REPUBLIC OF SOUTH AFRICA

CYBERCRIMES AND CYBERSECURITY BILL

(As introduced in the National Assembly (proposed section 75); explanatory summary of Bill published in Government Gazette No. 40487 of 9 December 2016)
(The English text is the official text of the Bill)

(MINISTER OF JUSTICE AND CORRECTIONAL SERVICES)

[B 6—2017]

ISBN 978-1-4850-0355-7

No. of copies printed 800

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

Definitions

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

"access", for purposes of Chapter 5, includes, without limitation, 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,

of an offence in terms of Chapter 2 or sections 16, 17 or 18 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;

"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 the computer system;

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

"computer system" means—

(a) one computer; or

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

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

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

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

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

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

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

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

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

"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);
"foreign State" means any State other than the Republic;
"Intelligence Services Act" means the Intelligence Services Act, 2002 (Act No. 65 of 2002);
"Intelligence Services Control Act" means the Intelligence Services Control Act, 1994 (Act No. 40 of 1994);
"International Co-operation in Criminal Matters Act" means the International Co-operation in Criminal Matters Act, 1996 (Act No. 75 of 1996);
"investigator" means any person who is not a member of the South African Police Service and who is—
(a) identified and authorised in terms of a search warrant contemplated in section 27(3); or
(b) requested by a police official in terms of sections 29(2), 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;
"magistrate" includes a regional court magistrate;
"Magistrates' Courts Act" 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" means the National Prosecuting Authority Act, 1998 (Act No. 32 of 1998);
"output of a computer program" means any—
(a) data or output of the data;
(b) computer program; or
(c) instructions,
generated by a computer program;
"output of data" means having data displayed or in any other manner;
"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" means the Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998);
"Protection from Harassment Act" means the Protection from Harassment Act, 2011 (Act No. 17 of 2011);
"public available data" means data which is accessible in the public domain without restriction;
"Public Finance Management Act" means the Public Finance Management Act, 1999 (Act No. 1 of 1999);
"Public Service Act" means the Public Service Act, 1994 (Proclamation No. 103 of 3 June 1994);
"Regulation of Interception of Communications and Provision of Communication-related Information Act" means the Regulation of Interception of 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 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—

(a) make oral applications for a search warrant or an amendment of a warrant contemplated in section 28;
(b) issue expedited preservation of data directions contemplated in section 39; or
(c) 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" means the South African Reserve Bank Act, 1989 (Act No. 90 of 1989);

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

"Tax Administration Act" 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

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;
(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; 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 the 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,
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), **"unauthorised"** means that the person—

(a) is not himself or herself lawfully entitled to secure access;

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

(c) exceeds his or her entitlement or consent, to secure access,

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

Unlawful acquiring of data

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.

(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.

Unlawful acts in respect of software or hardware tool

4. (1) Any person who unlawfully and intentionally possesses, manufactures, assembles, obtains, sells, purchases, makes available or advertises 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.

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

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

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

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

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

(e) acquiring, modifying, providing, making available, copying, using or cloning a password, access code or similar data or devices as defined in section 7(3).

Unlawful interference with data or computer program

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—

(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 computer data storage medium or computer system

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.

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

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.

(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

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) or interference with a computer data storage medium or a computer system as contemplated in section 6(2),

which—

(i) causes actual prejudice; or

(ii) is potentially prejudicial,

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

Cyber forgery and uttering

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

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—
(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

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, 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, 1996, including a court; or
(iii) 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, which—
(a) endangers the life or violates the physical integrity or physical freedom of, or causes bodily injury to, any person, or any number of persons;
(b) causes serious risk to the health or safety of the public or any segment of the public;
(c) causes the destruction of or substantial damage to any property;
(d) causes a serious interference with, or serious disruption of, an essential service, facility or system, or the delivery of any essential service;
(e) causes any major economic loss;
(f) creates a serious public emergency situation; or
(g) prejudices the security, defence, law enforcement or international relations of the Republic,
is guilty of an aggravated offence.
(3) A prosecution in terms of subsection (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

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

Penalties

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 five years or to both a fine and such imprisonment.

(2) Any person who contravenes the provisions of section 3(1) or (2), 4(1) or (2), 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 must, without excluding other relevant factors, consider as aggravating factors—

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

(b) the extent of the prejudice and loss suffered by the complainant or 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.

Competent verdicts

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.

(2) If the evidence on a charge of a contravention of section 3(1), does not prove the 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) 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, but proves—

(a) a contravention of section 2(1);
(b) a contravention of section 4(2) in so far as it relates to the use of a software or hardware tool for purposes of contravening section 5(1); or
(c) the offence of malicious injury to property,
the accused may be found guilty of the offence so proved.

(4) If the evidence on a charge of a contravention of section 6(1), does not prove the offence or attempt to commit the offence, but proves—
(a) a contravention of section 2(1);
(b) a contravention of section 4(2) in so far as it relates to the use of a software or hardware tool for purposes of contravening section 6(1); or
(c) the offence of malicious injury to property,
the accused may be found guilty of the offence so proved.

(5) *(a)* If the evidence on a charge of a contravention of section 7(1)*(a)* or *(d)* does not prove the offence, but proves—
(i) a contravention of section 2(1);
(ii) a contravention of section 7(2); or
(iii) a contravention of section 4(2) in so far as it relates to the use of a software or hardware tool 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, 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, but proves—
(a) a contravention of section 2(1);
(b) a contravention of section 4(2), 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);
(ii) interfering with a computer data storage medium or a computer system as contemplated in section 6(1); or
(iii) acquiring, modifying, providing, making available, copying, using or cloning a password, access code or similar data or devices as contemplated in section 7(1)*(a)* and *(d)*;
(c) a contravention of sections 9(1) or (2);
(d) the common law offence of fraud or attempt to commit that offence;
(e) the common law offence of forgery or uttering or attempt to commit that offence; or
(f) 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, but proves the common law offence of forgery, 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 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 sections 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 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.

CHAPTER 3

MALICIOUS COMMUNICATIONS

Data message which incites damage to property or violence

16. Any person who unlawfully 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 group of persons, is guilty of an offence.

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 purposes 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

(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;

(b) it 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) it intimidates, encourages or harasses a person to harm himself or herself or any other person; or

(d) it 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.

Distribution of data message of intimate image without consent

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 an identifiable person knowing that 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), **"intimate image"** means a visual depiction of a person made by any means—

(a) under circumstances that give rise to a reasonable expectation of privacy; and

(b) in which the person is nude, is exposing his or her genital organs or anal region or, in the case of a female, her breasts.

Order to protect complainant pending finalisation of criminal proceedings

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 sections 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 or her 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

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, broadcast 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—

(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,

broadcast 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, broadcast 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 a 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, broadcast 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

21. (1) Whenever a person is—

(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,

and 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 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 orders referred to in subsection (2)*(b)*, in so far as it relates to a person other than the accused, and subsection (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.

Penalties

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 three 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 two years or to both a fine and such imprisonment.

CHAPTER 4

JURISDICTION

Jurisdiction

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

(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;

(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 in 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 business 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.

CHAPTER 5

POWERS TO INVESTIGATE, SEARCH AND ACCESS OR SEIZE

Standard Operating Procedures

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 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*.

Application of provisions in this Chapter

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

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 under search warrant

27. (1) Subject to the provisions of sections 29, 30 and 31 of this Act, section 4(3) of the Customs and Excise Act, 1964, sections 69(2)*(b)* and 71 of the Tax Administration Act, 2011, and section 21*(e)* and *(f)* of the Customs Control Act, 2014, an article can only be searched for, accessed or seized by virtue of a search warrant issued—

(a) by a magistrate or judge of the High Court, on written application by a police official, if it appears to the magistrate or judge from information on oath or by way of affirmation 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 he or she 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

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—

(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 he or she 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 such an order as he or she deems fit in respect of how any article which is affected by his or her decision is to be dealt with.

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), 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 commission of 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 of performing the powers referred to in paragraphs *(a)* and *(b)* of the definition of ''seize'' in respect of a computer data storage medium or any part of a computer system referred to in 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 or her 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 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.

(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 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 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 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, 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 or her 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 for a search warrant,

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

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

Assisting member of law enforcement agency or investigator

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 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 two years or to both a fine and such imprisonment.

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

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 two years or to both such fine and such 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 two years or to both a fine and such imprisonment.

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

(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 two years or to both a fine and such imprisonment.

(2) If 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 changes required by the context with reference to such award.

Prohibition on disclosure of information

37. (1) No person, investigator, police official, electronic communications service provider, financial institution or employee of an electronic communications service provider or financial institution may, subject to subsection (2), disclose any information which he or she 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;

(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; or

(ii) between electronic communications service providers, financial institutions, the South African Police Service or any other person or entity which is aimed at preventing, investigating or mitigating cybercrime:

Provided that such information sharing may not prejudice any criminal investigation or criminal proceedings; or

(e) to any competent authority 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.

(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 three years or to both a fine and such imprisonment.

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

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 an interception direction issued in terms of section 16(4) or 18(3)*(a)* of that Act and must, subject to subsection (4), be dealt with further in the manner provided for in that Act.

(2) The obtaining of real-time communication-related information as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, on an ongoing basis, as it becomes available must take place in terms of a 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.

(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 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 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;

(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 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) 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 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

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 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;

(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; 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.

(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 or she cannot timeously or in a reasonable fashion comply with the direction.

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

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

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

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

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

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

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

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

Preservation of evidence direction

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;

(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;

(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 committed in a foreign State; 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 three years or to both a fine and such imprisonment.

(5) A person, electronic communications service provider or financial institution to whom a preservation of evidence direction referred to in subsection (1) is addressed may, in writing in the prescribed form and manner, apply to a magistrate or judge of the High Court in whose area of jurisdiction the person, electronic communications service provider or financial institution is situated for an amendment or the cancellation of the direction concerned on the ground that he or she 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

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—

(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

42. (1) Where—

(a) an expedited preservation of data direction or a preservation of evidence direction is in place; 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 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; 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 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; 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 two years or to both a fine and such imprisonment.

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

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—

(a) search for, access or perform the powers referred to in paragraphs *(c)* or *(d)* of the definition of ''seize'' in respect of publicly available data regardless of where the data is located geographically; or

(b) receive non-public 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.

CHAPTER 6

MUTUAL ASSISTANCE

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

Spontaneous information

45. (1) The National Commissioner 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), forward any information obtained during any investigation to a law enforcement agency of a foreign State if the National Commissioner is of the opinion that the disclosure of such information may—

(a) assist the foreign State if the initiation or carrying out of investigations regarding an offence committed within the jurisdiction of that foreign State; 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;

(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; 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.

(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; 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.

Foreign requests for assistance and cooperation

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;

(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; 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 subsection (3)*(a)*.

(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) 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, 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 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, and which must be obtained; or

(vi) data, which is an indirect communication, and 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 to 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; 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 or she 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

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

(a) the designated judge; and

(b) a foreign State,

of the outcome of the 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)*, 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 subsection (2); 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 a fine and such 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; 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 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 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

Establishment and functions of 24/7 Point of Contact

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.

(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 purposes of proceedings or investigations regarding the commission or intended commission of—

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

(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; 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;

(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 such 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

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 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 made by a person who, in that affidavit, states that he or she—
(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,
is, upon its mere production at such proceedings, *prima facie* proof of such fact.

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

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

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

(5) *(a)* For purposes of subsection (1), a document purporting to be an affidavit made by a person who in that affidavit alleges that he or she is in the service of a body in the Republic or 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).

(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 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 be submitted or that oral evidence be heard: Provided that oral evidence may only be heard if the court is of the opinion that it is in the interests of the administration of justice and that a party to the proceedings would be prejudiced materially if oral evidence is not heard.

CHAPTER 9

OBLIGATIONS OF ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS AND FINANCIAL INSTITUTIONS

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 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

(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 R50 000.

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

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

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

(5) This 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

STRUCTURES TO DEAL WITH CYBERSECURITY

Cyber Response Committee

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).

(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.

(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 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—

(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 cooperation 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 cooperation 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—

(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 cooperation 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.

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

(i) establish a 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 cooperation 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 subparagraph (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.

(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

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 in consultation with the Cabinet member responsible for the administration 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—

(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, after consultation with the sector, identify and establish a nodal point for that sector on such terms and conditions as he or she deems fit in order 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 subsections (2) or (3).

(5) *(a)* The Cabinet member responsible for telecommunications and postal services may make regulations, after consultation with a sector to further regulate—

(i) contributions to be made by entities in a sector to fund a nodal point established for a particular sector in terms of subsections (2) or (3); and

(ii) 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 that 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 a fine and such 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 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 that 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 a fine and such imprisonment.

Information sharing

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.

CHAPTER 11

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Protection of critical information infrastructure

57. (1) The State Security Agency—

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

(b) after consultation with the owner 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, defence, law enforcement or international relations of the Republic;

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

(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 in terms of 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) if 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 to the Constitution;

(bb) any matter outside the functional areas listed in Schedule 4 or 5 to 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 the Premier 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 to the Constitution; or

(bb) any matter outside the functional areas listed in Part B of Schedule 4 or 5 to 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 1 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—

(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, an 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, 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 contemplated in subsection (3)*(h)*, or company, entity or person contemplated in subsection (3)*(i)*, may dispute 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).

(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)*.

(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 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 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 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 specified in the notice, within the period specified in the notice.

(10) An owner or person in control of the critical information infrastructure who without reasonable cause refuses or fails to take the steps specified in the notice 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 a fine and such imprisonment.

(11) If the owner or person in control of the critical information infrastructure fails or refuses to take the steps specified in the notice 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.

(12) For purposes of this section—

(a) **"classification of data"**, 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 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 President by proclamation in the *Gazette* as contemplated in section 63;

(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

58. (1) The owner 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).

(2) Before an audit referred to in subsection (1) is performed on a critical information infrastructure, the owner 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 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 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 or person in control of a critical information infrastructure—

(a) fails to cause an audit to be performed on a critical information infrastructure in terms of 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 pursuant to a failure contemplated in 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 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 or person in control of a critical information infrastructure who—

(a) fails to cause an audit to be performed on a critical information infrastructure in terms of 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) 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 a 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 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 a 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

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;

(ii) any other offence in terms of the laws of the Republic which is or was committed by means 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 committed in a foreign State; 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;

(d) the establishment of 24/7 Point of Contact;

(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 it is 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

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, the outcome of those prosecutions and any other information relating to those prosecutions, which is determined by the Cabinet member responsible for the administration of justice.

(2) The statistics or information contemplated in subsection (1) must—

(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

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);

(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 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) and 54(2)*(b)*.

(3) *(a)* The Cabinet member responsible for State security must make regulations to prescribe 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 section 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 sections 54(4)*(c)* and 55(5).

(6) Any regulation made in terms of subsection (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

No. 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 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 000,00; 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.

No. and year of law	Short Title	Extent of repeal or amendment
		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	The deletion of section 24B.
Act No. 105 of 1997	Criminal Law Amendment Act, 1997	The addition of the following item to Part II of Schedule 2: ''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 000,00; 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.''.

No. and year of law	**Short Title**	**Extent of repeal or amendment**
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 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 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

No. and year of law	Short Title	Extent of repeal or amendment
		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 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 Cyber-

No. and year of law	Short Title	Extent of repeal or amendment
		security 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 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, 2017), 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;

No. and year of law	Short Title	Extent of repeal or amendment
		(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 *(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, software or hardware tool, 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, harmful disclosure of pornography or engaging sexual services of persons 18 years or older***''; (ii) the insertion after item 10 of the following item: ''**10A.** Harmful disclosure of pornography''; (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, child pornography and using children for pornographic purposes or benefiting from child pornography*''; and (iv) the insertion after item 19 of the following item: ''**19A.** Offences relating to child pornography''.

No. and year of law	Short Title	Extent of repeal or amendment
		(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 realistically depicted or described or presented as being, under the age of 18 years, of an explicit or sexual nature, whether 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

No. and year of law	Short Title	Extent of repeal or amendment
		(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 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;''. *(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** **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

No. and year of law	Short Title	Extent of repeal or amendment
		(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 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,

No. and year of law	Short Title	Extent of repeal or amendment
		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 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

No. and year of law	Short Title	Extent of repeal or amendment
		(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 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

No. and year of law	Short Title	Extent of repeal or amendment
		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 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***";

No. and year of law	Short Title	Extent of repeal or amendment
		(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. (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.

No. and year of law	Short Title	Extent of repeal or amendment
		(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— *(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 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

No. and year of law	Short Title	Extent of repeal or amendment
		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 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 five 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 two 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 two 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 two 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

No. and year of law	Short Title	Extent of repeal or amendment
		a period not exceeding five 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 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 000 000,00; or to imprisonment for a period not exceeding five years, or to both such fine and imprisonment; *(b)* in the case of a second or subsequent conviction, to a fine of R2 000 000,00; 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 five 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 000 000,00; or to imprisonment for a period not exceeding five years or to both such fine and imprisonment.”.

No. and year of law	**Short Title**	**Extent of repeal or amendment**
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, 2017; *(b)* section 5, 6, 7 or 11(1) of the Cybercrimes and Cybersecurity Act, 2017, where the damage caused is below an amount of R5000; *(c)* section 16, 17 or 18 of the Cybercrimes and Cybersecurity Act, 2017); or *(d)* section 8, 9 or 10 of the Cybercrimes and Cybersecurity Act, 2017, 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, 2017, where the damage caused exceeds an amount of R5000; *(b)* section 8, 9 or 10 of the Cybercrimes and Cybersecurity Act, 2017, where the amount involved exceeds R1500; or *(c)* section 11(2).".

MEMORANDUM ON THE OBJECTS OF THE CYBERCRIMES AND CYBERSECURITY BILL, 2017

INTRODUCTION

1. The primary aim of the Bill is to deal with cybercrimes and cybersecurity. There is not a general universal recognised definition of cybercrimes. However, an attempted definition of cybercrimes could be crimes which are committed by means of, or which were facilitated by or which involve data, a computer program, a computer data storage medium or a computer system. Cybersecurity on the other hand can more readily be defined as technologies, measures and practices designed to protect data, computer programs, computer data storage mediums or a computer systems against cybercrime, damage or interference.

INTERNATIONAL POSITION

2. Internationally, most countries have cyber-specific legislation, which—

    * criminalises conduct which is considered cybercrimes;

    * regulates jurisdiction in respect of cybercrimes;

    * specifically provides for the investigation of cybercrimes;

    * regulates mutual assistance relating to the investigation of cybercrimes;

    * regulates the admissibility of electronic evidence; and

    * places obligations on certain persons or entities to assist in the investigation of cybercrimes.

    Most countries have or are in the process of building cyber capacity to come to terms with the sudden surge of cybercrime, security breaches and attacks on critical information infrastructures, such as information infrastructures responsible for the management of electricity, water and transportation. Most countries are also in the process of putting special mechanisms in place to deal with the protection of their critical information infrastructures. Some countries are also establishing a cyber offensive and defensive capacity to protect the countries against politically motivated attacks on information and information systems of those countries. Various countries ratified international instruments to facilitate mutual assistance in the investigation of cybercrimes and to deal with aspects relevant to cybersecurity.

CURRENT POSITION IN SOUTH AFRICA

3. The laws on the Statute Book do not comprehensively and uniformly criminalise conduct which is internationally regarded as cybercrimes. The laws currently on the Statute Book are silo-based, since various Departments enacted legislation to protect their interests in cyberspace, which lead to varying proscriptions of cybercrimes and penalties for such conduct. The common law is used to prosecute some of the offences but needs to grapple with new concepts such as intangible data. Furthermore, our cybercrime laws are not in line with those of the international community, which is essential for purposes of international cooperation, and which is mostly based on reciprocal laws.

4. Although the Protection from Harassment Act, 2011 (Act No. 17 of 2011), comprehensively deals with harassment in the real and virtual world, many countries have recognised the seriousness of cyber harassment and have enacted specific laws which criminalise such harassment. Cyber harassment is currently not recognised as a specific category of conduct in terms of the South African law and should be criminalised.

5. In general, South African laws afford broad jurisdiction to criminal acts which affect national security in the Republic, whilst jurisdiction is significantly narrower in ordinary criminal cases. It is proposed that current jurisdiction should be expanded upon to deal with the transnational dimension of cybercrimes.

6. Currently, cybercrimes are investigated in terms of the Criminal Procedure Act, 1977 (Act No. 51 of 1977). The investigative procedures provided for in Chapter 2 of that Act are object based and do not deal with the specialised procedures which are required to investigate cybercrimes, and which involve electronic evidence which is of an incorporeal nature. Special procedures are further necessary to ensure the integrity of electronic evidence which is not catered for in the Criminal Procedure Act, 1977.

7. Current procedures for mutual assistance between South Africa and foreign countries in the investigation of cybercrimes do not take into account the transient nature of electronic evidence and the need to act expeditiously. The resultant effect is that essential evidence is lost. Various other countries enacted legislation to provide for urgent action to preserve information and to provide expeditious assistance in order to identify the origin of communications involved in a cybercrime.

8. The laws dealing with electronic evidence are, in general, sufficient for the purposes of criminal proceedings. However, certain improvements can be made to cater for new technologies.

9. There is no obligation on electronic communications service providers and financial institutions to report cybercrimes and to preserve evidence of cybercrimes on their systems.

10. There is no coherent and organised approach in South Africa to deal with cybercrime and cybersecurity. Different Government Departments enacted legislation to protect their own interests. The silo-based approached has the effect that various essential steps which are necessary for the cybersecurity wellness of South Africa are not addressed.

11. There is inadequate capacity, both in the private and public sector, to deal with cybercrimes and cybersecurity.

12. Information sharing about cyber incidents is limited. Information sharing will ensure that adequate and timeous measures are implemented against a cyber threat and are therefore essential for the cybersecurity wellness of South Africa and to effectively act against cybercrimes.

13. Critical information infrastructures are not adequately protected. Legislation exists for the protection of physical structures, which cannot be used to protect computer systems. The Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002), narrowly caters for the protection of databases only and not for other information infrastructures which need to be protected. No provision is currently made for the implementation of minimum security standards which are necessary to protect critical information infrastructures or to monitor compliance with those standards.

14. As part of Government's Outcome Based Priorities the JCPS Cluster signed the JCPS Delivery Agreement relating to Outcome 3 on 24 October 2010. This agreement focuses on certain areas and activities, clustered around specific outputs, where interventions will make a substantial and a positive impact on the safety of the people of South Africa. One such area relates to Output 8, which requires the development and implementation of a Cyber Security Policy and the development of capacity to combat and investigate cybercrime. In line therewith the National Cybersecurity Policy Framework (the NCPF) for South Africa was developed

which provides for measures to address national security in cyberspace; measures to combat cyber warfare, cybercrime and other cyber irregularities; the development, review and updating of existing substantive and procedural laws; and measures to build confidence and trust in the secure use of Information Communications Technologies. The NCPF was approved by Cabinet in 2012.

15. In terms of paragraph 16.1 of the NCPF, the Department of Justice and Constitutional Development (the DOJ&CD) must review and align the cybersecurity laws of the Republic to ensure that these laws are aligned with the NCPF and in order to provide for a coherent and integrated cybersecurity legal framework for the Republic. The Bill gives effect to this mandate of the DOJ&CD.

16. In terms of the Medium-Term Strategic Framework for Government 2014-2019, the Bill must be enacted and implemented by 2018/19.

OVERVIEW OF BILL

17. The Bill aims to rationalise the laws of South Africa which deal with cybercrime and cybersecurity into a single Bill and to that extent the Bill seeks to—

* create offences and impose penalties which have a bearing on cybercrime;

* criminalise the distribution of malicious communications and to provide for interim protection measures;

* regulate jurisdiction to provide for the transnational dimension of cybercrimes;

* regulate the power to investigate cybercrimes;

* regulates mutual assistance to deal with cross-border investigation of cybercrimes;

* provide for the establishment of a 24/7 Point of Contact to facilitate mutual assistance in the investigation of cybercrime;

* regulate the proof of certain facts by means of affidavit;

* impose obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes and to report cybercrimes;

* provide for the establishment of structures to promote cybersecurity and capacity building;

* provide for the identification and declaration of critical information infrastructures and the implementation of measures to protect critical information infrastructures;

* provide that the Executive may enter into agreements with foreign States to promote cybersecurity; and

* provide for the repeal and amendments of certain laws.

ANALYSIS OF BILL

Chapter 1

18. **Clause 1** contains various definitions aimed at facilitating the interpretation of the Bill

Chapter 2

19. This Chapter aims to criminalise unwanted conduct in cyberspace in line with international best practices and can be broken down in the following broad categories of criminal offences:

Offences against the integrity, confidentiality and availability of data, computer programs, data storage mediums and computer systems

20. **Clause 2** criminalises the unlawful securing of access to data, a computer program, a computer data storage medium or a computer system without authority. The criminalisation of such access represents an important deterrent to many other subsequent acts against the confidentiality, integrity and availability of data, computer programs, data storage mediums or computer systems, and other computer-related offences.

21. **Clause 3** creates the offence of unlawful acquiring of data. The offence aims to protect data which is stored or transmitted over an electronic communications system. The offence criminalises the overcoming of protection measures which are intended to prevent access to data and thereafter to acquire data within, or which is transmitted to or from, a computer system. The clause further criminalises—

    * the possession of data, with the knowledge that such data was acquired unlawfully; and

    * the possession of data, in respect of which there is a reasonable suspicion that such data was acquired unlawfully where the possessor is unable to give a satisfactory exculpatory account of such possession.

22. **Clause 4** aims to criminalise software or hardware tools which are used in the commission of cybercrimes. The criminalisation of such software and hardware is challenging in light of the fact that most of this software or hardware has dual usages, which may not be unlawful. In order to prevent over-criminalisation the Bill, in accordance with various international and regional benchmarks, requires a specific intent, namely to commit certain offences provided for in the Bill.

23. **Clauses 5 and 6** aim to criminalise unlawful interference with data or a computer program and a computer data storage medium or a computer system, respectively. The availability of the protected interests is vital for users, businesses and public administration, all of which depend on the integrity, workability and proper functioning of data, computer programs and computer systems. Lack of availability can result in considerable pecuniary damage and may disrupt public administration.

24. Passwords, access codes and similar data or devices, have a specific function in cyberspace, namely to protect unauthorised access to, the use of, or interference with data, a computer program, a data storage medium or a computer system from criminal purposes. This offence can be the subject of several constitutive acts, namely, the acts of obtaining, possessing, transferring and use of passwords, access codes or similar data or devices to commit an offence. **Clause 7** criminalises the afore-mentioned stages to curb the unlawful use of passwords, access codes and similar data or devices to commit an offence. The clause further criminalises the possession of passwords, access codes and similar data or devices —

    * with the knowledge that such data was acquired unlawfully; and

    * with regard to which there is a reasonable suspicion that it was acquired unlawfully where the possessor is unable to give a satisfactory exculpatory account of such possession.

Offences committed or facilitated by means of data, computer programs and computer systems

25. **Clause 8** aims to create the statutory offence of cyber fraud by specifically criminalising fraud by means of data or a computer program, or through the interference with data or a computer program.

26. **Clause 9** aims to create the statutory offences of cyber forgery and uttering. The elements of the offence of cyber forgery are the making, with the intention to defraud, of false data or a false computer program, to the actual or potential prejudice of another person. The elements of the offence of cyber uttering are the passing off, with the intention to defraud, of false data or a false computer program, to the actual or potential prejudice of another person.

27. **Clause 10** criminalises cyber extortion. The proscription is applicable where a person commits the offence of acquiring protected data, interference with data or a computer program, interference with a computer or computer system or the acquiring or use of a password, access code or related data or devices or threatens another person with the commission of such offences for the purpose of—

    * obtaining any advantage from another person; or

    * compelling another person to perform or to abstain from performing any act.

Aggravated offences

28. The objective of this category of offences is to protect essential computer systems and life, limb, property, essential services, the economy or the interests of the Republic, against criminal conduct in cyber space.

29. In terms of **clause 11(1)**, the offences of acquiring protected data and interfering with data, a computer program, computer data storage medium or a computer system which was committed against a restricted computer system are regarded as aggravated offences which are punishable with a fine or imprisonment of up to 15 years. In terms of **clause 11(2)**, the offences of interfering with data, a computer program, computer data storage medium or a computer system and cyber extortion which—

    * endangers the life, or violates the physical integrity or physical freedom of, or causes bodily injury to, any person, or any number of persons;

    * causes serious risk to the health or safety of the public or any segment of the public;

    * causes the destruction of or substantial damage to any property;

    * causes a serious interference with, or serious disruption of an essential service, facility or system, or the delivery of any essential service;

    * causes any major economic loss; or

    * creates a serious public emergency situation; or

    * prejudices the security, the defence, law enforcement or international relations of the Republic,

    are regarded as aggravated offences which are punishable with 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.

30. **Clause 12** provides that the attempt, conspiring with another person or the aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring of another person to commit an offence contemplated in Chapter 2 of the Bill amounts to an offence.

31. **Clause 13** provides that the common law offence of theft must be interpreted so as to include the theft of an incorporeal.

32. **Clause 14** deals with penalties and prescribes certain factors which must be taken into account as aggravating circumstances.

33. **Clause 15** deals with competent verdicts where a person is charged with an offence provided for in Chapter 2.

Chapter 3

Malicious communications

34. This Chapter aims to criminalise a data message—

* which incites the causing of any damage to any property belonging to, or violence against, a person or a group of persons (**clause 16**);

* which is harmful (a data message is considered harmful if—

  - it threatens a person with—

    → damage to any property belonging to, or violence against, that person; or

    → 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;

  - it 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;

  - intimidates, encourages or harasses a person to harm himself or herself or any other person; or 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) (**clause 17**); and

* which is intimate in nature (person is nude), and which is distributed without the consent of the person involved (**clause 18**).

35. **Clause 19** provides for an interim protection order pending finalisation of criminal proceedings. In terms of the protection order a court may—

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

* 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.

A person or electronic communications service provider who contravenes a protection order is guilty of an offence. Provision is made for interim proceedings where the accused person can request the court to set aside or amend the protection order. The order of a court is subject to appeal or review.

36. Electronic communications service providers are compelled to assist a court during proceedings in terms of clause 19 by making available particulars of any person who distributed the malicious communications in order to ensure that the interim protection order can be served on him or her (**clause 20**).

37. **Clause 21** provides for orders on completion of criminal proceedings, which includes a prohibition to further distribute, to destroy or to disable access to the malicious communication.

38. **Clause 22** prescribes penalties which a court may impose in respect of malicious communications or offences provided for in terms of clause 19, 20 or 21.

Chapter 4

Jurisdiction

39. In terms of **clause 23**, a court will have jurisdiction to try an offence contemplated in Chapter 2 or clauses 16, 17 and 18 if—

* the offence was committed in the Republic;

* 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;

* 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;

* 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.

* the offence was committed outside the Republic and the person to be charged—

  - is a citizen of the Republic;

  - ordinarily is resident in the Republic;

  - 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;

  - is a company, incorporated or registered under any law, in the Republic; or

  - is a body of persons, corporate or unincorporated, in the Republic; or

* the offence was committed outside the Republic by a person, other than a person provided in the previous paragraph and the offence affects or is intended to affect a public body, a business or any other person in the Republic and the person who committed the offence is found to be in the Republic.

The clause further provides that 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.

Chapter 5

Powers to investigate, search and access or seize

40. **Clause 24** provides for the issuing of Standard Operating Procedures which must be followed in the investigation of cyber offences or offences which have a cyber element. The Standard Operating Procedures provides for the manner to deal with

electronic evidence to maintain the integrity of evidence. This involves five principles, namely—

* legality;

* that no action taken should change data held on a computer or storage media which may subsequently be relied upon in court;

* that persons should be competent to access and be able to give evidence explaining the relevance and the implications of their actions;

* that an audit trail should be kept to enable an independent third party to examine those processes and arrive at the same result; and

* that any deviation from these principles should be explained.

41. **Clause 25** provides that the Criminal Procedure Act, 1977, applies in addition to the provisions of Chapter 5 in so far that it is not inconsistent with the provisions of that Chapter.

42. In terms of **clause 26**, a police official may, in accordance with the provisions of Chapter 5, search for, access or seize any article within the Republic. An ''article'' is widely defined in terms of clause 1 as any data, computer program, computer data storage medium, or computer system which—

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

* may afford evidence of the commission or suspected commission; or

* is intended to be used or is, on reasonable grounds, believed to be intended to be used in the commission,

of an offence in terms of Chapter 2 or clause 16, 17 or 18 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.

43. **Clause 27** provides that an article may only be searched for, accessed or seized by virtue of a search warrant issued by a judicial officer if it appears to the judicial officer, from information on oath or by way of affirmation that there are reasonable grounds for believing that an article is being used or is involved in the commission of an offence or is required as evidence at criminal proceedings. In terms of a warrant a police official may, amongst others—

* search for any article identified in the warrant to the extent as is set out in the warrant;

* access an article identified in the warrant to the extent as is set out in the warrant;

* seize an article identified in the warrant to the extent as is set out in the warrant; or

* 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 as is set out in the warrant.

Provision is also made that a search warrant 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. An ''investigator'' is defined in clause 1 as a person, who is not a

member of the South African Police Service and who is identified and authorised in terms of a search warrant 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.

44. **Clause 28** provides for oral applications for search warrants.

45. **Clause 29** provides for search for, access to, or seizure of an article without a search warrant with the consent of a person who has lawful authority to consent.

46. **Clause 30** provides that a police official may without a search warrant search any person or container or premises for the purposes of seizing a computer data storage medium or any part of a computer system involved in the commission of an offence, if the police official on reasonable grounds believes that a search warrant will be issued to him or her if he or she applies for such warrant and that the delay in obtaining such warrant would defeat the object of the search and seizure. A police official may only, however, access or seize data in respect of the computer data storage medium or a computer system in terms of a search warrant. Provision is further made that a police official may if he or she on reasonable grounds believes that a search warrant will be issued to him or her if he or she applies for such warrant and it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written or oral application for a search warrant he or she may access the device and search for and seize data on such a device.

47. **Clause 31** provides that a police official may without a warrant, as is contemplated in section 40 of the Criminal Procedure Act, 1977, arrest any person who commits or whom he or she reasonably suspects of having committed any offence or against whom a reasonable complaint has been made or credible information has been received or a reasonable suspicion exists that the person has committed an offence, contemplated in Chapter 2 or clause 16, 17 or 18 of the Bill 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. The clause further seeks to provide that on the arrest of such a person, or where any person is arrested in terms of a warrant issued in terms of section 40 or section 43 of the Criminal Procedure Act, 1977, a police official may search the person and seize a computer data storage medium or any part of a computer system which is found in the possession of or in the custody or under the control of the person. A police official may, however, only access or seize data in respect of the computer data storage medium or a computer system in terms of a search warrant. Provision is further made that a police official may if he or she on reasonable grounds believes that a search warrant will be issued to him or her if he or she applies for such warrant and it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written or oral application for a search warrant to access the article and seize data, he or she may perform these actions without a search warrant.

48 **Clause 32** imposes obligations on an electronic communications service provider, financial institution and other persons who are in control of data, a computer program, a computer data storage medium or a computer system to provide technical assistance and other assistance to a police official who is authorised in terms of a warrant to conduct an investigation, in order to search for, access and seize an article.

49. **Clause 33** criminalises the obstruction or hindering of a police official or investigator to conduct an investigation in terms of Chapter 5 and to authorise a police official to use such force as may be reasonably necessary to overcome any resistance.

50. **Clause 34** provides that the powers to search, access and seize must be conducted with strict regard to decency and order and with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence.

51. **Clause 35** criminalises wrongful—

    * searches, access and seizures; and

    * obtaining or using of 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.

    The clause also regulates the retention of passwords, decryption keys, data and other information. The clause further provides for civil liability which may result from a contravention of the clause.

52. **Clause 36** criminalises the giving of false information which results in—

    * the issuing of a search warrant;

    * a search and seizure in terms of the Bill; or

    * the issuing of a preservation of data direction, a preservation of evidence direction or a disclosure of data direction.

    The clause further provides for civil liability which may result from a contravention of the clause.

53. **Clause 37** prohibits the disclosure of any information which a person has obtained in the exercise of his or her powers or the performance of his or her functions in terms of Chapter 5 or 6 of the Bill. The clause further regulates the instances where the disclosure of information will not amount to a contravention of the clause.

54. **Clause 38** seeks to clarify the operation of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002) (''the RICA''), *vis-á-vis* the Bill. In terms of the clause, the interception of an indirect communication and obtaining of any real-time communication-related information on an ongoing basis, as it becomes available, must take place in terms of the RICA. Since not all electronic communications service providers are required in terms of Government Notice No. 1325 of 2005, to be interceptable or to store communication-related information, specific obligations are imposed on these electronic communications service providers to—

    * provide real-time communication-related information, on an ongoing basis, as it becomes available;

    * implement an expedited preservation of data direction;

    * implement a preservation of evidence direction; and

    * implement a disclosure of data direction;

    * to provide archived communication-related information in respect of a customer that was stored by the electronic communications service provider; or

    * any order of the designated judge in terms of clause 46 of the Bill (which deals with mutual assistance (Chapter 6)).

55. **Clause 39** provides for expedited preservation of data. In terms of this clause a specifically designated police official may 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 to preserve data which is on reasonable grounds believed to be involved in an offence provided for in Chapter 2 or clause 16, 17 or 18 of the Bill. In terms of the expedited preservation of data direction a person, electronic communications service provider or financial institution must, from the time of service of the direction and for a period of 21 days, preserve the data in order to preserve the availability and integrity of the data. However, 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 clause 42 (disclosure of data direction). A person, electronic communications service provider or financial institution to whom an expedited preservation of data direction is addressed may apply to a magistrate 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. Non-compliance with a preservation of data direction is criminalised.

56. **Clause 40** provides that a judicial officer may, on the written application of a police official 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, if it appears to the judicial officer 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 involved in the commission of an offence referred to in Chapter 2 or clause 16, 17 or 18 of the Bill. This is a procedure which is less invasive than seizure of an article and can be resorted to where it is not necessary to seize the article in question. In terms of a preservation of evidence direction a person, electronic communications service provider or financial institution must, for a time period specified in the direction (which may not exceed 90 days), preserve the article in question in order to preserve the availability of or integrity of the article. A person, electronic communications service provider or financial institution to whom a preservation of evidence direction is addressed may apply to a judicial officer 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. Non-compliance with the direction is criminalised. **Clause 41** provides for the oral application for a preservation of evidence direction.

57. In terms of **clause 42**, where—

    * an expedited preservation of data direction or a preservation of evidence direction is in place; or

    * where it is otherwise expedient to obtain data without issuing a search warrant contemplated in clause 27,

    a judicial officer may, on written application by a police official, if it appears to the judicial officer from information on oath that data which is relevant to an offence contemplated in Chapter 2 or clause 16, 17 or 18 is in possession of, is in control of, may be received by a person, electronic communications service provider or financial institution, issue a disclosure of data direction. Similar to clause 40, this is a procedure which may be resorted to where it is not necessary to utilize the more invasive procedure to seize the article in question. A person, electronic communications service provider or financial institution to whom a direction is addressed may apply to a judicial officer 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. Non-compliance with the direction is criminalised.

58. In terms of **clause 43** a police official may—

    * search for, access or seize publicly available data regardless of where the data is located geographically, without any specific authorisation; or

* receive non-public 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.

Chapter 6

Mutual assistance

59. Clauses 46 to 49 apply in addition to Chapter 2 of the International Co-operation in Criminal Matters Act, 1996 (Act No. 75 of 1996), and relate, unless specified otherwise, to the preservation of evidence, pending a request in terms of section 2 or 7 of the International Co-operation in Criminal Matters Act, 1996 (**clause 44**).

60. In terms of **clause 45**, the National Commissioner of the South African Police Service may, after obtaining the written approval of the National Director of Public Prosecutions (''the NDPP'') and on such conditions regarding confidentiality and limitation of use, forward any information obtained during any investigation to a law enforcement agency of a foreign State when the National Commissioner is of the opinion that the disclosure of such information may assist the foreign State in the initiation or carrying out of investigations regarding an offence committed within the jurisdiction of that foreign State or lead to further cooperation with a foreign State to carry out an investigation regarding cybercrimes or offences contemplated in clause 16, 17 or 18. The South African Police Service may similarly receive any information from a foreign State, subject to such conditions regarding confidentiality and limitation of use as may be agreed upon, which will assist the South African Police Service in the investigation of a cybercrime or offences contemplated in clause 16, 17 or 18.

61. Clauses 46 to 48 of the Bill deal with requests for assistance and cooperation received from a foreign State and provide as follows:

    (a) In terms of **clause 46**, a mutual assistance request from a foreign State must in general be submitted to the 24/7 Point of Contact contemplated in Chapter 7 of the Bill. The 24/7 Point of Contact must submit the request to the NDPP for consideration. Upon receipt of a request, the NDPP must satisfy himself or herself that—

        * proceedings have been instituted in the foreign State; or

        * there are reasonable grounds for believing that an offence has been committed in the 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 foreign State;

        * the offence in question is similar to those contemplated in Chapter 2 or clause 16, 17 or 18 or other offence recognised in South Africa; and

        * 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 proceeding or investigation in the foreign State.

    The NDPP 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. On receipt of the approval of the Cabinet member, the request must be submitted to the designated judge for consideration. Where the request relates to the expedited disclosure of traffic data, the NDPP must submit the request for assistance, together with his or her recommendations, to the designated judge. The designated judge may issue any order which he or she deems appropriate to ensure that the requested—

        * data or other article is preserved in accordance with clause 40;

* data is seized on an expedited basis in accordance with clause 27 and preserved;

* traffic data (which is data relating to a communication indicating the communication's origin, destination, route, format, time, date, size, duration or type of the underlying service), 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, is disclosed on an expedited basis in accordance with clause 42;

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

* data which is an indirect communication is intercepted and preserved, as is specified in the request.

The designated judge may only issue an order if—

* the facts alleged in the request substantiate the fact that—

  - an offence substantially similar to the offences contemplated in Chapter 2 or clause 16, 17 or 18 has been or is being or will probably be committed or 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

  - it is necessary, in the interests of justice, to give the order;

* the request clearly identifies—

  - the person, electronic communications service provider or financial institution—

    → that will receive, is in possession of, or is in control of the data or other article that must be preserved, or

    → from whose facilities the data or traffic data must be obtained or intercepted;

  - the data or other article which must be preserved;

  - the data which must be seized on an expedited basis;

  - the traffic data which must be disclosed on an expedited basis;

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

  - the data, which is an indirect communication, which is to be intercepted;

* the request is, where applicable, in accordance with 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; and

* the order is in accordance with any applicable law of the Republic.

Where a request relates to the expedited disclosure of traffic data, the designated judge may—

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

* refuse to issue an order 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.

In the case of urgency, a request by any authority, court or tribunal exercising jurisdiction in a foreign State may be submitted directly to the designated judge who must deal with the request in accordance with this clause.

An order by the designated judge must be executed by a specially designated police official, who must inform the designated judge and the NDPP, of the fact that an order has been executed. The NDPP must inform a foreign State of the fact that an order was issued and executed or not issued.

(b) **Clause 47** imposes obligations on a person, electronic communications service provider or financial institution to comply with an order of the designated judge issued in terms of clause 46. A person, electronic communications service provider or financial institution 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. Non-compliance with an order of the designated judge or the giving of false information in an application for amendment or cancellation of the order is criminalised.

(c) **Clause 48** provides that the NDPP must inform the designated judge and a foreign State of the outcome of its request for assistance and cooperation. The clause further provides that any traffic data which is made available on an expedited basis, in terms of an order in terms of clause 46, must be provided to the 24/7 Point of Contact for submission to a foreign State.

62. **Clause 49** deals with the requests for mutual assistance by South Africa to a foreign State. If there is reasonable grounds for believing that an offence, contemplated in Chapter 2 or clause 16, 17 or 18, or 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 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—

* preserve data or other articles;

* seize data or other articles on an expedited basis;

* disclose traffic data on an expedited basis;

* obtain data which is real-time communication-related information or archived communication-related information; or

* intercept data which is an indirect communication,

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

* that there are reasonable grounds for believing that an offence contemplated in the Bill has been committed in the Republic or that it is necessary to determine whether an offence has been committed;

* that an investigation in respect thereof is being conducted; and

* the nature of the mutual assistance that is required within the area of jurisdiction of a foreign State.

The NDPP is responsible for the transmission of the direction to the foreign State which is requested to provide assistance and cooperation.

Chapter 7

24/7 Point of Contact

63. **Clause 50** provides for the establishment and functions of the 24/7 Point of Contact as part of the South African Police Service. 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, which includes—

    * technical advice and assistance;

    * anything which is authorised under Chapters 5 and 6;

    * legal assistance;

    * identification and location of an article;

    * the identification and location of a suspect; and

    * cooperation with appropriate authorities of a foreign State,

    for the purpose of proceedings or investigations regarding the commission or intended commission of an offence under Chapter 2 or clause 16, 17 or 18 or any other offence which may be committed or facilitated by means of an article within the Republic or in a foreign State.

64. The Cabinet member responsible for policing may make regulations to further regulate any aspect which is necessary or expedient for the proper implementation of this clause. The NDPP must make available members of the National Prosecuting Authority 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.

Chapter 8

Evidence

65. **Clause 51** aims to regulate the proof of certain facts by affidavit. In terms of the clause, whenever any fact established by any examination or process requiring any skill in the interpretation of data, the design of, or functioning of data, a computer program, a computer data storage medium or a computer system, computer science, electronic communications networks and technology, software engineering or computer programming is relevant to criminal proceedings, an affidavit made by a person who, in that affidavit, states 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*;

    * possesses relevant qualifications, expertise and experience which make him or her competent to make the affidavit; and

    * has established such fact by means of an examination or process,

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

66. Any person who makes such an affidavit and wilfully states in such affidavit anything which is false is guilty of an offence. The clause further provides that any court before which an affidavit is produced as *prima facie* proof of the relevant contents thereof may, in its discretion, cause the person who made the affidavit 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. The clause also prescribes specific requirements which must be adhered to if the person who has made the affidavit alleges that he or she is in the service of a body in the Republic or foreign State designated by the Cabinet member responsible for the administration of justice.

Chapter 9

Obligations of electronic communications service providers and financial institutions

67. **Clause 52** imposes obligations on electronic communications service providers and financial institutions who are aware or becomes aware of the fact that their computer systems are involved in the commission of any category or class of offences provided for in Chapter 2 which is determined by the Cabinet member responsible for policing, to report such offences to the South African Police Service and to preserve any information which may be of assistance to the South African Police Service to investigate such offences. Non-compliance with the clause is criminalised. The clause is not applicable to a financial sector regulator or any function performed by the South African Reserve Bank in terms of section 10 of the South African Reserve Bank Act, 1989 (Act No. 90 of 1989).

Chapter 10

Structures to deal with cybersecurity

68. **Clause 53** establishes the Cyber Response Committee (''the CRC'') as the overseeing body to implement the cyber initiative of the Republic. The CRC consists of a chairperson who is the Director-General: State Security and members who are the Heads of the representative Departments and one of their nominees. The Cabinet member responsible for State security must—

    * oversee and exercise control over the performance of the functions of the CRC; and

    * at the end of each financial year, submit a report to the Chairperson of the Joint Standing Committee on Intelligence regarding progress that has been made towards achieving the objects and functions of the CRC.

69. **Clause 54** deals with the establishment of structures which supports cybersecurity and capacity building. In terms of the clause—

    * the Cabinet member responsible for State security must—

        - establish, equip, operate and maintain a computer security incident response team for Government;

        - establish and maintain sufficient human and operational capacity to give effect to cybersecurity measures falling within the Constitutional mandate of the State Security Agency and to deal with critical information infrastructure protection;

    * the Cabinet member responsible for policing must establish and maintain sufficient human and operational capacity to detect, prevent and investigate cybercrimes and must ensure that members of the South African Police Service receive basic training in aspects relating to the detection, prevention and investigation of cybercrimes;

    * the Cabinet member responsible for defence must establish and maintain a cyber offensive and defensive capacity as part of the defence mandate of the South African National Defence Force; and

* the Cabinet member responsible for telecommunications and postal services must—

  - establish and maintain a Cybersecurity Hub as part of the Department of Telecommunications and Postal Services to promote cybersecurity in the private sector; and

  - encourage and facilitate the establishment of nodal points and private sector computer security incident response teams in the private sector.

The clause further provides that the respective Cabinet members—

* may make regulations to regulate any aspect which is necessary or expedient for the proper implementation of this clause; and

* must report to Parliament regarding progress that has been made towards achieving the objects and functions as is provided in the clause.

70. **Clause 55** deals with the establishment of nodal points (structures which receive and distribute information regarding cybersecurity incidents) and the recognition of private sector computer security incident response teams (expert groups that handle cybersecurity incidents). In terms of the clause 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. Each sector must, within six months from the date of the publication of a notice identify and establish a nodal point, which will be responsible for—

* distributing information regarding cyber incidents to other entities within the sector;

* receiving and distributing information about cybersecurity incidents to the nodal points established for other sectors or any computer security incident response team;

* reporting cybersecurity incidents to the Cybersecurity Hub; and

* receiving information about cybersecurity incidents from the Cybersecurity Hub.

71. If a sector fails to identify or establish a nodal point, the Cabinet member responsible for telecommunications and postal services may, after consultation with the sector, identify and establish a nodal point for that sector on such terms and conditions as he or she deems fit. The different sectors are responsible for the establishment and operating costs of nodal points. The clause empowers the Cabinet member to make regulations regarding the funding of nodal points and to further regulate any aspect relating to the establishment, operation or functioning of a nodal point. The clause further provides that the Cabinet member may recognise any computer security incident response team which is established for a sector and provide for the making of regulations to further facilitate the effective functioning of such a computer security incident response team.

72. **Clause 56** empowers the Cabinet member responsible for the administration of justice to make regulations to regulate information sharing, for purposes of Chapter 10.

Chapter 11

Critical information infrastructure protection

73. **Clause 57** deals with the protection of critical information infrastructures.

74. The Cabinet member responsible for State security is empowered to declare information infrastructures which are of such a strategic nature that any interference with them or their loss, damage, disruption or immobilisation may—

    * substantially prejudice the security, the defence, law enforcement or international relations of the Republic;

    * substantially prejudice the health or safety of the public;

    * cause a major interference with or disruption of, an essential service;

    * cause any major economic loss;

    * cause destabilisation of the economy of the Republic; or

    * create a major public emergency situation,

    as critical information infrastructures.

    The clause provides for an extensive consultation process with the various parties involved before an information infrastructure may be declared a critical information infrastructure.

75. The Cabinet member responsible for State security must, within six months of the declaration of any information infrastructure as a critical information infrastructure, in consultation with the relevant Cabinet members (Cabinet members responsible for defence, telecommunications and postal services, justice and correctional services, policing and State security) and other specified persons, issue directives to the critical information infrastructure in order to regulate minimum standards relating to—

    * the classification of data held by the critical information infrastructure;

    * the protection of, the storing of, and archiving of data held by the critical information infrastructure;

    * cybersecurity incident management by the critical information infrastructure;

    * disaster contingency and recovery measures which must be put in place by the critical information infrastructure;

    * minimum physical and technical security measures that must be implemented in order to protect the critical information infrastructure;

    * the period within which the owner of, or person in control of a critical information infrastructure must comply with the directives; and

    * any other relevant matter which is necessary or expedient in order to promote cybersecurity in respect of the critical information infrastructure.

    The clause provides for a dispute mechanism, in terms of which an information infrastructure may dispute the decision by the Cabinet member responsible for State security to declare it a critical information infrastructure as well as the measures which the infrastructure needs to implement in terms of a direction which was issued to it.

76. A critical information infrastructure must at own cost, take steps to the satisfaction of the Cabinet member responsible for State security, to comply with a directive. If a critical information infrastructure fails to comply with a direction, 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. A critical information infrastructure which without reasonable cause refuses or fails to take the steps specified in the notice within the period specified therein, is guilty of an offence. 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, and the Cabinet member may recover the costs of those steps from the owner or person on whose behalf they were taken.

77. **Clause 58** provides for the auditing of critical information infrastructures to ensure compliance with a directive which is issued by the Cabinet member responsible for State security in terms of clause 57. The owner 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 directive. The critical information infrastructure must notify the Director-General: State Security of the date on which an audit is to be performed whereupon 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 the audit. The owner or person in control of a critical information infrastructure must, upon completion of the audit, report in the prescribed form and manner to the Director-General: State Security regarding the outcome of the audit in order to enable the Director-General to evaluate compliance with the directive. The failure to perform an audit or to comply with the various regulatory provisions of the clause is criminalised. 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 the clause.

Chapter 12

Agreements with foreign States

78. In terms of **clause 59**, the National Executive may enter into agreements with any foreign State regarding—

    * mutual assistance and cooperation relating to the investigation and prosecution of offences contemplated in the Bill;

    * research, information and technology-sharing and the development and exchange of information on cybersecurity-related matters;

    * the establishment of 24/7 Points of Contact; and

    * the implementation of measures to address cyber threats.

Chapter 13

General provisions

79. In terms of **clause 60**, the NDPP is obliged to keep statistics of the number of prosecutions instituted in terms of Chapter 2 or clause 16, 17 or 18, the outcome of such prosecution and any other information relating to such prosecutions determined by the Cabinet member responsible for the administration of justice. These statistics must be included in the report of the NDPP, referred to in section 22(4)*(g)* of the National Prosecuting Authority Act, 1998, and on the written request of the Chairperson of the CRC be made available to the CRC.

80. **Clause 61** provides for the repeal or amendment of various laws. The repeals and amendments are necessary to harmonise the various laws with the provisions of the Bill.

81. **Clause 62** provides for the making of regulations to further regulate aspects provided for in the Bill

82. **Clause 63** deals with the short title and commencement of the Bill.

DEPARTMENTS/BODIES CONSULTED

83. The Bill was finalised in consultation with the CRC, which was established in terms of the NCPF, to implement the NCPF. The CRC consists of the following Departments which form part of the JCPS cluster, namely—

- the Department of Defence;
- the Department of Home Affairs;
- the Department of International Relations and Cooperation;
- the Department of Justice and Constitutional Development;
- the Department of Science and Technology;
- the Department of Telecommunications and Postal Services;
- the South African Police Service; and
- the State Security Agency.

These Departments participated in the development of the Bill. Additional comments received from these Departments during the public consultation process were also accommodated in the finalisation of the Bill.

84. A notice was published in the *Gazette* on 2 September 2015, inviting the public to comment on the draft Bill. The request for comment on the Bill was also made available on the webpage of the DOJ&CD, Lexus Nexus and JUTA. The Bill was also specifically submitted to all national, provincial and local governments, Universities, the legal fraternity and the judiciary for comments. The deadline for comment was set as 30 November 2015, which was subsequently extended to 15 December 2015. Comments on the draft Bill were received from various individuals, Telkom, CellC, MTN, Vodacom, ISPA, the National Prosecuting Authority, the Banking Industry, SABRICS, Internet Solution, the Cape Bar Council, AccessNow, American Chamber of Commerce in South Africa, Association for Savings and Investment South Africa, Centre for Constitutional Rights, City of Cape Town, Legal Aid South Africa, Hollard, University of Pretoria, Association of Certified Fraud Examiners, Department of Rural Development and Land Reform, Stanlib, Africana Books, Soarsoft International, WITS, Electronic Frontier Foundation, the Financial Intelligence Centre, Google South Africa, IAB South Africa, Institute of Information Technology Professionals South Africa, ISACA SA Chapter, M&G Centre for Investigative Journalism, Microsoft SA, NAB, National Film and Video Foundation, Open Democracy Advice Centre, Phukubje Pierce Masithela Attorneys, Western Cape Government, Association for Progressive Communications, Banking Association South Africa, Affinity Health, Mozilla, Motion Picture Association (Europe, Asia, Africa), Law Society of South Africa, BusinessBrief, Dalro, Department of Water and Sanitation, CSIR, Cape Innovation & Technology Initiative, Media Monitoring Africa, PASA, Right2Know, Cyclotron, ESKOM, Freedom of Expression Institute, IBM, Justice College, National Cybersecurity Advisory Council, PEN SA, Research ICT Africa, South Africa Reserve Bank, South African Revenue Services, Department of Cooperative Governance, Sonke Gender Justice, the National Treasury and the South African Law Reform Commission.

85. After the public consultation process engagement with interested parties was pursued to clarify aspects. A working group consisting of knowledgeable persons within the private and public sectors was established to further refine the Bill, following the comments that were received during the consultation process.

FINANCIAL IMPLICATIONS FOR STATE

86. The main costs relating to the implementation of the Bill relate to structures in Government which must be established in order to ensure that the necessary cyber capacity is obtained to protect the Republic against cybercrimes and to ensure that critical information infrastructures are adequately protected. Training of judicial officers and prosecutors is underway. The implementation of the Bill will not have additional financial implications for the DOJ&CD with regard to this aspect.

87. The Department of Telecommunications and Postal Services has established the Cybersecurity Hub, which is currently operational. A computer security incident response team for Government has been established within the State security Agency. The South African Police Service (''SAPS'') has capacity to investigate cybercrimes. Mutual assistance between the SAPS and foreign countries is currently facilitated through the INTERPOL mechanism. SAPS has implemented a training course for first responders in the investigation of offences which have a cyber element.

88. Further implementation will ensue following engagement between the departments concerned and relevant authorities with regard to funding.

PARLIAMENTARY PROCEDURE

Tagging

89. Section 44[1] of the Constitution of the Republic of South Africa, 1996 (''the Constitution''), deals with the national legislative authority. Section 44(1) provides that the national legislative authority is vested in Parliament. The National Assembly has the power to amend the Constitution, to pass legislation with regard

---

[1] ''**National legislative authority**

44. (1) The national legislative authority as vested in Parliament—

(a) confers on the National Assembly the power—
  (i) to amend the Constitution;
  (ii) to pass legislation with regard to any matter, including a matter within a functional area listed in Schedule 4, but excluding, subject to subsection (2), a matter within a functional area listed in Schedule 5; and
  (iii) to assign any of its legislative powers, except the power to amend the Constitution, to any legislative body in another sphere of government; and

(b) confers on the National Council of Provinces the power—
  (i) to participate in amending the Constitution in accordance with section 74;
  (ii) to pass, in accordance with section 76, legislation with regard to any matter within a functional area listed in Schedule 4 and any other matter required by the Constitution to be passed in accordance with section 76; and
  (iii) to consider, in accordance with section 75, any other legislation passed by the National Assembly.

(2) Parliament may intervene, by passing legislation in accordance with section 76 (1), with regard to a matter falling within a functional area listed in Schedule 5, when it is necessary—

(a) to maintain national security;
(b) to maintain economic unity;
(c) to maintain essential national standards;
(d) to establish minimum standards required for the rendering of services; or
(e) to prevent unreasonable action taken by a province which is prejudicial to the interests of another province or to the country as a whole.

(3) Legislation with regard to a matter that is reasonably necessary for, or incidental to, the effective exercise of a power concerning any matter listed in Schedule 4 is, for all purposes, legislation with regard to a matter listed in Schedule 4.

(4) When exercising its legislative authority, Parliament is bound only by the Constitution, and must act in accordance with, and within the limits of, the Constitution.''

to any other matter, including a matter listed in Schedule 4 to the Constitution but excluding, subject to section 44(2) of the Constitution, a matter listed in Schedule 5 to the Constitution. The National Council of Provinces (''the NCOP'') has the power to participate in the amendment of the Constitution, to pass legislation in accordance with section 75 and 76[2] of the Constitution. Section 76(3) of the Constitution refers to the legislative procedure that must be followed when dealing with ordinary Bills affecting provinces. Section 76(3) provides that a Bill must be

---

[2] **Ordinary Bills affecting provinces**

76. (1) When the National Assembly passes a Bill referred to in subsection (3), (4) or (5), the Bill must be referred to the National Council of Provinces and dealt with in accordance with the following procedure:

(a) The Council must—
  (i) pass the Bill;
  (ii) pass an amended Bill; or
  (iii) reject the Bill.

(b) If the Council passes the Bill without amendment, the Bill must be submitted to the President for assent.

(c) If the Council passes an amended Bill, the amended Bill must be referred to the Assembly, and if the Assembly passes the amended Bill, it must be submitted to the President for assent.

(d) If the Council rejects the Bill, or if the Assembly refuses to pass an amended Bill referred to it in terms of paragraph (c), the Bill and, where applicable, also the amended Bill, must be referred to the Mediation Committee, which may agree on—
  (i) the Bill as passed by the Assembly;
  (ii) the amended Bill as passed by the Council; or
  (iii) another version of the Bill.

(e) If the Mediation Committee is unable to agree within 30 days of the Bill's referral to it, the Bill lapses unless the Assembly again passes the Bill, but with a supporting vote of at least two thirds of its members.

(f) If the Mediation Committee agrees on the Bill as passed by the Assembly, the Bill must be referred to the Council, and if the Council passes the Bill, the Bill must be submitted to the President for assent.

(g) If the Mediation Committee agrees on the amended Bill as passed by the Council, the Bill must be referred to the Assembly, and if it is passed by the Assembly, it must be submitted to the President for assent.

(h) If the Mediation Committee agrees on another version of the Bill, that version of the Bill must be referred to both the Assembly and the Council, and if it is passed by the Assembly and the Council, it must be submitted to the President for assent.

(i) If a Bill referred to the Council in terms of paragraph (f) or (h) is not passed by the Council, the Bill lapses unless the Assembly passes the Bill with a supporting vote of at least two thirds of its members.

(j) If a Bill referred to the Assembly in terms of paragraph (g) or (h) is not passed by the Assembly, that Bill lapses, but the Bill as originally passed by the Assembly may again be passed by the Assembly, but with a supporting vote of at least two thirds of its members.

(k) A Bill passed by the Assembly in terms of paragraph (e), (i) or (j) must be submitted to the President for assent.

(2) When the National Council of Provinces passes a Bill referred to in subsection (3), the Bill must be referred to the National Assembly and dealt with in accordance with the following procedure:

(a) The Assembly must—
  (i) pass the Bill;
  (ii) pass an amended Bill; or
  (iii) reject the Bill.

(b) A Bill passed by the Assembly in terms of paragraph (a) (i) must be submitted to the President for assent.

(c) If the Assembly passes an amended Bill, the amended Bill must be referred to the Council, and if the Council passes the amended Bill, it must be submitted to the President for assent.

(d) If the Assembly rejects the Bill, or if the Council refuses to pass an amended Bill referred to it in terms of paragraph (c), the Bill and, where applicable, also the amended Bill must be referred to the Mediation Committee, which may agree on—
  (i) the Bill as passed by the Council;
  (ii) the amended Bill as passed by the Assembly; or
  (iii) another version of the Bill.

(e) If the Mediation Committee is unable to agree within 30 days of the Bill's referral to it, the Bill lapses.

(f) If the Mediation Committee agrees on the Bill as passed by the Council, the Bill must be referred to the Assembly, and if the Assembly passes the Bill, the Bill must be submitted to the President for assent.

dealt with in accordance with the procedure established by either subsection (1) or (2) of section 76 if it falls within a functional area listed in Schedule 4 to the Constitution or provides for legislation envisaged in any of the sections mentioned in paragraphs (a) to (g) of section 76(3) of the Constitution. Schedule 4 to the Constitution lists the functional areas of national and provincial legislative competence.[3]

(g) If the Mediation Committee agrees on the amended Bill as passed by the Assembly, the Bill must be referred to the Council, and if it is passed by the Council, it must be submitted to the President for assent.

(h) If the Mediation Committee agrees on another version of the Bill, that version of the Bill must be referred to both the Council and the Assembly, and if it is passed by the Council and the Assembly, it must be submitted to the President for assent.

(i) If a Bill referred to the Assembly in terms of paragraph (f) or (h) is not passed by the Assembly, the Bill lapses.

(3) A Bill must be dealt with in accordance with the procedure established by either subsection (1) or subsection (2) if it falls within a functional area listed in Schedule 4 or provides for legislation envisaged in any of the following sections:

(a) Section 65(2);

(b) section 163;

(c) section 182;

(d) section 195(3) and (4);

(e) section 196; and

(f) section 197.

(4) A Bill must be dealt with in accordance with the procedure established by subsection (1) if it provides for legislation—

(a) envisaged in section 44 (2) or 220 (3); or

(b) envisaged in Chapter 13, and which includes any provision affecting the financial interests of the provincial sphere of government.

(5) A Bill envisaged in section 42 (6) must be dealt with in accordance with the procedure established by subsection (1), except that—

(a) when the National Assembly votes on the Bill, the provisions of section 53 (1) do not apply; instead, the Bill may be passed only if a majority of the members of the Assembly vote in favour of it; and

(b) if the Bill is referred to the Mediation Committee, the following rules apply:

(i) If the National Assembly considers a Bill envisaged in subsection (1)(g) or (h), that Bill may be passed only if a majority of the members of the Assembly vote in favour of it.

(ii) If the National Assembly considers or reconsiders a Bill envisaged in subsection (1)(e), (i) or (j), that Bill may be passed only if at least two thirds of the members of the Assembly vote in favour of it.

(6) This section does not apply to money Bills.''

[3] ''**Schedule 4**

FUNCTIONAL AREAS OF CONCURRENT NATIONAL AND PROVINCIAL LEGISLATIVE COMPETENCE

PART A

Administration of indigenous forests
Agriculture
Airports other than international and national airports
Animal control and diseases
Casinos, racing, gambling and wagering, excluding lotteries and sports pools
Consumer protection
Cultural matters
Disaster management
Education at all levels, excluding tertiary education
Environment
Health services
Housing
Indigenous law and customary law, subject to Chapter 12 of the Constitution
Industrial promotion
Language policy and the regulation of official languages to the extent that the provisions of section 6 of the Constitution expressly confer upon the provincial legislatures legislative competence
Media services directly controlled or provided by the provincial government, subject to section 192
Nature conservation, excluding national parks, national botanical gardens and marine resources
Police to the extent that the provisions of Chapter 11 of the Constitution confer upon the provincial legislatures legislative competence
Pollution control

90. In **Tongoane and Others v Minister of Agriculture and Land Affairs and Others** 2010 (8) BCLR 741 (CC), the Constitutional Court gave guidance in respect of the classification of Bills. In this judgment the Constitutional Court dealt with the classifications of the Communal Land Rights Act, 2004 (Act No. 11 of 2004), and the procedure that had to be followed in enacting that Act.

91. The Constitutional Court confirmed and endorsed the test for tagging that was formulated in paragraph 28 in **Ex Parte President of the Republic of South Africa: In re Constitutionality of the Liquor Bill** 2000 (1) BCLR 1 (CC), where the Constitutional Court held that—

> ''*(w)*hatever the proper characterisation of the Bill . . . a large number of its provisions must be characterised as falling 'within a functional area listed in Schedule 4', more particularly the concurrent national and provincial legislative competences in regard to 'trade' and 'industrial promotion'.'' (emphasis added).

92. At paragraph 56 of the **Tongoane** judgment, Ngcobo CJ held that—

> ''the heading of section 76, namely, 'Ordinary Bills affecting provinces' provides 'a strong textual indication that section 76(3) must be understood as requiring that any Bill whose provisions in substantial measure fall within a functional area listed in Schedule 4, be dealt with under section 76'.'' (footnote omitted and emphasis added).

Population development
Property transfer fees
Provincial public enterprises in respect of the functional areas in this Schedule and Schedule 5
Public transport
Public works only in respect of the needs of provincial government departments in the discharge of their responsibilities to administer functions specifically assigned to them in terms of the Constitution or any other law
Regional planning and development
Road traffic regulation
Soil conservation
Tourism
Trade
Traditional leadership, subject to Chapter 12 of the Constitution
Urban and rural development
Vehicle licensing
Welfare services

PART B

The following local government matters to the extent set out in section 155 (6)(a) and (7):
Air pollution
Building regulations
Child care facilities
Electricity and gas reticulation
Fire-fighting services
Local tourism
Municipal airports
Municipal planning
Municipal health services
Municipal public transport
Municipal public works only in respect of the needs of municipalities in the discharge of their responsibilities to administer functions specifically assigned to them under this Constitution or any other law
Pontoons, ferries, jetties, piers and harbours, excluding the regulation of international and national shipping and matters related thereto
Stormwater management systems in built-up areas
Trading regulations
Water and sanitation services limited to potable water supply systems and domestic waste-water and sewage disposal systems.

93. At paragraph 58 of the **Tongoane** judgment, Ngcobo CJ furthermore held as follows:

> ''What matters for the purposes of tagging is not the substance or the true purpose and effect of the Bill, rather, what matters is whether the provisions of the Bill 'in substantial measure fall within a functional area listed in Schedule 4' '' (emphasis added).

94. The Constitutional Court also held that the tagging test focusses on all the provisions of the Bill in order to determine the extent to which they substantially affect functional areas listed in Schedule 4 to the Constitution and not on whether any of the provisions of the Bill are incidental to the substance of the Bill. The process of tagging is concerned with the question of how the Bill should be considered by the provinces and in the NCOP, and how the Bill must be considered by the provincial legislatures depends on whether the Bill affects the provinces. The more it affects the interests, concerns and capacities of the provinces, the more say the provinces should have on its content.[4]

95. The question is therefore whether the provisions of the Bill in ''substantial measure'' fall within a functional area listed in Schedule 4 to the Constitution.

96. As indicated in the **Tongoane** judgment discussed above, the test for determining whether a Bill is an ordinary Bill affecting provinces requires that a Bill whose provisions to a substantive measure fall within a functional area listed in Schedule 4 to the Constitution must be dealt with under section 76 of the Constitution. In order to determine this, the focus must be on all the provisions of the Bill in order to determine the extent to which those provisions substantially affect functional areas listed in Schedule 4 to the Constitution.

97. The Bill seeks to ''create offences and impose penalties which have a bearing on cybercrime; to criminalise the distribution of data messages which incite damage to property or violence or which are harmful or intimate 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''.[5]

98. None of the provisions of the Bill fall within a functional area listed in Schedule 4 and the Bill must be dealt with in accordance with the procedure set out in section 75 of the Constitution.[6]

---

[4] Paragraphs 59 and 60 of the **Tongoane** judgment; see paragraph 94 above.

[5] Long title of the Bill.

[6] **"Ordinary Bills not affecting provinces**

75. (1) When the National Assembly passes a Bill other than a Bill to which the procedure set out in section 74 or 76 applies, the Bill must be referred to the National Council of Provinces and dealt with in accordance with the following procedure:

(a) The Council must—
  (i) pass the Bill;
  (ii) pass the Bill subject to amendments proposed by it; or
  (iii) reject the Bill.

(b) If the Council passes the Bill without proposing amendments, the Bill must be submitted to the President for assent.

Referral to National House of Traditional Leaders

99. The Office of the Chief State Law Adviser is of the opinion that it is not necessary to refer the Bill to the National House of Traditional Leaders in terms of section 18(1)*(a)* of the Traditional Leadership and Governance Framework Act, 2003 (Act No. 41 of 2003), since it does not contain provisions pertaining to customary law or customs of traditional communities.

(c) If the Council rejects the Bill or passes it subject to amendments, the Assembly must reconsider the Bill, taking into account any amendment proposed by the Council, and may—
  (i) pass the Bill again, either with or without amendments; or
  (ii) decide not to proceed with the Bill.

(d) A Bill passed by the Assembly in terms of paragraph (c) must be submitted to the President for assent.

(2) When the National Council of Provinces votes on a question in terms of this section, section 65 does not apply; instead—

(a) each delegate in a provincial delegation has one vote;

(b) at least one third of the delegates must be present before a vote may be taken on the question; and

(c) the question is decided by a majority of the votes cast, but if there is an equal number of votes on each side of the question, the delegate presiding must cast a deciding vote.''

Printed by Creda Communications

ISBN 978-1-4850-0355-7

MEMORANDUM ON THE OBJECTS OF THE CYBERCRIMES AND CYBERSECURITY BILL, 2017

The primary aim of the Bill is to deal with cybercrimes and cybersecurity. There is not a general universal recognised definition of cybercrimes. However, an attempted definition of cybercrimes is crimes which are committed by means of, or which was facilitated by or which involve data, a computer program, a computer data storage medium or a computer system. Cybersecurity on the other hand can more readily be defined as technologies, measures and practices designed to protect data, computer programs, computer data storage mediums or a computer systems against cybercrime, damage or interference.

1. **International position**

Internationally, most countries have cyber-specific legislation, which -

* criminalises conduct which is considered cybercrimes;
* regulates jurisdiction in respect of cybercrimes;
* specifically provides for the investigation of cybercrimes;
* regulates mutual assistance relating to the investigation of cybercrimes;
* regulates the admissibility of electronic evidence; and
* places obligations on certain persons or entities to assist in the investigation of cybercrimes.

Most countries have or are in the process of building cyber capacity to come to terms with the sudden surge of cybercrime, security breaches and attacks on critical information infrastructures, such as information infrastructures responsible for the management of electricity, water and transportation. Most countries are also in the process to put special mechanisms in place to deal with the protection of their critical information infrastructures. Some countries are also establishing a cyber offensive and defensive capacity to protect a country against politically motivated attacks on information and information systems of such a country. Various countries ratified international instruments to facilitate mutual assistance in the investigation of cybercrimes and/or to deal with aspects relevant to cybersecurity.

2. Current position in South Africa

The laws on the Statute Book do not comprehensively and uniformly criminalise conduct which is internationally regarded as cybercrimes. The laws currently on the Statute Book are silo-based, since various Departments enacted legislation to protect their interests in cyberspace, which lead to varying proscriptions of cybercrimes and penalisation of such conduct. The common law is used to prosecute some of the offences but needs to grapple with new concepts such as intangible data. Furthermore, our cybercrime laws are not in line with those of the international community, which is essential for purposes of international cooperation, which is mostly based on reciprocal laws.

Although the Protection of Harassment Act, 2011, was put on the Statute Book to comprehensively deal with harassment in the real and virtual world, many countries have recognised the seriousness of cyber harassment and have enacted specific laws which criminalise such communications. Cyber harassment is currently not recognised as a specific category of conduct in terms of the South African law and should be criminalised.

In general, our laws afford broad jurisdiction to criminal acts which affect national security in the Republic, whilst jurisdiction is significantly narrower in ordinary criminal cases. It is submitted that current jurisdiction should be expanded upon to deal with the transnational dimension of cybercrimes.

Currently, cybercrimes are investigated in terms of the Criminal Procedure Act, 1977. The investigative procedures provided for in Chapter 2 of the Criminal Procedure Act are object based and do not deal with the specialised procedures which are required to investigate cybercrimes, which involve electronic evidence which is of an incorporeal nature. Special procedures are further necessary to ensure the integrity of electronic evidence which is not catered for in the Criminal Procedure Act.

Current procedures for mutual assistance between South Africa and foreign countries in the investigation of cybercrimes do take into account the transient nature of electronic evidence and the need to act expeditiously. The resultant effect is that essential evidence is lost. Various other countries enacted legislation to provide for urgent action to preserve information and to provide expeditious assistance to identify the origin of communications involved in a cybercrime.

The laws dealing with electronic evidence are, in general, sufficient for the purposes of criminal proceedings. However, certain improvements can be made to cater for new technologies.

There is no obligation on electronic communications service providers and financial institutions to report cybercrimes and to preserve evidence of cybercrimes on their systems.

There is no coherent and organised approach in South Africa to deal with cybercrime and cybersecurity. Different Government Departments enacted legislation to protect their own interests. The silo-based approached has the effect that various essential steps which are necessary for the cybersecurity wellness of South Africa are not addressed.

There is inadequate capacity, both in the private and public sector, to deal with cybercrimes and cybersecurity

Information sharing about cyber incidents is limited. Information sharing will ensure that adequate and timeous measures are implemented against a cyber threat and are therefore essential for the cybersecurity wellness of South Africa and to effectively act against cybercrimes.

Critical information infrastructures are not adequately protected. Legislation exists for the protection of physical structures, which cannot be used to protect computer systems. The Electronic Communications and Transactions Act, 2002,

narrowly caters only for the protection of databases and not for other information infrastructures which need to be protected. No provision is currently made for the implementation of minimum security standards which are necessary to protect critical information infrastructures or to monitor compliance with such standards.

As part of Government's Outcome Based Priorities the JCPS Cluster signed the JCPS Delivery Agreement relating to Outcome 3 on 24 October 2010. This agreement focuses on certain areas and activities, clustered around specific outputs, where interventions will make a substantial and a positive impact on the safety of the people of South Africa. One such area relates to Output 8, which requires the development and implementation of a Cyber Security Policy and the development of capacity to combat and investigate cybercrime. In line therewith, the National Cybersecurity Policy Framework (the NCPF) for South Africa, was developed which provides for measures to address national security in cyberspace; measures to combat cyber warfare, cybercrime and other cyber irregularities; the development, review and updating of existing substantive and procedural laws; and measures to build confidence and trust in the secure use of Information Communications Technologies. The NCPF was approved by Cabinet in 2012.

In terms of paragraph 16.1 of the NCPF, the Department of Justice and Constitutional Development (the DOJ&CD) must review and align the cybersecurity laws of the Republic to ensure that these laws are aligned with the NCPF and provide for a coherent and integrated cybersecurity legal framework for the Republic. The Bill gives effect to this mandate of the DOJ&CD.

In terms of the Medium-Term Strategic Framework for Government 2014-2019, the Bill must be enacted and implemented by 2018/19.

3. **Overview of Bill**

The Bill aims to rationalise the laws of the RSA which deals with cybercrime and cybersecurity into a single Bill and to that extent the Bill:

* Creates offences and imposes penalties which have a bearing on cybercrime.
* Criminalises the distribution of malicious communications and provides for interim protection measures.
* Regulates jurisdiction to provide for the transnational dimension of cybercrimes.
* Regulates the powers to investigate cybercrimes.
* Regulates mutual assistance to deal with cross-border investigation of cybercrimes.
* Provides for the establishment of a 24/7 Point of Contact to facilitate mutual assistance in the investigation of cybercrime.
* Regulates the proof of certain facts by affidavit.
* Imposes obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes and to report cybercrimes.
* Provides for the establishment structures to promote cybersecurity and capacity building.
* Provides for the identification and declaration of critical information infrastructures and implementation of measures to protect critical information infrastructures.
* Provides that the Executive may enter into agreements with foreign States to promote cybersecurity.
* Provides for the repeal and amendments of certain laws.

4. **Chapter by chapter breakdown of Bill**

4.1 ***Chapter 1 (clause 1)***

This clause contains various definitions aimed at facilitating the interpretation of the Bill

4.2 ***Cybercrimes (Chapter 2***)

This Chapter aims to criminalise unwanted conduct in cyberspace in line with international best practices and can be broken down in the following broad categories of criminal offences:

4.2.1 Offences against the integrity, confidentiality and availability of data, computer programs, data storage mediums and computer systems.

(a) Clause 2 criminalises unlawful securing access without authority. The criminalisation of illegal access represents an important deterrent to many other subsequent acts against the confidentiality, integrity and availability of data, computer programs, data storage mediums or a computer system, and other computer-related offences. The offence criminalises the unauthorised securing of access to data, a computer program, a computer data storage medium or a computer system.

(b) Clause 3 creates the offence of unlawful acquiring of data. The offence aims to protect data which is stored or transmitted over an electronic communications system. The offence criminalises the overcoming of protection measures which are intended to prevent access to data and thereafter acquires data, within or which is transmitted to or from a computer system. The clause further criminalises -

* the possession of data, with the knowledge that such data was acquired unlawfully; and
* possession of data, in regard to which there is a reasonable suspicion that such data was acquired unlawfully where the possessor is unable to give a satisfactory exculpatory account of such possession.

(c) Clause 4 aims to criminalise software or hardware tools which are used in the commission of cybercrimes. The criminalisation of such software and hardware is challenging in light of the fact that most of this software or hardware has dual usages, which may not be unlawful. In order to prevent over-criminalisation the Bill, in accordance with various international and regional

benchmarks, requires a specific intent, namely to commit certain offences provided for in the Bill.

(d) Clauses 5 and 6 aim to criminalise unlawful interference with data or a computer program and a computer data storage medium or a computer system, respectively. The availability of the protected interests is vital for users, businesses and public administration, all of which depend on the integrity, workability and proper functioning of data, computer programs and computer systems. Lack of availability can result in considerable pecuniary damage and may disrupt public administration.

(e) Passwords, access codes and similar data or devices, have a specific function in cyberspace, namely to protect unauthorised access to, the use of, or interference with data, a computer program, a data storage medium or a computer system for criminal purposes. This offence can be the subject of several constitutive acts, namely, the acts of obtaining, possessing, transferring and use of passwords, access codes or similar data or devices to commit an offence. Clause 7 criminalises the afore-mentioned stages to curb the unlawful use of passwords, access codes and similar data or devices to commit an offence. The clause further criminalises -

* the possession of passwords, access codes and similar data or devices, with the knowledge that such data was acquired unlawfully; and
* possession of passwords, access codes and similar data or devices, in regard to which there is a reasonable suspicion that it was acquired unlawfully where the possessor is unable to give a satisfactory exculpatory account of such possession.

4.2.2 <u>Offences committed or facilitated by means of data, computer programs and computer systems</u>

(a) Clause 8 aims to create a statutory offence of cyber fraud to specifically criminalise fraud by means of data or a computer program, or through the interference with data or a computer program.

(b) Clause 9 aims to create statutory offences of cyber forgery and uttering. The elements of the offence of cyber forgery are the making, with the intention to defraud, of false data or a false computer program, to the actual or potential prejudice of another person. The elements of the offence of cyber uttering are the passing off, with the intention to defraud, of false data or a false computer program, to the actual or potential prejudice of another person.

(c) Clause 10 aims to criminalise cyber extortion. The proscription is applicable where a person commits the offence of acquiring protected data, interference with data or a computer program, interference with a computer or computer system or the acquiring or use of a password, access code or related data or devices or threatens another person with the commission of such offences for the purpose of -

- obtaining any advantage from another person; or
- compelling another person to perform or to abstain from performing any act.

4.2.3 Aggravated offences

The objective of this category of offences is to protect essential computer systems and life, limb, property, essential services, the economy or the interests of the Republic, against criminal conduct in cyber space.

(a) In terms of clause 11(1), the offences of acquiring protected data, interfering with data, a computer program, computer data storage medium or a computer system which was committed against a restricted computer system are regarded as aggravated offences which are punishable with a fine or imprisonment of up to 15 years.

(b) In terms of clause 11(2), the offences of interfering with data, a computer program, computer data storage medium or a computer system, or cyber extortion which -

* endangers the life, or violates the physical integrity or physical freedom of, or causes bodily injury to, any person, or any number of persons;

* causes serious risk to the health or safety of the public or any segment of the public;
* causes the destruction of or substantial damage to any property;
* causes a serious interference with, or serious disruption of an essential service, facility or system, or the delivery of any essential service;
* causes any major economic loss; or
* creates a serious public emergency situation; or
* prejudices the security, the defence, law enforcement or international relations of the Republic,

are regarded as aggravated offences which are punishable with a sentence, as provided for in section 276 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), which that court considers appropriate and which is within that court's penal jurisdiction.

4.2.4 Clause 12 provides that the attempt, or conspiring with another person, or the aiding, abetting, inducing, inciting, instigating, instructing, commanding, or procuring of another person, to commit an offence as contemplated in Chapter 2 of the Bill amounts to an offence.

4.2.5 Clause 13 provides that the common law offence of theft must be interpreted so as to include the theft of an incorporeal.

4.2.6 Clause 14 deals with penalties and prescribes certain factors which must be taken into account as aggravating circumstances.

4.2.7 Clause 14 deals with competent verdicts where a person is charged with an offence provided for in Chapter 2.

4.3 ***Malicious communications (Chapter 3)***

4.3.1 This Chapter aims to criminalise a data message:

(a) Which incites the causing of any damage to any property belonging to, or violence against, a person or a group of persons. (clause 16)

(b) Which is harmful. A data message is considered harmful if -

* it threatens a person with -
  - damage to any property belonging to, or violence against, that person; or
  - 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;
* it 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;
* intimidates, encourages or harasses a person to harm himself or herself or any other person; or
* 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 (clause 17)

(c) Which is intimate in nature (person is nude), and which is distributed without the consent of the person involved.

4.3.2 Clause 19 provides for an interim protection order pending finalisation of criminal proceedings. In terms of the protection order a court may -

(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.

A person or electronic communications service provider who contravenes a protection order is guilty of an offence. Provision is made for interim proceedings

where the accused person can request the court to set aside or amend the protection order. The order of a court is subject to appeal or review.

4.3.3 Electronic communications service providers are compelled to assist a court during proceedings in terms of clause 19 to make available particulars of a person who distributed the malicious communications in order to ensure that the interim protection order can be served on him or her (clause 20).

4.3.4 Clause 21 provides for orders on completion of criminal proceedings, which includes a prohibition to further distribute, to destroy or to disable access to the malicious communication.

4.3.5 Clause 22 prescribes penalties which a court may impose in respect of malicious communications or offences provided for in terms of clauses 19, 20 or 21.

4.4 ***Jurisdiction (Chapter 4)***

In terms of clause 23, a court will have jurisdiction to try an offence contemplated in Chapter 2 or clauses 16, 17 and 18 if -

* the offence was committed in the Republic;
* 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;
* 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;
* 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.
* the offence was committed outside the Republic and the person to be charged -
    - is a citizen of the Republic;

- ordinarily is resident in the Republic;
- 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;
- is a company, incorporated or registered under any law, in the Republic; or
- is any body of persons, corporate or unincorporated, in the Republic; or

* the offence was committed outside the Republic by a person, other than a person provided in the previous paragraph and the offence affects or is intended to affect a public body, a business or any other person in the Republic and the person who committed the offence is found to be in the Republic.

The clause further provides that 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.

4.5 ***Powers to investigate, search and access or seize (Chapter 5)***

4.5.1 Clause 24 provides for the issuing of Standard Operating Procedures which must be followed in the investigation of cyber offences or offences which have a cyber element. The Standard Operating Procedures provides for the manner to deal with electronic evidence to maintain the integrity of evidence. This involves five principles namely -

* legality;
* no action taken should change data held on a computer or storage media which may subsequently be relied upon in court;
* persons should be competent to access and be able to give evidence explaining the relevance and the implications of their actions;
* an audit trail should be kept to enable an independent third party to examine those processes and arrive at the same result; and

* any deviation from these principles should be explained..

4.5.2 Clause 25 provides that 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.

4.5.3 In terms of clause 26, a police official may, in accordance with the provisions of this Chapter, search for, access or seize any article, within the Republic. An "article" is widely defined in terms of clause 1 as any data, computer program, computer data storage medium, or computer system which -

* is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission;
* may afford evidence of the commission or suspected commission; or
* is intended to be used or is, on reasonable grounds, believed to be intended to be used in the commission,

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, whether within the Republic or elsewhere.

4.5.4 Clause 27 provides that an article can only be searched for, accessed or seized by virtue of a search warrant issued by a judicial officer if it appears to the judicial officer, from information on oath or by way of affirmation that there are reasonable grounds for believing that an article is being used or is involved in the commission of an offence or is required as evidence at criminal proceedings. In terms of a warrant a police official may, amongst others -

* search for any article identified in the warrant to the extent as is set out in the warrant;
* access an article identified in the warrant to the extent as is set out in the warrant;
* seize an article identified in the warrant to the extent as is set out in the warrant; or

* 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 as is set out in the warrant.

Provision is also made that a search warrant 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. An “investigator” is defined in clause 1 as a person, who is not a member of the South African Police Service and who is identified and authorised in terms of a search warrant 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.

4.5.5 Clause 28 provides for oral applications for search warrants.

4.5.6 Clause 29 provides for search for, access to, or seizure of an article without a search warrant with the consent of a person who has lawful authority to consent.

4.5.7 Clause 30 provides that a police official may without a search warrant search any person or container or premises for the purposes of seizing a computer data storage medium or any part of a computer system involved in the commission of an offence, if the police official on reasonable grounds believes that a search warrant will be issued to him or her if he or she applies for such warrant and that the delay in obtaining such warrant would defeat the object of the search and seizure. A police official may only access or seize data in respect of the computer data storage medium or a computer system in terms of a search warrant. Provision is further made that a police official may if he or she on reasonable grounds believes that a search warrant will be issued to him or her if he or she applies for such warrant and it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances,

to make a written or oral application for a search warrant he or she may access the device and search for and seize data on such a device.

4.5.8 Clause 31 provides that a police official may without a warrant, as contemplated in section 40 of the Criminal Procedure Act, 1977, arrest any person who commits or whom he or she reasonably suspects of having committed any offence or against whom a reasonable complaint has been made or credible information has been received or a reasonable suspicion exists that the person has committed an offence, contemplated in Chapter 2 or section 16, 17 or 18 of the Bill 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. The clause further provides that on the arrest of such a person, or where any person is arrested in terms of a warrant issued in terms of section40 or section 43 of the Criminal Procedure Act, 1977, a police official may search the person and seize a computer data storage medium or any part of a computer system which is found in the possession of or in the custody or under the control of the person. A police official may, however, only access or seize data in respect of the computer data storage medium or a computer system in terms of a search warrant. Provision is further made that a police official may if he or she on reasonable grounds believes that a search warrant will be issued to him or her if he or she applies for such warrant and it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written or oral application for a search warrant to access the article and seize data, he or she may perform these actions without a search warrant.

4.5.9 Clause 32 imposes obligations on an electronic communications service provider, financial institution and other persons, who are in control of data, a computer program, a computer data storage medium or a computer system to provide technical assistance and other assistance to a police official who is

authorised in terms of a warrant to conduct an investigation, in order to search for, access and seize an article.

4.5.10 Clause 33 criminalises the obstruction or hindering of a police official or investigator to conduct an investigation in terms of this Chapter and authorises a police official to use such force as may be reasonably necessary to overcome any resistance.

4.5.11 Clause 34 provides that the powers to search, access and seize must be conducted with strict regard to decency and order and with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence.

4.5.12 Clause 35 criminalises wrongful -

* searches, access and seizures; and
* obtaining or using of 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.

The clause also regulates the retention of passwords, decryption keys, data or other information. The clause further provides for civil liability which may result from a contravention of the clause.

4.5.13 Clause 36 criminalises the giving of false information which results in -

* the issuing of a search warrant;
* a search and seizure in terms of the Bill; or
* the issuing of a preservation of data direction, a preservation of evidence direction or a disclosure of data direction.

The clause further provides for civil liability which may result from a contravention of the clause.

4.5.14 Clause 37 prohibits the disclosure of any information which a person has obtained in the exercise of his or her powers or the performance of his or her functions in terms of Chapter 5 or 6 of the Bill. The clause further regulates the

instances where the disclosure of information will not amount to a contravention of the clause.

4.5.15 Clause 38 clarifies the operation of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (RICA), *vis-à-vis* the Bill. In terms of the clause the interception of an indirect communication and obtaining of any real-time communication-related information on an ongoing basis, as it becomes available, must take place in terms of the RICA. Since not all electronic communications service providers are required in terms of a Government Notice No. 1325 of 2005, to be interceptable or to store communication-related information, specific obligations are imposed on these electronic communications service provider to -

(i) provide real-time communication-related information, on an ongoing basis, as it becomes available;
(ii) implement an expedited preservation of data direction;
(iii) implement a preservation of evidence direction; and
(iv) implement a disclosure of data direction;
(v) to provide archived communication-related information in respect of a customer that was stored by the electronic communications service provider; or
(vi) any order of the designated judge in terms of clause 46 of the Bill (which deals with mutual assistance (Chapter 6)).

4.5.16 Clause 39 provides for expedited preservation of data. In terms of this clause a specifically designated police official may 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 to preserve data which is on reasonable grounds believed to be involved in an offence provided for in Chapter 2 or clause 16, 17 or 18 of the Bill. In terms of the expedited preservation of data direction a person, electronic communications service provider or financial institution must, from the time of service of the direction and for a period of 21 days, preserve the data in order to

preserve the availability and integrity of the data. However, 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 clause 42 (disclosure of data direction). A person, electronic communications service provider or financial institution to whom an expedited preservation of data direction is addressed may apply to a magistrate 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. Non-compliance with a preservation of data direction is criminalised.

4.5.17 Clause 40 provides that a judicial officer may, on the written application of a police official 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, if it appears to the judicial officer 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 involved in the commission of an offence referred to in Chapter 2 or clause 16, 17 or 18 of the Bill. This is a procedure which is less invasive than seizure of an article and can be resorted to where it is not necessary to seize the article in question. In terms of a preservation of evidence direction a person, electronic communications service provider or financial institution must, for a time period specified in the direction (which may not exceed 90 days), preserve the article in question in order to preserve the availability of or integrity of the article. A person, electronic communications service provider or financial institution to whom a preservation of evidence direction is addressed may apply to a judicial officer 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. Non-compliance with the direction is criminalised. Clause 41 provides for the oral application for a preservation of evidence direction.

4.5.18 In terms of clause 42, where -

* an expedited preservation of data direction or a preservation of evidence direction is in place; or
* where it is otherwise expedient to obtain data without issuing a search warrant contemplated in clause 27,

a judicial officer may, on written application by a police official, if it appears to the judicial officer from information on oath that data which is relevant to an offence contemplated in Chapter 2 or clause 16, 17 or 18 is in possession of, is in control of, may be received by a person, electronic communications service provider or financial institution, issue a disclosure of data direction. Similar to clause 40, this is a procedure which can be resorted to where it is not necessary to utilize the more invasive procedure to seize the article in question. A person, electronic communications service provider or financial institution to whom a direction is addressed may apply to a judicial officer 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. Non-compliance with the direction is criminalised.

4.5.19 In terms of clause 43 a police official may -

* search for, access or seize publicly available data regardless of where the data is located geographically, without any specific authorisation; or
* receive non-public 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.

4.6 ***Mutual assistance (Chapter 6)***

4.6.1 The provisions of clauses 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, pending a request in terms of section 2 or 7 of the International Co-operation in Criminal Matters Act (clause 44).

4.6.2 In terms of clause 44, the National Commissioner of the South African Police Service may, after obtaining the written approval of the National Director of Public Prosecutions (NDPP) and on such conditions regarding confidentiality and limitation of use, forward any information obtained during any investigation to a law enforcement agency of a foreign State when the National Commissioner is of the opinion that the disclosure of such information may assist the foreign State in the initiation or carrying out of investigations regarding an offence committed within the jurisdiction of that foreign state or lead to further cooperation with a foreign State to carry out an investigation regarding cybercrimes or offences contemplated in clause 16, 17 or 18. The South African Police Service may similarly receive any information from a foreign state, subject to such conditions regarding confidentiality and limitation of use as may be agreed upon, which will assist the South African Police Service in the investigation of a cybercrime or offences contemplated in clause 16, 17 or 18.

4.6.3 Clauses 46 to 48 of the Bill deal with requests for assistance and cooperation received from a foreign State and provide as follows:

(a) In terms of clause 46, a mutual assistance request from a foreign State must in general be submitted to the 24/7 Point of Contact contemplated in Chapter 7 of the Bill. The 24/7 point of contact must submit the request to the NDPP for consideration. Upon receipt of a request, the NDPP must satisfy himself or herself that -

* proceedings have been instituted in the foreign State; or
* there are reasonable grounds for believing that an offence has been committed in the 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 foreign State;
* the offence in question is similar to those contemplated in Chapter 2 or section 16, 17 or 18 of the Bill or other offence recognised in South Africa; and

* the State intends to submit a request in terms of section 7 of the International Co-operation in Criminal Matters Act, for obtaining the data, communication or article in the Republic for use in such proceeding or investigation in the foreign State.

The NDPP 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. On receipt of the approval of the Cabinet Member, the request must be submitted to the designated judge for consideration. Where the request relates to the expedited disclosure of traffic data, the NDPP must submit the request for assistance, together with his or her recommendations, to the designated judge. The designated judge may issue any order which he or she deems appropriate to ensure that the requested -

* data or other article is preserved in accordance with clause 40;
* data is seized on an expedited basis in accordance with clause 27 and preserved;
* traffic data (which is data relating to a communication indicating the communication's origin, destination, route, format, time, date, size, duration or type of the underlying service), 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, is disclosed on an expedited basis in accordance with clause 42;
* data, which is a real-time communication-related information, is obtained and preserved; or
* data which is an indirect communication is intercepted and preserved,

as is specified in the request.

The designated judge may only issue an order if the facts alleged in the request -

* substantiate the fact that -
    - an offence substantially similar to the offences contemplated in Chapter 2 or section 16, 17 or 18 has been or is being or will probably be committed or 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

- it is necessary, in the interests of justice, to give the order;

* clearly identifies the person, electronic communications service provider or financial institution that will receive, is in possession of, or is in control of the data or other article that must be preserved, or from whose facilities the data or traffic data must be obtained or intercepted; the data or other article which must be preserved; the data which must be seized on an expedited basis; the traffic data which must be disclosed on an expedited basis; the data, which is real-time communication-related information, which is to be obtained; or the data, which is an indirect communication, which is to be intercepted;
* the request is, where applicable, in accordance with 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; and
* the order is in accordance with any applicable law of the Republic.

Where a request relates to the expedited disclosure of traffic data, the designated judge may -

* specify conditions or restrictions relating to the disclosure of traffic data as he or she deems appropriate; or
* refuse to issue an order if he disclosure of the traffic data will or is likely to prejudice the sovereignty, security, public safety, or other essential interests of the Republic.

In the case of urgency, a request by any authority, court or tribunal exercising jurisdiction in a foreign State may be submitted directly to the designated judge who must deal with the request in accordance with this clause.

An order contemplated by the designated judge must be executed by a specially designated police official, who must inform the designated judge and the NDPP, of the fact that an order has been executed. The NDPP must inform a foreign State of the fact that an order was issued and executed or not issued.

(b) Clause 47 imposes obligations on a person, electronic communications service provider or financial institution to comply with an order of the designated judge issued in terms of clause 46. A person, electronic communications service provider or financial institution 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. Non-compliance with an order of the designated judge or the giving of false information is criminalised.

(c) Clause 48 provides that the NDPP must inform the designated judge and a foreign State of the outcome of its request for assistance and cooperation. The clause further provides that any traffic data which is made available on an expedited basis, in terms of an order in terms of clause 46, must be provided to the 24/7 Point of Contact for submission to a foreign State.

4.6.4 Clause 49 deals with the requests for mutual assistance by South Africa to a foreign State. In terms of the clause if there is reasonable grounds for believing that an offence, contemplated in Chapter 2 or clause 16, 17 or 18, or 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 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 -

* preserve data or other articles;
* seize data or other articles on an expedited basis;
* disclose traffic data on an expedited basis;
* obtain data which is real-time communication-related information or archived communication-related information; or
* intercept data which is an indirect communication,

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

* that there are reasonable grounds for believing that an offence contemplated in the Bill has been committed in the Republic or that it is necessary to determine whether an offence has been committed;
* that an investigation in respect thereof is being conducted; and
* the nature of the mutual assistance that is required within the area of jurisdiction of a foreign State.

The NDPP is responsible for the transmission of the direction to the foreign State which is requested to provide assistance and cooperation.

4.7 ***24/7 Point of Contact (Chapter 7)***

Clause 50 provides for the establishment and functions of the 24/7 Point of Contact as part of the South African Police Service. 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, which includes -

* technical advice and assistance;
* anything which is authorised under Chapters 5 and 6;
* legal assistance;
* identification and location of an article;
* the identification and location of a suspect; and
* cooperation with appropriate authorities of a foreign State,

for the purpose of proceedings or investigations regarding the commission or intended commission of an offence under Chapter 2 or section 16, 17 or 18 or any other offence which may be committed or facilitated by means of an article within the Republic or in a foreign State.

The Cabinet member responsible for policing may make regulations to further regulate any aspect which is necessary or expedient for the proper implementation of this clause. The NDPP must make available members of the National Prosecuting Authority 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.

4.8 ***Evidence (Chapter 8)***

Clause 51 aims to regulate the proof of certain facts by affidavit. In terms of the clause, whenever any fact established by any examination or process requiring any skill in the interpretation of data; the design of, or functioning of data, a computer program, a computer data storage medium or a computer system; computer science; electronic communications networks and technology; software

engineering; or computer programming, is relevant to criminal proceedings, an affidavit made by a person who, in that affidavit, states 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;
* possesses relevant qualifications, expertise and experience which make him or her competent to make the affidavit; and
* has established such fact by means of an examination or process,

is, upon its mere production at such proceedings, prima facie proof of such fact. Any person who makes such an affidavit wilfully states anything which is false, is guilty of an offence. The clause further provides that any court before which an affidavit is produced as *prima facie* proof of the relevant contents thereof may, in its discretion, cause the person who made the affidavit 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. The clause also prescribes specific requirements which must be adhered to if the person who has made the affidavit alleges that he or she is in the service of a body in the Republic or foreign State designated by the Cabinet member responsible for the administration of justice.

4.9 ***Obligations of electronic communications service providers and financial institutions (Chapter 9)***

Clause 52 imposes obligations on electronic communications service providers and financial institutions who are aware of, or becomes aware of the fact that their computer systems are involved in the commission of any category or class of offences provided for in Chapter 2 which is determined by the Cabinet member responsible for policing, to report such offences to the South African Police Service and to preserve any information which may be of assistance to the South African Police Service to investigate such offences. Non-compliance with the clause is criminalised. The clause is not applicable to a financial sector regulator

or any function performed by the South African Reserve Bank in terms of section 10 of the South African Reserve Bank Act, 1989.

4.10 ***Structures to deal with cybersecurity (Chapter 10)***

4.10.1 Clause 53 establishes the Cyber Response Committee (CRC) as the overseeing body to implement the cyber initiative of the Republic. The CRC consists of a chairperson who is the Director-General: State Security and members who are the Heads of the representative Departments and one of their nominees. The Cabinet member responsible for State security must -

* oversee and exercise control over the performance of the functions of the CRC; and
* at the end of each financial year, submit a report to the Chairperson of the Joint Standing Committee on Intelligence, regarding progress that has been made towards achieving the objects and functions of the Cyber Response Committee.

4.10.2 Clause 54 deals with the establishment of structures which supports cybersecurity and capacity building. In terms of the clause:

* The Cabinet member responsible for State security must—
  - establish, equip, operate and maintain a Computer Security Incident Response Team for Government;
  - establish and maintain sufficient human and operational capacity to give effect to cybersecurity measures falling within the Constitutional mandate of the State Security Agency and to deal with critical information infrastructure protection.
* The Cabinet member responsible for policing must establish and maintain sufficient human and operational capacity to detect, prevent and investigate cybercrimes and ensure that members of the South African Police Service receive basic training in aspects relating to the detection, prevention and investigation of cybercrimes.

* The Cabinet member responsible for defence must establish and maintain a cyber offensive and defensive capacity as part of the defence mandate of the South African National Defence Force.
* The Cabinet member responsible for telecommunications and postal services must -
  - establish and maintain a Cybersecurity Hub as part of the Department of Telecommunications and Postal Services to promote cybersecurity in the private sector; and
  - encourage and facilitate the establishment of nodal points and private sector computer security incident response teams in the private sector.
* The clause further provides that the respective Cabinet members -
  - may make regulations to regulate any aspect which is necessary or expedient for the proper implementation of this subsection; and
  - must report to Parliament regarding progress that has been made towards achieving the objects and functions as is provided in the clause.

4.10.3 Clause 55 deals with the establishment of nodal points (structures which receive and distribute information regarding cybersecurity incidents) and the recognition of private sector computer security incident response teams (expert groups that handle cybersecurity incidents). In terms of the clause 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.

Each sector must, within 6 months from the date of the publication of a notice identify and establish a nodal point, which will be responsible for -

* distributing information regarding cyber incidents to other entities within the sector;
* receiving and distributing information about cybersecurity incidents to the nodal points established for other sectors or any computer security incident response team;

* reporting cybersecurity incidents to the Cybersecurity Hub; and
* receiving information about cybersecurity incidents from the Cybersecurity Hub.

If a sector fails to identify or establish a nodal point, the Cabinet member responsible for telecommunications and postal services may, after consultation with the sector, identify and establish a nodal point for that sector on such terms and conditions as he or she deems fit. The different sectors are responsible for the establishment and operating costs of nodal points. The clause empowers the Cabinet member to make regulations regarding the funding of nodal points and to further regulate any aspect relating to the establishment, operation or functioning of a nodal point. The clause further provides that the Cabinet member may recognise any computer security incident response team which is established for a sector and provide for the making of regulations to further facilitate the effective functioning of such a computer security incident response team.

4.10.4 Clause 56 empowers the Cabinet member responsible for the administration of justice to make regulations to regulate information sharing, for purposes of Chapter 10.

4.11 ***Critical information infrastructure protection (Chapter 11)***

4.11.1 Clause 57 deals with the protection of critical information infrastructures. In terms of the clause:

* The Cabinet member responsible for State security is empowered to declare information infrastructures which are of such a strategic nature that any interference with them or their loss, damage, disruption or immobilisation may -

- substantially prejudice the security, the defence, law enforcement or international relations of the Republic;
- substantially prejudice the health or safety of the public;
- cause a major interference with or disruption of, an essential service;
- cause any major economic loss;
- cause destabilisation of the economy of the Republic; or
- create a major public emergency situation,

as critical information infrastructures.

* The clause provides for an extensive consultation process with the various parties involved before an information infrastructure may be declared a critical information infrastructure.

* The Cabinet member responsible for State security must, within six months of the declaration of any information infrastructure as a critical information infrastructure, in consultation with the relevant Cabinet members (Cabinet members responsible for defence, telecommunications and postal services, justice and correctional services, policing and State security) and other specified persons, issue directives to the critical information infrastructure in order to regulate minimum standards relating to -

- the classification of data held by the critical information infrastructure;
- the protection of, the storing of, and archiving of data held by the critical information infrastructure;
- cybersecurity incident management by the critical information infrastructure;
- disaster contingency and recovery measures which must be put in place by the critical information infrastructure;
- minimum physical and technical security measures that must be implemented in order to protect the critical information infrastructure;
- the period within which the owner of, or person in control of a critical information infrastructure must comply with the directives; and
- any other relevant matter which is necessary or expedient in order to promote cybersecurity in respect of the critical information infrastructure.

The clause provides for a dispute mechanism, in terms of which an information infrastructure may dispute the decision by the Cabinet member responsible for State security to declare it a critical information infrastructure as well as the measures which the infrastructure needs to implement in terms of a direction which was issued to it.

* A critical information infrastructure must at own cost, take steps to the satisfaction of the Cabinet member responsible for State security, to comply with a directive. If a critical information infrastructure fails to comply with a direction, 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. A critical information infrastructure which without reasonable cause refuses or fails to take the steps specified in the notice within the period specified therein, is guilty of an offence. 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, and the Cabinet member may recover the costs of those steps from the owner or person on whose behalf they were taken.

4.11.2 Clause 58 provides for the auditing of critical information infrastructures to ensure compliance with a directive which is issued by the Cabinet member responsible for State security in terms of clause 57. In terms of the clause:

* The owner 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 directive. The critical information infrastructure must notify the Director-General: State Security of the date on which an audit is to be performed whereupon 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 the audit.

* The owner or person in control of a critical information infrastructure must, upon completion of the audit, report in the prescribed form and manner to the Director-General: State Security regarding the outcome of the audit in order to enable the Director-General to evaluate compliance with the directive.

* The failure to perform an audit or to comply with the various regulatory provisions of the clause is criminalised.

* 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 the clause.

4.12 ***Agreements with foreign states (Chapter 12)***

In terms of clause 59, the National Executive may enter into agreements with any foreign State regarding -

* mutual assistance and cooperation relating to the investigation and prosecution of offences contemplated in the Bill;
* research, information and technology-sharing and the development and exchange of information on cybersecurity-related matters;
* the establishment of 24/7 contact points; and
* the implementation of measures to address cyber threats.

4.13 ***General provisions (Chapter 13)***

4.13.1 In terms of clause 60, the NDPP is obliged to keep statistics of the number of prosecutions instituted in terms of Chapter 2 or clause 16, 17 or 18 of the Bill, 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. These statistics must be included in the report of the NDPP, referred to in section 22(4)(*g*) of the National Prosecuting Authority Act, 1998, and on the written request of the Chairperson of the CRC be made available to the CRC.

4.13.2 Clause 61 repeals or amends the following laws:

	Law	**Extent of repeal or amendment**
(a)	South African Police Service Act, 1995 (Act 68 of 1995)	Section 71, which criminalises conduct which is now criminalised in terms of the Bill, is deleted.
(b)	Criminal Procedure Act, 1977 (Act 51 of 1977)	Schedule 5 is amended to further regulate bail proceedings in respect of offences contemplated in - * clauses 8, 9 or 10 which exceed R500 000 or involve aggravating circumstances; or * clause 11(2).
(c)	Criminal Law Amendment Act, 1997 (Act 105 of 1997)	Part II of Schedule 2 is amended in order to make the minimum sentence regime applicable to the offences contemplated in - * clauses 8, 9 or 10 involving amounts of more than R500 000, or involve aggravating circumstances; or * clause 11(2).
(d)	National Prosecuting Authority	Sections 40A and 41(4), which criminalise

	Law	Extent of repeal or amendment
	Act, 1998 (Act 32 of 1998)	conduct which is criminalised in terms of the Bill, are deleted.
(e)	Correctional Services Act, 1998 (Act 111 of 1998)	Section 128, which criminalises conduct which is criminalised in terms of the Bill, is deleted.
(f)	Financial Intelligence Centre Act, 2001 (Act 38 of 2001)	Sections 65, 66 and 67, which criminalise conduct which is criminalised in terms of the Bill, are deleted.
(g)	Electronic Communications and Transactions Act, 2002 (Act 25 of 2002)	* The definitions of "critical data", "critical database" and "critical database administrator" (section 1) and Chapter IX, are deleted/ * Sections 85, 86, 87, 88 and 90, which criminalise conduct which is criminalised in terms of the Bill, are deleted and section 89 is substituted to effect consequential amendments.
(h)	Disaster Management Act, 2002 (Act 57 of 2002)	The definition of "disaster", in section 1 is substituted to include damage to or disruption of critical information infrastructure as contemplated in section 51(2) of the Bill.
(i)	Regulation of Interception of Communications and Provision of Communication related Information Act, 2002 (Act 70 of 2002)	(i) Section 17(4) is substituted to provide for the issuing of a direction for the provision of real-time communication-related information on an ongoing basis if it is necessary for purposes of investigating an offence contemplated in the newly inserted Schedule 2. (ii) The Schedule to the Act is renamed to "Schedule I" and the following items are added to the Schedule: * The 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). * The offence contemplated in - - clause 8, 9(1) or (2) or 10 of the Bill which involves an amount of R200 000 or more; and - 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 the Bill. (iii) A new Schedule II is included to further regulate the provision of real-time communication-related information on an ongoing basis in respect of offences contemplated in sections 3(1), 4(2), 5, 6, 7(1), 8, 9(1) or (2), 10 of the Bill, which involves an amount in excess of R50 000.

	Law	Extent of repeal or amendment
		(iv) A consequential amendment is affected to the definition of a "serious offence".
(j)	Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act 33 of 2004)	(i) A definition of "critical information infrastructure" is inserted in section 1. (ii) The definition of "terrorist activity" is amended to include "the destruction of or substantial damage to, or interference with, a critical information infrastructure or any part thereof". (iii) Section 3(2) is amended to expand the offence connected with a terrorist activity to the provision or offering of a "software or hardware tool as defined in clause 4(3)" of the Bill, connected with the engagement in a terrorist activity, and who knows or ought reasonably to have known or suspected that such "software or hardware tool" so connected.
(k)	Films and Publications Act, 1996 (Act 65 of 1996)	Section 24B of the Act, which deals with child pornography and the sexual exploitation of children, is repealed.
(l)	Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act 32 of 2007)	(i) The definition of "child pornography" is amended to extend its application to "presentations". (ii) A definition of "electronic communications service provider" is inserted in section 1. (iii) The proposed section 10A aims to criminalise the disclosure of pornography, threats to disclose pornography and disclosure or threats to disclose pornography for the purposes of obtaining any advantage from a person. The proposed amendments further provides for interim court orders and orders on completion of criminal proceedings to protect a victim against the offences in question. (iv) The proposed clause 19A aims to comprehensively criminalise child pornography and the sexual exploitation of children in line with international instruments. (v) The current section 20 is amended to criminalise conduct which relates to live performance involving child pornography and the recruiting of a child for purposes of creating, making or producing child pornography or participating in a live performance involving child

	Law	Extent of repeal or amendment
		pornography. (vi) Section 56A is amended to provide for penalties which a court may impose in respect of the proposed offences.
(m)	Child Justice Act, 2008 (Act 75 of 2008)	Schedules 2 and 3 are amended to provide for the sentencing of child offenders who commit cyber offences.

4.13.3 Clause 62 provides for the making of regulations to further regulate aspects provided for in the Bill.

4.13.4 Clause 63 deals with the Short Title and commencement.