PORTFOLIO COMMITTEE ON JUSTICE AND CORRECTIONAL SERVICES

DATE: 26 February 2018

REPUBLIC OF SOUTH AFRICA

CYBERCRIMES AND CYBERSECURITY BILL

AMENDMENTS PROPOSED TO BILL

[ ] Words in bold type in square brackets indicate proposed omissions from existing enactments

_____ Words in bold type and underlined with a solid line indicate proposed insertions in existing enactments as proposed during the public consultation process

========= Words in bold type and underlined with a solid double line indicate proposed insertions in existing enactments as proposed during the consultation process with Departments on 13 February 2018

_____

(As introduced in the National Assembly (proposed section 75); explanatory summary of Bill published in Government Gazette No. …….. of …….. 2016) (The English text is the official text of the Bill)

_____

(MINISTER OF JUSTICE AND CORRECTIONAL SERVICES)

[B—2017]

BILL

To create offences and impose penalties which have a bearing on cybercrime; to criminalise the distribution of data messages which is 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 cybercrime; to provide for the establishment of a 24/7 Point of Contact; to further provide for the proof of certain facts by affidavit; to impose obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes and to report cybercrimes; to provide for the establishment of structures to promote cybersecurity and capacity building; to regulate the identification and declaration of critical information infrastructures and measures to protect critical information infrastructures; to provide that the Executive may enter into agreements with foreign States to promote cybersecurity; 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

Sections

CHAPTER 1

DEFINITIONS

1. Definitions

CHAPTER 2

CYBERCRIMES

2. Unlawful securing of access
3. Unlawful acquiring of data
4. Unlawful acts in respect of software or hardware tool
5. Unlawful interference with data or computer program
6. Unlawful interference with a computer data storage medium or computer system
7. Unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices
8. Cyber fraud
9. Cyber forgery and uttering
10. Cyber extortion
11. Aggravated offences

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

13. Theft of incorporeal

14. Penalties

15. Competent verdicts

CHAPTER 3

MALICIOUS COMMUNICATIONS

16. Data message which incites damage to property or violence

17. Data message which is harmful

18. Distribution of data message of intimate image without consent

19. Order to protect complainant pending finalisation of criminal proceedings

20. Electronic communications service provider or person in control of computer system to furnish particulars to court

21. Orders on finalisation of criminal proceedings

22. Penalties

CHAPTER 4

JURISDICTION

23. Jurisdiction

CHAPTER 5

POWERS TO INVESTIGATE, SEARCH AND ACCESS OR SEIZE

24. Standard Operating Procedures

25. Application of provisions in this Chapter

26. Search for and access to, or seizure of, certain articles

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

28. Oral application for search warrant or amendment of warrant

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

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

31. Search for, access to and seizure of article on arrest of person

32. Assisting member of law enforcement agency or investigator

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

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

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

36. False information under oath or by way of affirmation

37. Prohibition on disclosure of information

38. Interception of indirect communication, obtaining of real-time communication-related information and archived communication-related information

39. Expedited preservation of data direction

40. Preservation of evidence direction

41. Oral application for preservation of evidence direction

42. Disclosure of data direction

43. Search for, access to, and seizure of to data where no authorisation is required

CHAPTER 6

MUTUAL ASSISTANCE

44. Application of provisions in this Chapter

45. Spontaneous information

46. Foreign requests for assistance and cooperation

47. Complying with order of designated judge

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

49. Issuing of direction requesting foreign mutual assistance

CHAPTER 7

24/7 POINT OF CONTACT

50. Establishment and functions of 24/7 Point of Contact

CHAPTER 8

EVIDENCE

51. Proof of certain facts by affidavit

CHAPTER 9

OBLIGATIONS OF ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS AND FINANCIAL INSTITUTIONS

52. Obligations of electronic communications service providers and financial institutions

CHAPTER 10

STRUCTURES TO DEAL WITH CYBERSECURITY

53. Cyber Response Committee

54. Government structures supporting cybersecurity

55. Nodal points and private sector computer security incident response teams

56. Information sharing

CHAPTER 11

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

57. Protection of critical information infrastructure

58. Auditing of critical information infrastructures to ensure compliance

CHAPTER 12

AGREEMENTS WITH FOREIGN STATES

59. National Executive may enter into agreements

CHAPTER 13

GENERAL PROVISIONS

60. National Director of Public Prosecutions must keep statistics of prosecutions

61. Repeal or amendment of laws

62. Regulations

63. Short title and commencement

Schedule

CHAPTER 1

DEFINITIONS

Definitions

1. In this Act, unless the context indicates otherwise—

"**access**" for purposes of Chapter 5, includes without limitation[1] to make use of data, a computer program, a computer data storage medium or a computer system or their accessories or components or any part thereof or any ancillary device or component to the extent necessary to search for and seize an article;

"**article**" means any data, computer program, computer data storage medium, or computer system which—

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

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

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

[1] SAHRC contended that the phrase “without limitation” is vague. According to the Department the phrase “includes without limitation” is to ensure that the definitions is not restrictively interpreted. It would be impossible to list all the identifiers that may be used for a search and seizure or which may in the future become relevant to a search and seizure.

of an offence in terms of Chapter 2 or section 16, 17 or 18 of the Act or any other offence which may be committed by means of or facilitated through, the use of such an article/**same means**[2], whether within the Republic or elsewhere;

Option 1

... of an offence—

(i) in terms of Chapter 2 or section 16, 17 or 18 of the Act;

(ii) or any other offence,

[which may be committed by means of or facilitated through, the use of such an article,]

whether within the Republic or elsewhere;

"**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 all—

(a) input devices;

(b) output devices;

(c) processing devices;

(d) computer data storage mediums; and

(e) other equipment and devices, **[that are related to, connected with or used with such a device]**

that are related to, connected with or used with such a device[3];

---

[2] Western Cape: The word “article” is used in the definition of “article” and the words “the same means”. Option 1 is a further proposal regarding the wording of the relevant part of the definition to address the concern.

Option 1

"**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 all—**

(a) **input devices;**

(b) **output devices;**

(c) **processing devices;**

(d) **computer data storage mediums; and**

(e) **other equipment and devices,**

that are related to, connected with or used with such a device (this must be a separate sentence and not part of (e))][4]

"**computer data storage medium**" means any device or location 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;

---

[3] Comments p 38 to 41. Printing error. The words "that are related to, connected with or used with such a device" should form a separate sentence under paragraph (e).

[4] According to international benchmarks there are two primary definitions of "computer" (that is sometimes also defined under the terminology of "computer system" or "device"). The one definition narrowly defines a "computer" as a device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data. The other category of definitions includes ancillary devices related to or forming part of a computer. A third benchmark does not define the concept of computer (UK, New Zealand and Australia). **Option 1 is the preferred option.**

"**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;

"**Criminal Procedure Act, 1977**" means the Criminal Procedure Act, 1977 (Act No. 51 of 1977);

"**Customs and Excise Act, 1964**" means the Customs and Excise Act, 1964 (Act No. 91 of 1964);

"**Customs Control Act, 2014**" means the Customs Control Act, 2014 (Act No. 31 of 2014);

“cybercrime” means —

(a) any offence in terms of section 2, 3, 4, 5, 6, 7, 8, 9, 10 and 11 of this Act and a contravention of section 12 in respect of the aforementioned offences;

(b) **any offences in terms of section 16, 17 or 18 of this Act; or**

(c) **any other offence which is or was committed by means of or facilitated by the use of an article;**[5]

[5] The Committee requested the Department to look at a possible definition of a cybercrime. Chapter 2 of the Bill deals with two categories of offences, namely offences against a computer system and offences that is facilitated by a computer system and which is recognized as a

"cybersecurity"[6] means the implementation of measures to manage threats against critical information infrastructures;

---

specific form of cybercrime. Clauses 16, 17 and 18 deals with malicious communications (it must be pointed out that section 12 do not apply to such offences and sections 256 of the CPA that deals with attempt will be applicable. The Department previously pointed out that it serve no purpose to define "cybercrime" and that new categories of cybercrime is being recognized from time to time (among others copyright infringements, communications that is of a *racist and xenophobic* nature, child harm material offences, cyber terrorism, malicious communications etc). The Bill already acknowledges the investigation of other offences that is committed or facilitated by electronic means in Chapters 5 and 6 of the Bill and it is not necessary to define the investigative powers to the specific proscriptions in Chapter 2, section 16, 17 or 18 of the Bill or to include other offences in Chapter 2 to specifically provide that if they are committed by means of electronic technologies that such offences must be regarded as a cybercrime. Paragraph (c) of the definition caters for other crimes that is not specifically included in Chapter 2 of the Bill.

[6] The Department was requested to see if it is not possible to include a definition of "cybersecurity" in the Bill. The Department already indicated that it is not necessary to define "cybersecurity" for purposes of the Bill, that it is problematic to define cybersecurity since no general accepted definition exists and that cybersecurity changes due to developments in the cyberspace. Reference can be made to the article "Defining Cybersecurity" by Dan Craigen, Nadia Diakun-Thibault, and Randy Purse" where the authors made an evaluation of the existing definitions in the literature of cybersecurity, which are all criticized due to various shortcomings. The authors then proposes the following definition "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights". This definition probably includes all the necessary elements of cybersecurity but is rather vague and not suitable for legislative interpretation purposes. The proposed definition specifically caters for Chapter 11 of the Bill and is not a comprehensive definition of cybersecurity.
The basic elements of cybersecurity were discussed in the comment and responses document where it was indicated that cybersecurity includes: Emergency warning systems regarding cyber vulnerabilities; raising awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them; the identification of critical infrastructure and enhance protection of such infrastructures; tracing of attacks on information infrastructures and, where appropriate, the disclosure of tracing information; enhancement of response mechanisms to deal with attacks; continuity and contingency plans in the event of attacks on information infrastructure; adequate substantive and procedural laws, and trained personnel that can investigate and prosecute cyber offences and the ability to coordinate investigations with other countries; international co-operation when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analyzing information regarding

"**data**" means electronic representations of information in any form[7];

"**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 (Act No. 70 of 2002);

New definition:

"electronic communications identity number" means a technical identification label which represents the origin or destination of electronic communications traffic, as a rule clearly identified by a logical or virtual identity number or address assigned to a customer of an electronic communications service provider (such as a telephone number, cellular phone number, email address with

---

vulnerabilities, threats, and incidents, and coordinating investigations of attacks on such infrastructures in accordance with domestic laws; the promotion of national and international research and development and encouraging the application of security technologies that are certified according to international standards; the promotion of partnerships among stakeholders, both public and private, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures. It was indicated that the various Chapters of the Bill aims to achieve these objectives.

[7] According to the NPA it is a concern that subscriber data is not part of the definition. It is submitted that subscriber data is not specifically catered for since these information may be obtained in terms of the RICA (see among others section 19 (archived communication-related information), sections 39(3) and 40(7) (confirmation of particulars of client of an ECSP) and section 205 of the Criminal Procedure Act, 1977). These provisions may be used to obtain subscriber information. Clause 42(1)(*b*) of the Bill may also be used to obtain subscriber data under judicial authorisation. Clause 46 specifically caters for traffic data in relation to a request for mutual legal assistance, where the designated judge may make an order in terms of section 46(6)(*c*), that traffic data, in so far as it may indicate that a person, electronic communications service provider or financial institution was involved in the transmission of the communication, is disclosed on an expedited basis in accordance with clause 42.

or without a corresponding IP address, Web address with or without a corresponding IP address or other subscriber number);[8]

"**electronic communications service provider"** means any person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act, 2005;

"**financial institution**" means a ' financial institution' as defined in section 1 of the **[Financial Services Board Act, 1990 (Act No. 97 of 1990)]** **Financial Sector Regulation Act, 2017 (Act No.9 of 2017)**; [9]

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

"**International Co-operation in Criminal Matters Act, 1996**" means the International Co-operation in Criminal Matters Act, 1996 (Act No. 75 of 1996);

"**Intelligence Services Act, 2002**" means the Intelligence Services Act, 2002 (Act No. 65 of 2002);

---

[8] This definition is relevant to clause 20 of the Bill (obligations on ECSP to furnish information to the court iro malicious communications. This will identify the origin and destination of malicious communications and may be used to identify the person who sent the malicious communications as well as to confirm the fact that the communications in question was sent to the complainant.

[9] The definition of "financial institution" refers to the Financial Service Board Act, 1990. In June 2017 the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017), was passed, and which repeals the Financial Service Board Act. This definition should therefore be amended to refer to the definition in the Financial Sector Regulation Act, 2017.

"**Intelligence Services Control Act, 1994**" means the Intelligence Services Control Act, 1994 (Act No. 40 of 1994);

"**investigator**" means any **appropriately qualified, fit and proper person[10],** who is not a member of the South African Police Service and who is—

(a) identified and authorised in terms of a search warrant contemplated in section 27(3); or

(b) requested by a police official in terms of section 30(3) or 31(4),

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

Option 1[11]

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

(*a*) **declared a peace officer in terms of section 334(5) of the Criminal Procedure Act, 1977 (Act No.51 of 1977)[12]; and**

[(a)] **(i)** identified and authorised in terms of a search warrant contemplated in section 27(3); or

[(b)] **(ii)** requested by a police official in terms of section 30(3) or 31(4),

---

[10] This amendment gives effect to the request of the SAPS that only persons that are qualified in digital forensic investigations must be appointed as investigators.

[11] This option provides for the appointment of persons that are qualified in digital forensic investigations must be appointed as investigators in line with the request of the SAPS, but also ensures that such persons may be appointed as peace officers ito section 334 of the Criminal Procedure Act. The advantage of this clause is that the category of persons that may be appointed as "investigators" are preselected by way of the notice that must be published in terms of section 334 of the CPA, and which specifically addresses the liability of investigators.

[12] See proposed amendments to section 334 of the CPA, in the Schedule to the Bill.

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

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

"**Magistrates' Courts Act, 1944**" means the Magistrates' Courts Act, 1944 (Act No. 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 of the Republic of South Africa, 1996;

"**National Prosecuting Authority Act, 1998**" means the National Prosecuting Authority Act, 1998 (Act No. 32 of 1998);

"National Strategic Intelligence Act, 1994" means the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994);[13]

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

"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;][14]

---

[13] The National Strategic Intelligence Act are referred to more than once in the Bill and should therefore be defined.

[14] During the development of the Bill it was proposed that definitions in the Bill should as far as possible be included in clause 1 of the Bill. The Department, is however of the opinion that the definitions of "output of a computer program" and "output of data", should be moved to clause 2, since it only relates to that clause.

"**payment system institution**" means a clearing system participant, a designated clearing system participant, a designated settlement system, a designated settlement system operator, a designated settlement system participant, a PCH system operator, a Reserve Bank settlement system, a Reserve Bank settlement system participant, a payment system, a settlement system, a settlement system participant or a system operator, as defined in the National Payment System Act, 1998 (Act No. 78 of 1998), or any other entity or system subject to that Act;

"**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 (Act No. 68 of 1995);

"**Prevention of Organised Crime Act, 1998**" means the Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998);

"**Protection from Harassment Act, 2011**" means the Protection from Harassment Act, 2011 (Act No. 17 of 2011);

"**publicly**[15] **available data**" means data which is accessible in the public domain without restriction;

"**Public Finance Management Act, 1999**" means the Public Finance Management Act, 1999 (Act No. 1 of 1999);

"**Public Service Act, 1994**" means the Public Service Act, 1994 (Proclamation 103 of 3 June 1994);

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

[15] Grammatical correction.

Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002);

"**seize**" includes to—

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

(b) render inaccessible,[16] 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 output of data or a computer program;

"**specifically designated police official**" means a commissioned officer referred to in section 33 of the South African Police Service Act, 1995 (Act No. 68 of 1995), who has been designated in writing by the National Commissioner to—

(i) make oral applications for a search warrant or an amendment of a warrant contemplated in section 28;

(ii) issue expedited preservation of data directions contemplated in section 39; or

(iii) serve an order from the designated judge on a person, electronic communications service provider or financial institution, contemplated in section 46(10);

"**South African Reserve Bank**" means the South African Reserve Bank, referred to in section 223 of the Constitution of the Republic of South Africa, 1996, read with section 2 of the South African Reserve Bank Act, 1989;

"**South African Reserve Bank Act, 1989**" means the South African Reserve Bank Act, 1989 (Act No. 90 of 1989);

---

[16] Grammatical correction.

"**Superior Courts Act, 2013**" means the Superior Courts Act, 2013 (Act No. 10 of 2013);

"**Tax Administration Act, 2011**" means the Tax Administration Act, 2011 (Act No. 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.

CHAPTER 2

CYBERCRIMES[17]

Personal and financial information or data related offences

… . (1) Any person who unlawfully and intentionally—

(*a*) acquires by any means;

(*b*) possesses; or

(*c*) provides to another person,

the personal information of another person for purposes of committing an offence under this Act or any other law is guilty of an offence.

(2) Any person who unlawfully and intentionally—

(*a*) acquires by any means;

(*b*) possesses; or

(*c*) provides to another person,

[17] Summary of Comments and Responses Part A: Pages 48 to 58.

the financial information of another person for purposes of committing an offence under this Act or any other law is guilty of an offence.

(3) Any person who unlawfully and intentionally uses the personal information or financial information of another person to commit an offence under this Act or any other law is guilty of an offence.

(4) Any person who is found in possession of personal information or financial information of another person in regard to which there is a reasonable suspicion that such personal information or financial information–

(*a*) was acquired, is possessed, or is to be provided to another person for purposes of committing an offence under this Act or any other law; or

(*b*) was used or may be used to commit an offence under this Act or any other law,

and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

(6) For purposes of this section—

(*a*) "personal information" means any 'personal information' as defined in section 1 of the POPIA, 2013 (Act No. 4 of 2013); and

(*b*) "financial information" means any unique identifier that has been assigned to a person by a financial or other institution that enables a person to access funds, credit or other financial benefits.[18]

[18] Summary of Comments and Responses Part A: Paragraph 3.1.2 page 48 (comments of South African Communications Forum in respect of phishing and identity theft), paragraph 3.1.5 page 49 (joint submissions by Cell C, Telkom and Vodacom pages 49 to 51). This offence was in a previous version of the Bill but was removed on the basis that it may have unintended

Option 2

Financial information related offences

.... (1) Any person who unlawfully and intentionally—

(*a*) acquires by any means;

(*b*) possesses; or

(*c*) provides to another person,

the financial information of another person for purposes of committing an offence under this Act or any other law is guilty of an offence.

(2) Any person who intentionally and unlawfully uses the financial information of another person to commit an offence under this Act or any other law is guilty of an offence.

(3) Any person who is found in possession financial information of another person in regard to which there is a reasonable suspicion that such financial information–

(*a*) was acquired, is possessed, or is to be provided to another person for purposes of committing an offence under this Act or any other law; or

(*b*) was used or may be used to commit an offence under this Act or any other law,

and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

---

consequences in so far as it relates to personal information. Option 2, deal only with financial information.

(4) For purposes of this section "financial information" means any unique identifier that has been assigned to a person by a financial or other institution that enables a person to access funds, credit or other financial benefits.[19]

Unlawful securing of access

2. (1) Any person who unlawfully and intentionally secures access to—

(a) data;

(b) a computer program;

(c) a computer data storage medium; or

(d) a computer system;

is guilty of an offence.

(2) For purposes of this section a person secures access to—

(a) data when the person is in a position to—

(i) alter, modify or delete the data;

[19] Option 2, deal only with financial information and may be less objectionable on the basis that it limits the application of the clause to the use of financial information for purposes to commit offences. This may address the current harvesting of financial information to commit financial offences. It is submitted that clause 7 (Unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices) may partly address the proposal. However, clause 7 is only applicable to "a password, an access code or similar data or device for purposes of contravening the provisions of section 2(1), 3(1), 5(1), 6(1), 8 or 9(1)" and cannot be used to prosecute other offences such as real- world fraud or theft committed with harvested financial information. The phrase "unique identifier" is not defined further but will include credit card numbers, a pin, an access card etc.

(ii) copy or move the data to a different location in the computer data storage medium in which it is held or to any other computer data storage medium;

(iii) obtain its output **[data]**[20]; or

(iv) otherwise use the data;

(b) a computer program when the person is in a position to—

(i) alter, modify or delete the computer program;

(ii) copy or move the computer program to a different location in the computer data storage medium in which it is held or to any other computer data storage medium;

(iii) cause a computer program to perform any function;

(iv) obtain its output; or

(v) otherwise use the computer program;

(c) a computer data storage medium when the person is in a position to—

(i) access data as contemplated in paragraph *(a)* or access a computer program as contemplated in paragraph *(b)*, stored on the computer data storage medium;

(ii) store data or a computer program on a computer data storage medium; or

(iii) otherwise use the computer data storage medium; or

(d) a computer system when the person is in a position to—

(i) use any resources of;

(ii) instruct; or

(iii) communicate with,

---

[20] Word must be removed.

a computer system,

and the access contemplated in paragraph *(a)*, *(b)*, *(c)* or *(d)* which the person secures is unauthorised.

(3) For purposes of subsection (2)—

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

(*b*) "output of a computer program" means any—

[(a)](i) data or output of the data;

[(b)](ii) computer program; or

[(c)](iii) instructions,

generated by a computer program; and

(*c*) "**unauthorised**" means that the person—

***[(a)]*(i)** is not himself or herself lawfully entitled to secure access;

***[(b)]*(ii)** does not have the lawful consent of another person who is lawfully entitled to secure access; or

***[(c)]*(iii)** exceeds his or her entitlement or consent, to secure access,

to data, a computer program, a computer data storage medium or a computer system.

Option 1[21]

Unlawful [securing of] access

[21] Summary of Comments and Responses Part A: Page 58 to 59 (Paragraph 3.2.1 - Cell C, Telkom and Vodacom that proposes that the proscription should follow the Budapest Convention)

2. (1) Any person who unlawfully and intentionally—

(*a*) overcomes any protection measure[22] which is intended to prevent access to; and

(*b*) thereafter accesses,

data, a computer program, a computer data storage medium, a computer system, is guilty of an offence.

(2) For purposes of subsection (1)—

(*a*) "access" means to make use of data, a computer program, a computer data storage medium or a computer system; and

Option on paragraph (a)[23]

(a) a person accesses—

(i) data when the person is in a position to—

(*aa*) alter, modify or delete the data;

(*bb*) copy or move the data to a different location in the computer data storage medium in which it is held or to any other computer data storage medium;

(*cc*) obtain its output **[data]**; or

(*dd*) otherwise use the data;

(ii) a computer program when the person is in a position to—

(*aa*) alter, modify or delete the computer program;

---

[22] Many computer devices are not protected by security measures such as firewalls or passwords and this may fall outside the criminalizing provision.

[23] During the consultation process on the Bill concerns were raised that the Bill does not define what entails.

(*bb*) copy or move the computer program to a different location in the computer data storage medium in which it is held or to any other computer data storage medium;

(*cc*) cause a computer program to perform any function;

(*dd*) obtain its output; or

(*ee*) otherwise use the computer program;

(iii) a computer data storage medium when the person is in a position to—

(*aa*) access data as contemplated in subparagraph (i) or access a computer program as contemplated in subparagraph (ii), stored on the computer data storage medium;

(*bb*) store data or a computer program on a computer data storage medium; or

(*cc*) otherwise use the computer data storage medium; or

(iv) a computer system when the person is in a position to—

(*aa*) use any resources of;

(*bb*) instruct; or

(*cc*) communicate with,

a computer system; and

(*b*) “protection measures” means any measure that restricts access to data, a computer program, a computer data storage medium and a computer system.

(3) For purposes of this section—

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

(*b*) "output of a computer program" means any—

[(a)](i) data or output of the data;

[(b)](ii) computer program; or

[(c)](iii) instructions,

generated by a computer program; and

(*c*) the actions of a person, to the extent that such actions exceed his or her lawful authority to access data, a computer program, a computer data storage medium or a computer system, must be regarded as unlawful.[24]

Unlawful acquiring of data [25]

3. (1) Any person who unlawfully and intentionally—

(a) overcomes any protection measure which is intended to prevent access to data; and

(b) acquires 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, with the knowledge that such data was acquired unlawfully as contemplated in subsection (1), is guilty of an offence.

---

[24] The proposed paragraph (*c*) is to ensure that unlawfulness is not restricted to unauthorised actions of a person which is the basis for unlawfulness in clause 2 of the Bill. Furthermore, authority is a concept that has extensively been interpreted in the criminal law and it is not necessary in the Bill to spell out when conduct is unauthorised.

[25] Summary of Comments and Responses Part A: Pages 63 to 68.

(3) Any person who is found in possession of data, in regard to which there is a reasonable suspicion that such data was acquired 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 "**acquire**" means—

(a) use;

(b) examine or capture data or any output thereof;

(c) copy data;

(d) move data to—

(i) a different location in a computer system in which it is held; or

(ii) any other location; or

(e) divert data from its intended destination to any other destination.

Option 1[26]

Unlawful interception of data

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

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

[26]Summary of Comments and Responses Part A: Page 63 to 64 (paragraph 3.3.1) – Recommendation by Cell C, Telkom and Vodacom.

(3) Any person who is found in possession 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 the purposes of subsection (1) "interception of data" means the use of technical means to acquire data stored within or which is transmitted to or from a computer system, including electromagnetic emissions[27] from a computer system carrying such data.

Unlawful acts in respect of software or hardware tool[28]

4. (1) Any person who unlawfully and intentionally possesses, manufactures, assembles, obtains, sells, purchases, makes available or advertises any software or hardware tool for the purposes of contravening the provisions of section 2(1), 3(1), 5(1), 6(1) or 7(1)*(a)* or *(d)*, is guilty of an offence.

(2) Any person who unlawfully and intentionally uses any software or hardware tool for purposes of contravening the provisions of section 2(1), 3(1), 5(1), 6(1) or 7(1)*(a)* or *(d)*, is guilty of an offence.

(3) For purposes of this section "**software or hardware tool**" means any electronic, mechanical or other instrument, device, equipment, apparatus or a

[27] Computer equipment, like every other type of electrical equipment emits electromagnetic impulses that can be intercepted and decoded to obtain the content of data.

[28] Summary of Comments and Responses Part A : Pages 68 to 73.

substantial component of such a device or a computer program, which is designed or adapted primarily for the purposes to—

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

(b) acquire 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, modify, provide, make available, copy, use or clone a password, access code or similar data or devices as defined in section 7(3).

Option 1[29]

4. **[(1) Any person who unlawfully and intentionally possesses, manufactures, assembles, obtains, sells, purchases, makes available or advertises any software or hardware tool for the purposes of contravening the provisions of section 2(1), 3(1), 5(1), 6(1) or 7(1)*(a)* or *(d)*, is guilty of an offence.**

(2)] (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), 3(1), 5(1), 6(1) or 7(1)*(a)* or *(d)*, is guilty of an offence.

[29] Subclause (1) is deleted as a result of criticism during the development of the Bill and concerns raised before the Committee especially in so far as it relates to the development, distribution and use of these tools for vulnerability testing.

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

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

(b) acquire 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**[, modify, provide, make available, copy,] or** use **[or clone]**[30] a password, access code or similar data or devices as defined in section 7(3).

Unlawful interference with data or computer program [31]

5. (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 "**interference with data or a computer program**" means to permanently or temporarily—

[30] The two words “acquire” and “use” is sufficient to prescribe the purpose of the software or hardware tool.

[31] Summary of Comments and Responses Part A : Page 73

(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.

Unlawful interference with a computer data storage medium or computer system[32]

6. (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 "**interference with a computer data storage medium or a computer system**" means to permanently or temporarily—

(a) alter any resource of; or

(b) interrupt or impair—

(i) the functioning of;

(ii) the confidentiality of;

(iii) the integrity of; or

(iv) the availability of,

a computer data storage medium or a computer system.

[32] Summary of Comments and Responses Part A: Pages 73 to 75

Unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices[33]

7. (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), 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), 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.

[33]Summary of Comments and Responses Part A: Pages 75 to 76

(3) For purposes of this section **"password, access codes or similar data or device"** means without limitation—

(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—

(i) financial transactions; or

(ii) user authentication in order to access or use data, a computer program, a computer data storage medium or a computer system.

Cyber fraud[34]/[35]

---

[34] Summary of Comments and Responses Part A: Page 76

[35] The SAPS ask the question as to why only certain common law offences identified as “cyber-offences” and not others. Specific reference is made to section 13, which aims to extend the definition of theft to theft of incorporeal property. It is the submission of the Department that it is not necessary to redefine all common law offences as to include a cyber element. The so called “common law offences” in the Bill are offences that forms part of Conventions, model laws and legislation of some countries (the so called computer facilitated offences). In the AU and SADC context, the primary offences that were identified to be criminalised are fraud, forgery and uttering and extortion (other offences that may be committed by digital means are however recognised by these documents such as cyber terrorism, child pornography offences, copyright offences, other property related offences etc.
One of the aims of the Bill is to consolidate current laws and to ensure that it can specifically be prosecuted with reference conduct that facilitates such offences in cyber space.
* The common law offence of fraud requires a misrepresentation that causes prejudice to another. Clause 8(a) is similar to the common law offence in that a misrepresentation can be made by means of data. However, the clause expands on the manner of making a

8. 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 subsection 5(2)**(*a*), (*b*) or (*e*)**[36] or interference with a computer data storage medium or a computer system as contemplated in section 6(2)**(*a*)**,

which—

(i) causes actual prejudice; or

(ii) is potentially prejudicial,

to another person is guilty of the offence of cyber fraud.

---

misrepresentation that is cyber specific namely through a computer program, interference with data or a computer program or a computer system.
* Clause 9, is substantially similar to the common law offence of forgery and uttering, however, it expands on and clarify the "document" requirement that is an element of the common law offence. The first scenario addresses false data, which may as a result of the ECTA be regarded as a document. The second scenario relates to a computer program, which does not currently qualify as a document.
* The offence of cyber extortion contemplated in clause 10 differs from the common law offence since it does not require that and advantage be handed over. As part of the proscription a requirement of the offence is that the perpetrator must have committed or must threaten the victim that specified offences in the Bill will be committed to extort an advantage from the victim.
* South African courts already recognised the theft of certain incorporeal property, but the extent of what property qualify as the object of the crime is yet undefined (see S v NDEBELE AND OTHERS 2012 (1) SACR 245 (GSJ). Clause 13 is an instruction to courts to further develop this offence to specifically recognise the theft of an incorporeal.
The Bill specifically recognise the fact that other offences on the Statute Book can be committed by electronic means, and for this purposes, Chapters 5 and 6 of the Bill provides for procedural aspects relating to the investigation of offences that is specified in the Bill as well as any other offence that may be committed or facilitated by electronic means. It is submitted that it is not necessary to redefine other common law offences so as to include a cyber element.

[36] These insertions further clarify the clause.

Cyber forgery and uttering[37]

9. (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.

Cyber extortion[38]

10. Any person who unlawfully and intentionally—

(a) threatens to commit any offence; or

(b) commits any offence,

contemplated in sections 3(1), 5(1), 6(1) or 7(1)*(a)* or *(d)*, for the purpose of—

[37] Summary of Comments and Responses Part A: Page 76

[38] Summary of Comments and Responses Part A: Pages 76 to 78.

(i) obtaining any advantage from another person; or

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

is guilty of the offence of cyber extortion.

Aggravated offences[39]

11. (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**[40]**,** 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 under the control of, or exclusively used by—

(i) any financial institution;

[(ii) an organ of state as set out in section 239 of the Constitution of the Republic of South Africa, including a court;][41] or

---

[39] Summary of Comments and Responses Part A : Page 78.

[40] It is more equitable to insert a specific intention requirement in this clause that must be an element of the crime.

[(iii)](ii) a critical information infrastructure as contemplated in section 57(2).

(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**[42] [which] **will**—

(i) endanger**[s]** the life, or violate**[s]** the physical integrity or physical freedom of, or cause**[s]** bodily injury to, any person, or any number of persons;

(ii) cause**[s]** serious risk to the health or safety of the public or any segment of the public;

(iii) cause**[s]** the destruction of or substantial damage to any property;

(iv) cause**[s]** a serious interference with, or serious disruption of an essential service, facility or system, or the delivery of any essential service;

(v) cause**[s]** any major economic loss;

(vi) create**[s]** a serious public emergency situation; or

(vii) prejudice**[s]** the security, the defence, law enforcement or international relations of the Republic,

is guilty of an aggravated offence.

---

[41] It is submitted that this provision may be unduly wide and may include structures that is so critical that they should not be protected by enhance penalties. In terms of section 239(b) of the Constitution an "organ of state" includes "(b) any other functionary or institution-

(i) exercising a power or performing a function in terms of the Constitution or a provincial constitution; or

(ii) exercising a public power or performing a public function in terms of any legislation….".

If any structure that resorts under the definition of "organ of state", should be protected, that structure should be declared a critical information infrastructure as contemplated in clause 57 of the Bill.

[42] It is again submitted that it is more equitable to insert a specific intention requirement in this clause that must be an element of the crime.

(3) A prosecution in terms of subsections (1) or (2) must be authorised in writing by the Director of Public Prosecutions having jurisdiction.

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

12. 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 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.

Theft of incorporeal[43]

13. The common law offence of theft must be interpreted so as not to exclude the theft of **[an]** incorporeal **property**[44].

[43] Summary of Comments and Responses Part A: Pages 78 to 80.

[44] Western Cape Paragraph 3.12.1

[Penalties] Sentencing[45]/[46]

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

(2) Any person who contravenes the provisions of section 3(1) or (2), 4(1) **[or (2)]**[47], 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—

---

[45] Summary of Comments and Responses Part A: Pages 80 to 83.

[46] This clause should be renamed since it deals with other aspects relevant to sentencing and not only penalties.

[47] To be deleted in light of the proposed amendment to clause 4(1).

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

(b) the extent of the prejudice and loss suffered by the complainant or 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) If a person is convicted of any offence provided for in section 2(1), 3(1), 5(1), 6(1), 7(1), 8, 9(1) or (2), 10 or 11(1) or (2), a court which imposes any sentence in terms of those sections where the offence was committed—

(a) by a person; or

(b) 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 which was involved in the offence, must, unless substantial and compelling circumstances justifying the imposition of another sentence impose, with or without a fine, a period of direct imprisonment which may not be suspended as contemplated in section 297(4) of the Criminal Procedure Act, 1977.

(7) *(a)* Upon the conviction of any person for an offence in terms of this Chapter, the public prosecutor must, if any person has suffered any loss as a result of such offence, apply in terms of section 300 of the Criminal Procedure Act, 1977 (Act 51 of 1977), for an order for the payment of compensation to such a person who has suffered a loss.

(*b*) A regional court or a magistrate's court shall not make an order for the payment of compensation, contemplated in paragraph (a) if the compensation applied for exceeds the amount determined by the Minister from time to time by notice in the *Gazette* in respect of the respective courts, which amount may differ from the amounts determined in terms of section 300(1)(*a*) of the Criminal Procedure Act, 1977.[48]

Competent verdicts[49]

15. (1) If the evidence in criminal proceedings does not prove the commission of the offence charged but proves a contravention of section 12—

(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.

---

[48] Although section 300 of the Criminal Procedure Act, 1977, will always be applicable if a person suffered a loss as a result of an offence, a peremptory application for a compensation order may enhance the effectiveness of the prescribe sentencing options. In terms of Government Notice No. R. 62 published in GG 36111 of 30 January 2013 amounts of R1 000 000 in respect of a regional court, and R300 000 in respect of a magistrates' court were prescribed. Subclause (7)(b) make it possible to prescribe amounts lower than or in excess of amounts determined in terms of section 300(1)(*a*) of the CPA. See page 83 paragraph 3.13.7 of the Summary of Comments and Responses where TBCSA hints that losses which are incurred as a result of a cyber offence should be a factor that should be considered during sentencing. (Section 15 of the Stock Theft Act, 1959 (Act 57 of 1959); section 7 of the Game Theft Act, 1991 (Act 105 of 1991), section 22(2)(*b*) of the Witness Protection Act, 1998 (Act 112 of 1998), also provides for peremptory compensation order applications.

[49] Summary of Comments and Responses Part A: Page 84.

(2) If the evidence on a charge of a contravention of section 3(1), does not prove the offence **or a contravention of section 12 in respect of that offence**, but proves—

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

(b) a contravention of section 3(2) or (3); or

(c) a contravention of section 4**[(2)](1)**[50] in so far as it relates to the use 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 12 in respect of that offence**, but proves—

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

(b) a contravention of section 4**[(2)](1)**[51] in so far as it relates to the use of a software or hardware tool for purposes of contravening section 5(1); or

(c) or 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 attempt to commit the offence] or a contravention of section 12 in respect of that offence**, but proves—

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

---

[50] To be deleted in light of the proposed amendment to clause 4(1).

[51] To be deleted in light of the proposed amendment to clause 4(1).

(b) a contravention of section 4**[(2)](1)** in so far as it relates to the use of a software or hardware tool for purposes of contravening section 6(1); or

(c) or 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 12 in respect of that offence**, but proves—

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

(ii) a contravention of section 7**(1)(*b*) or (*c*)** or (2); or

(iii) a contravention of section 4**[(2)](1)** in so far as it relates to the use of a software or hardware tool **to acquire or use a password, access code or similar data or devices for purposes of contravening section 7(1)*(a)* or *(d)***,

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 12 in respect of that offence**, but proves a contravention of section 7(2), the accused may be found guilty of the 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 12 in respect of the offence**, but proves—

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

(b) a contravention of section 4**[(2)](1)**, in so far as it relates to the use 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); **[or**

(iii) acquire, modify, provide, make available, copy, or use a password, access code or similar data and devices as contemplated in section 7(1)*(a)* or *(d)*;]

(*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;

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

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

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

([f]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 12 in respect of the offence**, but proves—

(i) the common law offence of forgery**; or**,

(ii) a contravention of section 9(2),

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 3(1), 5(1), 6(1) or 7(1) as contemplated in]** section 11(1), and the evidence on the charge does not prove a contravention of section 11(1), but a proves a contravention of—

(a) section 2(1);

(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 5(1), 6(1) or 10, as contemplated in]** section 11(2), and the evidence on the charge does not prove a contravention of section 11(2), but a proves a contravention of—

(a) section 2(1);

(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 not referred to in the preceding subsections does not prove the commission of the offence so charged 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.[52]

[52] Subclause (10), similar to section 270 of the Criminal Procedure Act, 1977, is a catch-all clause. A person may for instance be charged with a contravention of clause 7(1) (unlawful acquiring of a password). Evidence, however, proves that the accused received a stolen a USB without and password on it in contravention section 37 of the General Law Amendment Act, 1955 (Act 62 of 1955) (receiving of stolen property). In such an instance the accused may be convicted in terms of subclause (10) of the offence of contravening section 37 of the aforementioned Act.

CHAPTER 3[53]

MALICIOUS COMMUNICATIONS

Definitions

…. For purposes of this Chapter, unless the context indicates otherwise—

"damage to property" means damage to property, whether corporeal or incorporeal, of a serious nature;

"data message" ……..[54]

"identifiable group of persons" means characteristic that identifies an individual as a member of a group of persons including, but not limited to association, nationality, religion, conscience, belief, status, culture, race, ethnic or social origin; and

"violence" means —

(*a*) conduct that is likely to cause bodily injury; or

(*b*) unwanted conduct of a sexual nature that offends, intimidates or humiliates.

Data message which incites damage to property or violence [55]

---

[53] Summary of Comments and Responses Part A: Pages 84 to 129.

[54] The definition in clause 1 of "data message" can conveniently be inserted under this Chapter.

[55] Summary of Comments and Responses Part A : Pages 98 to 100.

16. Any person who unlawfully **and intentionally**[56] makes available, broadcasts or distributes by means of a computer system, a data message to a **[specific]** person, group of persons or the general public with the intention to incite—

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

(b) violence against,

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

Data message which is harmful[57]

17. (1) Any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message which is harmful, is guilty of an offence.

(2) For purposes of subsection (1), a data message is harmful when it—

(a) threatens a person with—

(i) damage to any property belonging to, or violence against, that person; or

(ii) damage to any property belonging to, or violence against, any member of the family or household of the person or any other person in a close relationship with the person;

[56] Printing error.

[57] Summary of Comments and Responses Part A: Pages 100 to 113.

(b) threatens a group of persons with damage to any property belonging to, or violence against, the group of persons or any identified person forming part of the group of persons or who is associated with the group of persons;

(c) intimidates, encourages or harass a person to harm himself or herself or any other person; or

(d) is inherently false in nature and it is aimed at causing mental, psychological, physical or economic harm to a specific person or a group of persons,

and a reasonable person in possession of the same information and with regard to all the circumstances would regard the data message as harmful.

New options[58]

Data message which is harmful

17. (1) Any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message which is harmful, is guilty of an offence.

(2) For purpose of subsection (1), a data message is harmful when—

(a) it threatens a person with—

(i) damage to any property belonging to, or violence against, that person; or

[58] This option is mainly a redraft of clause 17.

(ii) damage to any property belonging to, or violence against, any member of the family or household of that person or any other person in a close relationship with that person; or

(*b*) it threatens—

(i) an identifiable group of persons;

(ii) any person forming part of that group of persons; or

(iii) any person associated with that group of persons,

with damage to any property belonging to, or violence against—

(*aa*) that group of persons;

(*bb*) any person who forms part of that group of persons; or

(*cc*) any person who is associated with that group of persons; or

(*c*) it, either by itself or in conjunction with any other data message, intimidates, [encourages] coerces or harasses a person to—

(i) [harm] commit an act of violence against himself or herself;

(ii) [or another person]commit an act of violence against another person; or

(iii) cause damage to any property belonging to himself or herself or another person,[; or

(*d*) is inherently false in nature and it is aimed at causing mental, psychological, physical or economic harm to a specific person or a group of persons,]

and a reasonable person in possession of the same information and with regard to all the circumstances would regard the data message as harmful.

Option:

Data message which is false that is aimed at causing mental, psychological, physical or economic harm [59]

… **(1) Any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message which is false, is guilty of an offence.**

(2) For purpose of subsection (1), a data message is false when it—

(*a*) is inherently false in nature;

(*b*) is made available, broadcasted or distributed with the aim to cause mental, psychological, physical or economic harm to a specific person or an identifiable group of persons; and

(*c*) is not—

(i) a honestly-held opinion that was expressed after taking into account all relevant information and presented in a manner that appears clearly to be an opinion or comment; or

(ii) a bona fide artistic creativity, performance or other form of expression, to the extent that such creativity, performance or expression does not aim to cause mental, psychological, physical or economic harm to a specific person or an identifiable group of

[59] The redrafted clause aims to introduce additional safeguards to guard against unintended consequences – Page 86 paragraph 4.1.4.

persons,

and a reasonable person in possession of the same information and with regard to all the circumstances would regard the data message as false.

(3) (*a*) Any prosecution in terms of this section must be authorised by the Director of Public Prosecutions having jurisdiction.

(*b*) Paragraph (*a*) must not be construed so as to prohibit a complainant—

(i) to apply for a protection order referred to in section 19 of this Act pending the decision of the Director of Public Prosecutions having jurisdiction; or

(ii) where the Director of Public Prosecutions having jurisdiction decided not to prosecute, to apply for a protection order against harassment as contemplated in the Protection from Harassment Act, 2011.

Distribution of data message of intimate image without consent[60]

18. (1) Any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message of an intimate image of a**[n identifiable]** person **[knowing that]** **without the permission of**[61]

[60] Summary of Comments and Responses Part A: Pages 113 to 121.

[61] Summary of Comments and Responses Part A: page 119, paragraph 4.4.8 (d) – The words "knows that consent has not been given" should be replaced with wording to the effect that criminal liability will attached unless the perpetrator "knows consent has been given". This will also cater for instances where a person has given consent but later retract such consent.

the person **[depicted in the image did not give his or her consent to the making available, broadcasting or distribution of the data message]**, is guilty of an offence.

(2) For purposes of subsection (1)—

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

(i) real or simulated [made by any means] in which—

(*aa*) the person is nude, is exposing his or her genital organs or anal region or, in the case of a female, her breasts; or

(*bb*) the person's covered genital or anal region or in the case of a female of her breasts, is displayed in an unduly manner that violate or offend the sexual integrity or dignity of that person[62];

(ii) made by any means; and

(iii) [(i) under circumstances that give rise to a reasonable expectation of privacy; and] in respect of which the person so depicted retains a reasonable expectation of privacy at the time the data message was made; and

(*b*) "person"[63] means—

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

---

[62] The proposed amendment aims to cater for "creep shots" – (pictures of women that show cleavage/ men that show bulging) and for "upskirt images" and "downblouse images" – See Summary of Comments and Responses Part A : Page114 paragraph 4.4.3, page 115, paragraph 4.4.5, page 120 paragraph 4.4.8 (f).

[63] The amendment propose to deal with the issue of surrounding circumstances identification and incorrectly identified images - Summary of Comments and Responses Part A: Page 115, paragraph 4.4.5 (b); page 118, paragraph 4.4.8 (c)

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

(iii) any person who can be identified from other information as being depicted in the data message.

Option

Distribution of data message of intimate image without consent

18. (1) A person (“A”) who unlawfully and intentionally makes available, broadcasts or distributes by means of a computer system an intimate image of a person (“B”), is guilty of an offence.

(2) A person (“A”) who unlawfully and intentionally threatens a person (“B”), a member of the family of B or a person in close relationship with B with the making available, broadcasting or distribution by means of a computer system of an intimate image of B, is guilty of an offence.

(2) For purposes of subsection (1) and (2)—

(*a*) "intimate image" means a data message real or simulated made by any means in which—

(i) B is nude, is exposing his or her genital organs or anal region or, in the case of a female, her breasts; or

(ii) the covered genital or anal region or in the case of a female of her breasts of B, is displayed in an unduly manner that violate or offend the sexual integrity or dignity of B;

(ii) in respect of which B so displayed retained a reasonable expectation of privacy at the time the data message was made; and

(iii) B so displayed did not give his or her consent that the data massage may be made available, broadcasted or distributed by A; and

(*b*) "person" ("B")[64] 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 he or she cannot be identified as being displayed in the data message; and

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

Order to protect complainant pending finalisation of criminal proceedings[65]

---

[64] The amendment propose to deal with the issue of surrounding circumstances identification and incorrectly identified images - Summary of Comments and Responses Part A: Page 115, paragraph 4.4.5 (b); page 118, paragraph 4.4.8 (c)

[65] Summary of Comments and Responses Part A : Pages 121 to 126

19. (1) A complainant who lays a charge with the South African Police Service that an offence contemplated in section 16, 17 or 18 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 an order pending the finalisation of the criminal proceedings to—

(a) prohibit any person from further making available, broadcasting or distributing the data message contemplated in section 16, 17 or 18 which relates to the charge; or

(b) order an electronic communications service provider or person in control of a computer system to remove or disable access to the data message in question.

(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 proceedings.

(3) If the court is satisfied that there is *prima facie* evidence that the data message in question constitutes an offence as contemplated in section 16, 17 or 18, the court may issue the order referred to in subsection (1), in the prescribed form.

(4) The order must be served on the person referred to in subsection (1)*(a)* or electronic communications service provider or person referred to in subsection (1)*(b)* in the prescribed form and manner: Provided, that if the 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 manner specified in that order.

(5) An order referred to in subsection (1) 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 or person referred to in subsection 1*(b)*.

(6) A person referred to in subsection (1)*(a)* or electronic communications service provider or person referred to in subsection (1)*(b)* may, within 30 days after the order has been served on him, her or it in terms of subsection (4), 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 (1).

(7) 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 shall form part of the record of the proceedings.

(8) The court may, for purposes of subsections (2) and (7), in the prescribed 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 or electronic communications service provider who fails to comply with an order referred to in subsection (5) 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.

Electronic communications service provider or person in control of computer system to furnish particulars to court[66]

20. (1) If an application for a protection order is made in terms of section 19(1) and the court is satisfied in terms of section 19(3) that a protection order must be issued and the identity or address of the person who made available, broadcasted or distributed the data message in question 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 or person in control of a computer system to furnish the court in the prescribed manner by means of an affidavit in the prescribed form with—

[66] Summary of Comments and Responses Part A: Pages 127 to 128

(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 complainant; and

(iv) any other information that is available to an electronic communications service provider or a person in control of a computer system which may be of assistance to the court to identify the person who made available, broadcasted or distributed the data message in question or the electronic communications service provider or person in control of a computer system which provides a service to the person who made available, broadcasted or distributed the data message.

(2) If the court issues a direction in terms of subsection (1) the court must direct that the direction be served on the electronic communications service provider or person in control of a computer system in the prescribed manner.

(3) *(a)* The information referred to in subsection (1)*(b)*(i), (ii), (iii) and (iv) 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 or person.

(b) An electronic communications service provider or person in control of a computer system 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 either the respondent or complainant or related person; or

(*bb*) the requested information is not available in the records of the electronic communications service provider or person in control of a computer system.

(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 affidavit from the electronic communications service provider or the person in control of a computer system as it deems fit;

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

(d) must inform the electronic communications service provider or the person in control of a computer system in the prescribed form and in the prescribed manner of the outcome of the application.

(5) *(a)* The court may, on receipt of an affidavit from an electronic communications service provider or person in control of a computer system which contains the information referred to in subsection (1)*(b)*(i) and (ii), consider the issuing of a protection order in terms of section 19(3) against the person who made available,

broadcasted or distributed the data message contemplated in section 16, 17 or 18 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 19(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 or persons in control of a computer system for providing the information referred to in subsection (1)*(b)*.

(7) Any electronic communications service provider, employee of an electronic communications service provider or person in control of a computer system 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 or person 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.

Orders on finalisation of criminal proceedings[67]

21. (1) Whenever a person is—

[67] Summary of Comments and Responses Part A: Page 128.

(a) convicted of an offence in terms of section 16, 17 or 18; or

(b) acquitted of an offence in terms of section 16, 17 or 18,

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 provisions of that Act shall apply with the necessary changes required by the context.

(2) The trial court must, on convicting a person for the commission of an offence contemplated in section 16, 17 or 18 order—

(a) that person to refrain from further making available, broadcasting or distributing the data message contemplated in section 16, 17 or 18 which relates to the charge on which he or she is convicted;

(b) that person or any other person to destroy the data message in question or any copy of the data message; or

(c) an electronic communications service provider or person in control of a computer system 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 accused, and (2)*(c)*, must be in the prescribed form and must be served on the electronic communications service provider or person in control of a computer system 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 manner specified in that order.

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

(5) 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.

(6) Whenever a person is convicted of an offence in terms of section 16, 17 or 18, the trial court must issue an order that the person must reimburse all expenses incurred by—

(a) a complainant as a result of any direction issued in terms of section 20(1)(*b*); or

(b) an electronic communications service provider or person in control of a computer system to remove or disable access to the data message in question,

whereupon the provisions of section 300 shall apply with the necessary changes required by the context, to such order.[68]

[68] The proposed amendment is to ensure that the perpetrator should be liable for costs that result from his or her unlawful conduct.

Penalties[69]

22. (1) Any person who contravenes the provisions of section 16, 17 or 18 is liable on conviction to a fine or to imprisonment for a period not exceeding 3 years or to both a fine and such imprisonment.

(2) Any person or electronic communications service provider who contravenes the provisions of section 19(9) or (10), 20(7) or 21(4) is liable on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both a fine and such imprisonment.

CHAPTER 4

JURISDICTION[70]

Jurisdiction

23. (1) A court in the Republic trying an offence in terms of Chapter 2 or section 16, 17 or 18 has jurisdiction where—

(a) the offence was committed in the Republic;

(b) any act in preparation for the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;

---

[69] Summary of Comments and Responses Part A: Page 128.

[70] Summary of Comments and Responses Part A: Page 129.

(c) the offence was committed in the Republic or outside the Republic by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or

(d) the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

(2) If the act alleged to constitute an offence in terms of Chapter 2 or section 16, 17 or 18 occurred outside the Republic, a court of the Republic, regardless of whether or not the act constitutes an offence at the place of its commission, has jurisdiction in respect of that offence if the person to be charged—

(a) is a citizen of the Republic;

(b) is ordinarily resident in the Republic;

(c) was arrested in the territory of the Republic, or in its territorial waters or on board a ship or aircraft registered or required to be registered in the Republic at the time the offence was committed;

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

(e) is any body of persons, corporate or unincorporated, in the Republic.

(3) Any act alleged to constitute an offence in terms of Chapter 2 or section 16, 17 or 18 and which is committed outside the Republic by a person, other than a person contemplated in subsection (2), is, regardless of whether or not the act constitutes an offence or not at the place of its commission, deemed also to have been committed in the Republic if that—

(a) act affects or is intended to affect a public body, **a financial institution or other** business, **a critical information infrastructure** or any other person in the Republic;

(b) person is found to be in South Africa; and

(c) person is for one or other reason not extradited by South Africa or if there is no application to extradite that person.

(4) 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 acted.

(5) *(a)* A prosecution in terms of subsections (2) and (3)—

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

(6) The National Director of Public Prosecutions appointed in terms of section 179 (1) of the Constitution, in consultation with National Commissioner of the South African Police Service, 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 contemplated in subsections (2) and (3). [71]

CHAPTER 5

POWERS TO INVESTIGATE, SEARCH AND ACCESS OR SEIZE[72]/[73]/[74]

Standard Operating Procedures[75]

---

[71] The SAPS requested that the National Director should issue policy prescripts that must be complied with in the investigation of offences as contemplated in subsections (2) and (3). It is submitted that the appropriate functionary to issue such instructions is the National Commissioner. It is further submitted that the proposed subclause (6) is not necessary since the National Commissioner may in any event regulate the conduct of the SAPS in respect of the investigation of criminal offence that originate outside the Republic to clarify the place where or component of the SAPS that should investigate such an offence. Subclause (5)(*a*)(ii) already clarifies the concern regarding jurisdiction of a court. No other law specifically provides for policy prescripts in the event of extra-tertorial jurisdiction (see among others section 61 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act 32 of 2007; Section 30A of the Films and Publications Act, 1996 (Act 65 of 1996); and section 12 of the Prevention and Combating of Trafficking in Persons Act, 2013 (Act 7 of 2013).

[72] Summary of Comments and Responses Part A: Pages 129 to 184.

[73] General comments - Summary of Comments and Responses Part A : Pages 129 to 135.

[74] According to the NPA, the Bill or an amendment to the RICA should provide for remote searches. The NPA did not fully discuss what this entails in their responses to questions in the Committee. The concept of remote searches entails the installing of software on a computer system that makes available data on such computer or otherwise interfere with the use of a computer. The use of such tools is the flipside of the actions of cybercriminals which use the tools to commit various offences. Various countries specifically recognise the use of remote access tools in the investigation of offences in the cyber domain. The primary aim of the Bill is to provide for search and seizure of devices and data stored on such devices. The use of remote access tools relates closely to the interception of information. Due to the far reaching implications of this procedure it should be address in the RICA, which is currently in a process of revision.

[75] Summary of Comments and Responses Part A: Pages 135 to136.

24. (1) The Cabinet member responsible for policing, in consultation with 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 six 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 provision of any other law to investigate any offence in terms of any law,

in the investigation of any offence in terms of Chapter 2 or section 16, 17 or 18 of this Act or any other offence which is or was committed by means of or facilitated by 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*.[76]

Application of provisions in this Chapter[77]

[76] The SAPS proposed that the SOPS should not be made available to the public since it may provide information of SAPS investigating procedures. Various other countries, among others the UK (ACPO) made their SOPS available to the general public. The purpose of SOPS is not to discuss the procedures that are used by the law enforcement agencies to obtain digital evidence but set out established standards and procedures that must be followed in order to ensure the integrity of digital evidence in order to ensure that a court can rely on such evidence. These SOPs must comply with international standards that are in any event publicly available. The Department disagree with this secrecy proposal of the SAPS which may have the effect that persons may be prejudiced in criminal trial proceedings. A basis of fair criminal proceedings is, among others, that laws and other prescripts must be available to the accused person to challenge allegations. The SAPS is still of the opinion that the period referred to in clause 24(1) must be extended to 18 months due to the consultation requirement. The opinion is held that the SAPS may take the necessary preparatory work to draft the SOPS whilst the Bill is in the Parliamentary process.

25. 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.

Search for and access to, or seizure of, certain articles[78]

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

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

27. (1) Subject to the provisions of sections 29, 30 **[and]** 31 **and 38(1) and (2)**[79] 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

---

[77] The NPA is of the view that the Criminal Procedure act, 1977, should be amended to provide for procedural aspects relevant to the investigation of cybercrime. It is submitted that such an approach may be followed. Various countries followed this approach by amending their procedural laws to provide for an integrated approach in the investigation of real-world crime and cybercrime (see among others New Zealand (Search and Surveillance Act 2012); Australia (Crimes Act 1914); UK (Police and Criminal Evidence Act, 1984) (however see the Computer Misuse Act, 1990, that contain specific section that deals with the authorisation of warrants regarding computer searches (sections 14 and 15). RICA on the other hand also deals with specific measures to investigate criminal matters, and do not form part of the Criminal Procedure Act, 1977. Since the Bill aims to deal comprehensively with all aspects relating to cybercrime it may be preferable to deal separately with the powers to search and seize and not to incorporate these powers in the Criminal Procedure Act, 1977. Clause 25 of the Bill ensures that the Criminal Procedure Act applies in addition to the Bill, in so far as the CPA is not inconsistent with the Bill.

[78] Summary of Comments and Responses Part A: Pages 137 to 147

[79] This insertion further clarifies the interaction between the Bill and the RICA.

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 that there are reasonable grounds for believing that an article is—

(i) within his or her area of jurisdiction; or

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

(*aa*) within his or her 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 in the commission of an offence; or

(b) by a magistrate or judge 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 and 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 of 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).

Oral application for search warrant or amendment of warrant[80]

---

[80] According to the SAPS oral applications are not very effective (this criticism applies equally to clause 41). This remark of the SAPS must be evaluated together with their remarks relating to clause 31(3), where oral applications are considered as an additional step that may frustrate investigation of cybercrime. This aspect is therefore discussed under clause 31 of the Bill. In a follow-up meeting with the SAPS it is requested that this clause be deleted as well as other references to oral applications for a search warrant. According to the SAPS, a police official should have the same powers in respect of an article as are afforded to a police official in terms of section 22(b) of the CPA (search and seize without a warrant on reasonable grounds to believe that a search warrant will be issued to him or her and that the delay in obtaining such warrant would defeat the object of the search). During the consultation process the powers of the SAPS to search and seize without a warrant was an issue that was criticised by all. The criticism was based on the following factors:
* Computer systems are complex and the SAPS do not have the necessary expertise to conduct investigations which may result in damage to systems and substantial pecuniary losses.
* Cyber searches and seizures have the potential of substantial infringements on constitutional rights of persons and search and seizures should therefore not be undertaken without judicial authority.
* Only in exceptional circumstances should the SAPS be allowed the powers to search and seize computer systems.

28. (1) An application referred to in section 27(1)*(a)*, or an application for the amendment of a warrant issued in terms of section 27(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 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 him or her in terms of subsection (1) and subject to subsection (4), issue a warrant or amend a warrant as contemplated in section 27(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—

---

* The need for the SAPS to search and seize in exigent circumstances are recognised but an expedited procedure for applications for a warrant must be introduced.
To cater for the afore-mentioned concerns, the oral application procedure was provided for in the Bill.

(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 his or her 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 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) A warrant or any amendment to a warrant issued under subsection (3) must—

(a) be in writing;

(b) be transmitted electronically to the member of the law enforcement agency; 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 he or she is not available, any other magistrate or judge of the High Court must, upon receipt of a written application

submitted to him or her in terms of subsection (4)*(b)*, reconsider that application whereupon he or she 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 as he or she deems fit how any article which is affected by his or her decision is to be dealt with.

Option

Clause be deleted to address concerns of the SAPS.

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

29. (1) Any police official may, without a search warrant, execute the powers referred to in section 27(2) of this Act, 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, request an investigator to assist him or her with the search for, access to, or seizure of the article in question.

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

30. (1) A police official may without a search warrant referred to in section 27(1)*(a)* search any person or container or premises for the purposes 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 the definition of "article", if the police official on reasonable grounds believes—

(a) that a search warrant will be issued to him or her under section 27(1)*(a)* if he or she applies 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 27(1)*(a)*: Provided that a police official may if he or she on reasonable grounds believes—

(a) that a search warrant will be issued to him under section 27(1)*(a)* if he or she applies 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]**[81] application for a search warrant,

he or she may access and perform the powers referred to in paragraphs *(c)* or *(d)* of the definition of "seize" without a search warrant.

---

[81] See discussion under clause 28. SAPS request that they be allowed to access a device and to search and seize data on similar grounds as section 22(b) of the CPA (search and seize without a warrant on reasonable grounds to believe that a search warrant will be issued to him or her and that the delay in obtaining such warrant would defeat the object of the search),without the need of an oral application. Also see discussion under clause 31.

(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).

Search for, access to and seizure of article on arrest of person

31. (1) A 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 Chapter 2 or section 16, 17 or 18 of this Act in his or her presence;

(b) whom he or she reasonably suspects of having committed any offence in terms of Chapter 2 or section 16, 17 or 18; or

(c) who has been concerned with or against whom a reasonable complaint has been made or credible information has been received or a reasonable suspicion exists that he or she has been concerned with an offence in terms of Chapter 2 or section 16, 17 or 18 of this Act or any other offence substantially similar to an offence recognised in the Republic which is or was committed by means of, or facilitated by the use of an article, in a foreign State and for which he or she is, 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 a section 40 or in terms of a warrant issued in terms of section 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 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 paragraphs *(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 27(1)*(a)*: Provided that a police official may if he or she on reasonable grounds believes—

(a) that a search warrant will be issued to him under section 27(1)*(a)* if he or she applies 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[82] for a search warrant,

---

[82] The SAPS indicated in respect of clauses 28 and 41 that the oral application process in terms of section 23 of the RICA is not very effective. The SAPS also raise to following concerns in relation to the additional safeguard, namely that the circumstances is of such a nature that it is not reasonable practical to orally apply for a search warrant before a search and seizure without a warrant may take place:

* If a suspicious person who is not necessarily investigated by the Police, is arrested by the Police and found with a computer device/cellular phone in his/her possession which may afford evidence of the commission of a crime, the SAPS will not be able to apply for a search warrant unless they know what criminal evidence is stored on the device/cellular phone.

* The clause deviates from section 23 of the Criminal Procedure Act, 1977, in that that section provides that where a person is arrested, he or she maybe searched and any article found in possession/custody of such a person may be seized. Reference is made to State v Miller 2015 JDR 1808 (WCC) where it was remarked that “the reason that a cell phone is seized in a case such as this is to enable the police to access and examine its contents, be they phone numbers and addresses, SMS messages, emails or photographs. Possession of the instrument per se would be of no assistance to an organised crime investigation such as was undertaken here”. It must be mentioned that the matter was decided on the basis that “access” to a device

contravened section 86(1) of the ECTA since only cyber inspectors are allowed to access information on a device and that the member of the SAPS contravened section 86 and that the evidence should be excluded on that basis.

The SAPS does not take into account that section 23 of the CPA makes provision for two distinct possibilities of search and seizure. In terms of section 23(1), a person may be searched and articles referred to in section 20 may be seized if it is found in the possession of or in the custody or under the control of the person arrested. In terms of this clause the articles that may be seized are articles-

(a) which is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within the Republic or elsewhere;
(b) which may afford evidence of the commission or suspected commission of an offence, whether within the Republic or elsewhere; or
(c) which is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence

Where the articles fall outside the ambit of section 20 of the CPA, the SAPS may in terms of section 23(2), place in safe custody any object found on the person arrested and which may be used to cause bodily harm to himself or others.
It is submitted that clause 31 similar to section 23 of the CPA, provides that not all articles may be seized but only articles that is related to or involve in a offence. Section 23(2) of the CPA will be applicable to an articles seized in terms of clause 31 if it does not fall within the definition of an article in terms of the Bill.

The right to privacy *vis-a-vi* warrantless searches of computers have to date not authoritatively been decided by our courts. The position in Canada is as follows:
R. v. VU [2013] 3 S.C.R.
First, the police must obtain judicial authorization for a search before they conduct it, usually in the form of a search warrant. Second, an authorized search must be conducted in a reasonable manner, ensuring that the search is no more intrusive than is reasonably necessary to achieve its objectives. The privacy interests implicated by computer searches are markedly different from those at stake in searches of receptacles such as cupboards and filing cabinets. It is difficult to imagine a more intrusive invasion of privacy than the search of a personal or home computer. Computers potentially give police access to an almost unlimited universe of information that users cannot control, that they may not even be aware of, may have tried to erase and which may not be, in any meaningful sense, located in the place of search. The numerous and striking differences between computers and traditional receptacles call for distinctive treatment under s. 8 of the Charter. The animating assumption of the traditional rule — that if the search of a place is justified, so is the search of receptacles found within it — simply cannot apply with respect to computer searches. In effect, the privacy interests at stake when computers are searched require that those devices be treated, to a certain extent, as a separate place. Prior authorization of searches is a cornerstone of our search and seizure law. The purpose of the prior authorization process is to balance the privacy interest of the individual against the interest of the state in investigating criminal activity

before the state intrusion occurs. Only a specific, prior authorization to search a computer found in the place of search ensures that the authorizing justice has considered the full range of the distinctive privacy concerns raised by computer searches and, having done so, has decided that this threshold has been reached in the circumstances of a particular proposed search. This means that if police intend to search any computers found within a place they want to search, they must first satisfy the authorizing justice that they have reasonable grounds to believe that any computers they discover will contain the things they are looking for. If police come across a computer in the course of a search and their warrant does not provide specific authorization to search computers, they may seize the computer, and do what is necessary to ensure the integrity of the data. If they wish to search the data, however, they must obtain a separate warrant.
(Also see R. v. Cole, 2012 SCC 53, [2012] 3 S.C.R. 34; R. v. Spencer [2014] 2 S.C.R.)

R. v. Fearon, 2014 SCC 77, [2014] S.C.R. 621
The power to search incident to arrest is extraordinary in that it permits reasonable searches when the police have neither a warrant nor reasonable and probable grounds. That the exercise of this extraordinary power has been considered in general to meet constitutional muster reflects the important law enforcement objectives which are served by searches of people who have been lawfully arrested. This power must be exercised in the pursuit of a valid purpose related to the proper administration of justice and the search must be truly incidental to the arrest. Like other searches incident to arrest, prompt cell phone searches incident to arrest may serve important law enforcement objectives: they can assist police to identify and mitigate risks to public safety; locate firearms or stolen goods; identify accomplices; locate and preserve evidence; prevent suspects from evading or resisting law enforcement; locate the other perpetrators; warn officers of possible impending danger; and follow leads promptly. Cell phone searches also have an element of urgency, which supports the extension of the power to search incident to arrest. Safeguards must be added to the law of search of cell phones incident to arrest in order to make that power compliant with s. 8 of the Charter. Ultimately, the purpose of the exercise is to strike a balance that gives due weight to the important law enforcement objectives served by searches incidental to arrest and to the very significant privacy interests at stake in cell phone searches. *Consequently, four conditions must be met in order for the search of a cell phone or similar device incidental to arrest to comply with s. 8. First, the arrest must be lawful. Second, the search must be truly incidental to the arrest. This requirement should be strictly applied to permit searches that must be done promptly upon arrest in order to effectively serve the law enforcement purposes. In this context, those purposes are protecting the police, the accused or the public; preserving evidence; and, if the investigation will be stymied or significantly hampered absent the ability to promptly conduct the search, discovering evidence. Third, the nature and the extent of the search must be tailored to its purpose. In practice, this will mean that only recently sent or drafted emails, texts, photos and the call log will, generally, be available, although other searches may, in some circumstances, be justified. Finally, the police must take detailed notes of what they have examined on the device and how they examined it. The notes should generally include the applications searched, the extent of the search, the time of the search, its purpose and its duration. The record-keeping requirement is*

he or she may access and perform the powers referred to in paragraphs *(c)* or *(d)* of the definition of "seize" without a search warrant.

---

important to the effectiveness of after-the-fact judicial review. It will also help police officers to focus on whether what they are doing in relation to the phone falls squarely within the parameters of a lawful search incident to arrest.

US
Riley v California 573 US
Warrant is necessary to search a cell phone unless one of the exceptions that will render such a search lawful applies. A warrantless search violates the Fourth Amendment (right to privacy. The law enforcement agencies may seize a cell phone but a second warrant is necessary to access search and seize info on a cell phone.(Cell phone is regarded as a separate container)

Australia
R v Varga[2015] QDC 82
If person consents, the law enforcement agencies may access a cell phone. If there is no consent, the police must rely on their statutory powers, which by implication includes a reasonable suspicion.

New Zealand
Section 88 of the Search and Surveillance Act, 2012, provides that a warrantless search is authorised, among others, if there is ***reasonable grounds to believe that anything that is carried by the person so arrested is evidential material in respect of the offence for which the person was arrested or detained****.*

UK
Under the Police and Criminal Evidence Act 1984, law enforcement officers may search, seize and retain data from a mobile phone belonging to anyone who has been arrested on suspicion of committing an offence, provided that they have a **reasonable belief that it contains evidence of an offence or has been obtained in consequence of the commission of an offence**.
.
Oral applications for warrants is recognised in laws of various countries, see among others section 184 of the Canadian Criminal Code, section 103 of the New Zealand Search and Surveillance Act, 2012, section 3R of the Australian Crimes Act, 1914. Section 23 of the RICA, as pointed out by the SAPS, is the only law that deals with oral applications for authorisation to investigate. Oral applications must in terms of clause 28(2) comply with directives issued by the Chief Justice, which in turn will ensure that it can effectively be implemented.

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

Assisting member of law enforcement agency or investigator[83]

32. (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 27(1) must, if required, provide—

(a) technical assistance; and

(b) such other assistance as may be **reasonable**[84] necessary,

to a police official or investigator in order to search for, access and 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 not exceeding 2 years or to both such fine and imprisonment.

Obstructing or hindering police official or investigator and authority to overcome resistance

---

[83] Summary of Comments and Responses Part A : Pages 151 to 153.
[84] Summary of Comments and Responses Part A: Pages 151 to 152, paragraph 6.8.1

33. (1) Any person who unlawfully and intentionally obstructs or hinders a police official or an investigator in the exercise of his or her powers or the performance of his or her duties or functions in terms of this Chapter or who refuses or fails to comply with a search warrant issued in terms of section 27(1), is guilty of an offence and is liable on conviction to a fine or imprisonment not exceeding 2 years or to both such fine and imprisonment.

(2) *(a)* A police official who may lawfully execute any power conferred upon him or her in terms of section 27(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 he or she has audibly demanded admission to the premises, vehicle, facility, ship or aircraft and has notified the purpose of his or her 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.

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

34. (1) The powers conferred upon a police official or an investigator in terms of section 27(2), 29, 30 or 31, 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 27(2)*(a)*, *(c)* or *(d)* or 31, 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.

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

35. (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 27(1); or

(ii) consent granted in terms of section 29(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 investigator—

(i) searches for, accesses or seizes data, a computer program, a computer data storage medium or any part of a computer system or any other information, instrument, device or equipment; 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 police official or an investigator who obtains or uses any instrument, device, equipment, password, decryption key, data or other information contemplated in section 27(2)*(h)*—

(a) 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

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

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

(ii) it will not be required for purposes of any criminal 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

(iii) 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.

(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 such fine and imprisonment.

(4) Where a police official or an investigator is convicted of an offence referred to in subsection **[(1) or (2)]**(3)[85], 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, apply with the necessary changes required by the context to such award.

False information under oath or by way of affirmation

36. (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 29 took place on the basis of such information;

(c) a computer data storage medium or any part of a computer system is seized in terms of section 30;

(d) an expedited preservation of data direction contemplated in section 39 is issued;

(e) a preservation of evidence direction contemplated in section 40 is issued; or

---

[85] A reference to subsections (1) and (2) is not incorrect. However, a reference to the criminalizing provision, in this instance subsection (3), is technical more in line with drafting practices.

(f) a disclosure of data direction contemplated in section 42 is issued,

is guilty of an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding 2 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, apply with the necessary changes required by the context **[with reference]**[86] to such award.

Prohibition on disclosure of information[87]

37. (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 he, she or it has obtained in the exercise of his, her or its powers or the performance of his, her or its duties in terms of Chapters 5 and 6 of this Act, except—

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

(b) if he or she is a person who of necessity supplies such information in the performance of his or her duties or functions in terms of this Act;

---

[86] Deletion necessary to ensure consistency with other similar provisions – see clause 35(4)
[87] Summary of Comments and Responses Part A: Pages 154 to156.

(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—

(i) contemplated in Chapter 10 of this Act; or

(ii) between electronic communications service providers, financial institutions the South African Police Service, **any competent authority in a foreign State**[88] 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 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 protected or authorised under the Protected Disclosures Act, 2000 (Act No. 26 of 2000), the Companies Act, 2008 (Act No. 71 of 2008), the Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004), the National Environmental Management Act, 1998 (Act No. 107 of 1998), or the Labour Relations Act, 1995 (Act No. 66 of 1995);

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

(c) reveals a criminal activity.

---

[88] This is common practice among financial institutions and the various CSIRTs that ensure cybersecurity in the financial sectors.

(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 contravenes the provisions of subsection (1) is guilty of an offence and is liable on conviction to a fine or imprisonment not exceeding 3 years or to both such fine and imprisonment.

Interception of indirect communication, obtaining of real-time communication-related information and archived communication-related information[89]/[90]

38. (1) The interception of data which is 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**[n interception]** direction issued in terms of section 16(4) or 18(3)**[*(a)*]** of that Act and

---

[89] Summary of Comments and Responses Part A: Pages 156 to 164.

[90] The SAPS contends that section 4(2) of the RICA prohibits a member of the SAPS to take screenshots of computers since it may constitute the interception of communications contemplated in that section. For purposes of the SOPs that need to be enacted in terms of clause 24 of the Bill, the recording of the crime scene during a forensic search and seizure is extremely important as part of the principle of an audit trail or record of the forensic process. In general, in the new digital era, the recording of information at a crime scene is essential. It is submitted that section 4 of the RICA is unfortunately worded in that-

(a) a forensic digital investigator will not be part of the communication; and

(b) the seriousness of the offence that is being investigated may not fall within the ambit of section 16(5) of the RICA, that in general only allows for the investigation of serious offences as contemplated in the Schedule to the RICA.

The recording of what a person hears or see cannot be prohibited. Legislation of other countries specifically authorised law enforcement to use digital means to record what they hear and see at a crime scene, see among others section 47 of the NZ Search and Surveillance Act 2012, section 64 of the Police and Criminal Evidence Act, 1984 (UK). An amendment to section 4 of the RICA is proposed in the Schedule to the Bill.

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 **[real-time communication-related]** direction issued in terms of section 17(3) or 18(3)**[*(b)*]** of that Act, and must, subject to subsection (4), be dealt with further in the manner provided for in that Act.[91]/[92]

---

[91] The interface between the RICA and the Bill should be clarified. Clause 38(1) for instance, provides that the interception of indirect communications must be authorised in terms of an interception direction issued in terms of RICA. Clause 27(2)(f), on the other hand, authorises access to an article (which includes data) on the strength of a search warrant issued by any Magistrate or Judge. It is not clear whether both a RICA direction by the designated Judge as well as a search warrant has to be obtained before data can be accessed by the SAPS.
It is submitted that the distinction between the RICA and the Bill is adequate dealt with in clauses 38(1) and (2). The SAPS should have taken cognisance of the judgement State v Miller 2015 JDR 1808 (WCC) which was referred to in another context in their presentation, where this was clarified as follows by the learned Judge at page 29 of the original transcript:
"Data not transmitted but stored on a computer will not fall under the interception directions in RICA. Anyone who needs such information as part of a criminal investigation will have to apply for a search warrant in terms of chapter 2 of the Criminal Procedure Act or other legislation that provides for search warrants.
Section 20(b) of the Criminal Procedure Act allows the State to seize 'anything (in this Chapter referred to as an article) that may afford evidence of the commission or suspected commission of an offence whether within the Republic or elsewhere". "Anything" has been held to extend to documents and money and will certainly extend to a computer or hard drive in which messages are stored".
An interception of an indirect communication takes place when the communication is transferred from person x to person y by means of an electronic communications service, see the definition of an "indirect communication" which is defined as:
"the transfer of information, including a message or any part of a message, whether-
(a) in the form of-
(i) speech, music or other sounds;
(ii) data;
(iii) text;
(iv) visual images, whether animated or not;

(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 **[referred to]** **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 39 of this Act in terms of which the electronic communications service provider

---

(v) signals; or
(vi) radio frequency spectrum; or
(b) in any other form or in any combination of forms,

that is transmitted in whole or in part by means of a …. telecommunication system;"
Once the information is not transmitted by an electronic communications system, for instance where it is stored on a data storage medium, it cannot be regarded as an indirect communication that is still being transmitted. Real-time communication-related information may accompany an indirect communication, and can at that stage be intercepted in terms of section 17 of the RICA. Some of the information that accompanies an indirect communication may be recorded and stored on an electronic database of an ECSP. If such information falls within the ambit of the retention requirement in the RICA, the RICA must be used to obtain such information. An e-mail header that is stored on a computer similarly contain real-time communications related information, but does not fall within the retention regime of the RICA and as such will not qualify as real-time communications related information.

is directed to preserve real-time communication-related information or archived communication-related information in respect of a customer;

(iii) a preservation of evidence direction contemplated in section 40 in terms of which the electronic communications service provider is directed to preserve real-time communication-related information or archived communication-related information in respect of a customer;

(iv) a disclosure of data direction contemplated in section 42 in terms of which the electronic communications service provider is directed to provide archived communication-related information in respect of a customer that was stored by the electronic communications service provider; or

(v) any order of the designated judge in terms of **[subsection (1) or (2) or]**[93] section 46(6), in terms of which the electronic communications service provider is ordered to—

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

(bb) furnish traffic data, in so far as it may indicate that an electronic communications service provider in a foreign State was involved in the transmission of the communication.

(4) Any indirect communication **[referred to in subsection (1)]**[94] which is intercepted or any real-time communication-related information which is obtained on an ongoing basis, or archived communication-related information which was obtained

---

[93] This must be omitted.

[94] This must be omitted.

and stored 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 46(6), which is issued by the designated judge.

Expedited preservation of data direction[95]

39. (1) Subject to section 38(1) and (2), a specifically designated police official may, if he or she on reasonable grounds believes that any person, an electronic communications service provider **referred to in section 38(3)**[96]**,** or a financial institution, is in possession of, is to receive, or is in control of data—

(a) which is relevant to;

(b) which was used or may be used in;

(c) for the purposes of or in connection with;

(d) which has facilitated or may facilitate; or

(e) which may afford evidence of,

the commission or intended commission of—

(i) an offence under Chapter 2 or section 16, 17 or 18 of this Act;

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

(iii) an offence—

---

[95] Summary of Comments and Responses Part A: Pages 164 to 178.

[96] The aim of the amendment is to clarify the applicability of a preservation order in so far as it relates to ECSPs - See among others the remarks and interpretations in paragraph 6.13.1, 6.13.2, 6.13.3 of the Summary of Comments and Responses Part A: Pages 164 to 168.

(*aa*) similar to those contemplated in Chapter 2 or section 16, 17 or 18 of this Act; or

(*bb*) substantially similar to an offence recognised in the Republic which is or was committed by means of, or facilitated by the use of an article,

in a foreign State,

issue, with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence in question, 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 information which must be stored for a certain period in terms of any other law and that period is due to come to an end.

(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 42.

(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 40 of this Act**, once, for an additional period which may not exceed 90 days[97].**

(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 he, she or it 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—

---

[97] The proposed amendment clarifies the period of operation of the expedited preservation of data direction that is extended in terms of clause 40.

(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 not exceeding 2 years or to both such fine and imprisonment.

Preservation of evidence direction[98]

40. (1) A magistrate or judge of the High Court may, on written application by a police official, if it appears to the magistrate or judge, from information on oath or by way of affirmation that there are reasonable grounds for believing that any person, electronic communications service provider or financial institution may receive, is in possession of, or is in control of an article—

(a) relevant to;

[98] Summary of Comments and Responses Part A: Page 178.

(b) which was used or may be used in;

(c) for the purpose of or in connection with;

(d) which has facilitated or may facilitate; or

(e) which may afford evidence of,

the commission or intended commission of—

(i) an offence under Chapter 2 or section 16, 17 or 18 of this Act;

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

(iii) an offence—

(*aa*) similar to those contemplated in Chapter 2 or or section 16, 17 or 18 of this Act; or

(*bb*) any other offence substantially similar to an offence recognised in the Republic which is or was committed by means of, or facilitated by the use of an article,

in a foreign State,

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 of or integrity of the evidence.

(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 3 years or to both such fine and 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 he, she or it cannot timeously or in a reasonable fashion, comply with the order.

(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.

Oral application for preservation of evidence direction[99]

41. (1) An application referred to in section 40(1), may be made orally by a police official, if he or she is of the opinion that it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make 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 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 him or her in terms of subsection (1), with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence in question, 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—

[99] Summary of Comments and Responses Part A : Page 178

(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 preserve the integrity of the evidence; 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.

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

Disclosure of data direction[100] and search for, access to and seizure articles subject to preservation of evidence direction[101]

[100] Summary of Comments and Responses Part A: Pages 178 to 180.

[101] Summary of Comments and Responses: Page 179 paragraph 6.16.3 – where question was raised regarding the process to obtained preserved evidence. Also see the proposed subclause (10) that addresses the concern of the MCO.

42. (1) Where—

(a) an expedited preservation of data direction or a preservation of evidence direction is in place **and it is expedient to obtain data without issuing a search warrant contemplated in section 27(1)**; or

(b) it is otherwise expedient to obtain data without issuing a search warrant contemplated in section 27(1),

a magistrate or judge of the High Court may, subject to section 4(3) of the Customs and Excise Act, 1964, sections 69(2)*(b)* and section 71 of the Tax Administration Act, 2011 and section 21*(e)* and *(f)* of the Customs Control Act, 2014, on written application by a police official, if it appears to the magistrate or judge from information on oath or by way of affirmation that there are reasonable grounds for believing that a person, electronic communications service provider or financial institution, other than the person, electronic communications service provider or financial institution who is suspected of having committed the offence which is being investigated, may receive, is in possession of, or is in control of data which is relevant to or which may afford evidence of the commission or intended commission of—

(i) an offence under Chapter 2 or section 16, 17 or 18 of this Act; or

(ii) any other offence in terms of the laws of the Republic which is or was committed by means of, or facilitated by the use of an article,

issue a disclosure of data direction.

(2) An application contemplated in subsection (1) must—

(a) contain the identity of the police official who applies for the disclosure of data direction;

(b) identify the **[customer, if known, or the service or communication in respect of whom]** data **which** is to be provided;

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

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

(e) contain a description of the offence which has been or is being or will probably be committed; and

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

(3) Upon receipt of an application in terms of subsection (1), a magistrate or judge must satisfy himself or herself—

(a) that there are reasonable grounds for believing that—

(i) an offence in terms of Chapter 2 or section 16, 17 or 18 of this Act; or

(ii) any other offence in terms of the laws of the Republic which is or was committed by means of, or facilitated by the use of an article,

has been, is being or will probably be committed or that it is necessary to determine whether such an offence has been so committed; and

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

(4) 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.

(5) The disclosure of data direction—

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

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

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

(6) A person, electronic communications service provider or financial institution to whom a disclosure of data direction referred to in subsection (5) is addressed 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 he or she cannot timeously or in a reasonable fashion comply with the direction.

(7) The magistrate or judge to whom an application is made in terms of subsection (6) 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 of the outcome of the application.

(8) Any data which is 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.

(9) 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 (6); or

(c) fails to comply with subsection (8),

is guilty of an offence and is liable on conviction to a fine or imprisonment not exceeding 2 years or to both such fine and imprisonment.

(10) (*a*) Articles subject to a preservation of evidence direction that is not "data" must be searched for, access or seize seized in terms of a warrant referred to in section 27(1).

(*b*) A police official may, at any time, apply for a search warrant in terms of section 27(1) to search for, access or seize an article (which includes "data") that is or was subject to a preservation of evidence direction.[102]

[102] The proposed amendment aims to address the concerns of the MCOs that it is unclear how and under what circumstances evidence must be transferred to a criminal investigator.

Search for, access to, and seizure of to data where no authorisation is required[103]

43. A police official may, without being specifically authorised thereto in terms of this Chapter, for the purposes of investigating any offence under Chapter 2 or section 16, 17 or 18 of this Act—

(a) **[search for, access or perform the powers referred to in paragraphs *(c)* or *(d)* of the definition of "seize" in respect of]** **obtain and use** publicly available data regardless of where the data is located geographically[104]; or

(b) receive non-public**ly**[105] available data, regardless of where the data is located geographically, if the person who has the lawful authority to disclose the data, voluntarily and on such conditions regarding confidentiality and limitation of use which he or she deems necessary, discloses the data to a police official. [106]

---

[103] Summary of Comments and Responses Part A: Pages 180 to 184.

[104] Summary of Comments and Responses Part A : Page 182 – Where a police official accesses publicly data and download or print it, it should not be regarded as a seizure.

[105] Grammatical correction.

[106] According to the SAPS, the wording of Clause 43(*b*) is problematic and subject to multiple interpretations. They contend that the SAPS can receive information from any source, whether obtained lawfully or unlawfully. It is implied in this clause that information that is not obtained lawfully by a source, cannot be received or used by a police official for policing purposes or evidence.
Clause 43(b), aims to provide a carve-out to the SAPS by providing that non-publicly available data may be received "**without being specifically authorised thereto in terms of this Chapter, for the purposes of investigating any offence under Chapter 2 or section 16, 17 or 18 of this Act**" regardless of where the data is located geographically, if the person who has the lawful authority to disclose the data, voluntarily and on such conditions regarding confidentiality and limitation of use which he or she deems necessary, discloses the data to a police official. This is to ensure that the obtaining of evidence cannot be challenged on the basis that it was not seized under judicial authority or the other provisions of Chapter 5 of the Bill. The

fact that unlawfully obtained evidence is brought to the attention of the SAPS which is used to initiated an investigation is not prohibited by this clause. Similar to the CPA, there is no authorisation for the SAPS to receive unlawfully obtained information that is used to initiate an investigation or any prohibition that the SAPS may not receive such information.

CHAPTER 6

MUTUAL ASSISTANCE[107]

Application of provisions in this Chapter

44. The provisions of sections 46 to 49 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 evidence **regarding the commission or intended commission of—**

(*a*) an offence under Chapter 2 or section 16, 17 or 18 of this Act;

(*b*) any other offence in terms of the laws of the Republic which is or was committed by means of, or facilitated by the use of an article; or

(*c*) an offence—

(i) similar to those contemplated in Chapter 2 or or section 16, 17 or 18 of this Act; or

(ii) any other offence substantially similar to an offence recognised in the Republic which is or was committed by means of, or facilitated by the use of an article,

in a foreign State[108],

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

---

[107] Summary of Comments and Responses Part A: Pages 184 to 185.

[108] The proposed insertion clarifies the word “evidence”.

Spontaneous information[109]

45. (1) The National Commissioner **or the National Head of the**[110] **Directorate referred to in section 17CA(1) of the South African Police Service Act, 1995, respectively,** may, on such conditions regarding confidentiality and limitation of use as he or she may determine **[and after obtaining the written approval of the National Director of Public Prosecutions as contemplated in subsection (2),]**[111] forward 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 i**[f]n**[112] the initiation or carrying out of investigations **[regarding an offence committed within the jurisdiction of that foreign State]**; or

---

[109] Summary of Comments and Responses Part A: Page 184.

[110] This clause does not recognise the structural and operational independence of the Directorate for Priority Crime Investigation (DPCI) as the DPCI does not report to the National Commissioner. The clause should therefore refer to both the National Commissioner and the Head of the DPCI. The Department agrees.

[111] According to the SAPS this wording is problematic since the NDPP is requested to make decisions regarding the combatting, investigation and prevention of criminal offences and aspects relating to intelligence. The Department agree that the involvement of the NDPP may be omitted from this clause.

[112] Printing error

(b) lead to further cooperation with a foreign State to carry out an investigation**,** regarding the commission or intended commission of—

(i) an offence contemplated in Chapter 2 or section 16, 17 or 18, of this Act;

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

(iii) an offence—

(*aa*) similar to those contemplated in Chapter 2 or section 16, 17 or 18 of this Act; or

(*bb*) any other offence substantially similar to an offence recognised in the Republic which is or was committed by means of or facilitated by the use of an article,

in that foreign State.

[(2) The National Director of Public Prosecutions must consider a request by the National Commissioner in terms of subsection (1) and may only grant approval referred to in subsection (1) if he or she is satisfied that the forwarding of information—

(a) **will not adversely affect any pending criminal proceedings or investigations within the Republic;**

(b) **will not be prejudicial to the interests of the Republic; and**

(c) **is in accordance with any applicable law of the Republic.]**[113]

---

[113] According to the SAPS the involvement of the NDPP since he or she is requested to make decisions regarding the combatting, investigation and prevention of criminal offences and aspects relating to intelligence. The Department agree that the involvement of the NDPP may be omitted from this clause.

(3) 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 will—

(a) assist the South African Police Service in the initiation or carrying out of investigations **[regarding an offence committed within the Republic]**; or

(b) lead to further cooperation with a foreign State to carry out an investigation, regarding the commission or intended commission of—

(i) an offence contemplated in Chapter 2 or section 16, 17 or 18 of this Act; or

(ii) any other offence in terms of the laws of the Republic which may be committed by means of or facilitated by, an article**[.],**

in the Republic.

Foreign requests for assistance and cooperation[114]

46. (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, in so far as it may indicate that a person, electronic communications service provider or financial institution in another state was involved in the transmission of the communication;

[114] Summary of Comments and Responses Part A: Page 185.

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

(e) interception of data which is an indirect communication,

must, subject to subsection (7), be submitted to the 24/7 Point of Contact.

(2) The 24/7 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—

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

(ii) that 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) that the offence in question is—

(*aa*) similar to those contemplated in Chapter 2 or section 16, 17 or 18 of this Act; or

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

(iv) that 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, communication or article in the Republic for use in such proceedings or investigation in the foreign State.

(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 the said subsections.

(4) *(a)* The National Director of Public Prosecutions must submit the request for assistance, together with his or her recommendations, to the Cabinet member responsible for the administration of justice, for his or her 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)*(a)* or *(b)* to the designated judge for consideration.

(5) Where the request relates to the expedited disclosure of traffic data, in so far as it may indicate that a person, electronic communications service provider or financial institution in a foreign State was involved in the transmission of the communication, subsections (3)*(a)*(iv) and (4) do not apply and the National Director of Public Prosecutions must submit the request for assistance, together with his or her 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 which he or she deems appropriate to ensure that the requested—

(a) data or other article is preserved in accordance with section 40;

(b) data is seized on an expedited basis in accordance with section 27 and preserved;

(c) traffic data, in so far as it may indicate that a person, electronic communications service provider or financial institution **[in a foreign State]** was involved in the transmission of the communication, is disclosed on an expedited basis in accordance with section 42;

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

(e) data which is an indirect communication is 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 Chapter 2 or section 16, 17 or 18 of this Act, has been or is being or will probably be committed; or

(ii) any other offence substantially similar to an offence recognised in the Republic was 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 or traffic data must be obtained or intercepted; and

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

(iii) the data which must be seized on an expedited basis;

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

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

(vi) data, which is an indirect communication, which is 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 59 of this Act; and

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

(8) Where a request relates to the expedited disclosure of traffic data as contemplated in subsection (6)*(c),* the designated judge may—

(a) specify conditions or restrictions relating to the disclosure of traffic data as he or she deems appropriate; or

(b) refuse to issue an order referred to in subsection (6)*(c)*, if the disclosure of the traffic data will, or is likely to, 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)* An order contemplated in subsection (6) must be executed by a specifically designated police official.

(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 executed.

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

Complying with order of designated judge

47. (1) A person, electronic communications service provider or financial institution must comply with an order of the designated judge issued in terms of section 46(6).

(2) A person electronic communications service provider or financial institution to whom an order referred to in section 46(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 he, she or it 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 46(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 not exceeding two years or to both a fine and such imprisonment.

Informing foreign State of outcome of request for mutual assistance and expedited disclosure of traffic data[115]

[115] Summary of Comments and Responses Part A: Page 185.

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

(a) the designated judge; and

(b) a foreign State,

of the outcome of its request for assistance and cooperation**.**

(2) Any traffic data which is made available in terms of an order referred to in section 46(6)*(c)* of this Act, must be—

(a) provided to the 24/7 Point of Contact for submission to an authority, court or tribunal of a foreign State; and

(b) accompanied by—

(i) a copy of the order referred to in section 46(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 information referred to in subsection (2)*(a)*, together with the copy of the order and affidavit referred to in subsection (2)*(b)*, must be provided to the authority, court or tribunal exercising jurisdiction in a foreign State which requested the assistance in terms of section 46(1).

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

(a) fails to comply with subsections (2) or (3); 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 not exceeding two years or to both such fine and imprisonment.

Issuing of direction requesting foreign mutual assistance

49. (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 Chapter 2 or section 16, 17 or 18 of this Act; or

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

(i) preserve data or other articles;

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

(iii) disclose traffic data on an expedited basis;

(iv) obtain data which is real-time communication-related information or archived communication-related information; or

(v) intercept data which is an indirect communication,

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 this Act has been committed in the Republic or that it is necessary to determine whether 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 **[an]** **other** article is to be seized on an expedited basis and be preserved;

(iii) traffic data, in so far as it may indicate that a person, electronic communications service provider or financial institution in a foreign State was involved in the transmission of the communication, specified in the direction, be disclosed on an expedited basis;

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

(v) data specified in the direction, which is an indirect communication, 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 which is requested to provide assistance and cooperation; or

(b) a designated point of contact in the foreign State which is requested to provide assistance and cooperation.

CHAPTER 7

24/7 POINT OF CONTACT[116]

Establishment and functions of 24/7 Point of Contact[117]

50. (1) The Cabinet member responsible for policing must—

(a) establish an office to be known as the 24/7 Point of Contact for the Republic; and

(b) equip, operate and maintain the 24/7 Point of Contact.

(2) The Cabinet member responsible for policing exercises final responsibility over the administration and functioning of the 24/7 Point of Contact.

---

[116] Summary of Comments and Responses Part A: Pages 185 to 186.

[117] The NPA asked the question why it is necessary to specifically legislate for a 24/7 point of contact. According to them they are under an obligation in terms of section 17F(4) of the South African Police Services Act, 1995, to assist the South African Police Service. According to the Department section 17F(4) relates to the functions of the Directorate for Priority Crime Investigation, only and not offences that fall outside the mandate of the Directorate. The need to establish a 24/7 Point of Contact by means of legislation is necessary to specifically spell out the functions of the relevant Departments, to ensure that there is a specific obligation on the Minister of Police to establish the point of contact and to ensure that the Minister is accountable to Parliament for the establishment of, staffing of and the functioning of the 24/7 Point of Contact. Similar to section 17F(4) of the South African Police Services Act, 1995, clause 50 aims to ensure that the NPA do render legal assistance in respect of cybercrime matters irrespective of the fact that it does not necessary fall within the ambit of section 17F(4) of the South African Police Service Act, 1995. It is correct that only a few countries have legislated for a 24/7 point of contact, all developed countries have points of contact to ensure international cooperation.

(3) *(a)* The 24/7 Point of Contact must operate on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate expedited assistance for the purpose of proceedings or investigations regarding the commission or intended commission of—

(i) an offence under Chapter 2 or section 16, 17 or 18 of this Act;

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

(iii) an offence—

(*aa*) similar to those contemplated in Chapter 2 or section 16, 17 or 18 of this Act; or

(*bb*) any other offence substantially similar to an offence recognised in the Republic which is or was committed by means of, or facilitated by 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 5 and 6 of this Act;

(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 24/7 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 **[(Act No. 39 of 1994)]**, to the satisfaction of the National Director of Public Prosecutions,

to provide legal assistance to the 24/7 Point of Contact as may be necessary or expedient for the effective operation of the 24/7 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 Control Act, 1994, on the functions and activities of the 24/7 Point of Contact.

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

(i) the number of matters in which technical advice and assistance were provided to a foreign State; and

(ii) the number of matters in which technical advice and assistance were received from a foreign State.

CHAPTER 8

EVIDENCE[118]

Proof of certain facts by affidavit

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

(a) the interpretation of data;

(b) the design of, 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 solemn or attested declaration** made by a person who, in that affidavit, states that he or she—

[118] Summary of Comments and Responses Part A: Page 186 to 189.

(i) is 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) possesses relevant qualifications, expertise and experience which make him or her competent to make the affidavit; and

(iii) has established such fact by means of an examination or process **that is fully documented in the affidavit**[119],

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

(2) Any person who makes an affidavit **or 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 not exceeding 2 years.

(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.

---

[119] Summary of Comments and Responses Part A: Page 188, paragraph 9.2(c).

(5) *(a)* For the purposes of subsection (1), a document purporting to be an affidavit **or solemn or attested declaration** made by a person who in that affidavit alleges that he or she is 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—

(i) it is 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) it is 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 **[(Act No. 16 of 1963)]**[120].

(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 solemn or attested declaration** contemplated in paragraph *(a)* is placed may, in order to clarify any obscurities in the said affidavit and at the request of a party to the proceedings, order that a supplementary affidavit **or 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

---

[120] Definition of this Act inserted in clause 1.

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 9

OBLIGATIONS OF ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS AND FINANCIAL INSTITUTIONS[121]

Obligations of electronic communications service providers and financial institutions

52. (1) An electronic communications service provider or financial institution that is aware or becomes aware that its computer system is involved in the commission of any category or class of offences provided for in Chapter 2 of this Act 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 law enforcement agencies 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

[121] Summary of Comments and Responses Part A: Pages 189 to 200.

(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 **[of]** **not exceeding** R50 000.[122]

(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 Chapter 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.

CHAPTER 10[123]

STRUCTURES TO DEAL WITH CYBERSECURITY

Cyber Response Committee[124]

[122] Summary of Comments and Responses Part A: Page 190 paragraph 10.3.

[123] Summary of Comments and Responses Part B: Pages 1 to 13.

[124] Summary of Comments and Responses Part B: Pages 5 to 9.

53. (1) The Cyber Response Committee is hereby established.

(2) The Cyber Response Committee consists of—

(a) a chairperson who is the Director-General: State Security;

(b) members who are the Heads of the representative Departments and one of their nominees who must be officials—

(i) at the rank of at least a chief director or equivalent, of a representative Department, who are specifically nominated by a Head of that representative Department to serve on the Cyber Response Committee; and

(ii) to whom a security clearance certificate has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 **[(Act No. 39 of 1994)]**[125].

(3) The Cabinet member responsible for State security must appoint a member to act as chairperson whenever the chairperson is absent from the Republic or from duty, or for any reason is temporarily unable to carry out the responsibilities as chairperson.

(4) The work incidental to the performance of the functions of the Cyber Response Committee must be performed by a secretariat, consisting of designated administrative personnel of the State Security Agency.

(5) The objects and functions of the Cyber Response Committee are to implement Government policy relating to cybersecurity.

---

[125] The Act is now defined in clause 1.

(6) The Cabinet member responsible for State security must oversee and exercise control over the performance of the functions of the Cyber Response Committee.

(7) The Cabinet member responsible for State security 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 Control Act, 1994, regarding progress that has been made towards achieving the objects and functions of the Cyber Response Committee.

(8) For purposes of this section—

(a) "**Head of a Department**" means the incumbent of a post mentioned in Column 2 of Schedule 1, 2 or 3 to the Public Service Act, 1994, and includes any employee acting in such post; and

(b) "**representative Department**" means—

(i) the Department of Defence;

(ii) the Department of Home Affairs;

(iii) the Department of International Relations and Cooperation;

(iv) the Department of Justice and Constitutional Development;

(v) the Department of Science and Technology;

(vi) the Department of Telecommunications and Postal Services;

(vii) the Financial Intelligence Centre, established by section 2 of the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001);

(viii) the National Prosecuting Authority;

(ix) the National Treasury;

(x) the South African Police Service;

(xi) the South African Reserve Bank;

(xii) the South African Revenue Service;

(xiii) the State Security Agency; and

(xiv) any **[other Department, or public entity]—**

(*aa*) department of State or administration in the national, provincial or local sphere of government;

(*bb*) any other functionary or institution exercising a public power or performing a public function in terms of any legislation; and

(*cc*) any person or entity,[126]

which is requested, in writing, by the Chairperson of the Cyber Response Committee to assist the Committee.

Government structures supporting cybersecurity

54. (1) *(a)* The Cabinet member responsible for State security must—

(i) establish, equip, operate and maintain a computer security incident response team for Government;

(ii) establish and maintain sufficient human and operational capacity to—

[126] This insertion aims to address the concerns that the CRC is a closed structure that do not allow for participation of other entities or persons when decisions are made that may impact on the rights of private persons or the functions of other functionaries in the the national, provincial or local sphere of government.

(*aa*) give effect to cybersecurity measures falling within the Constitutional mandate of the State Security Agency; and

(*bb*) effectively deal with critical information infrastructure protection; and

(iii) in co-operation with any institution of higher learning, in the Republic or elsewhere, develop and implement accredited training programs for members of the State Security Agency in order to give effect to subparagraphs (i) and (ii).

(b) The Cabinet Member responsible for State security may make regulations to further regulate any aspect referred to in paragraph *(a)*.

(c) The Cabinet member responsible for State security 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 Control Act, 1994, on the progress made with the implementation of this subsection.

(2) *(a)* The Cabinet member responsible for policing must—

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

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

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

(b) The Cabinet Member responsible for policing may make regulations to further regulate any aspect referred to in paragraph *(a)*.

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

(i) progress made with the implementation of this subsection;

(ii) the number of—

(*aa*) offences provided for in Chapter 2 or sections 16, 17 or 18, which were reported to the South African Police Services;

(*bb*) cases which were, in terms of item (*aa*), reported to the South African Police Service which resulted in criminal prosecutions; and

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

(iii) the number of members of the South African Police Service who received training as contemplated in paragraph *(a)*(iii).

(3) *(a)* The Cabinet member responsible for defence must[127]—

(i) establish and maintain a cyber offensive and defensive capacity as part of the defence mandate of the South African National Defence Force; and

(ii) in co-operation with any institution of higher learning, in the Republic or elsewhere, develop and implement accredited training programs for members of the South African National Defence Force in order to give effect to subparagraph (i).

(b) The Cabinet Member responsible for defence may make regulations to regulate any aspect which is necessary or expedient for the proper implementation of this subsection.

(c) The Cabinet member responsible for defence must, at the end of each financial year, submit a report to the Chairperson of the Joint Standing Committee on Defence of Parliament on the progress made with the implementation of this subsection.

---

[127] The SANDF requested that a clause that deals with the establishment of the Cyber Command be reconsidered for possible insertion in the Bill (the clause is attached as Annexure A). The SANDF is of the opinion that the clause is necessary in that it defines the role of the SANDF in relation to cyber-related matters and provide guidance what the SANDF should implement to give effect to their mandate.

(4) *(a)* The Cabinet member responsible for telecommunications and postal services must—

(i) establish a**nd**[128] maintain a Cybersecurity Hub as part of the Department of Telecommunications and Postal Services to—

(*aa*) promote cybersecurity in the private sector;

(*bb*) act as a central point of contact between Government and the private sector on cybersecurity;

(cc) encourage and facilitate the establishment of nodal points and private sector computer security incident response teams in the private sector; and

(*dd*) respond to cybersecurity incidents;

(ii) equip, operate and maintain the Cybersecurity Hub; and

(iii) in co-operation with any institution of higher learning, in the Republic or elsewhere, develop and implement accredited training programs for members of the Cybersecurity Hub in order to give effect to item (i).

(b) The Cabinet member responsible for telecommunications and postal services exercises final responsibility over the administration and functioning of the Cybersecurity Hub.

(c) The Cabinet Member responsible for telecommunications and postal services may make regulations to regulate any aspect which is necessary or expedient for the proper implementation of this subsection.

---

[128] Correction of an error.

(d) The Cabinet member responsible for telecommunications and postal services must, at the end of each financial year, submit a report to Parliament regarding progress that has been made towards achieving the objects and functions of the Cybersecurity Hub contemplated in paragraph *(a)*.

Nodal points and private sector computer security incident response teams[129]

55. (1) *(a)* The Cabinet member responsible for telecommunications and postal services must, by notice in the *Gazette*, after following a consultation process with the persons or entities in a sector, declare different sectors which provide an electronic communications service for which a nodal point must be established.

(b) The declaration of different sectors referred to in paragraph *(a)* must be done—

(i) **if the said Cabinet member is not responsible for the administration of that sector,** in consultation with the Cabinet member responsible for the administration of that sector**; and**

(ii) **after consultation with any regulatory body, established in terms of any**[130] **law, which exercises regulatory control over the entities of that sector**.

(2) Each sector must, within six months from the date of the publication of a notice referred to in subsection (1)*(a)* identify and establish a nodal point, which will be responsible for—

---

[129] Summary of Comments and Responses Part B: Pages 9 to 11.

[130] This is to ensure that all functionaries responsible for a sector are consulted.

(a) distributing information regarding cyber incidents to other entities within the sector;

(b) receiving and distributing information about cybersecurity incidents to the nodal points established for other sectors or any computer security incident response team recognised in terms of subsection (6);

(c) reporting cybersecurity incidents to the Cybersecurity Hub contemplated in section 54(4); and

(d) receiving information about cybersecurity incidents from the Cybersecurity Hub.

(3) If a sector fails to identify or establish a nodal point contemplated in subsection (2), the Cabinet member responsible for telecommunications and postal services may**[,]—**

(a) if the said Cabinet member is not responsible for the administration of that sector, in consultation with the Cabinet member responsible for the administration of that sector; and

(b) after consultation with the sector **and any regulatory body, established in terms of any law, which exercises regulatory control over the entities of that sector,**

identify **[and] or** establish a nodal point for that sector on such terms and conditions as he or she deems fit to give effect to the objects of this section.

(4) A particular sector is responsible for the establishment and operating costs of a nodal point established in terms of subsection (2) or (3).

(5) *(a)* The Cabinet member responsible for telecommunications and postal services may make regulations—

(i) **if the said Cabinet member is not responsible for the administration of that sector, in consultation with the Cabinet member responsible for the administration of that sector; and**

(ii) after consultation with the sector **and any regulatory body, established in terms of any law, which exercises regulatory control over the entities of that sector**—

[(i)](*aa*) to further regulate contributions to be made by entities in a sector to fund a nodal point established for a particular sector in terms of subsection (2) or (3); and

[(ii)](*bb*) to further regulate any aspect relating to the establishment, operation or functioning of a nodal point which is established for a sector.

(b) The regulations contemplated in paragraph *(a)* may provide that any person or entity who contravenes or fails to comply with a regulation is guilty of an offence and is liable on conviction to a fine or to imprisonment not exceeding one year or to both such fine and imprisonment.

(6) *(a)* The Cabinet member responsible for telecommunications and postal services may, by notice in the *Gazette*, recognise any computer security incident response team which is established for a sector.

(b) The Cabinet member responsible for telecommunications and postal services may—

(i) after consultation with any computer security incident response team which is established for a sector and the entities of that sector; and

(ii) in consultation with the Cabinet member responsible for the administration of the sector **and any regulatory body, established in terms of any law, which exercises regulatory control over the entities of that sector** for which a computer security incident response team has been recognised in terms of paragraph *(a)*,

make regulations to further facilitate the effective functioning of such a computer security incident response team.

(c) The regulations contemplated in paragraph *(b)* may provide that any person or entity who contravenes or fails to comply with a regulation is guilty of an offence and is liable on conviction to a fine or to imprisonment not exceeding one year or to both such fine and imprisonment.

Information sharing[131]

56. Subject to any other law, the Cabinet member responsible for the administration of justice must make regulations to regulate information sharing, for purposes of this Chapter, regarding—

(a) cybersecurity incidents; and

(b) the detection, prevention, investigation or mitigation of cybercrime.

[131] Summary of Comments and Responses Part B: Pages 11 to 13.

CHAPTER 11

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION[132]

Protection of critical information infrastructure[133]

57. (1) The State Security Agency—

(a) in consultation with the Cyber Response Committee; and

(b) after consultation with the owner of, or the person in control of any information infrastructure which is identified as a potential critical information infrastructure,

must within 12 months of the fixed date, submit to the Cabinet member responsible for State security, information and recommendations regarding information infrastructures which need to be declared as critical information infrastructures.

(2) The Cabinet member responsible for State security may, subject to subsection (3), after considering any information and recommendations made to him or her in terms of subsection (1), by notice in the *Gazette*, declare any information infrastructure, or category or class of information infrastructures or any part thereof, as critical information infrastructures if such information infrastructure or information infrastructures are of such a strategic nature that any interference with them or their loss, damage, disruption or immobilisation may—

(a) substantially prejudice the security, the defence, law enforcement or international relations of the Republic;

(b) substantially prejudice the health or safety of the public;

---

[132] Summary of Comments and Responses Part B: Pages 13 to 43
[133] Summary of Comments and Responses Part B: Pages 20 to 37

(c) cause a major interference with or disruption of, an essential service;

(d) cause any major economic loss;

(e) cause destabilisation of the economy of the Republic; or

(f) create a major public emergency situation.

(3) Before the Cabinet member responsible for State security declares an information infrastructure a critical information infrastructure as contemplated in subsection (2), he or she must—

(a) with the exception of the State Security Agency, as referred to in section 3(1) of the Intelligence Services Act, 2002, where the information infrastructure, or any part thereof, belongs to, or is under the control of, a Department of State, consult with the Cabinet member responsible for that Department;

(b) where the information infrastructure, or any part thereof—

(i) is under the functional control or administration of a Provincial Government; or

(ii) relates to, or is incidental to—

(*aa*) a functional area listed in Schedule 4 or 5 of the Constitution;

(*bb*) any matter outside the functional areas listed in Schedule 4 or 5 of the Constitution that is expressly assigned to the province by national legislation; or

(*cc*) any matter for which a provision of the Constitution envisages the enactment of provincial legislation,

consult with**, and obtain the concurrence of** the Premier[134] of the province concerned;

(c) where the information infrastructure, or any part thereof—

(i) is under the functional control or administration of a municipality; or

(ii) relates to, or is incidental to—

(*aa*) any matter listed in Part B of Schedule 4 and Part B of Schedule 5 of the Constitution; or

(*bb*) any matter outside the functional areas listed in Part B of Schedule 4 or 5 of the Constitution and that is expressly assigned by national or provincial legislation to a Municipal Council,

consult with the municipal manager of the municipality concerned;

(d) where the information infrastructure, or any part thereof, belongs to a constitutional institution contemplated in Schedule I to the Public Finance Management Act, 1999, or the Public Service Commission, consult with the chief executive officer of the institution concerned;

(e) where the information infrastructure, or any part thereof, belongs to a public entity contemplated in Schedule 2 or Parts A and B of Schedule 3 to the Public Finance Management Act, 1999, consult with the Cabinet member responsible for the administration of the national public entity and the chief executive officer of the national public entity;

(f) where the information infrastructure, or any part thereof, belongs to a financial sector regulator, consult with—

---

[134] Summary of Comments and Responses Part B: Page 27 paragraph 12.2.10.

(i) the Cabinet member responsible for finance; and

(ii) the financial sector regulator concerned;

(*g*) where the information infrastructure, or any part thereof, belongs to, or is under the control of, the South African Reserve Bank or is a payment system institution, consult with the Cabinet member responsible for finance and the Governor of the South African Reserve Bank;

(h) where the information infrastructure, or any part thereof, belongs to, or is under the control of a financial institution, consult with each applicable financial sector regulator and—

(i) consult with that financial institution;

(ii) afford the financial institution the opportunity to make written representations on any aspect relating to the Cabinet member's intention to declare the information structure, as a Critical Information Infrastructure;

(iii) consider the representations of the financial institution; and

(iv) give a written decision to the financial institution and each applicable financial sector regulator; or

(*i*) where the information infrastructure, or any part thereof, belongs to, or is under the control of, a company, or entity or a person not referred to in paragraphs *(a)* to *(h)*—

(i) consult with the company, entity or person;

(ii) consult with any regulatory body, established in terms of any law, which exercises regulatory control over actions of the company, entity or person;

(iii) afford the company, entity, person and the regulatory body concerned the opportunity to make written representations on any aspect relating to the Cabinet member's intention to declare the information infrastructure as a Critical Information Infrastructure;

(iv) consider the representations of the company, entity, person and regulatory body; and

(v) give a written decision to the company, entity or person and regulatory body concerned.

(4) The Cabinet member responsible for State security must, within six months of the declaration of any information infrastructure, or category or class of information infrastructure or any part thereof, as a critical information infrastructure, in consultation with the relevant Cabinet members, issue directives to the critical information infrastructure in order to regulate minimum standards relating to—

(a) the classification of data held by the critical information infrastructure;

(b) the protection of, the storing of, and archiving of data held by the critical information infrastructure;

(c) cybersecurity incident management by the critical information infrastructure;

(d) disaster contingency and recovery measures which must be put in place by the critical information infrastructure;

(e) minimum physical and technical security measures that must be implemented in order to protect the critical information infrastructure;

(f) the period within which the owner of, or person in control of a critical information infrastructure must comply with the directives; and

(*g*) any other relevant matter which is necessary or expedient in order to promote cybersecurity in respect of the critical information infrastructure.

(5) A directive or any amendment to a directive referred to in subsection (4) must be issued in consultation with the relevant Cabinet members, and if it is a critical information infrastructure referred to in—

(a) subsection (3)*(a)*, *(b)* or *(c)*, in consultation with the Cabinet member responsible for that Department or the Premier of the province concerned or the municipal manager of the municipality concerned;

(b) subsection 3*(d)*, in consultation with the chief executive officer of the institution concerned;

(c) subsection 3*(e)*, in consultation with the Cabinet member responsible for the administration of the national public entity and the chief executive officer of the national public entity;

(d) subsection (3)*(f)*, in consultation with the Cabinet member responsible for finance and the financial sector regulators concerned;

(e) subsection 3(*g*), in consultation with the Cabinet member responsible for finance and the Governor of the South African Reserve Bank;

(f) subsection 3*(h)*—

(i) in consultation with the financial sector regulator concerned; and

(ii) after consultation with the financial institution; or

(*g*) subsection 3(*i*)—

(i) in consultation with any applicable regulatory body concerned; and

(ii) after consultation with the company, entity or person.

(6) Any information infrastructure declared a critical information infrastructure must, within the period stipulated in the directives, comply with the directives issued in terms of subsection (4).

(7) *(a)* A financial institution **or a financial sector regulator**[135] contemplated in subsection (3)*(h)*, or company, entity or person contemplated in subsection (3)(*i*), may dispute**—**

(i) the decision of the Cabinet member responsible for State security**[—**

(i)]in terms of subsection (3)*(h)*(iv), or (*i*)(v); or

(ii) any aspect relating to the directives referred to in subsection (4) **or any subsequent amendment of the directive**[136].

(b) A dispute in terms of—

(i) paragraph *(a)*(i) must be lodged within 30 days from the date on which the decision in terms of subsection (3)*(h)*(iv) or (*i*)(v) is made known by the Cabinet member; or

(ii) paragraph *(a)*(ii) must be lodged before the end of the period within which the owner of, or person in control of a critical information infrastructure must comply with the directives as contemplated in subsection (4)*(f)*,

and set out the grounds for the dispute.

(c) The Cabinet member responsible for State security or his or her representative must take appropriate steps to settle the dispute by consensus within 30 days from lodging the dispute referred to in paragraph *(b)*.

---

[135] Summary of Comments and Responses Part B: Page 33 paragraph 12.2.17.

[136] Summary of Comments and Responses Part B: Page 28 paragraph 12.2.13.

(d) The Cabinet member responsible for State security, in consultation with the Cabinet member responsible for the administration of justice, must make regulations to provide for—

(i) the form and manner in which a dispute must be lodged in terms of paragraph *(b)*; and

(ii) matters necessary or incidental to the process for settlement of disputes as contemplated in paragraph *(c)*.

(e) If the dispute is not settled within 30 days, as contemplated in paragraph *(c)*, the dispute must be referred for arbitration, at the request of the Cabinet member responsible for State security, by a recognised body concerned with the facilitation and promotion of the resolution of disputes by means of mediation or arbitration to be agreed on between the financial institution, financial sector regulator, company, entity, person or regulating body concerned and the Cabinet member responsible for State security.

(f) An arbitrator referred to in paragraph *(e)* must be a person appointed on account of his or her knowledge of—

(i) the law;

(ii) cybersecurity;

(iii) protection of critical information infrastructures; and

(iv) the activities of the financial institution, company, entity or person concerned.

(*g*) The provisions of the Arbitration Act, 1965 (Act No. 42 of 1965), apply, with the changes required by the context, to an arbitration contemplated in paragraph *(e)*.

(h) The unsuccessful party in the arbitration proceedings is responsible for the costs of the arbitration proceedings.

(*i*) The Cabinet member responsible for State security**[, company, entity or person] or a financial institution or a financial sector regulator contemplated in subsection (3)(*h*), or company, entity or person contemplated in subsection (3)(i)**,[137] may appeal the decision of the arbitrator to the High Court.

(*j*) An appeal in terms of paragraph (*i*) must—

(i) be lodged within 180 days from the date on which the arbitration award is made or such later date as the High Court permits;

(ii) set out the grounds for the appeal; and

(iii) be proceeded with as if it were an appeal from a magistrate's court to the High Court.

(8) The owner of, or person in control of a critical information infrastructure must in consultation with the Cabinet member responsible for State security, at own cost, take steps to the satisfaction of the Cabinet member for purposes of complying with the directives contemplated in subsection (4).

(9) If the owner of, or person in control of a critical information infrastructure fails to take the steps referred to in subsection (8), the Cabinet member responsible for State security may, by written notice, order him or her to take such steps in respect of the critical information infrastructure as may be specified in the notice, within the period specified in the notice.

---

[137] [137] Summary of Comments and Responses Part B: Page 34 paragraph 12.2.19.

(10) An owner of, or person in control of the critical information infrastructure who without reasonable cause refuses or fails to take the steps specified in the notice **referred to in subsection (9),** within the period specified therein, 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 such imprisonment.

(11) **(*a*)** If the owner of, or person in control of, the critical information infrastructure fails or refuses to take the steps specified in the notice **referred to in subsection (9),** within the period specified therein, the Cabinet member responsible for State security may take or cause to be taken those steps which the owner or person failed or refused to take, irrespective of whether the owner or person has been charged or convicted in connection with that failure or refusal, and the Cabinet member may recover the costs of those steps from the owner or person on whose behalf they were taken.

(*b*) A failure by a provincial government to take the steps specified in the notice referred to in subsection (9), within the period specified therein, must be dealt with in accordance with section 100 of the Constitution.[138]

(12) For purposes of this section—

(a) "**classification of data**", for purposes of subsection (4)*(a)*, means to assign a level of sensitivity, value and criticality to the data for purposes of security controls for the protection of the data;

(b) "**day**" means a calendar day, and must be calculated by excluding the first and including the last day, unless the last day falls on a Saturday, a Sunday or any

[138] Summary of Comments and Responses Part B: Pages 27 to 28 paragraph 12.2.11.

public holiday, in which case the number of days shall be calculated by excluding the first day and also any such Saturday, Sunday or public holiday: Provided that the days between 16 December of a year and 5 January of the following year, both inclusive, shall not be taken into account in determining days;

(c) "**fixed date**" means the date fixed by the State President by proclamation in the *Gazette* as contemplated in section 63 on advice of the Cabinet member responsible for State security;

(d) "**information infrastructure**" means any data, computer program, computer data storage medium, computer system or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto; and

(e) "**relevant Cabinet members**" means the Cabinet members responsible for defence, telecommunications and postal services, the administration of justice, policing and State security.

Auditing of critical information infrastructures to ensure compliance[139]

58. (1) The owner of, or person in control of, a critical information infrastructure must, once every 24 months, at own cost, cause an audit to be performed on the critical information infrastructure by an independent auditor in order to evaluate compliance with the directives issued in terms of section 57(4).

[139] Summary of Comments and Responses Part B: Pages 38 to 42.

(2) Before an audit referred to in subsection (1) is performed on a critical information infrastructure, the owner of, or person in control of, a critical information infrastructure must, at least 30 days in advance of the date of the audit, notify the Director-General: State Security, in writing of—

(a) the date on which an audit is to be performed; and

(b) the particulars and contact details of the person who is responsible for the overall management and control of the audit.

(3) The Director-General: State Security may designate any member of the State Security Agency or any other person to monitor, evaluate and report on the adequacy and effectiveness of any audit referred to in subsection (1).

(4) The owner of, or person in control of a critical information infrastructure must, within 40 days after an audit referred to in subsection (1) has been completed, report in the prescribed form and manner to the Director-General: State Security regarding the outcome of the audit referred to in subsection (1).

(5) The Director-General: State Security may request the owner of, or person in control of, a critical information infrastructure to provide such additional information as may be necessary within a specified period, in order to evaluate the report referred to in subsection (4).

(6) If the owner of, or person in control of a critical information infrastructure—

(a) fails to cause an audit to be performed on a critical information infrastructure as contemplated in subsection (1) in order to evaluate compliance with the directives issued in terms of section 57(4);

(b) fails to give a report referred to in subsection (4) to the satisfaction of the Director-General: State Security;

(c) fails to provide such additional information as may be necessary within a specified period, in order to evaluate the report after he or she has been requested to do so in terms of subsection (5), to the satisfaction of the Director-General: State Security; or

(d) requests the Director-General: State Security to perform an audit referred to in subsection (1),

the Director-General: State Security must, subject to subsections (3) and (7), cause an audit to be performed on the critical information infrastructure by an independent auditor in order to evaluate compliance with the provisions of section 57(4).

(7) Before an audit is performed in terms of subsection (6)*(a)*, *(b)* or *(c)*, the Director-General: State Security must, in respect of a critical information infrastructure referred to in—

(i) section 57(3)*(f)*, consult with the Director-General: National Treasury and the financial sector regulator concerned;

(ii) section 57(3)(*g*), consult with the Cabinet member responsible for finance and the Governor of the South African Reserve Bank; or

(iii) section 57(3)*(h)*, consult each relevant financial sector regulator.

(8) No person may perform an audit on a critical information infrastructure pursuant to the provisions of subsection (6) unless he or she—

(a) has been authorised in writing by the Director-General: State Security to perform such audit;

(b) is in possession of a certificate of appointment, in the prescribed form, issued by the Director-General: State Security, which certificate must be submitted to the owner of, or person in control of a critical information infrastructure at the commencement of the audit; and

(c) is accompanied by a person in control of the critical information infrastructure or a person designated by such a person.

(9) The person contemplated in subsection (8)*(c)* and any other employee of the critical information infrastructure must assist and provide technical assistance and support to any person who is authorised, in terms of subsection (8)*(a)*, to carry out an audit.

(10) The critical information infrastructure which is audited pursuant to the provisions of subsection (6) is responsible for the cost of the audit.

(11) The owner of, or person in control of, a critical information infrastructure who—

(a) fails to cause an audit to be performed on a critical information infrastructure, as contemplated in subsection (1), in order to evaluate compliance with the provisions of section 57(4);

(b) fails to notify the Director-General: State Security, in writing of an audit to be performed as contemplated in subsection (2);

(c) fails to—

(i) report on the outcome of the audit within 40 days as contemplated in subsection (4); or

(ii) fails to provide, within the specified time period the additional information requested by the Director-General: State Security as contemplated in subsection (5); or

(d) furnishes—

(i) a report referred to in subsection (4); or

(ii) any additional information referred to in subsection (5),

to the Director-General: State Security which he or she knows to be false or which he or she does not know or believe to be true,

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 such imprisonment.

(12) Any person who—

(a) hinders, obstructs or improperly attempts to influence any member of the State Security Agency, person or entity to monitor, evaluate and report on the adequacy and effectiveness of an audit as contemplated in subsection (3);

(b) hinders, obstructs or improperly attempts to influence any person authorised to carry out an audit in the exercise of his or her powers or the performance of his or her functions or duties;

(c) fails to accompany any person authorised to carry out an audit as contemplated in subsection (8)*(c)*; or

(d) fails to assist or provide technical assistance and support to a person authorised to carry out an audit as contemplated in subsection (9),

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 such imprisonment.

(13) The Cabinet member responsible for State security must, by notice in the *Gazette*, prescribe the persons or the category or class of persons who are competent to be appointed to perform an audit as contemplated in this section.

CHAPTER 12

AGREEMENTS WITH FOREIGN STATES

National Executive may enter into agreements[140]

59. (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 Chapter 2 or section 16, 17 or 18 of this Act;

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

(iii) an offence—

(*aa*) similar to those contemplated in Chapter 2 or section 16, 17 or 18 of this Act; or

(*bb*) any other offence substantially similar to an offence recognised in the Republic which is or was committed by means of, or facilitated by the use of, an article,

in that foreign State;

(b) the implementation of cyber threat response activities;

(c) research, information and technology-sharing and the development and exchange of information on cybersecurity-related matters;

---

[140] Summary of Comments and Responses Part B: Pages 42 to 43.

(d) the establishment of 24/7 contact points;

(e) the implementation of emergency cross-border response mechanisms to address cyber threats;

(*f*) the reciprocal implementation of measures to curb cybercrime; and

(g) the establishment of emergency centres to deal with cyber-related threats.

(2) A member of the National Executive must, as soon as practical after Parliament has agreed to the ratification of, accession to or amendment or revocation of an agreement referred to in subsection (1), give notice thereof in the *Gazette*.

CHAPTER 13

GENERAL PROVISIONS

National Director of Public Prosecutions must keep statistics of prosecutions[141]

60. (1) The National Director of Public Prosecutions must keep statistics of the number of prosecutions instituted in terms of Chapter 2 or section 16, 17 or 18 of this Act, the outcome of such prosecution 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—

[141] Summary of Comments and Responses Part B: Pages 43 to 45.

(a) 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; and

(b) on the written request of the Chairperson of the Cyber Response Committee referred to in section 53, be made available to the Chairperson of the Cyber Response Committee.

Repeal or amendment of laws[142]

61. The laws mentioned in the Schedule are hereby repealed or amended to the extent reflected in the third column of the Schedule.

Regulations

62. (1) The Cabinet member responsible for the administration of justice must make regulations—

(a) to prescribe the—

(i) form and manner of the application contemplated in section 19(1);

(ii) form of the order contemplated in section 19(3);

(iii) form and manner of serving the order contemplated in section 19(4);

(iv) form and manner of the application contemplated in section 19(6);

(v) manner in which the court may subpoena a person as contemplated in section 19(8);

[142] Summary of Comments and Responses Part B: Pages 45 to 50.

(vi) form of the direction and affidavit and manner to furnish information to court as contemplated in section 20(1)*(b)*;

(vii) manner of serving a direction as contemplated in section 20(2);

(viii) manner of, and the form of the affidavit to apply for an extension of the time period or cancellation of the direction as contemplated in section 20(3)*(b)*;

(ix) manner for requesting additional information as contemplated in section 20(4)*(b)*;

(x) form and manner of informing an electronic communications service provider or person of the outcome of application as contemplated in section 20(4)*(d)*;

(xi) tariffs of compensation payable to an electronic communications service provider as contemplated in section 20(6);

(xii) form of the order and manner of service of the order as contemplated in section 21(3);

(xiii) the form of the expedited preservation of data direction and manner of service as contemplated in section 39(3);

(xiv) form and manner for the making of an application contemplated in section 39(7);

(xv) form of the preservation of evidence direction and manner of service contemplated in in section 40(2);

(xvi) form and manner for an application to set aside a preservation of evidence direction as contemplated in section 40(5);

(xvii) form of the disclosure of data direction and manner of service as contemplated in section 42(4);

(xviii) form and manner of an application for the amendment or setting aside of a disclosure of data direction as contemplated in section 42(6);

(xix) form of the affidavit contemplated in section 42(8)*(b)*;

(xx) form of the affidavit contemplated in section 48(2)*(b)*(ii); and

(xxi) form of the direction contemplated in section 49(1); and

(b) to regulate information sharing as contemplated in section 56.

(2) *(a)* The Cabinet member responsible for policing must make regulations in terms of section 52(2), prescribing the—

(i) category or class of offences which must be reported to the South African Police Service in terms of section 52(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 52(2)*(b)*.

(b) The Cabinet member responsible for policing may make regulations to further regulate aspects contemplated in section 50(4) an 54(2).

(3) *(a)* The Cabinet member responsible for State Security must make regulations, prescribing the—

(i) form and manner in which a dispute must be lodged as contemplated in section 57(7)*(d)*;

(ii) form of the report and manner of reporting to the Director-General: State Security as contemplated in section 58(4);

(iii) form of the certificate as contemplated in section 58(8)*(b)*; and

(iv) persons or the category or class of persons who are competent to be appointed to perform an audit as contemplated in section 58(13).

(b) The Cabinet member responsible for State Security may make regulations as contemplated in sections 53(8) and 54(1)*(b)*.

(4) The Cabinet member responsible for defence may make regulations as contemplated in subsection 54(3)*(b)*.

(5) The Cabinet member responsible for telecommunications and postal services may make regulations as contemplated in section 54(4)*(c)* and 55(5).

(6) Any regulation made in terms of subsections (1), (2), (3), (4), (5) or (6), must be submitted to Parliament before publication thereof in the *Gazette*.

Short title and commencement

63. (1) This Act is called the Cybercrimes and Cybersecurity Act, 2017, 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

(Section 61)

LAWS REPEALED OR AMENDED

Number and year of law	Short title	Extent of repeal or amendment
Act No. 51 of 1977	Criminal Procedure Act, 1977	*(a)* The addition of the following subsections to section 334: **(5) (*a*) The Minister may by notice in the *Gazette* declare that any appropriately qualified, fit and proper person or persons who falls within any category defined in the notice, shall, within an area specified in the notice, be a peace officer for the purpose of exercising, with reference to any provision of Chapter 5 of the Cybercrimes and Cybersecurity Act, 2017, the powers defined in the notice.** **(*b*) No person who is a peace officer by virtue of a notice issued under paragraph (*a*) shall exercise any power conferred upon him or her under that paragraph unless he or she is at the time of exercising such power—** **(i) in possession of a certificate of appointment by the National Commissioner of the South African Police Service, appointed by the President in terms of section 207(1) of the Constitution of the Republic of South Africa, 1996, which certificate shall be produced on demand; and** **(ii) (*aa*) was identified and authorised in terms of a search warrant contemplated in section 27(3); or** **(bb) was requested by a police official in terms of section 30(3) or 31(4),** **to, subject to the direction or control of a police official, assist a police official with the search for, access or seizure of an article.** **(c) A power exercised contrary to the provisions of paragraph (*a*) shall have no legal force or effect.** **(*d*) The Minister may by notice in the Gazette prescribe—** **(i) the conditions which shall be complied with before a certificate of appointment may validly be issued under paragraph (*b*)(i);** **(ii) any matter which shall appear in or on such certificate of appointment.**

Number and year of law	Short title	Extent of repeal or amendment
		(e) Where any person who becomes a peace officer under the provisions of this subsection would be liable for damages arising out of any act or omission by such person in the discharge of any power conferred upon him or her under this subsection, the State will be liable for such damages.[143] (b) A power exercised contrary to the provisions of pa *(b)* The addition of the following items to Schedule 5: "A contravention of sections 8, 9 or 10 of the Cybercrimes and Cybersecurity Act, 2017— *(a)* involving amounts of more than R500 000,00; *(b)* involving amounts of more than R100 000,00, if it is proven that the offence was committed— (i) by a person, group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; (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 which was involved in the offence; or (iii) if it is proven that the offence was committed by any law enforcement officer— (*aa*) involving amounts of more than R10 000; or (*bb*) 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 (*cc*) with the collusion or assistance of another person, who as part of

[143] See clause 1 – definition of “investigator”.

Number and year of law	Short title	Extent of repeal or amendment
		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 which was involved in the offence. A contravention of section 11(2) of the Cybercrimes and Cybersecurity Act, 2017.".
Act No. 68 of 1995	South African Police Service Act, 1995	The deletion of section 71.
Act No. 65 of 1996	Films and Publications Act, 1996	**(*a*) The amendment of section 1 by the substitution for the definition of " child pornography" of the following definition:** **"child pornography" means a "child pornography" as defined in section 1 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act No. 32 of 2007).**[144] **(*b*)** The deletion of section**s** 24B, **27A and 30B(1)(*b*).**
Act No. 105 of 1997	Criminal Law Amendment Act, 1997	The addition of the following item to Part II of Schedule 2: of the following Part: "A contravention of sections 8, 9 or 10 of the Cybercrimes and Cybersecurity Act, 2017— *(a)* involving amounts of more than R500 000,00; *(b)* involving amounts of more than R100 000,00, if it is proven that the offence was committed— (i) by a person, group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; (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 which was involved in the offence; or (iii) if it is proven that the offence was

[144] Summary of Comments and Responses Part B: Pages 45 to 50 paragraph 14.2.2.

Number and year of law	Short title	Extent of repeal or amendment
		committed by any law enforcement officer— (*aa*) involving amounts of more than R10 000; or (*bb*) 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 (*cc*) 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 which was involved in the offence. A contravention of section 11(2) of the Cybercrimes and Cybersecurity Act, 2017.".
Act No. 32 of 1998	National Prosecuting Authority Act, 1998	The deletion of sections 40A and 41(4).
Act No. 111 of 1998	Correctional Services Act, 1998	The deletion of section 128.
Act No. 38 of 2001	Financial Intelligence Centre Act, 2001	The deletion of sections 65, 66 and 67.
Act No. 25 of 2002	Electronic Communications and Transactions Act, 2002	*(a)* The amendment of section 1 by the deletion of the definitions of ''critical data'', ''critical database'' and ''critical database administrator''. *(b)* The deletion of Chapter IX. *(c)* The deletion of sections 85, 86, 87, 88 and 90. *(d)* The substitution for section 89 of the following section: ''**Penalties** **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. **[(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 No. 57 of 2002	Disaster Management Act, 2002	The amendment of section 1 by the substitution for paragraph *(a)* of the definition of ''**disaster**'' of the following paragraph: ''*(a)* causes or threatens to cause— (i) death, injury or disease; (ii) damage to property, infrastructure or

Number and year of law	Short title	Extent of repeal or amendment
		the environment; **[or]** (ii*A*) damage to or disruption of critical information infrastructure as contemplated in section 57(2) of the Cybercrimes and Cybersecurity Act, 2017; or (iii) disruption of the life of a community; and".
Act No. 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: "*(a)* offence mentioned in **[the]** Schedule 1; or". ***(b)*** **The amendment of section 4 by the addition of the following subsection:** **"(3) Notwithstanding subsection (2), a law enforcement officer who is authorised in terms of the Criminal Procedure Act, 1977, the Cybercrimes and Cybersecurity Act, 2017 or any other law to engage or to apprehend a suspect or to enter premises in respect of the commission of 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—** **(*a*) the recording relates directly to the purpose for which the suspect was apprehended or the law enforcement officer entered the premises; and** **(*b*) the law enforcement officer has—** **(i) identified himself or herself as such; and** **(ii) verbally informed any person concerned that his or her direct communications are to be recorded before such recording is made.".** *(b)* The substitution for subsection (4) of section 17 of the following subsection: "(4) A real-time communication-related direction may only be issued if it appears to the designated judge concerned, on the facts alleged in the application concerned, that there are reasonable grounds to believe that— *(a)* a serious offence or an offence mentioned in Schedule II has been or is being or will probably be committed; *(b)* the gathering of information concerning an actual threat to the

Number and year of law	Short title	Extent of repeal or amendment
		public health or safety, national security or compelling national economic interests of the Republic is necessary; *(c)* the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary; *(d)* the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime, 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— (i) accordance with an international mutual assistance agreement; or (ii) the interests of the Republic's international relations or obligations; or *(e)* the gathering of information concerning property which is or could probably be an instrumentality of a serious offence, or an offence mentioned in Schedule II or is or could probably be the proceeds of unlawful activities is necessary, and that the provision of real-time communication-related information is necessary for purposes of investigating such offence or gathering such information.". *(c)* The renaming of the Schedule to the Act as "Schedule I" and the addition of the following items: "**15.** Any offence contemplated in sections 17, 18, 19A or 20 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act 32 of 2007). **16.** Any offence contemplated in— *(a)* section 8, 9(1) or (2) or 10 of the Cybercrimes and Cybersecurity Act, 2017, which involves an amount of R200 000, 00 or more; or *(b)* section 11(1) or (2) or 12 (in so far as the section relates to the offences referred to in section 11(1) or (2)) of

Number and year of law	Short title	Extent of repeal or amendment
		that Act.". *(d)* The addition of the following Schedule after Schedule I: "**Schedule II** **1.** Any offence referred to in— *(a)* sections 3(1), 4(2), 5, 6, 7(1), 8, 9(1) or (2), or 10; or *(b)* section 12 (in so far as the section relates to the offences referred to in paragraph *(a)*), of the Cybercrimes and Cybersecurity Act, 20… (Act …… of ….), involving an amount of more that R50 000, 00. **2.** Any offence which is substantially similar to an offence referred to in item 1 which is or was committed in a foreign State.".
Act No. 33 of 2004	Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004	*(a)* The amendment of section 1— (i) by the insertion after the definition of "convention offence" of the following definition: " '**Critical information infrastructure**' means information infrastructure which is declared critical information infrastructure in terms of section 57(2) of the Cybercrimes and Cybersecurity Act, 2017;"; and (ii) by the insertion after item (v) of the definition of "terrorist activity" of the following item: "(v*A*) causes the destruction of or substantial damage or interference to a critical information infrastructure or any part thereof;". *(b)* The substitution for subsection (2) of section 3 of the following subsection: "(2) Any person who— *(a)* provides or offers to provide any— (i) weapon; or (ii) software or hardware tool as defined in section 4(3) of the Cybercrimes and Cybersecurity Act, 2017, to any other person for use by or for the benefit of an entity; *(b)* solicits support for or gives support to an entity; *(c)* provides, receives or participates in training or instruction, or recruits an entity to receive training or instruction; *(d)* recruits any entity; *(e)* collects or makes a document; or

Number and year of law	Short title	Extent of repeal or amendment
		(f) possesses a thing, connected with the engagement in a terrorist activity, and who knows or ought reasonably to have known or suspected that such weapons, <u>software or hardware tool,</u> soliciting, training, recruitment, document or thing is so connected, is guilty of an offence connected with terrorist activities.''.
Act No. 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 by— (i) the substitution for the heading to Part 3 of Chapter 2 of the following heading: ''*Persons 18 years or older: Compelling or causing persons 18 years or older to witness sexual offences, sexual acts or self-masturbation, exposure or display of or causing exposure or display of genital organs, anus or female breasts (''flashing''), child pornography to persons 18 years or older<u>, harmful disclosure of pornography</u> or engaging sexual services of persons 18 years or older'';* (ii) the insertion after item 10 of the following item: ''**<u>10A.</u>** <u>Harmful disclosure of pornography</u>''; (iii) the substitution for the heading to Part 2 of Chapter 3 of the following heading: ''*Sexual exploitation and sexual grooming of children, exposure or display of or causing exposure or display of child pornography or pornography to children, <u>child pornography</u> and using children for pornographic purposes or benefiting from child pornography*''; and (iv) the insertion after item 19 of the following item: ''**<u>19A.</u>** <u>Offences relating to child pornography</u>''. *(b)* The amendment of section 1— (i) by the substitution for the definition of ''child pornography'' of the following definition: ''**child pornography**'' means any image, however created, or any description or presentation of a person, real or simulated, who is, or who is <u>realistically</u> depicted or described or presented as being, under the age of 18 years, of an explicit or sexual nature, whether

Number and year of law	Short title	Extent of repeal or amendment
		such image or description or presentation is intended to stimulate erotic or aesthetic feelings or not, including any such image, presentation or description of such person— *(a)* engaged in an act that constitutes a sexual offence; *(b)* engaged in an act of sexual penetration; *(c)* engaged in an act of sexual violation; *(d)* engaged in an act of self-masturbation; *(e)* displaying the genital organs of such person in a state of arousal or stimulation; *(f)* unduly displaying the genital organs or anus of such person; (*g*) displaying any form of stimulation of a sexual nature of such person's breasts; *(h)* engaged in sexually suggestive or lewd acts; (*i*) engaged in or as the subject of sadistic or masochistic acts of a sexual nature; (*j*) engaged in any conduct or activity characteristically associated with sexual intercourse; (*k*) showing or describing such person— (i) participating in, or assisting or facilitating another person to participate in; or (ii) being in the presence of another person who commits or in any other manner being involved in, any act contemplated in paragraphs *(a)* to (j); or (*l*) showing or describing the body, or parts of the body, of such person in a manner or in circumstances which, within the context, violate or offend the sexual integrity or dignity of that person or any category of persons under 18 or is capable of being used for the

Number and year of law	Short title	Extent of repeal or amendment
		purposes of violating or offending the sexual integrity or dignity of that person, any person or group or categories of persons;"; and (ii) by the insertion after the definition of "Director of Public Prosecutions" of the following definition: **"electronic communications service provider" [means an entity or a person who is licensed or exempted from being licensed in terms of Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), to provide an electronic communications service;] means any person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act, 2005**[145]". *(c)* Chapter 2 is hereby amended by— (i) the substitution for the heading to Part 3 of Chapter 2 of the following heading: "***Persons 18 years or older: Compelling or causing persons 18 years or older to witness sexual offences, sexual acts or self-masturbation, exposure or display of or causing exposure or display of genital organs, anus or female breasts ("flashing"), child pornography to persons 18 years or older, harmful disclosure of pornography or engaging sexual services of persons 18 years or older***"; and (ii) by the insertion for the following section after section 10: "**Harmful disclosure of pornography**

[145] Summary of Comments and Responses Part B: Pages 45 paragraph 14.2.1

Number and year of law	Short title	Extent of repeal or amendment
		10A. (1) A person ("A") who unlawfully and intentionally discloses or causes the disclosure of pornography in which a person 18 years or older ("B") appears or is described and such disclosure— *(a)* takes place without the consent of B; and *(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, is guilty of the offence of harmful disclosure of pornography. (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. (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. (4) *(a)* Any person who lays a charge with the South African Police Service that an offence contemplated in subsections (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 an order— (i) to prohibit any person to disclose or cause the disclosure of pornography

Number and year of law	Short title	Extent of repeal or amendment
		as contemplated in subsections (1), (2) or (3); or (ii) ordering an electronic communications service provider or person in control of a computer system to remove or disable access to the pornography in question. *(b)* The court must as soon as is reasonably possible consider an application submitted to it in terms of paragraph *(a)* 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 proceedings. *(c)* The court may, for purposes of paragraph *(b)*, 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. *(d)* If the court is satisfied that there is *prima facie* evidence that the pornography in question constitutes an offence as contemplated in subsection (1), (2) or (3), the court may issue the order referred to in paragraph *(a)*, in the prescribed form. *(e)* The order must be served on the person referred to in paragraph *(a)*(i) or electronic communications service provider or person referred to in paragraph *(a)*(ii), in the prescribed form and manner: Provided, that if the 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 manner specified in that order. *(f)* An order referred to in paragraph *(d)* is of force and effect from the time it is

Number and year of law	Short title	Extent of repeal or amendment
		issued by the court and the existence thereof has been brought to the attention of the person or electronic communications service provider. (*g*) Any person or electronic communications service provider who fails to comply with an order referred to in paragraph *(d)* is guilty of an offence. *(h)* Any person who is subpoenaed in terms of paragraph *(c)* to attend proceedings and who fails to— (i) attend or to remain in attendance; (ii) appear at the place and on the date and at the time to which the proceedings in question may be adjourned; (iii) remain in attendance at those proceedings as so adjourned; or (iv) produce any book, document or object specified in the subpoena, is guilty of an offence. (*i*) The provisions in respect of appeal and review as provided for in the Magistrates' Courts Act, 1944 (Act No. 32 of 1944), and the Superior Courts Act, 2013 (Act No. 10 of 2013), apply to proceedings in terms of this subsection. (5) Whenever a person is— *(a)* convicted of an offence in terms of subsections (1), (2) or (3); or *(b)* acquitted of an offence in terms of subsections (1), (2) or (3), and evidence produced at the trial proves that the person engaged in, or attempted to engage in, harassment as contemplated in the Protection from Harassment Act, 2011 (Act No. 17 of 2011), the trial court may, after holding an enquiry, issue a protection order as contemplated in section 9(4) of the Protection from Harassment Act, against the person, whereafter the

Number and year of law	Short title	Extent of repeal or amendment
		provisions of that Act shall apply with the necessary changes required by the context. (6) A court must, on convicting a person of the commission of an offence contemplated in subsection (1), (2) or (3) order— *(a)* that person to refrain from further making available, broadcasting or distributing the data message contemplated in subsection (1), (2) or (3) which relates to the charge on which he or she is convicted; *(b)* that person or any other person to destroy the data message in question or any copy of the data message; or *(c)* an electronic communications service provider or person in control of a computer system to remove or disable access to the data message in question. (7) The order referred to in subsection (6)*(b)*, in so far as it relates to a person other than the accused, and (6)*(c)* must be served on the person or electronic communications service provider or person in control of a computer system in the prescribed form and 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 manner specified in that order. (8) Any person contemplated in subsection (6)*(a)* or *(b)* or an electronic communications service provider or person in control of a computer system as contemplated in subsection (6)*(c)* who fails to comply with an order referred to in subsection (7), is guilty of an offence. (9) For purposes of subsection (5), a "trial

Number and year of law	Short title	Extent of repeal or amendment
		court" means— *(a)* a magistrate's court established under section 2(1)*(f)*(i) of the Magistrates' Courts Act, 1944 (Act No. 32 of 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 (Act No. 10 of 2013). (10) Section 20 of the Cybercrimes and Cybersecurity Act, 2017, applies with the necessary changes required by the context to an application for a protection order in terms of subsection (4).". *(d)* Chapter 3 is hereby amended— (i) by the substitution for the heading to Part II of Chapter 3 of the following heading: "***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 insertion of the following section after section 19 of the Act: "**Offences relating to child pornography** **19A.** (1) Any person who unlawfully and intentionally creates, makes or produces child pornography, is guilty of an offence. (2) Any person who unlawfully and intentionally, in any manner knowingly assists in, or facilitates the creation, making or production of child pornography, is guilty of an offence. (3) Any person who unlawfully and intentionally possesses child pornography is guilty of an offence.

Number and year of law	Short title	Extent of repeal or amendment
		(4) Any person who unlawfully and intentionally, in any manner— *(a)* distributes; *(b)* makes available; *(c)* transmits; *(d)* offers for sale; *(e)* sells; *(f)* offers to procure; (*g*) procures; *(h)* accesses; (*i*) downloads; or (*j*) views, child pornography, is guilty of an offence. (5) Any person who unlawfully and intentionally, in any manner knowingly assists in, or facilitates the— *(a)* distribution; *(b)* making available; *(c)* transmission; *(d)* offering for sale; *(e)* selling; *(f)* offering to procure; *(g)* procuring; (*h*) accessing; *(i)* downloading; or (*j*) viewing, of child pornography, is guilty of an offence. (6) Any person who unlawfully and intentionally advocates, advertises, encourages or promotes— *(a)* child pornography; or *(b)* the sexual exploitation of children; is guilty of an offence. (7) Any person who unlawfully and intentionally processes or facilitates a financial transaction, knowing that such transaction will facilitate a contravention of subsections (1) to (6), is guilty of an offence. (8) Any person who, having knowledge of the commission of any offence referred to in subsections (1) to (7), or having reason to suspect that such an offence has been or is being committed and unlawfully and intentionally fails to—

Number and year of law	Short title	Extent of repeal or amendment
		(a) report such knowledge or suspicion as soon as possible to the South African Police Service; or (b) furnish, at the request of the South African Police Service, all particulars of such knowledge or suspicion, is guilty of an offence. (9) An electronic communications service provider that is aware or becomes aware that its electronic communications system **or service** is used or involved in the commission of any offence provided for in subsections (1) to (7), must— (a) immediately report the offence to the South African Police Service; (b) preserve any information which may be of assistance to the law enforcement agencies in investigating the offence; and (c) take all reasonable steps to prevent access to the child pornography by any person.". (iii) the amendment of section 20, by the addition of the following subsections: "(3) Any person who unlawfully and intentionally— (a) attends; or (b) views, a live performance involving child pornography, is guilty of the offence of attending or viewing a performance involving child pornography. (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— (a) creating, making or producing any image, publication, depiction, description or sequence in any manner whatsoever of child pornography, is guilty of the offence of recruiting a child for

Number and year of law	Short title	Extent of repeal or amendment
		child pornography; or *(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."; and *(e)* the amendment of section 56A, by the addition of the following subsections: "(3) *(a)* Any person who contravenes the provisions of section 10A(1) or (2) is liable, on conviction to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment. *(b)* Any person who contravenes the provisions of section 10A(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. *(c)* Any person or electronic communications service provider who contravenes the provisions of subsection 10A(4)(*g*) is liable, on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment. *(d)* Any person who contravenes the provisions of subsection 10A(4)*(h)* is liable, on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment. *(e)* Any person or electronic communications service provider who contravenes the provisions of section 10A(8), is liable on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment. (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— *(a)* in the case of a first conviction, to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment; *(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 *(c)* in the case of a third or subsequent

Number and year of law	Short title	Extent of repeal or amendment
		conviction, to a fine or to imprisonment for a period not exceeding 15 years or to both such fine and imprisonment. (5) Any person who contravenes the provisions of section 19A(4)(a), (b), (c), (d), or (e), (5)(a), (b), (c), (d) or (e), (6) or 20(3), is liable— *(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 *(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. (6) Any person who contravenes the provisions of section 19A(7), is liable— *(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; *(b)* in the case of a second or subsequent conviction, to a fine of R2000 000 or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment. (7) Any person who contravenes the provisions of section 19A(8), 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 19A(9), 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 No. 75 of 2008	Child Justice Act, 2008	*(a)* The addition of the following item to Schedule 2: "**26.** Any offence contemplated in— *(a)* section 2, 3 or 4 of the Cybercrimes and Cybersecurity Act, 20… (Act No. …… of 20…; *(b)* section 5, 6, 7 or 11(1) of the Cybercrimes and Cybersecurity Act, 20…, where the damage caused is below an amount of R5000; *(c)* section 16, 17 or 18 of the Cybercrimes and Cybersecurity Act,

Number and year of law	Short title	Extent of repeal or amendment
		20…); or *(d)* section 8, 9 or 10 of the Cybercrimes and Cybersecurity Act, 20…, where the amount involved exceeds R1500.". *(b)* The addition of the following item to Schedule 3: "23. Any offence contemplated in— *(a)* section 5, 6, 7 or 11(1) of the Cybercrimes and Cybersecurity Act, 20…, where the damage caused exceeds an amount of R5000; *(b)* section 8, 9 or 10 of the Cybercrimes and Cybersecurity Act, 20…, where the amount involved exceeds R1500; or *(c)* section 11(2).".

Annexure A

Cyber Command

55. (1) The Cabinet member responsible for defence must, in consultation with the Cabinet member responsible for national financial matters—

(*a*) establish a Cyber Command as part of the Intelligence Division of the South African National Defence Force contemplated in section 33 of the Defence Act, 2002 (Act 42 of 2002); and

(*b*) equip, operate and maintain the Cyber Command.

(2) The Cabinet member responsible for defence exercises final responsibility over the administration and functioning of the Cyber Command.

(3) (*a*) The Chief of the South African National Defence Force must appoint a member or employee from the South African National Defence Force—

(i) who, on the grounds of his or her technical knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued in terms of section 37 of the Defence Act, 2002 (Act No. 42 of 2002),

as General Officer Commanding of the Cyber Command.

(*b*) The General Officer Commanding must exercise the powers and perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Chief of the South African National Defence Force or under this Act, subject to the control and directions of the Chief of the South African National Defence Force.

(*c*) Whenever the General Officer Commanding is for any reason temporarily unable to exercise, perform and carry out his or her powers, functions and duties, the Chief of the South African National Defence Force must appoint a member or employee from the South African National Defence Force—

(i) who, on the grounds of his or her technical knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued in terms of section 37 of the Defence Act, 2002 (Act No. 42 of 2002),

as acting General Officer Commanding.

(*d*) The General Officer Commanding must, in exercising the powers, performing the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Chief of the South African National Defence Force or under this Act, be assisted, subject to his or her control and directions, by—

(i) members and employees of the South African National Defence Force, to whom a security clearance has been issued in terms of section 37 of the Defence Act, 2002 (Act No. 42 of 2002);

(ii) any person or an entity—

(*aa*) who or which has particular knowledge and skills in respect of any aspect dealt with in this Act;

(*bb*) who or which is, from time to time, appointed to assist the General Officer Commanding; and

(*cc*) to whom a security clearance has been issued in terms of section 37 of the Defence Act, 2002 (Act No. 42 of 2002).

(*e*) In order to achieve the objects of this Act, the General Officer Commanding must—

(i) carry out the administrative duties relating to the functioning of the Cyber Command;

(ii) exercise control over the members and employees of the Defence Force or persons or entities contemplated in subsection (3)(*d*)(ii);

(iii) manage and exercise administrative and technical control over the Cyber Command;

(iv) regulate the procedure and determine the manner in which the provisions of this Act must be carried out by Cyber Command;

(v) co-ordinate the activities of the Cyber Command with those of the 24/7 Point of Contact, the Cyber Security Centre, the Government Security Incident Response Teams, the National Cybercrime Centre, the Cyber Security Hub and the Private Sector Security Incident Response Teams.

(*f*) The General Officer Commanding is, for the purposes of exercising the powers, performing of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the the Chief of the South African National Defence Force or under this Act, accountable to the Chief of the South African National Defence Force.

(*g*) The General Officer Commanding must, on a monthly basis, or as the Chief of the South African National Defence Force requires, submit a written report to the Chief of the South African National Defence Force regarding any matter relevant to, incidental to, or which may impact on the objects and functions of the Cyber Command as set out in subsection (4).

(*h*) The General Officer Commanding must, on a quarterly basis, or as the Chairperson of the Cyber Response Committee requires, submit a written report to the Cabinet member responsible for defence and the Chairperson of the Cyber Response Committee regarding—

(i) cyber security-related threats, any measures implemented to address such cyber security-related threats and shortcomings in addressing such cyber security-related threats which may impact on the defence of the Republic;

(ii) any matter relevant to, incidental to or which may impact on the objects and functions of the Cyber Command as set out in subsection (4); or

(iii) any other matter relating to this Act which the General Officer Commanding wishes to or may want to bring to the attention of the Cyber Response Committee.

(4) The objects and functions of the Cyber Command are to—

(*a*) facilitate the operational coordination of cyber security incident response activities regarding national defence;

(*b*) develop measures to deal with cyber security matters impacting on national defence;

(*c*) facilitate the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange and threats on national defence in order to improve technical response coordination;

(*d*) provide guidance to and facilitate the identification, protection and securing of National Critical Information Infrastructures relevant to national defence;

(*e*) ensure, on the written command of the Chief of the South African National Defence Force, regular assessments and testing of National Critical Information Infrastructures relevant to national defence, including vulnerability assessments, threat and risk assessments and penetration testing;

(*f*) ensure the conducting of cyber security audits, assessments and readiness exercises and provide advice on the development of national response plans in so far as they relate to national defence;

(*g*) act as a point of contact regarding matters relating to national defence; and

(*h*) coordinate and implement cyber offensive and defensive measures as part of its defence mandate.

(5) The Cabinet Member responsible for defence may, after consultation with the Cyber Response Committee, make regulations to further—

(a) regulate any aspect provided for in subsection (4);

(*b*) impose additional duties upon the Cyber Command; and

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

(6) The Cabinet member responsible for defence may, in consultation with the Cabinet member responsible for national finance matters, make regulations regarding travelling, subsistence, remuneration and other expenses and allowances payable to a person or entity referred to in subsection (3)(*d*)(ii).

(7) The Cabinet member responsible for defence must, at the end of each financial year, submit a report to Chairperson of the Joint Standing Committee on Defence of Parliament, on the functions of the Cyber Command.