybercrimes Act, 2020;<br>(b) section 5, 6, 7 or 11(1) of the Cybercrimes Act, 2020, where the damage caused does not exceed an amount of R5000;<br>(c) section 14, 15 or 16 of the Cybercrimes Act, 2020; or<br>(d) section 8, 9 or 10 of the Cybercrimes Act, 2020, where the amount involved does not exceed R1500.<br>27. An offence contemplated in section 11A(1) and (2) of Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007.'' |
| | | (b) The addition of the following item to Schedule 3:<br>''23. Any offence contemplated in—<br>(a) section 5, 6, 7 or 11(1) of the Cybercrimes Act, 2020, where the damage caused exceeds an amount of R5000;<br>(b) section 8, 9 or 10 of the Cybercrimes Act, 2020, where the amount involved exceeds R1500; or<br>(c) section 11(2) of the Cybercrimes Act, 2020.<br>24. An offence contemplated in section 11A(3) of Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007.''. |