JOBNAME: w/t 2916 PAGE: 1 SESS: 78 OUTPUT: Thu Nov 5 09:29:05 2020 SUM: 0C92C735
/first/Parliament−GJ/BillsandActs−2020/parl−bills−B6C−2017−GJ/B6C−2017−GJ

REPUBLIC OF SOUTH AFRICA

PORTFOLIO COMMITTEE ON JUSTICE AND CORRECTIONAL SERVICES PROPOSED AMENDMENTS TO THE

CYBERCRIMES BILL

[B 6B—2017]

(As agreed to by the Portfolio Committee on Justice and Correctional Services (National Assembly))

[B 6C—2017]

ISBN 978-1-4850-0660-2

No. of copies printed 100

PROPOSED AMENDMENTS AGREED TO

CYBERCRIMES BILL
[B 6B—2017]

CLAUSE 1

1. On page 5, from line 6, omit the definition of ôarticle'' and to **substitute**:

"article" means any—
(a) data;
(b) computer program;
(c) computer data storage medium; or
(d) computer system,
which—
(i) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission;
(ii) may afford evidence of the commission or suspected commission; or
(iii) is intended to be used or is, on reasonable grounds believed to be intended to be used in the commission or intended commission,
of—
(aa) an offence in terms of Part I and Part II of Chapter 2;
(bb) any other offence in terms of the law of the Republic; or
(cc) an offence in a foreign State that is substantially similar to an offence contemplated in Part I or Part II of Chapter 2 or another offence recognised in the Republic;

2. On page 5, in line 16, to omit " **"Companies Act, 2008"** means the Companies Act, 2008 (Act No. 71 of 2008);''.

3. On page 5, after line 36, to insert:

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

4. On page 5, after line 50, to insert:

"Electronic Communications Act, 2005" means the Electronic Communications Act, 2005 (Act No. 36 of 2005);

5. On page 5, from line 51, to omit the definition of **"electronic communications identity number**''.

6. On page 5, after line 57, to insert:

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

7. On page 5 before line 58, to insert:

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

8. On page 5, from line 58, to omit the definition of "**electronic communications service provider"**, and to substitute:

> **"electronic communications service provider"** means—
> *(a)* any person who provides an electronic communications service to the public, sections of the public, the State, or the subscribers to such service, under and in accordance with an electronic communications service licence issued to that person in terms of the Electronic Communications Act, 2005, or who is deemed to be licenced or exempted from being licenced as such in terms of that Act; and
> *(b)* a person who has lawful authority to control the operation or use of a private electronic communications network used primarily for providing electronic communications services for the owner's own use and which is exempted from being licensed in terms of the Electronic Communications Act, 2005;

9. On page 6, in line 12, to omit "**"Labour Relations Act, 1995"** means the Labour Relations Act, 1995 (Act No. 66 of 1995);".

10. On page 6, in line 19, after "Constitution" to omit "of the Republic of South Africa, 1996".

11. On page 6, in line 21, after "Constitution" to omit "of the Republic of South Africa, 1996".

12. On page 6, in line 23, to omit "**"National Environmental Management Act, 1998"** means the National Environmental Management Act, 1998 (Act No. 107 of 1998);".

13. On page 6, in line 26, after "1995" to omit "(Act No. 68 of 1995)".

14. On page 6, in line 39, after "1995" to omit "(Act No. 68 of 1995)".

15. On page 6, in line 40, to omit "**"Prevention and Combating of Corrupt Activities Act, 2004"** means the Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004);".

16. On page 6, in line 44, to omit "**"Protected Disclosures Act, 2000"** means the Protected Disclosures Act, 2000 (Act No. 26 of 2002);".

17. On page 6, after line 55, to insert:

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

18. On page 6, before line 56, to insert:

> **"South African Police Service Act, 1995"** means the South African Police Service Act, 1995 (Act No. 68 of 1995);

19. On page 6, in line 57, after "Constitution" to omit "of the Republic of South Africa, 1996".

20. On page 6, from line 61, to omit the definition for ''specifically designated police official'', and to substitute:

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

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

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

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

21. On page 7, from line 13, to omit sub-clause (2) and to substitute:

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

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

(b) section 72; or

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

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

CLAUSE 2

1. On page 7, from line 26, to omit clause 2, and to substitute:

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

(a) in respect of a computer system; or

(b) a computer data storage medium,

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

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

(b) For purposes of paragraph *(a)*—

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

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

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

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

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

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

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

(c) For purposes of paragraph *(b)*—

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

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

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

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

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

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

(bb) obtains the output of data.

CLAUSE 3

1. On page 8, from line 8, to omit sub-clauses (2) and (3), and to substitute:

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

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

CLAUSE 4

1. On page 8, in line 29, after ‘‘2(1)’’, to insert ‘‘or (2)’’.

2. On page 8, in line 34, after ‘‘2(1)’’, to insert ‘‘or (2)’’.

CLAUSE 5

1. On page 8, after line 54, to insert ‘‘held in a computer system or a computer data storage medium.’’.

CLAUSE 6

1. On page 9, from line 4, to omit sub-clause (2), and to substitute:

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

(a) alter any resource ; or

(b) interrupt or impair—

(i) the functioning;

(ii) the confidentiality;

(iii) the integrity; or

(iv) the availability,

of a computer data storage medium or a computer system.

CLAUSE 7

1. On page 9, in line 21, after ‘‘2(1)’’, to insert ‘‘or (2)’’.

2. On page 9, in line 29, after ‘‘2(1)’’, to insert ‘‘or (2)’’.

3. On page 9, from line 32, to omit sub-clause (3), and to substitute:

(3) For purposes of this section **"password, access code or similar data or device"** includes—
(a) a secret code or pin;
(b) an image;
(c) a security token;
(d) an access card;
(e) any device;
(f) biometric data; or
(g) a word or a string of characters or numbers,
used for financial transactions or user-authentication in order to access or use data, a computer program, a computer data storage medium or a computer system.

CLAUSE 8

1. On page 9, from line 46, to omit clause 8, and to substitute:

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 section 5(2)*(a)*, *(b)* or (e) or interference with a computer data storage medium or a computer system as contemplated in section 6(2)*(a)*,
which causes actual or potential prejudice to another person, is guilty of the offence of cyber fraud.

CLAUSE 10

1. On page 10, from line 13, to omit clause 10, and to substitute:

10. Any person who unlawfully and intentionally commits or threatens to commit any offence as contemplated in sections 3(1), 5(1), 6(1) or 7(1)*(a)* or *(d)*, for the purpose of—
(a) obtaining any advantage from another person; or
(b) compelling another person to perform or to abstain from performing any act,
is guilty of the offence of cyber extortion.

CLAUSE 11

1. On page 10, from line 21, to omit clause 11, and to substitute:

11. (1) *(a)* Any person who commits an offence referred to in—
(i) section 3(1), 5(1) or 6(1), in respect of; or
(ii) section 7(1), in so far as the passwords, access codes or similar data and devices relate to,
a restricted computer system, and who knows or ought reasonably to have known or suspected that it is a restricted computer system, is guilty of an aggravated offence.
(b) For purposes of paragraph *(a)* a **"restricted computer system"** means any data, computer program, computer data storage medium or computer system—
(i) under the control of, or exclusively used by—
(aa) a financial institution; or
(bb) an organ of state as set out in section 239 of the Constitution, including a court; and

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

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

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

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

(c) create a serious public emergency situation,

is guilty of an aggravated offence.

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

CLAUSE 13

1. On page 11, in line 3, to omit ''In this Part II'', to insert ''In Part II''.

2. On page 11, after line 4, to insert:

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

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

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

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

CLAUSE 14

1. On page 11, from line 13, to omit clause 14, and to substitute:

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

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

(b) violence against,

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

CLAUSE 15

1. On page 11, from line 20, to omit clause 15, and to substitute:

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

(a) threatens a person with—

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

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

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

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

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

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

CLAUSE 16

1. On page 11, in line 38, to omit ''Distribution'', to insert ''Disclosure''.

2. On page 11, from line 39, to omit clause 16, and to substitute:

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

(2) For purposes of subsection (1)—

(a) **"B"** means—

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

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

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

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

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

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

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

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

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

(bb) amounts to sexual exploitation.

CLAUSE 18

1. On page 12, from line 27, to omit sub-clause (2), and to substitute:

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

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

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

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

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

2. On page 12, in line 36, after "2(1)", to insert "or (2)".

3. On page 12, in line 43, after "2(1)", to insert "or (2)".

4. On page 12, from line 48, to omit sub-clause (5), and to substitute:

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

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

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

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

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

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

5. On page 13, in line 5, after "2(1)", to insert "or (2)".

6. On page 13, in line 33, after "2(1)", to insert "or (2)".

7. On page 13, in line 41, after "but", to omit "a".

8. On page 13, in line 42, after "2(1)", to insert "or (2)".

CLAUSE 19

1. On page 13, in line 58, after "2(1)", to insert "or (2)".

2. On page 14, from line 22, to omit sub-clause (6), and to substitute:

(6) *(a)* If a person is convicted of any offence provided for in section 2(1) or (2), 3(1), 5(1), 6(1), 7(1), 8, 9(1) or (2), 10 or 11(1) or (2), a court imposing any sentence in terms of those sections must, unless substantial and compelling circumstances justify the imposition of another sentence, impose a period of direct imprisonment, with or without a fine, if the offence was committed—

(i) by the person; or

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

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

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

CLAUSE 20

1. On page 14, from line 40, to omit clause 20, and to substitute:

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

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

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

(2) The court must as soon as it reasonably possible consider an application submitted to it in terms of subsection (1) and may, for that purpose, consider any additional evidence it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings.

(3) If the court is satisfied that there is—

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

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

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

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

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

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

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

(7) *(a)* The court must as soon as reasonably possible consider an application submitted to it in terms of subsection (6) and may for that purpose, consider such additional evidence as it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings.

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

(8) The court may, for purposes of subsection (2) and (7), in the prescribed form and manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or

object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case.

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

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

(a) attend or to remain in attendance;

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

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

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

is guilty of an offence.

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

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

CLAUSE 21

1. On page 15, from line 33, to omit clause 21, and to substitute:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) must consider the application;

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

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

(d) must inform the electronic communications service provider in the prescribed form and 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 which contains the information referred to in subsection (1)*(b)*, consider the issuing of a protection order in terms of section 20(3) against the person or electronic communications service provider on the date to which the proceedings have been adjourned.

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

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

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

(a) fails to furnish the required information within five ordinary court days from the time that the direction is served on such

electronic communications service provider to a court in terms of subsection (3)*(a)* or such extended period allowed by the court in terms of subsection (3)*(b)*; or

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

is guilty of an offence.

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

CLAUSE 22

1. On page 16, from line 49, to omit clause 22, and to substitute:

22. (1) Whenever a person is—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) attend or to remain in attendance;

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

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

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

is guilty of an offence.

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

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

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

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

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

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

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

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

CLAUSE 23

1. On page 17, from line 31, to omit clause 23, and to substitute:

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

CLAUSE 24

1. On page 17, from line 38, to omit clause 24 and to substitute:

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

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

(b) the person to be charged is—

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

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

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

(c) the offence was committed—

(i) in the territory of the Republic; or

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

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

(i) in the territory of the Republic; or

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

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

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

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

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

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

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

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

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

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

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

(b) that person—

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

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

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

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

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

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

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

(5) The National Commissioner and the National Head of the Directorate, in consultation with the National Director of Public Prosecutions, must issue directives, with which all police officials

must comply in the execution of their functions in terms of this Act regarding the investigation of offences that were committed outside the Republic.

CLAUSE 25

1. On page 18, from line 47, to omit the definition of ''access'', and to substitute:

''**access**'' includes without limitation to make use of—
(a) a computer data storage medium, or a computer system, or their accessories or components or any part thereof or any ancillary device or component thereto; and
(b) data or a computer program held in a computer data storage medium or a computer system,
to the extent necessary to search for and seize an article.

CLAUSE 26

1. On page 19, from line 6, to omit sub-clause (1), and to substitute:

(1) The Cabinet member responsible for policing, in consultation with the National Commissioner, the National Head of the Directorate, the National Director of Public Prosecutions and the Cabinet member responsible for the administration of justice must, after following a process of public consultation, within 12 months of the commencement of this Chapter, issue Standard Operating Procedures which must be observed by—
(a) the South African Police Service; or
(b) any other person or agency who or which is authorised in terms of the provision of any other law to investigate any offence in terms of any law,
in the investigation of any offence or suspected offence in terms of Part I or Part II of Chapter 2 or any other offence or suspected offence which may be committed by means of or facilitated through the use of an article.

CLAUSE 29

1. On page 19, in line 36, to omit ''his or her'', to insert ''their''.

2. On page 19, in line 39, to omit ''his or her'', to insert ''their''.

3. On page 19, in line 41, after ''involved'', to insert ''or has been used or was involved''.

4. On page 19, in line 47, after ''access'', to omit ''and''.

5. On page 19, in line 47, before ''seize'', to insert ''or'',

6. On page 20, in line 6 to omit ''of''.

CLAUSE 30

1. On page 20, from line 46, to omit ''him or her'', to insert ''them''.

2. On page 20, in line 57, to omit ''his or her'', to insert ''their''.

3. On page 20, in line 59, after ''involved'', to insert ''or has been used or was involved''.

4. On page 21, from line 14 to omit sub-clause (6), and to substitute:

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

5. On page 21, from line 19, to omit sub-clause 17, and to substitute:

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

CLAUSE 31

1. On page 21, in line 30, to omit ''him or her'', to insert ''them''.

CLAUSE 32

1. On page 21, in line 38, after ''in'', to insert ''paragraph *(c)* or *(d)* of''.

2. On page 21, in line 40, to omit ''him or her'', to insert ''them''.

3. On page 21, from line 40, to omit ''he or she applies'', to insert ''they apply''.

4. On page 21, in line 47, to omit ''.'' to insert:

: Provided that a police official may, if they on reasonable grounds believe—

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

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

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

CLAUSE 33

1. On page 21, from line 52, to omit sub-clause (1), and to substitute:

(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 Part I or Part II of Chapter 2 in their presence;

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

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

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

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

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

2. On page 22, in line 13, after ''in'', to insert ''paragraph *(c)* or *(d)* of''.

3. On page 22, in line 14, after '' ''article'', close quotation marks.

4. On page 22, in line 19, to omit ''.'', to insert:

: Provided that a police official may, if they on reasonable grounds believe—

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

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

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

CLAUSE 35

1. On page 22, in line 39, to omit ''his or her'', to insert ''their''.

2. On page 22, from line 39, to omit ''his or her'', to insert ''their''.

3. On page 22m from line 44, to omit ''him or her'', to insert ''them''.

4. On page 22, in line 50, to omit ''he or she has'', to insert ''they have''.

5. On page 22, in line 51, to omit ''has'', to insert ''have''.

6. On page 22, in line 51, to omit ''his or her'', to insert ''their''.

CLAUSE 37

1. On page 23, in line 21, after ''computer'', to insert ''system''.

CLAUSE 39

1. On page 24, in line 27, to omit ''he, she or it has'', to insert ''they have''.

2. On page 24, in line 27, to omit ''his, her or its'', to insert ''their''.

3. On page 24, in line 28, to omit ''his or her'', to insert ''their''.

4. On page 24, from line 29, to omit ''his or her'' and to insert ''their''.

5. On page 24, in line 31, to omit ''he or she is' and to insert ''they are''.

6. On page 24, in line 32 to omit ''his or her'' and to insert ''their''.

7. On page 24, from line 45, to omit sub-clause (2), and to substitute:

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

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

(b) reveals a criminal activity.

CLAUSE 40

1. On page 25, in line 3, to omit ''data which is''.

2. On page 25, in line 34, after ''was'', to insert ''preserved or otherwise''.

3. On page 25, in line 39, before ''furnish'', to insert ''obtain and''.

4. On page 25, from line 40, to omit sub-clause (4), and to substitute:

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

CLAUSE 41

1. On page 25, from line 47, to omit sub-clause (1), and to substitute:

(1) A specifically designated police official may—

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

(i) in possession of;

(ii) to receive; or

(iii) in control of,

data as contemplated in paragraph *(a)* of the definition of ''article''; and

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

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

2. On page 26, in line 16, after ''data'', to insert ''which''.

3. On page 26, in line17, to omit ''which''.

4. On page 26, in line19, to omit ''which''.

5. On page 26, in line 46, to omit ''he, she or it'' and to insert ''they''.

CLAUSE 42

1. On page 27, from line 2, to omit sub-clause (1), and to substitute:

(1) A magistrate or judge of the High Court, may—
(a) upon written application by a police official;
(b) if it appears to the magistrate or judge upon consideration of the information provided under oath or by way of affirmation, as set out in the application, that there are reasonable grounds to believe that any person, electronic communications service provider or financial institution—
(i) may receive;
(ii) is in possession of; or
(iii) is in control of,
an article; and
(c) with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence in question,
issue a preservation of evidence direction.

2. On page 27, in line 44, to omit "he, she or it", to insert "they".

3. On page 27, in line 45, to omit "order", to insert "direction".

CLAUSE 43

1. On page 27, from line 53, to omit sub-clause (1), and to substitute:

(1) A police official may orally make an application referred to in section 42(1), if they are of the opinion that it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application.

2. On page 28, from line 4, to omit sub-clause (3), and to substitute:

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

3. On page 28, from line 26, to omit sub-clause (6), and to substitute:

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

CLAUSE 44

1. On page 28, from line 31, to omit clause 44, and to substitute:

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

44. (1) *(a)* A police official may, where it is expedient, other than by way of a search and seizure in terms of a warrant contemplated in section 29(1), to obtain—
(i) data which is subject to preservation in terms of an expedited preservation of data direction or a preservation of evidence direction; or

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

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

(bb) available to a computer system,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) there are reasonable grounds for believing that—

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

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

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

(bb) available to a computer system,

within their area of jurisdiction; and

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

issue the disclosure of data direction applied for.

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

(4) The disclosure of data direction—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CLAUSE 45

1. On page 30, in line 9, to omit ''he or she deems'', to insert ''they deem''.

CLAUSE 47

1. On page 30, in line 29, to omit ''he or she'', to insert ''they''.

CLAUSE 48

1. On page 31, in line 12, to omit ''(7)'', to insert ''(9)''.

2. On page 31, from line 34, to omit sub-clauses (4), (5), (6), (7) and (8), and to substitute:

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

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

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

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

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

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

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

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

(e) indirect communications are intercepted and preserved,

as is specified in the request.

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

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

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

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

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

(b) the request clearly identifies—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. On page 32, from line 40, to omit sub-clause (10)*(a)*, and to substitute:

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

CLAUSE 50

1. On page 33, in line 16, after ''data'', to omit ''which is''.

2. On page 33, in line 19, to omit ''in''.

3. On page 33, from line 26, to omit sub-clause (3), and to substitute:

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

CLAUSE 51

1. On page 33, from line 54, to omit ''this Act'', to insert ''subsection (1)*(a)* or *(b)*''.

2. On page 33, in line 56, after ''whether'', to insert ''such''.

CLAUSE 52

1. On page 34, in line 40, to omit ''or'', to insert ''and''.

CLAUSE 53

1. On page 35, from line 12, to omit sub-clause (1), and to substitute:

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

(a) the interpretation of data;

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

(c) computer science;

(d) electronic communications networks and technology;

(e) software engineering; or

(f) computer programming,

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

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

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

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

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

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

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

2. On page 35, from line 50, to omit ''he or she is'', to insert ''they are''.

3. On page 35, in line 53, after ''unless'', to insert ''it is''.

4. On page 35, in line 54, to omit ''it is''.

5. On page 35, in line 56, to omit ''it is''.

CLAUSE 54

1. On page 36, in line 18, to omit ''computer system'', to insert ''electronic communications service or electronic communications network''.

CLAUSE 55

1. On page 37, in line 8, to omit ''Services'', to insert ''Service''.

CLAUSE 59

1. On page 38, from line 2, to omit sub-clause (1), and to substitute:

(1) The Cabinet member responsible for the administration of justice—

(a) must make regulations to prescribe the—

(i) form and manner of the application as contemplated in section 20(1);

(ii) form of the order as contemplated in section 20(3);

(iii) manner of serving the order as contemplated in section 20(4);

(iv) form and manner of the application as contemplated in section 20(6);

(v) manner in which the court may subpoena a person as contemplated in section 20(8);

(vi) form of the direction and affidavit and manner to furnish information to a court as contemplated in section 21(1)*(b)*;

(vii) manner of serving a direction as contemplated in section 21(2);

(viii) manner and the form of the affidavit to apply for an extension of the time period or cancellation of the direction as contemplated in section 21(3)*(b)*;

(ix) manner for requesting additional information as contemplated in section 21(4)*(b)*;

(x) form and manner of informing an electronic communications service provider of the outcome of application as contemplated in section 21(4)*(d)*;

(xi) tariffs of compensation payable to an electronic communications service provider as contemplated in section 21(6);

(xii) form of the order and manner of service of the order as contemplated in section 22(3);

(xiii) form and manner of the application as contemplated in section 22(5);

(xiv) form and manner in which the court may subpoena a person as contemplated in section 22(7);

(xv) the form of the expedited preservation of data direction and manner of service as contemplated in section 41(3);

(xvi) form and manner for the making of an application as contemplated in section 41(7);

(xvii) form of the preservation of evidence direction and manner of service as contemplated in section 42(2);

(xviii) form and manner for an application to set aside a preservation of evidence direction as contemplated in section 42(5);

(xix) form of the disclosure of data direction and manner of service as contemplated in section 44(3);

(xx) form and manner of an application for the amendment or setting aside of a disclosure of data direction as contemplated in section 44(5);

(xxi) form of the affidavit as contemplated in section 44(7)*(b)*;

(xxii) manner in which traffic data must be submitted to the designated Point of Contact as contemplated in section 50(2);

(xxiii) form of the affidavit as contemplated in section 50(2)*(b)*(ii); and

(xxiv) form of the direction as contemplated in section 51(1); and

(b) may make regulations which are not inconsistent with this Act or any other law to prescribe any matter which in terms of this Act may be prescribed or which may be necessary or expedient to prescribe in order to achieve or promote the objects of this Act.

CLAUSE 60

1. On page 38, in line 56, to omit ‘‘2019’’, to insert ‘‘2020’’.

SCHEDULE

1, From page 39 to omit the ''Schedule'', and to substitute:

Schedule

(Section 58)

LAWS REPEALED OR AMENDED

Number and year of law	**Short title**	**Extent of repeal or amendment**
Act No. 51 of 1977	Criminal Procedure Act, 1977	The addition of the following items to Schedule 5: ''A contravention of section 8, 9 or 10 of the Cybercrimes Act, 2020— *(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 of another person in respect of which the offences in question were committed; or (iii) by any law enforcement officer— *(aa)* involving amounts of more than R10 000; or *(bb)* as a member of a group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; or *(cc)* with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offences in question were committed.

Number and year of law	Short title	Extent of repeal or amendment
		A contravention of section 11(2) of the Cybercrimes Act, 2020.''.
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 section 8, 9 or 10 of the Cybercrimes Act, 2020— *(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 of another person in respect of which the offences in question were committed; or (iii) if it is proven that the offence was committed by any law enforcement officer— *(aa)* involving amounts of more than R10 000; or *(bb)* as a member of a group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; or *(cc)* with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offences in question were committed.''.

Number 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 deletion of sections 85, 86, 87 and 88. *(b)* 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. 70 of 2002	Regulation of Interception of Communications and Provision of Communication related Information Act, 2002	*(a)* The amendment of section 1 by the substitution for paragraph *(a)* of the definition of ''serious offence'' of the following paragraph: "*(a)* offence mentioned in **[the]** Schedule 1; or''. *(b)* The amendment of section 4 by the addition of the following subsection: ''(3) Notwithstanding subsection (2), a law enforcement officer or a person who is authorised in terms of the Criminal Procedure Act, 1977, the Cybercrimes Act, 2020, or any other law to engage or to apprehend a suspect or to enter premises in respect of the commission or suspected commission of any offence, may during the apprehension of the suspect or during the time that he or she is lawfully on the premises, record what he or she observes or hears if— *(a)* the recording relates directly to the purpose for which the suspect was apprehended or the law enforcement officer or person entered the premises; and *(b)* the law enforcement officer or person has— (i) identified himself or herself as such; and

Number and year of law	Short title	Extent of repeal or amendment
		(ii) verbally informed any person concerned that his or her direct communications are to be recorded, before such recording is made.''. *(c)* The substitution for subsection (4) of section 17 of the following subsection: ''(4) A real-time communication-related direction may only be issued if it appears to the designated judge concerned, on the facts alleged in the application concerned, that there are reasonable grounds to believe that— *(a)* a serious offence or an offence mentioned in Schedule II has been or is being or will probably be committed; *(b)* the gathering of information concerning an actual threat to the 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.''.

Number and year of law	Short title	Extent of repeal or amendment
		(d) The substitution for subsection (4) of section 19 of the following subsection: "(4) An archived communication-related direction may only be issued if it appears to the judge of a High Court, regional court magistrate or magistrate concerned, on the facts alleged in the application concerned, that there are reasonable grounds to believe that— *(a)* a serious offence 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 archived communication-related information is necessary for purposes of investigating such offence or gathering such information.". *(e)* The renaming of the Schedule to the Act as "Schedule I" and the addition of the following items:

Number and year of law	Short title	Extent of repeal or amendment
		"15 Any offence contemplated in section 17, 18, 19A or 20 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act No. 32 of 2007). 16 Any offence contemplated in— *(a)* section 8, 9(1) or (2) or 10 which involves an amount of R200 000, 00 or more; or *(b)* section 11(1) or (2) or 17 (in so far as the section relates to the offences referred to in section 11(1) or (2)), of the Cybercrimes Act, 2020.". *(f)* The addition of the following Schedule after Schedule I: "**Schedule II** 1 Any offence referred to in— *(a)* sections 3(1), 5, 6, 7(1), 8, 9(1) or (2), or 10; or *(b)* section 17 (in so far as the section relates to the offences referred to in paragraph *(a)*), of the Cybercrimes Act, 2020, which involves an amount of R50 000, 00 or more. 2 Any offence which is substantially similar to an offence referred to in item 1 which is or was committed in a foreign State, which involves an amount of R50 000, 00 or more.".
Act 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 insertion of the following Part and items after item 11: "***Part 3A*** *Persons 18 years or older: Harmful disclosure of pornography and orders to protect complainant against the harmful effects of disclosure of pornography* 11A Harmful disclosure of pornography 11B Orders to protect complainant against harmful disclosure of pornography pending finalisation of criminal proceedings 11C Electronic communications service provider to furnish particulars to court 11D Orders on finalisation of criminal proceedings"; (ii) the substitution for the heading to Part 2 of Chapter 3 of the following heading:

Number and year of law	Short title	Extent of repeal or amendment
		"*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 (iii) the insertion after item 19 of the following item: "19A. Offences relating to child pornography". *(b)* The amendment of section 1— (i) by the insertion, after the definition of "Director of Public Prosecutions" of the following definition: "'**disclose**' and **'disclosure'**, in relation to the harmful disclosure of pornography contemplated in section 11A, includes— *(a)* to send the pornography to a person who is the intended recipient of the electronic communication or any other person; *(b)* to store the pornography on an electronic communications network, where the pornography can be viewed, copied or downloaded; or *(c)* to send or otherwise make available to a person, a link to the pornography that has been stored on an electronic communication network, where the pornography can be viewed, copied or downloaded; **'Electronic Communications Act'** means the Electronic Communications Act, 2005 (Act No. 36 of 2005); **'electronic communications identity number'** means a technical identification label which represents the origin or destination of electronic communications traffic; **'electronic communications network'** means an 'electronic communications network' as defined in section 1 of the Electronic Communications Act, 2005, and includes a computer system;

Number and year of law	Short title	Extent of repeal or amendment
		‘**electronic communications service**’ means any service which consists wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services as defined in section 1 of the Electronic Communications Act, 2005; **‘electronic communications service provider**’ means— *(a)* any person who provides an electronic communications service to the public, sections of the public, the State, or the subscribers to such service, under and in accordance with an electronic communications service licence issued to that person in terms of the Electronic Communications Act, 2005, or who is deemed to be licensed or exempted from being licensed as such in terms of that Act; and *(b)* a person who has lawful authority to control the operation or use of a private electronic communications network used primarily for providing electronic communications services for the owner’s own use and which is exempted from being licensed in terms of the Electronic Communications Act, 2005;’’; and (ii) by the insertion, after the definition of ‘‘genital organs’’ of the following definitions: ‘‘**‘host’** means to store information on an electronic communications network that is used to provide an electronic communications service, where it can be viewed, copied or downloaded; **‘live performance involving child pornography’** means an event where a child is used to create, make or produce child pornography;’’.

Number and year of law	Short title	Extent of repeal or amendment
		(c) The following Part and sections are hereby inserted in Chapter 2 after section 11: "***Part 3A*** ***Persons 18 years or older: Harmful disclosure of pornography and orders to protect complainant against the harmful effects of disclosure of pornography*** **Harmful disclosure of pornography** **11A.** (1) A person ("A") who unlawfully and intentionally discloses or causes the disclosure of pornography in which a person ("B") appears or is described and such disclosure— *(a)* takes place without the consent of B; and *(b)* causes any harm, including mental, psychological, physical, social or economic harm, to B or any member of the family of B or any other person in a close relationship to B, is guilty of the offence of harmful disclosure of pornography. (2) A person ("A") who unlawfully and intentionally threatens to disclose or threatens to cause the disclosure of pornography referred to in subsection (1) and such threat causes, or such disclosure could reasonably be expected to cause, any harm referred to in subsection (1)(*b*), is guilty of the offence of threatening to disclose pornography that will cause harm. (3) A person ("A") who unlawfully and intentionally threatens to disclose or threatens to cause the disclosure of pornography referred to in subsection (1), for the purposes of obtaining any advantage from B or any member of the family of B or any other person in a close relationship to B, is guilty of the offence of harmful disclosure of pornography related extortion.

Number and year of law	Short title	Extent of repeal or amendment
		Orders to protect complainant against harmful disclosure of pornography pending finalisation of criminal proceedings **11B.** (1) A complainant (hereinafter referred to as the applicant) who lays a charge with the South African Police Service that an offence contemplated in section 11A(1), (2) or (3) has allegedly been committed against him or her, may on an *ex parte basis* in the prescribed form and manner, apply to a magistrate's court for a protection order pending the finalisation of the criminal proceedings to— *(a)* prohibit any person to disclose, or cause the disclosure or threaten the applicant with the disclosure or causing the disclosure of pornography which relates to the charge; or *(b)* order an electronic communications service provider whose electronic communications service is used to host or disclose the pornography which relates to the charge, to remove or disable access to such pornography. (2) The court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (1) and may, for that purpose consider any additional evidence it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings. (3) If the court is satisfied that there is — *(a)* *prima facie* evidence that an offence referred to in section 11A(1), (2) or (3), has allegedly been committed against the applicant; and *(b)* reasonable grounds to believe that a person referred to in subsection (1)(*a*), disclosed or caused the disclosure or threatened the applicant with the disclosure or causing the disclosure of such pornography; or *(c)* reasonable grounds to believe that the electronic communications service of the electronic communications service provider is used to host or disclose such pornography, the court may, subject to such conditions as the court may deem fit, issue the order referred to in subsection (1), in the prescribed form.

Number and year of law	Short title	Extent of repeal or amendment
		(4) The order, referred to in subsection (3), must be served on the person referred to in subsection (1)(*a*) or electronic communications service provider, referred to in subsection (1)(*b*), in the prescribed manner: Provided, that if the court is satisfied that the order cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form or manner specified in that order. (5) An order referred to in subsection (3) is of force and effect from the time it is issued by the court and the existence thereof has been brought to the attention of the person referred to in subsection (1)(*a*) or electronic communications service provider referred to in subsection (1)(*b*). (6) A person referred to in subsection (1)(*a*), other than the person who is accused of having committed the offence in question, or an electronic communications service provider, referred to in subsection (1)(*b*) may, within 14 days after the order has been served on him, her or it in terms of subsection (4) or within such further period as the court may allow, upon notice to the magistrate's court concerned, in the prescribed form and manner, apply to the court for the setting aside or amendment of the order referred to in subsection (3). (7) *(a)* The court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (6) and may for that purpose, consider such additional evidence as it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings. *(b)* The court may if good cause has been shown for the variation or setting aside of the protection order, issue an order to this effect. (8) The court may, for purposes of subsections (2) and (7), in the prescribed form and manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case.

Number and year of law	Short title	Extent of repeal or amendment
		(9) A person referred to in subsection (1)(*a*) or electronic communications service provider, referred to in subsection (1)(*b*), that fails to comply with an order referred to in subsection (3) or any variation thereof, is guilty of an offence. (10) Any person who is subpoenaed in terms of subsection (8) to attend proceedings and who fails to— *(a)* attend or to remain in attendance; *(b)* appear at the place and on the date and at the time to which the proceedings in question may be adjourned; *(c)* remain in attendance at those proceedings as so adjourned; or *(d)* produce any book, document or object specified in the subpoena, is guilty of an offence. (11) The provisions in respect of appeal and review as provided for in the Magistrates' Courts Act, 1944, and the Superior Courts Act, 2013, apply to proceedings in terms of this section. (12) Sections 8 and 9(3) of the Protection from Harassment Act, 2011 (Act No. 17 of 2011), applies with the necessary changes required by the context to proceedings contemplated in subsections (2) and (7). **Electronic communications service provider to furnish particulars to court** **11C.** (1) If an application for a protection order is made in terms of section 11B(1) and the court is satisfied in terms of section 11B(3) that a protection order must be issued and the particulars of the person referred to in section 11B(1)(*a*) or the electronic communications service provider, referred to in section 11B(1)(*b*), whose service is used to host or disclose such pornography, is not known, the court may— *(a)* adjourn the proceedings to any time and date on the terms and conditions which the court deems appropriate; and *(b)* issue a direction in the prescribed form, directing an electronic communications service provider, that is believed to be able to furnish such particulars, to furnish the court in the prescribed manner by means of an affidavit in the prescribed form with—

Number and year of law	Short title	Extent of repeal or amendment
		(i) the electronic communications identity number from where such pornography 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 such pornography was or was not sent from the electronic communications identity number of the person to the electronic communications identity number of the applicant; (iv) any information that is available to an electronic communications service provider that may be of assistance to the court to identify the person referred to in section 11B(1)(*a*) or the electronic communications service provider referred to in section 11B(1)(*b*), which provides a service to that person; (v) any information that is available to an electronic communications service provider which— *(aa)* confirms whether or not its electronic communications service is used to host or was or is used to disclose such pornography; or *(bb)* may be of assistance to the court to identify the electronic communications service provider whose service is used to host or was or is used disclose such pornography; and (vi) an assessment whether or not the electronic communications service provider is in a position to— *(aa)* remove such pornography or a link to such pornography; or *(bb)* disable access to such pornography or a link to such pornography.

Number and year of law	Short title	Extent of repeal or amendment
		(2) If the court issues a direction in terms of subsection (1)*(b)* the court must direct that the direction be served on the electronic communications service provider in the prescribed manner: Provided, that if the court is satisfied that the direction cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form or manner specified in that order. (3) *(a)* The information referred to in subsection (1)*(b)* must be provided to the court within five ordinary court days from the time that the direction is served on an electronic communications service provider. *(b)* An electronic communications service provider on which a direction is served, may in the prescribed manner by means of an affidavit in the prescribed form apply to the court for— (i) an extension of the period of five ordinary court days referred to in paragraph (*a*) for a further period of five ordinary court days on the grounds that the information cannot be provided timeously; or (ii) the cancellation of the direction on the grounds that— *(aa)* it does not provide an electronic communications service to the applicant or the person referred to in section 11B(1)(*a*); *(bb)* the requested information is not available in the records of the electronic communications service provider; or *(cc)* its service is not used to host or was or is not used disclose such pornography. (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 as it deems fit; *(c)* must give a decision in respect thereof; and *(d)* must inform the electronic communications service provider in the prescribed form and manner of the outcome of the application.

Number and year of law	Short title	Extent of repeal or amendment
		(5) *(a)* The court may, on receipt of an affidavit from an electronic communications service provider which contains the information referred to in subsection (1)(*b*), consider the issuing of a protection order in terms of section 11B(3) against the person or electronic communications service provider on the date to which the proceedings have been adjourned. *(b)* Any information furnished to the court in terms of subsection (1)(*b*) forms part of the evidence that a court may consider in terms of section 11B(3). (6) The Cabinet member responsible for the administration of justice may, by notice in the *Gazette*, prescribe reasonable tariffs of compensation payable to electronic communications service providers for providing the information referred to in subsection (1)(*b*). (7) Any electronic communications service provider or employee of an electronic communications service provider who— *(a)* fails to furnish the required information within five ordinary court days from the time that the direction is served on such electronic communications service provider to a court in terms of subsection (3)(*a*) or such extended period allowed by the court in terms of subsection (3)(*b*); or *(b)* makes a false statement in an affidavit referred to in subsection (1)(*b*) or (3)(*b*) in a material respect, is guilty of an offence. **Orders on finalisation of criminal proceedings** **11D.** (1) The trial court, on convicting a person of any offence referred to in section 11A(1), (2) or (3), must order— *(a)* that person to destroy the pornography and to submit an affidavit in the prescribed form to the prosecutor identified in the order, that the pornography has been so destroyed; or *(b)* an electronic communications service provider whose service is used to host or disclose such pornography to remove or disable access to such pornography.

Number and year of law	Short title	Extent of repeal or amendment
		(2) The order referred to in subsection (1)(*b*), must be in the prescribed form and must be served on the electronic communications service provider in the prescribed manner: Provided, that if the trial court is satisfied that the order cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form or manner specified in that order. (3) Any person or electronic communications service provider who fails to comply with an order referred to in subsection (1) is guilty of an offence. (4) An electronic communications service provider, may, within 14 days after the order referred to in subsection (1)(*b*) has been served on it, in terms of subsection (2), upon notice to the trial court concerned, in the prescribed form and manner, apply to the trial court for the setting aside or amendment of the order. (5) (*a*) The trial court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (4) and may for that purpose, consider such additional evidence as it deems fit, including oral evidence or evidence by affidavit, which shall form part of the record of the proceedings. *(b)* The trial court may if good cause has been shown for the variation or setting aside of the order, issue an order to this effect. (6) The trial court may, for purposes of subsections (5)(*a*), in the prescribed form and manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case. (7) Any person who is subpoenaed in terms of subsection (6) 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. (8) For purposes of this section **"trial court"** means—

Number and year of law	Short title	Extent of repeal or amendment
		(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. (9) Whenever a person is convicted of an offence referred to in section 11A(1), (2) or (3), the trial court must issue an order that the person so convicted must reimburse all expenses reasonably incurred by— *(a)* a complainant as a result of any direction issued in terms of section 11C(1)(*b*); or *(b)* an electronic communications service provider to remove or disable access to such pornography, whereupon the provisions of section 300 of the Criminal Procedure Act, 1977, shall apply with the necessary changes required by the context, to such order.''. *(d)* Chapter 3 is hereby amended— (i) by the substitution for the heading to Part II of Chapter 3 of the following heading: ''***Sexual exploitation and sexual grooming of children, exposure or display of or causing exposure or display of child pornography or pornography to children, offences relating to child pornography and using children for pornographic purposes or benefiting from child pornography***''; (ii) by the addition to section 17 of the following subsection: ''(7) Any person who unlawfully and intentionally in any manner advocates, advertises, encourages or promotes the sexual exploitation of a child, is guilty of an offence.''. (iii) by the insertion of the following section after section 19: ''**Offences relating to child pornography** **19A.** (1) Any person who unlawfully and intentionally creates, makes or produces child pornography in any manner, other than by using a child for child pornography as contemplated in section 20(1), is guilty of an offence.

Number and year of law	Short title	Extent of repeal or amendment
		(2) Any person who unlawfully and intentionally, in any manner assists in, or facilitates the creation, making or production of child pornography, is guilty of an offence. (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 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; *(j)* viewing, of child pornography, is guilty of an offence. (6) Any person who unlawfully and intentionally processes or facilitates a financial transaction, knowing that such transaction will facilitate a contravention of subsections (1) to (5), is guilty of an offence.”; and (iv) by the addition to section 20 of the following subsections: “(3) Any person who unlawfully and intentionally— *(a)* attends; *(b)* views; or *(c)* participates in, a live performance involving child pornography, is guilty of the offence of attending, viewing or participating in, a performance involving child pornography.

Number and year of law	Short title	Extent of repeal or amendment
		(4) Any person (''A'') who unlawfully and intentionally recruits a child complainant (''B''), with or without the consent of B, whether for financial or other reward, favour or compensation to B or a third person (''C'') or not, for purposes of— *(a)* creating, making or producing 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.''. *(e)* Section 54 of the Act is amended by the addition of the following subsections: ''(3) Any person who, having knowledge of the commission of any offence referred to in section 19A, or having reason to suspect that such an offence has been or is being or will probably be committed and unlawfully and intentionally fails to— *(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. (4) An electronic communications service provider that is aware or becomes aware that its electronic communications service or electronic communications network is used or involved in the commission of any offence provided for in section 19A, must— *(a)* immediately report the offence to the South African Police Service; *(b)* preserve any information which may be of assistance to the South African Police Service in investigating the offence; and *(c)* take all reasonable steps to prevent access to the child pornography by any person.''. *(f)* Section 56A of the Act is amended by the addition of the following subsections:

Number and year of law	Short title	Extent of repeal or amendment
		"(3) *(a)* Any person who contravenes the provisions of section 11A(1) or (2) is liable, on conviction to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment. *(b)* Any person who contravenes the provisions of section 11A(3) is liable, on conviction to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment. *(c)* Any person or electronic communications service provider that is convicted of an offence referred to in section 11B(9) or (10), is liable, on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment. *(d)* Any person or electronic communications service provider that is convicted of an offence referred to in section 11C(7), is liable, on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment. *(e)* Any electronic communications service provider or person that is convicted of an offence referred to in section 11D(3) or (7), is liable, on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment. (4) Any person who contravenes the provisions of section 19A(3), (4)*(f)*, *(g)*, *(h)*, *(i)* or *(j)*, or (5)*(f)*, *(g)*, *(h)*, *(i)* or *(j)* is liable— *(a)* in the case of a first conviction, to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment; *(b)* in the case of a second conviction, to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment; or *(c)* in the case of a third or subsequent 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 17(7), 19A(1), (2), (4)*(a)*, *(b)*, *(c)*, *(d)*, or *(e)*, (5)*(a)*, *(b)*, *(c)*, *(d)* or *(e)* or 20(3) or (4), is liable— *(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

Number and year of law	Short title	Extent of repeal or amendment
		(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(6), is liable— *(a)* in the case of a first conviction, to a fine of R1 000 000 or to imprisonment for a period not exceeding 5 years, or to both such fine and imprisonment; or *(b)* in the case of a second or subsequent conviction, to a fine of R 2 000 000 or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment. (7) Any person who contravenes the provisions of section 54(3), is liable, on conviction to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment. (8) Any electronic communications service provider who contravenes the provisions of section 54(4), is liable, on conviction to a fine not exceeding R1 000 000 or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.”.
Act 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 Act, 2020; *(b)* section 5, 6, 7 or 11(1) of the Cybercrimes Act, 2020, where the damage caused does not exceed an amount of R5000; *(c)* section 14, 15 or 16 of the Cybercrimes Act, 2020; or *(d)* section 8, 9 or 10 of the Cybercrimes Act, 2020, where the amount involved does not exceed R1500. 27. An offence contemplated in section 11A(1) and (2) of Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007.”. *(b)* The addition of the following item to Schedule 3: “23. Any offence contemplated in— *(a)* section 5, 6, 7 or 11(1) of the Cybercrimes Act, 2020, where the damage caused exceeds an amount of R5000; *(b)* section 8, 9 or 10 of the Cybercrimes Act, 2020, where the amount involved exceeds R1500; or

Number and year of law	Short title	Extent of repeal or amendment
		(c) section 11(2) of the Cybercrimes Act, 2020. 24. An offence contemplated in section 11A(3) of Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007.”

JOBNAME: w/t 2916 PAGE: 52 SESS: 78 OUTPUT: Thu Nov 5 09:29:05 2020 SUM: 0412A52A
/first/Parliament−GJ/BillsandActs−2020/parl−bills−B6C−2017−GJ/B6C−2017−GJ

Printed by Creda Communications

ISBN 978-1-4850-0660-2