Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Government Gazette

REPUBLIC OF SOUTH AFRICA

Vol. 672 | Cape Town Kaapstad | 1 June 2021 | No. 44651

THE PRESIDENCY

No. 324 **1 June 2021**

It is hereby notified that the President has assented to the following Act, which is hereby published for general information:—

Act No. 19 of 2020: Cybercrimes Act, 2020

DIE PRESIDENSIE

No. 324 **1 Junie 2021**

Hierby word bekend gemaak dat die President sy goedkeuring geheg het aan die onderstaande Wet wat hierby ter algemene inligting gepubliseer word:—

Wet No. 19 van 2020: Wet op Kubermisdade, 2020

ISSN 1682-5845

AIDS HELPLINE: 0800-0123-22 Prevention is the cure

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

GENERAL EXPLANATORY NOTE:

[ ]	Words in bold type in square brackets indicate omissions from existing enactments.
_______________	Words underlined with a solid line indicate insertions in existing enactments.

(English text signed by the President)
(Assented to 26 May 2021)

ACT

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

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

ARRANGEMENT OF SECTIONS

Sections

CHAPTER 1

DEFINITIONS AND INTERPRETATION

1. Definitions and interpretation

CHAPTER 2

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

PART I: CYBERCRIMES

2. Unlawful access
3. Unlawful interception of data
4. Unlawful acts in respect of software or hardware tool
5. Unlawful interference with data or computer program

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

ALGEMENE VERDUIDELIKENDE NOTA:

[ ] Woorde in vet druk tussen vierkantige hake dui skrappings uit bestaande verordeninge aan.

________ Woorde met volstreep daaronder, dui invoegings in bestaande verordeninge aan.

(Engelse teks deur die President geteken)
(Goedgekeur op 26 Mei 2021)

WET

Ten einde misdrywe te skep wat op kubermisdaad betrekking het; om die openbaarmaking van skadelike databoodskappe te kriminaliseer en om vir tussentydse beskermingsbevele voorsiening te maak; om jurisdiksie ten opsigte van kubermisdade verder te reël; om die bevoegdhede om kubermisdade te ondersoek, verder te reël; om aspekte aangaande onderlinge bystand ten opsigte van die ondersoek van kubermisdaad verder te reël; om voorsiening te maak vir die instelling van 'n aangewese Kontakpunt; om verder voorsiening te maak vir die bewys van sekere feite deur beëdigde verklaring; om verpligtinge op te lê om kubermisdade aan te meld; om voorsiening te maak vir kapasiteitsbou; om te bepaal dat die Uitvoerende Gesag ooreenkomste met vreemde State kan aangaan om maatreëls te bevorder wat op die bespeuring, voorkoming, mitigering en ondersoek van kubermisdade gemik is; om bepalings van sekere wette te skrap en te wysig; en om voorsiening te maak vir aangeleenthede wat daarmee in verband staan.

DIE PARLEMENT van Suid-Afrika verorden, soos volg:—

INDELING VAN ARTIKELS

Artikels

HOOFSTUK 1

WOORDOMSKRYWING EN UITLEG

1. Woordomskrywing en uitleg

HOOFSTUK 2

KUBERMISDADE, KWAADWILLIGE KOMMUNIKASIES, VONNISOPLEGGING EN BEVELE TER BESKERMING VAN KLAERS TEEN SKADELIKE UITWERKING VAN KWAADWILLIGE KOMMUNIKASIES

DEEL I: KUBERMISDADE

2. Wederregtelike toegang
3. Wederregtelike onderskepping van data
4. Wederregtelike handelinge ten opsigte van sagteware- of hardewarenutsmiddel
5. Wederregtelike inmenging met data of rekenaarprogram

Reproduced by LexisNexis under Government Printer’s Authorisation (Authorisation No. 11802) dated 13 November 2018

6. Unlawful interference with a computer data storage medium or computer system
7. Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device
8. Cyber fraud
9. Cyber forgery and uttering
10. Cyber extortion
11. Aggravated offences
12. Theft of incorporeal property

PART II: MALICIOUS COMMUNICATIONS

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

PART III: ATTEMPTING, CONSPIRING, AIDING, ABETTING, INDUCING, INCITING, INSTIGATING, INSTRUCTING, COMMANDING OR PROCURING TO COMMIT OFFENCE

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

PART IV: COMPETENT VERDICTS

18. Competent verdicts

PART V: SENTENCING

19. Sentencing

PART VI: ORDERS TO PROTECT COMPLAINANTS FROM HARMFUL EFFECT OF MALICIOUS COMMUNICATIONS

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

CHAPTER 3

JURISDICTION

24. Jurisdiction

CHAPTER 4

POWERS TO INVESTIGATE, SEARCH, ACCESS OR SEIZE

25. Definitions
26. Standard Operating Procedures
27. Application of Criminal Procedure Act, 1977
28. Search for, access to, or seizure of certain articles
29. Article to be searched for, accessed or seized under search warrant
30. Oral application for search warrant or amendment of warrant
31. Search for, access to, or seizure of article without search warrant with consent of person who has lawful authority to consent

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

6. Wederregtelike inmenging met 'n rekenaardatabergingsmedium of rekenaarstelsel
7. Wederregtelike verkryging, besit, voorsiening, ontvangs of gebruik van wagwoord, toegangskode of soortgelyke data of toestel
8. Kuberbedrog
9. Kubervervalsing en- uitgifte
10. Kuberafpersing
11. Verswarende misdrywe
12. Diefstal van onliggaamlike eiendom

DEEL II: KWAADWILLIGE KOMMUNIKASIES

13. Woordomskrywing
14. Databoodskap wat beskadiging van eiendom of geweld aanhits
15. Databoodskap wat persone met beskadiging van eiendom of geweld dreig
16. Openbaarmaking van databoodskap van intieme beeld

DEEL III: POGING, SAMESWERING, HULPVERLENING, AANSTIGTING, UITLOKKING, AANHITSING, AANMOEDIGING, AANRAAIING, BEVEL, RAADGEWING OF VERKRYGING OM MISDRYF TE PLEEG

17. Poging, sameswering, hulpverlening, aanstigting, uitlokking, aanhitsing, aanmoediging, aanraaiing, bevel, raadgewing of verkryging om misdryf te pleeg

DEEL IV: GEOORLOOFDE UITSPRAKE

18. Geoorloofde uitsprake

DEEL V: VONNISOPLEGGING

19. Vonnisoplegging

DEEL VI: BEVELE TER BESKERMING VAN KLAERS TEEN SKADELIKE UITWERKING VAN KWAADWILLIGE KOMMUNIKASIES

20. Bevel ter beskerming van klaer hangende afhandeling van strafregtelike verrigtinge
21. Elektroniese kommunikasiediensverskaffer moet besonderhede aan hof verskaf
22. Bevele by afhandeling van strafregtelike verrigtinge
23. Strawwe

HOOFSTUK 3

JURISDIKSIE

24. Jurisdiksie

HOOFSTUK 4

BEVOEGDHEDE VAN ONDERSOEK, DEURSOEKING, TOEGANG OF BESLAGLEGGING

25. Woordomskrywing
26. Standaardbedryfsprosedures
27. Toepassing van bepalings van Strafproseswet, 1977
28. Deursoeking vir, toegang tot, of beslaglegging op, sekere items
29. Deursoeking vir, toegang tot of beslaglegging op item kragtens deursoekingslasbrief
30. Mondelinge aansoek om deursoekingslasbrief of wysiging van lasbrief
31. Deursoeking vir, toegang tot, of beslaglegging op item sonder deursoekingslasbrief met toestemming van persoon met wettige magtiging om toe te stem

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

32. Search for, access to, or seizure of article involved in the commission of an offence without search warrant
33. Search for, access to, or seizure of article on arrest of person
34. Assisting police official or investigator
35. Obstructing or hindering police official or investigator and authority to overcome resistance
36. Powers conferred upon police official or investigator to be conducted in decent and orderly manner with due regard to rights of other persons
37. Wrongful search, access or seizure and restriction on use of instrument, device, password or decryption key or information to gain access
38. False information under oath or by way of affirmation
39. Prohibition on disclosure of information
40. Interception of indirect communication and obtaining of real-time communication-related information
41. Expedited preservation of data direction
42. Preservation of evidence direction
43. Oral application for preservation of evidence direction
44. Disclosure of data direction and search for, access to, and seizure of articles subject to preservation
45. Obtaining and using publicly available data or receiving data from person who is in possession of data

CHAPTER 5

MUTUAL ASSISTANCE

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

CHAPTER 6

DESIGNATED POINT OF CONTACT

52. Establishment and functions of designated Point of Contact

CHAPTER 7

EVIDENCE

53. Proof of certain facts by affidavit

CHAPTER 8

REPORTING OBLIGATIONS AND CAPACITY BUILDING

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

32. Deursoeking vir, toegang tot, of beslaglegging op item betrokke in pleging van misdryf, sonder deursoekingslasbrief
33. Deursoeking vir, toegang tot of beslaglegging op item by inhegtenisneming van persoon
34. Bystand aan polisiebeampte of ondersoeker
35. Dwarsboming of belemmering van polisiebeampte of ondersoeker en magtiging om teenstand te oorkom
36. Bevoegdhede aan polisiebeampte of ondersoeker opgedra moet op behoorlike en ordelike wyse uitgevoer word met behoorlike inagneming van regte van ander persone
37. Wederregtelike deursoeking, toegang of beslaglegging en beperking op gebruik van instrument, toestel, wagwoord of dekripteringsleutel of inligting om toegang te kry
38. Vals inligting onder eed of deur plegtige verklaring
39. Verbod op openbaarmaking van inligting
40. Onderskepping van onregstreekse kommunikasie en verkryging van intydse kommunikasie-verwante inligting
41. Lasgewing vir bespoedigde bewaring van data
42. Lasgewing vir bewaring van getuienis
43. Mondelinge aansoek om lasgewing vir bewaring van getuienis
44. Lasgewing vir openbaarmaking van data en deursoeking vir, toegang tot en beslaglegging op items onderworpe aan bewaring
45. Verkryging en gebruik van openbaar beskikbare data of ontvangs van data van persoon wat in besit is van data

HOOFSTUK 5

ONDERLINGE BYSTAND

46. Toepassing van bepalings van Hoofstuk
47. Spontane inligting
48. Buitelandse versoeke om bystand en samewerking
49. Voldoening aan bevel van aangewese regter
50. Verwittiging van vreemde Staat van uitslag van versoek om onderlinge bystand en bespoedigde openbaarmaking van verkeersdata
51. Uitreiking van lasgewing om onderlinge bystand van vreemde Staat te versoek

HOOFSTUK 6

AANGEWESE KONTAKPUNT

52. Instelling en werksaamhede van aangewese Kontakpunt

HOOFSTUK 7

GETUIENIS

53. Bewys van sekere feite deur beëdigde verklaring

HOOFSTUK 8

RAPPORTERINGSVERPLIGTINGE EN KAPASITEITSBOU

54. Verpligtinge van elektroniese kommunikasiediensverskaffers en finansiële instellings
55. Kapasiteit om kubermisdade te bespeur, te voorkom en te ondersoek
56. Nasionale Direkteur van Openbare Vervolgings moet statistieke van vervolgings hou

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

CHAPTER 9

GENERAL PROVISIONS

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

Schedule

CHAPTER 1

DEFINITIONS AND INTERPRETATION

Definitions and interpretation

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

"article" means any—

(a) data;
(b) computer program;
(c) computer data storage medium; or
(d) computer system,

which—

(i) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission;
(ii) may afford evidence of the commission or suspected commission; or
(iii) is intended to be used or is, on reasonable grounds believed to be intended to be used in the commission or intended commission,

of—

(aa) an offence in terms of Part I and Part II of Chapter 2;
(bb) any other offence in terms of the law of the Republic; or
(cc) an offence in a foreign State that is substantially similar to an offence contemplated in Part I or Part II of Chapter 2 or another offence recognised in the Republic;

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

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

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

"computer system" means—

(a) one computer; or
(b) two or more inter-connected or related computers, which allow these inter-connected or related computers to—
  (i) exchange data or any other function with each other; or
  (ii) exchange data or any other function with another computer or a computer system;

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

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

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

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

HOOFSTUK 9

ALGEMENE BEPALINGS

57. Nasionale Uitvoerende Gesag kan ooreenkomste aangaan
58. Herroeping of wysiging van wette
59. Regulasies
60. Kort titel en inwerkingtreding

Bylae

HOOFSTUK 1

WOORDOMSKRYWING EN UITLEG

Woordomskrywing en uitleg

1. (1) In hierdie Wet, tensy die samehang anders aandui, beteken—

"aangewese Kontakpunt" die kantoor ingevolge artikel 52 ingestel of aangewys;

"aangewese regter" 'n aangewese regter soos omskryf in artikel 1 van die Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting, 2002;

"data" elektroniese voorstellings van inligting in enige formaat;

"databoodskap" data gegenereer, gestuur, ontvang of geberg by wyse van elektroniese middele, waar enige uitset van die data in 'n verstaanbare vorm is;

"Doeane- en Aksynswet, 1964" die Doeane- en Aksynswet, 1964 (Wet No. 91 van 1964);

"elektroniese kommunikasiediens" enige diens wat in geheel of hoofsaaklik bestaan uit die oordrag, op enige wyse, van elektroniese kommunikasies oor 'n elektroniese kommunikasienetwerk, met uitsondering van uitsaaidienste soos omskryf in artikel 1 van die Wet op Elektroniese Kommunikasie, 2005;

"elektroniese kommunikasiediensverskaffer"—

(a) enige persoon wat 'n elektroniese kommunikasiediens verskaf aan die publiek, dele van die publiek, die Staat, of die intekenaars tot sodanige diens, kragtens en ooreenkomstig 'n elektroniese kommunikasiedienslisensie aan daardie persoon uitgereik ingevolge die Wet op Elektroniese Kommunikasie, 2005, of wat geag word gelisensieer of vrygestel van lisensiëring as sodanig te wees ingevolge daardie Wet; en

(b) 'n persoon wat wettige magtiging het om die bedryf of gebruik van 'n private elektroniese kommunikasienetwerk te beheer wat hoofsaaklik gebruik word vir voorsiening van elektroniese kommunikasiedienste vir die eienaar se eie gebruik en wat van lisensiëring vrygestel is ingevolge die Wet op Elektroniese Kommunikasie, 2005;

"elektroniese kommunikasienetwerk" 'n elektroniese kommunikasienetwerk soos omskryf in artikel 1 van die Wet op Elektroniese Kommunikasie, 2005, en sluit 'n rekenaarstelsel in;

"finansiële instelling" 'n "financial institution" soos omskryf in artikel 1 van die "Financial Sector Regulation Act", 2017 (Wet No. 9 van 2017);

"Grondwet" die Grondwet van die Republiek van Suid-Afrika, 1996;

"item" enige—

(a) data;
(b) rekenaarprogram;
(c) rekenaardatabergingsmedium; of
(d) rekenaarstelsel,

wat—

(i) betrokke is by, in verband staan met of, op redelike gronde, geag word betrokke te wees by of in verband te staan met die pleging of vermeende pleging;
(ii) tot bewys kan strek van die pleging of vermeende pleging; of
(iii) wat bestem is om gebruik te word, of op redelike gronde vermeen word bestem te wees by, die pleging of voorgenome pleging van—
(aa) 'n misdryf ingevolge Deel I en Deel II van Hoofstuk 2;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

"data message" means data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form;
"designated judge" means a designated judge as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002;
"designated Point of Contact" means the office established or designated in terms of section 52;
"Electronic Communications Act, 2005" means the Electronic Communications Act, 2005 (Act No. 36 of 2005);
"electronic communications network" means an electronic communications network as defined in section 1 of the Electronic Communications Act, 2005, and includes a computer system;
"electronic communications service" means any service which consists wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services as defined in section 1 of the Electronic Communications Act, 2005;
"electronic communications service provider" means—

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

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

"financial institution" means a financial institution as defined in section 1 of the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017);
"foreign State" means any State other than the Republic;
"Intelligence Services Oversight Act, 1994" means the Intelligence Services Oversight Act, 1994 (Act No. 40 of 1994);
"International Co-operation in Criminal Matters Act, 1996" means the International Co-operation in Criminal Matters Act, 1996 (Act No. 75 of 1996);
"Justices of the Peace and Commissioners of Oaths Act, 1963" means the Justices of the Peace and Commissioners of Oaths Act, 1963 (Act No. 16 of 1963);
"magistrate" includes a regional court magistrate;
"Magistrates' Courts Act, 1944" means the Magistrates' Courts Act, 1944 (Act No. 32 of 1944);
"National Commissioner" means the National Commissioner of the South African Police Service, appointed by the President under section 207(1) of the Constitution;
"National Director of Public Prosecutions" means the person contemplated in section 179(1)*(a)* of the Constitution and appointed in terms of section 10 of the National Prosecuting Authority Act, 1998;
"National Head of the Directorate" means a person appointed in terms of section 17CA(1) of the South African Police Service Act, 1995;
"National Prosecuting Authority Act, 1998" means the National Prosecuting Authority Act, 1998 (Act No. 32 of 1998);
"National Strategic Intelligence Act, 1994" means the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994);
"output of a computer program" means any—

(a) data or output of the data;
(b) computer program; or
(c) instructions,

generated by a computer program;
"output of data" means by having data displayed or in any other manner;
"person" means a natural or a juristic person;
"police official" means a member of the South African Police Service as defined in section 1 of the South African Police Service Act, 1995;
"Prevention of Organised Crime Act, 1998" means the Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998);
"Protection from Harassment Act, 2011" means the Protection from Harassment Act, 2011 (Act No. 17 of 2011);

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(bb) enige ander misdryf ingevolge die reg van die Republiek; of

(cc) 'n misdryf in 'n vreemde Staat wat wesenlik soortgelyk is aan 'n misdryf in Deel I of Deel II van Hoofstuk 2 beoog of 'n ander misdryf in die Republiek erken;

"landdros" ook 'n streekhoflanddros;

"Nasionale Direkteur van Openbare Vervolging" die persoon in artikel 179(1)*(a)* van die Grondwet beoog en aangestel ingevolge artikel 10 van die Wet op die Nasionale Vervolgingsgesag, 1998;

"Nasionale Hoof van die Direktoraat" 'n persoon ingevolge artikel 17CA(1) van die Wet op die Suid-Afrikaanse Polisiediens, 1995, aangestel;

"Nasionale Kommissaris" die Nasionale Kommissaris van die Suid-Afrikaanse Polisiediens, deur die President aangestel kragtens artikel 207(1) van die Grondwet;

"openbaar beskikbare data" data wat toeganklik is in die publieke domein sonder beperking;

"persoon" 'n natuurlike of regspersoon;

"polisiebeampte" 'n lid van die Suid-Afrikaanse Polisiediens soos omskryf in artikel 1 van die Wet op die Suid-Afrikaanse Polisiediens, 1995;

"rekenaar" enige elektroniese, programmeerbare toestel gebruik, hetsy alleen of as deel van 'n rekenaarstelsel of enige ander toestel of toerusting of enige deel daarvan, om voorafbepaalde rekenkundige, logiese, roeterings-, verwerkings- of bergingsoperasies ooreenkomstig vasgestelde instruksies te verrig, en sluit in enige data, rekenaarprogram of rekenaardatabergingsmedium wat verband hou met, gekoppel is aan of gebruik word met sodanige toestel;

"rekenaardatabergingsmedium" enige toestel waarvandaan data of 'n rekenaarprogram gereproduseer kan word of waarop data of 'n rekenaarprogram geberg kan word, deur 'n rekenaarstelsel ongeag of die toestel fisies verbonde is aan of gekoppel is met 'n rekenaarstelsel;

"rekenaarprogram" data wat instruksies of stellings verteenwoordig wat, wanneer dit in 'n rekenaarstelsel uitgevoer word, die rekenaarstelsel 'n funksie laat verrig;

"rekenaarstelsel"—

(a) een rekenaar; of

(b) twee of meer rekenaars wat onderling gekoppel of verbandhoudend is, wat hierdie rekenaars wat onderling gekoppel is of verbandhoudend is, toelaat om—

(i) data of enige ander funksie met mekaar uit te ruil; of

(ii) data of enige ander funksie met 'n ander rekenaar of 'n rekenaarstelsel uit te ruil;

"spesifiek aangewese polisiebeampte" 'n polisiebeampte met die rang van kaptein of hoër bedoel in artikel 33 van die Wet op die Suid-Afrikaanse Polisiediens, 1995, wat skriftelik deur onderskeidelik die Nasionale Kommissaris en die Nasionale Hoof van die Direktoraat aangewys is om—

(a) mondeling aansoek te doen om 'n deursoekingslasbrief of 'n wysiging van 'n lasbrief in artikel 30 bedoel;

(b) lasgewings vir bespoedigde bewaring van data in artikel 41 bedoel, uit te reik; of

(c) 'n lasgewing van die aangewese regter in artikel 48(10) beoog, te beteken of tenuitvoer te lê;

"Strafproseswet, 1977" die Strafproseswet, 1977 (Wet No. 51 van 1977);

"Suid-Afrikaanse Reserwebank" die Suid-Afrikaanse Reserwebank, bedoel in artikel 223 van die Grondwet, gelees met die Wet op die Suid-Afrikaanse Reserwebank, 1989;

"uitset van data" deur data te vertoon of op enige ander wyse te hê;

"uitset van 'n rekenaarprogram" enige—

(a) data of uitset van die data;

(b) rekenaarprogram; of

(c) instruksies,

deur 'n rekenaarprogram gegenereer;

"verantwoordelike party" 'n verantwoordelike party soos omskryf in artikel 1 van die Wet op die Beskerming van Persoonlike Inligting, 2013;

"verkeersdata" data aangaande 'n kommunikasie wat die kommunikasie se oorsprong, bestemming, roete, formaat, tyd, datum, grootte, duur of tipe van die onderliggende diens aandui;

"vreemde Staat" enige Staat anders as die Republiek;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

"Protection of Personal Information Act, 2013" means the Protection of Personal Information Act, 2013 (Act No. 4 of 2013);

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

"Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002" means the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002);

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

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

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

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

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

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

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

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

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

"Tax Administration Act, 2011" means the Tax Administration Act, 2011 (Act No. 28 of 2011); and

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

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

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

(b) section 72; or

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

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

CHAPTER 2

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

PART I: CYBERCRIMES

Unlawful access

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

(a) a computer system; or

(b) a computer data storage medium,

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

"Wet op Belastingadministrasie, 2011" die Wet op Belastingadministrasie, 2011 (Wet No. 28 van 2011);
"Wet op Beskerming teen Teistering, 2011" die Wet op Beskerming teen Teistering, 2011 (Wet No. 17 van 2011);
"Wet op Beskerming van Persoonlike Inligting, 2013" die Wet op Beskerming van Persoonlike Inligting, 2013 (Wet No. 4 van 2013);
"Wet op die Nasionale Vervolgingsgesag, 1998" die Wet op die Nasionale Vervolgingsgesag, 1998 (Wet No. 32 van 1998);
"Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting, 2002" die Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting, 2002 (Wet No. 70 van 2002);
"Wet op die Suid-Afrikaanse Polisiediens, 1995" die Wet op die Suid-Afrikaanse Polisiediens, 1995 (Wet No. 68 van 1995);
"Wet op die Suid-Afrikaanse Reserwebank, 1989" die Wet op die Suid-Afrikaanse Reserwebank, 1989 (Wet No. 90 van 1989);
"Wet op die Voorkoming van Georganiseerde Misdaad, 1998" die Wet op die Voorkoming van Georganiseerde Misdaad, 1998 (Wet No. 121 van 1998);
"Wet op Doeanebeheer, 2014" die Wet op Doeanebeheer, 2014 (Wet No. 31 van 2014);
"Wet op Elektroniese Kommunikasie, 2005" die Wet op Elektroniese Kommunikasie, 2005 (Wet No. 36 van 2005);
"Wet op Hoër Howe, 2013" die Wet op Hoër Howe, 2013 (Wet No. 10 van 2013);
"Wet op Internasionale Samewerking in Strafregtelike Aangeleenthede, 1996" die Wet op Internasionale Samewerking in Strafregtelike Aangeleenthede, 1996 (Wet No. 75 van 1996);
"Wet op Landdroshowe, 1944" die Wet op Landdroshowe, 1944 (Wet No. 32 van 1944);
"Wet op Nasionale Strategiese Intelligensie, 1994" die Wet op Nasionale Strategiese Intelligensie, 1994 (Wet No. 39 van 1994);
"Wet op Toesig oor Intelligensiedienste, 1994" die Wet op Toesig oor Intelligensiedienste, 1996 (Wet No. 40 van 1994); en
"Wet op Vrederegters en Kommissarisse van Ede, 1963" die Wet op Vrederegters en Kommissarisse van Ede, 1963 (Wet No. 16 van 1963).

(2) By die toepassing van artikel 2, 3(2) of (3), of 7(1) of (2) van hierdie Wet, moet, enige versuim deur 'n verantwoordelike party om te voldoen aan—

(a) die voorwaardes vir regmatige prosessering van persoonlike inligting in Hoofstuk 3 bedoel;
(b) artikel 72; of
(c) die bepalings van 'n gedragskode uitgereik ingevolge artikel 60,

van die Wet op Beskerming van Persoonlike Inligting, 2013, ingevolge Hoofstuk 10 van daardie Wet hanteer word.

HOOFSTUK 2

KUBERMISDADE, KWAADWILLIGE KOMMUNIKASIES, VONNISOPLEGGING EN BEVELE TER BESKERMING VAN KLAERS TEEN SKADELIKE UITWERKING VAN KWAADWILLIGE KOMMUNIKASIES

DEEL I: KUBERMISDADE

Wederregtelike toegang

2. (1) Enige persoon wat wederregtelik en opsetlik 'n handeling verrig ten opsigte van—

(a) 'n rekenaarstelsel; of
(b) 'n rekenaardatabergingsmedium,

wat die persoon wat die handeling verrig het of enige ander persoon in 'n posisie stel om 'n misdryf beoog in subartikel (2), artikel 3(1), 5(1) of 6(1) te pleeg, is skuldig aan 'n misdryf.

(2) *(a)* Enige persoon wat wederregtelik en opsetlik toegang tot 'n rekenaarstelsel of 'n rekenaardatabergingmedium verkry, is skuldig aan 'n misdryf.

This gazette is also available free online at www.gpwonline.co.za

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(b) For purposes of paragraph *(a)*—
- (i) a person accesses a computer data storage medium, if the person—
  - *(aa)* uses data or a computer program stored on a computer data storage medium; or
  - *(bb)* stores data or a computer program on a computer data storage medium; and
- (ii) a person accesses a computer system, if the person—
  - *(aa)* uses data or a computer program held in a computer system;
  - *(bb)* stores data or a computer program on a computer data storage medium forming part of the computer system; or
  - *(cc)* instructs, communicates with, or otherwise uses, the computer system.

(c) For purposes of paragraph *(b)*—
- (i) a person uses a computer program, if the person—
  - *(aa)* copies or moves the computer program to a different location in the computer system or computer data storage medium in which it is held or to any other computer data storage medium;
  - *(bb)* causes a computer program to perform any function; or
  - *(cc)* obtains the output of a computer program; and
- (ii) a person uses data, if the person—
  - *(aa)* copies or moves the data to a different location in the computer system or computer data storage medium in which it is held or to any other computer data storage medium; or
  - *(bb)* obtains the output of data.

Unlawful interception of data

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

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

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

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

Unlawful acts in respect of software or hardware tool

4. (1) Any person who unlawfully and intentionally—
- *(a)* uses; or
- *(b)* possesses,

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

(2) For purposes of this section **"software or hardware tool"** means any electronic, mechanical or other instrument, device, equipment, apparatus or a substantial component thereof or a computer program, which is designed or adapted primarily for the purpose to—
- *(a)* access as contemplated in section 2(1) or (2);
- *(b)* intercept data as contemplated in section 3(1);

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(b) By die toepassing van paragraaf *(a)*—

(i) verkry 'n persoon toegang tot 'n rekenaardatabergingsmedium, indien die persoon—

(aa) data of 'n rekenaarprogram wat op 'n rekenaardatabergingsmedium geberg is, gebruik; of

(bb) data of 'n rekenaarprogram berg op 'n rekenaardatabergingsmedium; en

(ii) verkry'n persoon toegang tot 'n rekenaarstelsel indien die persoon—

(aa) data of 'n rekenaarprogram wat in 'n rekenaarstelsel gehou word, gebruik;

(bb) data of 'n rekenaarprogram op 'n rekenaardatabergingsmedium wat deel van die rekenaarstelsel uitmaak, berg; of

(cc) die rekenaarstelsel opdragte gee, daarmee kommunikeer of dit andersins gebruik.

(c) By die toepassing van paragraaf *(b)*—

(i) gebruik 'n persoon 'n rekenaarprogram, indien die persoon—

(aa) die rekenaarprogram kopieer of verskuif na 'n ander ligging in die rekenaarstelsel of rekenaardatabergingsmedium waarin dit gehou word of na enige ander rekenaardatabergingsmedium;

(bb) 'n rekenaarprogram enige funksie laat verrig; of

(cc) die uitset van 'n rekenaarprogram verkry; en

(ii) gebruik 'n persoon data, indien die persoon—

(aa) die data kopieer of verskuif na 'n ander ligging in die rekenaarstelsel of rekenaardatabergingsmedium waarin dit gehou word of na enige ander rekenaardatabergingsmedium; of

(bb) die uitset van data verkry.

Wederregtelike onderskepping van data

3. (1) Enige persoon wat wederregtelik en opsetlik data onderskep, met inbegrip van elektromagnetiese emissies van 'n rekenaarstelsel wat daardie data dra, binne-in of wat oorgesend word na of van 'n rekenaarstelsel, is skuldig aan 'n misdryf.

(2) Enige persoon wat wederregtelik en opsetlik data, of die uitset van data besit, met die wete dat daardie data wederregtelik onderskep is soos in subartikel (1) beoog, is skuldig aan 'n misdryf.

(3) Enige persoon wat in besit van data of die uitset van data gevind word, ten opsigte waarvan daar 'n redelike vermoede is dat daardie data wederregtelik onderskep is soos in subartikel (1) beoog en wat nie bevredigend verontskuldigend rekenskap kan gee van daardie besit nie, is skuldig aan 'n misdryf.

(4) By die toepassing van hierdie artikel, beteken **"onderskepping van data"** die verkryging, besigtiging, vaslegging of kopiëring van data van 'n nie-publieke aard deur die gebruik van 'n hardeware- of sagtewarenutsmiddel in artikel 4(2) beoog of enige ander wyse, ten einde sommige van of al die data beskikbaar te stel aan 'n persoon, anders as die wettige eienaar of houer van die data, die sender of die ontvanger of die bedoelde ontvanger van daardie data, en sluit in die—

(a) ondersoeking of inspeksie van die inhoud van die data; en

(b) verleiding van die data of enige deel daarvan van die bedoelde bestemming na enige ander bestemming.

Wederregtelike handelinge ten opsigte van sagteware- of hardewarenutsmiddel

4. (1) Enige persoon wat wederregtelik en opsetlik enige sagteware- of hardewarenutsmiddel—

(a) gebruik; of

(b) besit,

met die doel om die bepalings van artikel 2(1) of (2), 3(1), 5(1), 6(1) of 7(1)*(a)* of *(d)* te oortree, is skuldig aan 'n misdryf.

(2) By die toepassing van hierdie artikel, beteken **"sagteware- of hardewarenutsmiddel"** enige elektroniese, meganiese of ander instrument, toestel, toerusting, apparaat of 'n wesenlike komponent daarvan of 'n rekenaarprogram, wat hoofsaaklik ontwerp of aangepas is vir die doeleindes van—

(a) toegang soos in artikel 2(1) of (2) beoog;

(b) onderskepping van data soos in artikel 3(1) beoog;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(c) interfere with data or a computer program as contemplated in section 5(1);
(d) interfere with a computer data storage medium or a computer system as contemplated in section 6(1); or
(e) acquire, make available or use a password, access code or similar data or device as defined in section 7(3).

Unlawful interference with data or computer program

5. (1) Any person who unlawfully and intentionally interferes with—
(a) data; or
(b) a computer program,
is guilty of an offence.

(2) For purposes of this section **"interfere with data or a computer program"** means to permanently or temporarily—
(a) delete data or a computer program;
(b) alter data or a computer program;
(c) render vulnerable, damage or deteriorate data or a computer program;
(d) render data or a computer program meaningless, useless or ineffective;
(e) obstruct, interrupt or interfere with the lawful use of, data or a computer program; or
(f) deny access to data or a computer program,
held in a computer data storage medium or a computer system.

Unlawful interference with computer data storage medium or computer system

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

(2) For purposes of this section **"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.

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

7. (1) Any person who unlawfully and intentionally—
(a) acquires;
(b) possesses;
(c) provides to another person; or
(d) uses,
a password, an access code or similar data or device for purposes of contravening the provisions of section 2(1) or (2), 3(1), 5(1), 6(1), 8 or 9(1), is guilty of an offence.

(2) Any person who is found in possession of a password, an access code or similar data or device in regard to which there is a reasonable suspicion that such password, access code or similar data or device—
(a) was acquired;
(b) is possessed;
(c) is to be provided to another person; or
(d) was used or may be used,
for purposes of contravening the provisions of section 2(1) or (2), 3(1), 5(1), 6(1), 8 or 9(1), and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(*c*) inmenging met data of 'n rekenaarprogram soos in artikel 5(1) beoog;
(*d*) inmenging met 'n rekenaardatabergingsmedium of 'n rekenaarstelsel soos in artikel 6(1) beoog; of
(*e*) verkryging, beskikbaarstelling of gebruikmaking van 'n wagwoord, toegangskode of soortgelyke data of toestel soos in artikel 7(3) omskryf.

Wederregtelike inmenging met data of rekenaarprogram

5. (1) Enige persoon wat wederregtelik en opsetlik inmeng met—
(*a*) data; of
(*b*) 'n rekenaarprogram,
is skuldig aan 'n misdryf.

(2) By die toepassing van hierdie artikel beteken **"inmenging met data of 'n rekenaarprogram"** om permanent of tydelik—
(*a*) data of 'n rekenaarprogram uit te wis;
(*b*) data of 'n rekenaarprogram te verander;
(*c*) data of 'n rekenaarprogram kwesbaar te maak, te beskadig of te laat agteruitgaan;
(*d*) data of 'n rekenaarprogram betekenisloos, nutteloos of ondoeltreffend te maak;
(*e*) die wettige gebruik van data of 'n rekenaarprogram te belemmer, te onderbreek of daarmee in te meng; of
(*f*) toegang tot data of 'n rekenaarprogram te weier,
wat in 'n rekenaardatabergingsmedium of 'n rekenaarstelsel gehou word.

Wederregtelike inmenging met rekenaardatabergingsmedium of rekenaarstelsel

6. (1) Enige persoon wat wederregtelik en opsetlik met 'n rekenaardatabergingsmedium of 'n rekenaarstelsel inmeng, is skuldig aan 'n misdryf.

(2) By die toepassing van hierdie artikel beteken **"inmenging met 'n rekenaardatabergingsmedium of 'n rekenaarstelsel"** om permanent of tydelik—
(*a*) enige bron te verander; of
(*b*) die—
(i) werking;
(ii) vertroulikheid;
(iii) integriteit; of
(iv) beskikbaarheid,
te onderbreek of te belemmer,
van 'n rekenaardatabergingsmedium of 'n rekenaarstelsel.

Wederregtelike verkryging, besit, voorsiening, ontvangs of gebruik van wagwoord, toegangskode of soortgelyke data of toestel

7. (1) Enige persoon wat wederregtelik en opsetlik 'n wagwoord, 'n toegangskode of soortgelyke data of toestel—
(*a*) verkry;
(*b*) besit;
(*c*) aan iemand anders voorsien; of
(*d*) gebruik,
met die doel om die bepalings van artikel 2(1) of (2), 3(1), 5(1), 6(1), 8 of 9(1) te oortree, is skuldig aan 'n misdryf.

(2) Enige persoon wat in besit van 'n wagwoord, 'n toegangskode of soortgelyke data of toestel gevind word, ten opsigte waarvan 'n redelike verdenking bestaan dat sodanige wagwoord, toegangskode of soortgelyke data of toestel—
(*a*) verkry is;
(*b*) besit word;
(*c*) aan iemand anders voorsien gaan word; of
(*d*) gebruik is of gebruik kan word,
met die doel om die bepalings van artikel 2(1) of (2), 3(1), 5(1), 6(1), 8 of 9(1) te oortree en wat nie 'n bevredigende, verontskuldigende verduideliking vir sodanige besit kan gee nie, is skuldig aan 'n misdryf.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(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.

Cyber fraud

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

(a) by means of data or a computer program; or
(b) through any interference with data or a computer program as contemplated in 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.

Cyber forgery and uttering

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

(a) false data; or
(b) a false computer program,

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

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

(a) false data; or
(b) a false computer program,

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

Cyber extortion

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

(a) obtaining any advantage from another person; or
(b) compelling another person to perform or to abstain from performing any act,

is guilty of the offence of cyber extortion.

Aggravated offences

11. (1) *(a)* Any person who commits an offence referred to in—

(i) section 3(1), 5(1) or 6(1), in respect of; or
(ii) section 7(1), in so far as the passwords, access codes or similar data and devices relate to,

a restricted computer system, 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.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(3) By die toepassing van hierdie artikel beteken **"wagwoord, toegangskode of soortgelyke data of toestel"** ook—

(a) 'n geheime kode of pin;
(b) 'n beeld;
(c) 'n sekuriteitsbewys;
(d) 'n toegangskaart;
(e) enige toestel;
(f) biometriese data; of
(g) 'n woord of 'n string karakters of nommers,

gebruik vir finansiële transaksies of gebruikeroutentisering ten einde data, 'n rekenaarprogram, 'n rekenaardatabergingsmedium of 'n rekenaarstelsel te gebruik.

Kuberbedrog

8. Enige persoon wat wederregtelik en met die opset om te bedrieg, 'n wanvoorstelling maak—

(a) deur middel van data of 'n rekenaarprogram; of
(b) deur enige inmenging met data of 'n rekenaarprogram soos beoog in artikel 5(2)*(a)*, *(b)* of *(e)* of inmenging met 'n rekenaardatabergingsmedium of 'n rekenaarstelsel soos beoog in artikel 6(2)*(a)*,

wat werklike of potensiële benadeling vir iemand anders veroorsaak, is skuldig aan die misdryf van kuberbedrog.

Kubervervalsing en -uitgifte

9. (1) Enige persoon wat wederregtelik en met die opset om te bedrieg—

(a) vals data; of
(b) 'n vals rekenaarprogram,

maak tot die werklike of potensiële benadeling van 'n ander persoon, is skuldig aan die misdryf van kubervervalsing.

(2) Enige persoon wat wederregtelik en met die opset om te bedrieg—

(a) vals data; of
(b) 'n vals rekenaarprogram,

uitgee, tot die werklike of potensiële benadeling van 'n ander persoon, is skuldig aan die misdryf van kuberuitgifte.

Kuberafpersing

10. Enige persoon wat wederregtelik en opsetlik 'n misdryf beoog in artikel 3(1), 5(1), 6(1) of 7(1)*(a)* of *(d)* pleeg of dreig om sodanige misdryf te pleeg, met die doel om—

(a) enige voordeel van iemand anders te verkry; of
(b) iemand anders te dwing om enige handeling te verrig of nie te verrig nie,

is skuldig aan die misdryf van kuberafpersing.

Verswarende misdrywe

11. (1) *(a)* Enige persoon wat 'n misdryf pleeg bedoel in—

(i) artikel 3(1), 5(1) of 6(1), ten opsigte van; of
(ii) artikel 7(1), vir sover die wagwoorde, toegangskodes of soortgelyke data en toestelle verband hou met,

'n beperkte rekenaarstelsel en wat weet of redelikerwys moes geweet het of vermoed het dat dit 'n beperkte rekenaarstelsel is, is skuldig aan 'n verswarende misdryf.

(b) By die toepassing van paragraaf *(a)*, beteken 'n **"beperkte rekenaarstelsel"** enige data, rekenaarprogram, rekenaardatabergingsmedium of rekenaarstelsel—

(i) onder die beheer van, of uitsluitlik gebruik deur—
    (aa) 'n finansiële instelling; of
    (bb) 'n staatsorgaan soos uiteengesit in artikel 239 van die Grondwet, met inbegrip van 'n hof; en
(ii) wat deur sekuriteitsmaatreëls teen ongemagtigde toegang of gebruik beskerm word.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

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

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

(c) create a serious public emergency situation,

is guilty of an aggravated offence.

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

Theft of incorporeal property

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

PART II: MALICIOUS COMMUNICATIONS

Definitions

13. In Part II, unless the context indicates otherwise—

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

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

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

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

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

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

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

"violence" means bodily harm.

Data message which incites damage to property or violence

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.

Data message which threatens persons with damage to property or violence

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(2) Enige persoon wat 'n misdryf bedoel in artikel 5(1), 6(1) of 10 pleeg en wat weet of redelikerwys moes geweet het of vermoed het dat die betrokke misdryf—

(a) die lewe in gevaar sal stel of ernstige ligaamlike beserings aan, of die dood veroorsaak van, enige persoon, of enige aantal of groep persone;

(b) 'n ernstige risiko vir die gesondheid of veiligheid van die publiek of enige segment van die publiek sal veroorsaak; of

(c) 'n ernstige openbare noodsituasie skep,

is skuldig aan 'n verswarende misdryf.

(3) 'n Vervolging ingevolge subartikel (1) of (2) moet skriftelik deur die Direkteur van Openbare Vervolgings met regsbevoegdheid gemagtig word.

Diefstal van onliggaamlike eiendom

12. Die gemeneregmisdryf van diefstal moet uitgelê word sodat dit nie die diefstal van onliggaamlike eiendom uitsluit nie.

DEEL II: KWAADWILLIGE KOMMUNIKASIES

Woordomskrywing

13. In Deel II, tensy dit uit die samehang anders blyk, beteken—

"beskadiging van eiendom" skade aan enige liggaamlike of onliggaamlike eiendom;

"geweld" liggaamlike leed;

"groep persone" eienskappe wat 'n individu identifiseer as 'n lid van 'n groep, welke eienskappe sonder beperking, ras, geslagtelikheid, geslag, swangerskap, huwelikstatus, etniese of sosiale herkoms, kleur, seksuele georiënteerdheid, ouderdom, gestremdheid, godsdiens, gewete, oortuiging, kultuur, taal, geboorte of nasionaliteit, insluit;

"openbaar maak" ten opsigte van 'n databoodskap in artikels 14, 15 en 16 bedoel, om—

(a) die databoodskap aan 'n persoon wat die bedoelde ontvanger van die elektroniese kommunikasie is of enige ander persoon te stuur;

(b) die databoodskap op 'n elektroniese kommunikasienetwerk te berg, waar die databoodskap besigtig, gekopieer of afgelaai kan word; of

(c) 'n skakel na die databoodskap wat op 'n elektroniese kommunikasienetwerk geberg is aan 'n persoon te stuur of andersins beskikbaar te stel, waar die databoodskap besigtig, gekopieer of afgelaai kan word; en

"verwante persoon" enige lid van die gesin of huishouding van 'n persoon of enige ander persoon in 'n noue verhouding met daardie persoon.

Databoodskap wat beskadiging van eiendom of geweld aanhits

14. Enige persoon wat 'n databoodskap openbaar maak deur middel van 'n elektroniese kommunikasiediens, aan 'n persoon, groep persone of die algemene publiek met die bedoeling om—

(a) beskadiging van enige eiendom wat behoort aan; of

(b) geweld teen,

'n persoon of 'n groep persone aan te hits, is skuldig aan 'n misdryf.

Databoodskap wat persone met beskadiging van eiendom of geweld dreig

15. 'n Persoon pleeg 'n misdryf as hulle, by wyse van 'n elektroniese kommunikasiediens, wederregtelik en opsetlik 'n databoodskap openbaar maak wat—

(a) 'n persoon dreig met—

(i) beskadiging van eiendom wat behoort aan daardie persoon of 'n verwante persoon; of

(ii) geweld teen daardie persoon of 'n verwante persoon; of

(b) 'n groep persone of enige persoon wat deel van daardie groep persone is, of geassosieer is met daardie groep persone, dreig met—

(i) beskadiging van eiendom wat behoort aan daardie groep persone of enige persoon wat deel uitmaak van, of geassosieer is met, daardie groep persone; of

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(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.

Disclosure of data message of intimate image

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.

PART III: ATTEMPTING, CONSPIRING, AIDING, ABETTING, INDUCING, INCITING, INSTIGATING, INSTRUCTING, COMMANDING OR PROCURING TO COMMIT OFFENCE

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

17. Any person who unlawfully and intentionally—

(a) attempts;
(b) conspires with any other person; or
(c) aids, abets, induces, incites, instigates, instructs, commands or procures another person,

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

PART IV: COMPETENT VERDICTS

Competent verdicts

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

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(ii) geweld teen die groep persone of enige persoon wat deel is van, of geassosieer is met, daardie groep persone,

en 'n redelike persoon in besit van dieselfde inligting en met inagneming van al die omstandighede, die databoodskap, hetsy alleen of saam met enige ander databoodskap of informasie, sal beskou as 'n dreigement van beskadiging van eiendom of geweld teenoor 'n persoon of kategorie persone in onderskeidelik paragraaf *(a)* of *(b)* beoog.

Openbaarmaking van databoodskap van intieme beeld

16. (1) Enige persoon (**"A"**) wat wederregtelik en opsetlik 'n databoodskap van 'n intieme beeld van 'n persoon (**"B"**) openbaar maak deur middel van 'n elektroniese kommunikasiediens, sonder die toestemming van B, is skuldig aan 'n misdryf.

(2) By die toepassing van subartikel (1) beteken —

(a) **"B"** —

(i) die persoon wat identifiseer kan word as die persoon wat in die databoodskap vertoon word;

(ii) enige persoon wat beskryf word as vertoon te wees in die databoodskap, ongeag dat die persoon nie geïdentifiseer kan word as die persoon wat in die databoodskap vertoon word nie; of

(iii) enige persoon wat uit ander inligting geïdentifiseer kan word as die persoon wat in die databoodskap vertoon word; en

(b) **"intieme beeld"** 'n uitbeelding van 'n persoon—

(i) werklik of gesimuleer en op enige wyse gemaak waarin—

(aa) B kaal is, of die geslagsorgane of anale area van B vertoon word, of indien B 'n vroulike persoon, transgenderpersoon of interseksperoon is, hul borste, vertoon word; of

(bb) die bedekte geslagsorgane of anale area van B, of indien B 'n vroulike persoon, transgenderpersoon of intersekspersoon is, hul bedekte borste, vertoon word; en

(ii) ten opsigte waarvan B aldus vertoon 'n redelike verwagting van privaatheid gehad het toe die databoodskap gemaak is op 'n wyse wat—

(aa) die seksuele integriteit of waardigheid van B skend of krenk; of

(bb) op seksuele uitbuiting neerkom.

DEEL III: POGING, SAMESWERING, HULPVERLENING, AANSTIGTING, UITLOKKING, AANHITSING, AANMOEDIGING, AANRAAIING, BEVEL, RAADGEWING OF VERKRYGING OM MISDRYF TE PLEEG

Poging, sameswering, hulpverlening, aanstigting, uitlokking, aanhitsing, aanmoediging, aanraaiing, bevel, raadgewing of verkryging om misdryf te pleeg

17. Enige persoon wat wederregtelik en opsetlik—

(a) poog;

(b) met 'n ander persoon saamsweer; of

(c) 'n ander persoon help, aanstig, uitlok, aanhits, aanraai, beveel of verkry,

om 'n misdryf ingevolge Deel I of Deel II van hierdie Hoofstuk te pleeg, is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met die straf waarvoor 'n persoon wat aan die werklike pleging van daardie misdryf skuldig bevind is, onderhewig sal wees.

DEEL IV: GEOORLOOFDE UITSPRAKE

Geoorloofde uitsprake

18. (1) Indien getuienis in strafregtelike verrigtinge nie die pleging van die ten laste gelegde misdryf bewys nie, maar 'n oortreding van artikel 17 bewys—

(a) ten opsigte van die ten laste gelegde misdryf; of

(b) ten opsigte van enige ander misdryf waaraan 'n beskuldigde op die ten laste gelegde misdryf skuldig bevind kan word,

kan die beskuldigde aan die aldus bewese misdryf skuldig bevind word.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

(a) section 2(1) or (2);
(b) section 3(2) or (3); or
(c) section 4(1), in so far as it relates to the use or possession of a software or hardware tool, for purposes of contravening section 3(1),

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

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

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

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

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

(a) a contravention of section 2(1) or (2);
(b) a contravention of section 4(1), in so far as it relates to the use or possession of a software or hardware tool, for purposes of contravening section 6(1); or
(c) the offence of malicious injury to property,

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

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

(i) section 2(1) or (2);
(ii) section 7(1)*(b)* or *(c)* or (2); or
(iii) section 4(1), in so far as it relates to the use or possession of a software or hardware tool, to acquire or use a password, access code or similar data or device,

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

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

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

(a) a contravention of section 2(1) or (2);
(b) a contravention of section 4(1), in so far as it relates to the use or possession of a software or hardware tool, for the purposes of—
  (i) interfering with data or a computer program as contemplated in section 5(1); or
  (ii) interfering with a computer data storage medium or a computer system as contemplated in section 6(1);
(c) a contravention of section 7(1) or (2), in so far as the password, access code or similar data or device was acquired, possessed, provided to another person or used for purposes of contravening the provisions of section 8;
(d) a contravention of section 9(1) or (2);
(e) the common law offence of fraud or attempt to commit that offence;
(f) the common law offence of forgery or uttering or attempt to commit that offence; or
(g) the common law offence of theft or attempt to commit that offence,

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

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

(i) the common law offence of forgery;
(ii) a contravention of section 9(2); or

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(2) Indien die getuienis op 'n aanklag van 'n oortreding van artikel 3(1), nie die misdryf of 'n oortreding van artikel 17 ten opsigte van daardie misdryf bewys nie, maar 'n oortreding van—

(a) artikel 2(1) of (2);
(b) artikel 3(2) of (3); of
(c) artikel 4(1), vir sover dit verband hou met die gebruik of besit van 'n sagteware- of hardewarenutsmiddel, vir doeleindes van oortreding van artikel 3(1),

bewys, kan die beskuldigde aan die aldus bewese misdryf skuldig bevind word.

(3) Indien die getuienis op 'n aanklag van 'n oortreding van artikel 5(1), nie die misdryf of 'n oortreding van artikel 17 ten opsigte van daardie misdryf bewys nie, maar—

(a) 'n oortreding van artikel 2(1) of (2);
(b) 'n oortreding van artikel 4(1), vir sover dit verband hou met die gebruik of besit van 'n sagteware- of hardewarenutsmiddel vir doeleindes van oortreding van artikel 5(1); of
(c) die misdryf van opsetlike saakbeskadiging,

bewys, kan die beskuldigde aan die aldus bewese misdryf skuldig bevind word.

(4) Indien die getuienis op 'n aanklag van 'n oortreding van artikel 6(1), nie die misdryf of 'n oortreding van artikel 17 ten opsigte van daardie misdryf bewys nie, maar—

(a) 'n oortreding van artikel 2(1) of (2);
(b) 'n oortreding van artikel 4(1), vir sover dit verband hou met die gebruik of besit van 'n sagteware- of hardewarenutsmiddel vir die doeleindes van 'n oortreding van artikel 6(1); of
(c) die misdryf van opsetlike saakbeskadiging,

bewys, kan die beskuldigde aan die aldus bewese misdryf skuldig bevind word.

(5) *(a)* Indien die getuienis op 'n aanklag van 'n oortreding van artikel 7(1)*(a)* of *(d)* nie die misdryf of 'n oortreding van artikel 17 ten opsigte van daardie misdryf bewys nie, maar 'n oortreding van—

(i) artikel 2(1) of (2);
(ii) artikel 7(1)*(b)* of *(c)* of (2); of
(iii) artikel 4(1), vir sover dit verband hou met die gebruik of besit van 'n sagteware- of hardewarenutsmiddel om 'n wagwoord, toegangskode of soortgelyke data of toestel te verkry of te gebruik,

bewys, kan die beskuldigde aan die aldus bewese misdryf skuldig bevind word.

(b) Indien die getuienis op 'n aanklag van 'n oortreding van artikel 7(1)*(b)* of *(c)* nie die misdryf of 'n oortreding van artikel 17 ten opsigte van daardie misdryf bewys nie, maar 'n oortreding van artikel 7(2) bewys, kan die skuldige aan die aldus bewese misdryf skuldig bevind word.

(6) Indien die getuienis op 'n aanklag van 'n oortreding van artikel 8, nie die misdryf of 'n oortreding van artikel 17 ten opsigte van daardie misdryf bewys nie, maar—

(a) 'n oortreding van artikel 2(1) of (2);
(b) 'n oortreding van artikel 4(1), vir sover dit verband hou met die gebruik of besit van 'n sagteware- of hardewarenutsmiddel vir die doeleindes van—
  (i) inmenging met data of 'n rekenaarprogram soos in artikel 5(1) beoog; of
  (ii) inmenging met 'n rekenaardatabergingsmedium of 'n rekenaarstelsel soos in artikel 6(1) bedoel;
(c) 'n oortreding van artikel 7(1) of (2) vir sover die wagwoord, toegangskode of soortgelyke data of toestelle verkry, besit, aan iemand anders voorsien of gebruik is vir die doeleindes van oortreding van die bepalings van artikel 8;
(d) 'n oortreding van artikel 9(1) of (2);
(e) die gemeneregmisdryf van bedrog of poging om daardie misdryf te pleeg;
(f) die gemeneregmisdryf van vervalsing of uitgifte of poging om daardie misdryf te pleeg; of
(g) die gemeneregmisdryf van diefstal of poging om daardie misdryf te pleeg,

bewys, kan die beskuldigde aan die aldus bewese misdryf skuldig bevind word.

(7) *(a)* Indien die getuienis op 'n aanklag van 'n oortreding van artikel 9(1), nie die misdryf of 'n oortreding van artikel 17 ten opsigte van daardie misdryf, bewys nie, maar—

(i) die gemeneregmisdryf van vervalsing;
(ii) 'n oortreding van artikel 9(2); of

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(iii) the common law offence of uttering,

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

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

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

(a) section 2(1) or (2);
(b) section 3(1) or any competent verdict provided for in subsection (2);
(c) section 5(1) or any competent verdict provided for in subsection (3);
(d) section 6(1) or any competent verdict provided for in subsection (4); or
(e) section 7(1) or any competent verdict provided for in subsection (5),

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

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

(a) section 2(1) or (2);
(b) section 5(1) or any competent verdict provided for in subsection (3); or
(c) section 6(1) or any competent verdict provided for in subsection (4),

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

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

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

PART V: SENTENCING

Sentencing

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

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

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

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

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(iii) die gemeneregmisdryf van uitgifte,

bewys, kan die beskuldigde aan die aldus bewese misdryf skuldig bevind word.

(b) Indien die getuienis op 'n aanklag van 'n oortreding van artikel 9(2), nie die misdryf bewys nie, maar die gemeneregmisdryf van uitgifte, kan die beskuldigde aan die aldus bewese misdryf skuldig bevind word.

(8) Indien 'n beskuldigde van 'n oortreding van artikel 11(1) aangekla word, en die getuienis op die aanklag nie 'n oortreding van artikel 11(1) of 'n oortreding van artikel 17 ten opsigte van daardie misdryf bewys nie, maar 'n oortreding van—

(a) artikel 2(1) of (2);
(b) artikel 3(1) of enige bevoegde uitspraak waarvoor subartikel (2) voorsiening maak;
(c) artikel 5(1) of enige bevoegde uitspraak waarvoor subartikel (3) voorsiening maak;
(d) artikel 6(1) of enige bevoegde uitspraak waarvoor subartikel (4) voorsiening maak; of
(e) artikel 7(1) of enige bevoegde uitspraak waarvoor subartikel (5) voorsiening maak,

bewys, kan die beskuldigde aan die aldus bewese misdryf skuldig bevind word.

(9) Indien 'n beskuldigde van 'n oortreding van artikel 11(2) aangekla word, en die getuienis op die aanklag nie die misdryf of 'n oortreding van artikel 17 ten opsigte van die misdryf bewys nie, maar 'n oortreding van—

(a) artikel 2(1) of (2);
(b) artikel 5(1) of enige bevoegde uitspraak waarvoor subartikel (3) voorsiening maak; of
(c) artikel 6(1) of enige bevoegde uitspraak waarvoor subartikel (4) voorsiening maak,

bewys, kan die beskuldigde aan die aldus bewese misdryf skuldig bevind word.

(10) Indien die getuienis op 'n aanklag vir enige misdryf in die voormelde subartikels nie die pleging van die aldus ten laste gelegde misdryf of enige geoorloofde uitspraak ten opsigte van die misdryf nie bewys nie, maar die pleging van 'n misdryf bewys wat weens die wesenlike elemente van daardie misdryf in die aldus ten laste gelegde misdryf inbegrepe is, kan die beskuldigde aan die aldus bewese misdryf skuldig bevind word.

(11) Indien 'n beskuldigde van 'n oortreding van artikel 14, 15 of 16 aangekla word, en die getuienis oor die aanklag nie die betrokke misdryf of 'n oortreding van artikel 17 ten opsigte van die misdryf bewys nie, maar die pleging van 'n misdryf bewys wat uit hoofde van die wesenlike elemente van daardie misdryf in die aldus ten laste gelegde misdryf inbegrepe is, kan die beskuldigde aan die aldus bewese misdryf skuldig bevind word.

DEEL V: VONNISOPLEGGING

Vonnisoplegging

19. (1) Enige persoon wat die bepalings van artikel 2(1) of (2), 3(3) of 7(2) oortree, is by skuldigbevinding strafbaar met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens vyf jaar of met beide 'n boete en sodanige gevangenisstraf.

(2) Enige persoon wat die bepalings van artikel 3(1) of (2), 4(1), 5(1), 6(1) of 7(1) oortree, is by skuldigbevinding strafbaar met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens 10 jaar of met beide 'n boete en sodanige gevangenisstraf.

(3) Enige persoon wat die bepalings van artikel 11(1) oortree, is by skuldigbevinding strafbaar met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens 15 jaar of met beide 'n boete en sodanige gevangenisstraf.

(4) 'n Hof wat 'n persoon aan 'n misdryf ingevolge artikel 8, 9(1) of (2), 10 of 11(2) skuldig bevind, kan, waar 'n straf ten opsigte van daardie misdryf nie deur enige ander wetsbepaling voorgeskryf word nie, 'n vonnis oplê soos in artikel 276 van die Strafproseswet, 1977, bepaal, wat daardie hof gepas ag en wat binne daardie hof se strafjurisdiksie is.

(5) 'n Hof wat enige vonnis ingevolge hierdie artikel oplê, of waar 'n persoon aan die misdryf van diefstal wat gepleeg of gefasiliteer is deur elektroniese middele, skuldig bevind is, moet, sonder om enige ander tersaaklike faktore uit te sluit—

(a) die feit dat die misdryf met elektroniese middele gepleeg is;
(b) die mate van die benadeling en verlies deur die klaer of enige ander persoon gely as gevolg van die pleging van so 'n misdryf;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

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

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

(i) by the person; or

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

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

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

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

PART VI: ORDERS TO PROTECT COMPLAINANTS FROM THE HARMFUL EFFECT OF MALICIOUS COMMUNICATIONS

Order to protect complainant pending finalisation of criminal proceedings

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 a protection order pending the finalisation of the criminal proceedings to—

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

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

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

(3) If the court is satisfied that there—

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

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

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

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

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(c) die mate waartoe die persoon finansieel voordeel getrek het of enige guns, voordeel, beloning, vergoeding of enige ander voordeel uit die pleging van die misdryf gekry het; of

(d) die feit dat die misdryf in samewerking met een of meer persone gepleeg is,

as verswarende omstandighede in ag neem.

(6) *(a)* Indien 'n persoon aan enige misdryf in artikel 2(1) of (2), 3(1), 5(1), 6(1), 7(1), 8, 9(1) of (2), 10 of 11(1) of (2) skuldig bevind is, moet 'n hof wat enige vonnis ingevolge daardie artikels oplê, tensy wesenlike en dwingende omstandighede die oplegging van 'n ander vonnis regverdig, 'n tydperk van direkte gevangenisstraf, met of sonder 'n boete, oplê waar die misdryf—

(i) deur die persoon; of

(ii) met die samespanning of bystand van 'n ander persoon,

gepleeg is, wat as deel van hul pligte, werksaamhede of wettige magtiging verantwoordelik was vir, in beheer was van, of toegang gehad het tot data, 'n rekenaarprogram, 'n rekenaardatabergingsmedium of 'n rekenaarstelsel behorende aan 'n ander persoon ten opsigte waarvan die betrokke misdryf gepleeg was.

(b) 'n Vonnis opgelê ingevolge paragraaf *(a)*, mag nie opgeskort word soos in artikel 297(4) van die Strafproseswet, 1977, beoog nie.

(7) Enige persoon wat die bepalings van artikel 14, 15 of 16 oortree is by skuldigbevinding strafbaar met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens drie jaar of met beide 'n boete en sodanige gevangenisstraf.

DEEL VI: BEVELE TER BESKERMING VAN KLAERS TEEN DIE SKADELIKE UITWERKING VAN KWAADWILLIGE KOMMUNIKASIES

Bevel ter beskerming van klaer hangende afhandeling van strafregtelike verrigtinge

20. (1) 'n Klaer (hierna die applikant genoem) wat 'n klag by die Suid-Afrikaanse Polisiediens indien dat 'n misdryf in artikel 14, 15 of 16 beoog na bewering teen hulle gepleeg is, kan op 'n *ex parte*-grondslag op die voorgeskrewe vorm of wyse, by 'n landdroshof aansoek doen om 'n beskermingsbevel hangende die afhandeling van die strafregtelike verrigtinge om—

(a) enige persoon te belet om die databoodskap wat met die klag verband hou, openbaar te maak of verder openbaar te maak; of

(b) 'n elektroniese kommunikasiediensverskaffer wie se elektroniese kommunikasiediens gebruik word om die databoodskap wat met die klag verband hou, te huisves of openbaar te maak, te beveel om die betrokke databoodskap te verwyder of toegang daartoe te deaktiveer.

(2) Die hof moet 'n aansoek ingevolge subartikel (1) aan die hof voorgelê, so gou as redelik moontlik oorweeg en kan vir daardie doel enige bykomende getuienis wat die hof gepas ag, oorweeg, met inbegrip van mondelinge getuienis of getuienis by wyse van beëdigde verklaring, wat deel van die oorkonde van die verrigtinge moet uitmaak.

(3) Indien die hof oortuig is dat daar—

(a) *prima facie*-getuienis is dat 'n misdryf bedoel in artikel 14, 15 of 16 na bewering teen die applikant gepleeg is; en

(b) redelike gronde is om te glo dat 'n persoon in subaritkel (1)*(a)* bedoel die betrokke databoodskap openbaar gemaak het; of

(c) redelike gronde is om te glo dat die elektroniese kommunikasiediens van die elektroniese kommunikasiediensverskaffer in subartikel (1)*(b)* bedoel, gebruik word om daardie databoodskap te huisves of gebruik was of word om daardie boodskap openbaar te maak,

kan die hof, onderworpe aan sodanige voorwaardes wat die hof gepas ag, die bevel bedoel in subartikel (1) in die voorgeskrewe vorm uitreik.

(4) Die bevel in subartikel (3) bedoel, moet aan die persoon in subartikel (1)*(a)* of elektroniese kommunikasiediensverskaffer in subartikel (1)*(b)* bedoel, op die voorgeskrewe wyse beteken word: Met dien verstande dat, indien die hof oortuig is dat die bevel nie op die voorgeskrewe wyse beteken kan word nie, die hof 'n bevel kan gee wat betekening in die vorm of op die wyse in daardie bevel gespesifiseer, toelaat.

(5) 'n Bevel in subartikel (3) bedoel, is van krag vanaf die oomblik dat dit deur die hof uitgereik word en die bestaan daarvan onder die aandag van die persoon in subartikel (1)*(a)* of elektroniese kommunikasiediensverskaffer in subartikel (1)*(b)* bedoel, gebring is.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

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

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

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

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

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

(a) attend or to remain in attendance;
(b) appear at the place and on the date and at the time to which the proceedings in question may be adjourned;
(c) remain in attendance at those proceedings as so adjourned; or
(d) produce any book, document or object specified in the subpoena,

is guilty of an offence.

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

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

Electronic communications service provider to furnish particulars to court

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 discloses the data message, or the electronic communications service provider referred to in section 20(1)*(b)*, whose service is used to host or was or is used to disclose the data message, is not known, the court may—

(a) adjourn the proceedings to any time and date on the terms and conditions which the court deems appropriate; and
(b) issue a direction in the prescribed form, directing an electronic communications service provider, that is believed to be able to furnish such particulars, to furnish the court in the prescribed manner by means of an affidavit in the prescribed form with—
  (i) the electronic communications identity number from where the data message originated;
  (ii) the name, surname, identity number and address of the person to whom the electronic communications identity number has been assigned;
  (iii) any information which indicates that the data message was or was not sent from the electronic communications identity number of the person to the electronic communications identity number of the applicant;
  (iv) any information that is available to an electronic communications service provider that may be of assistance to the court to identify the person

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(6) 'n Persoon in subartikel (1)*(a)* bedoel, anders as die persoon wat van die pleging van die betrokke misdryf beskuldig word, of 'n elektroniese kommunikasie-diensverskaffer in subartikel (1)*(b)* bedoel, kan, binne 14 dae nadat die bevel ingevolge subartikel (4) aan hulle beteken is, of binne sodanige verdere tydperk soos die hof mag toelaat, by kennisgewing aan die betrokke landdroshof, op die voorgeskrewe vorm en wyse, by die hof aansoek doen om die tersydestelling of wysiging van die bevel in subartikel (3) bedoel.

(7) *(a)* Die hof moet 'n aansoek ingevolge subartikel (6) aan die hof voorgelê, so gou as redelik moontlik oorweeg en kan vir daardie doel sodanige bykomende getuienis wat die hof gepas ag, oorweeg, met inbegrip van mondelinge getuienis of getuienis by wyse van beëdigde verklaring, wat deel van die oorkonde van die verrigtinge moet uitmaak.

(b) Die hof kan, by die aanvoer van goeie gronde vir die wysiging of tersydestelling van die beskermingsbevel, 'n bevel te dien effekte uitreik.

(8) Die hof kan, by die toepassing van subartikels (2) en (7), op die voorgeskrewe vorm en wyse enige persoon laat dagvaar as 'n getuie by daardie verrigtinge of om enige boek, dokument of voorwerp voor te lê, indien die getuienis van daardie persoon of boek, dokument of voorwerp vir die hof noodsaaklik blyk te wees vir die regverdige beslissing van die saak.

(9) Enige persoon in subartikel (1)*(a)* bedoel of 'n elektroniese kommunikasie-diensverskaffer in subartikel (1)*(b)* bedoel, wat versuim om aan 'n bevel in subartikel (3) bedoel of enige wysigings daarvan te voldoen, is skuldig aan 'n misdryf.

(10) Enige persoon wat ingevolge subartikel (8) gedagvaar is om verrigtinge by te woon en wat versuim om—

(a) dit by te woon of teenwoordig te bly;
(b) te verskyn by die plek en op die datum en die tyd waarheen die betrokke verrigtinge verdaag mag word;
(c) teenwoordig te bly by daardie verrigtinge aldus verdaag; of
(d) enige boek, dokument of voorwerp in die dagvaarding gespesifiseer, voor te lê,

is skuldig aan 'n misdryf.

(11) Die bepalings ten opsigte van appèl en hersiening soos in die Wet op Landdroshowe, 1944, en die Wet op Hoër Howe, 2013, bepaal, is van toepassing op verrigtinge ingevolge hierdie artikel.

(12) By die toepassing van hierdie artikel en artikels 21 en 22 beteken **"om 'n databoodskap te huisves"** om die databoodskap op 'n elektroniese kommunikasie-netwerk te berg wat gebruik word om 'n elektroniese kommunikasiediens te verskaf, waar dit besigtig, gekopieer of afgelaai kan word.

Elektroniese kommunikasiediensverskaffer moet besonderhede aan hof verskaf

21. (1) Indien daar ingevolge artikel 20(1) om 'n beskermingsbevel aansoek gedoen word en die hof ingevolge artikel 20(3) oortuig is dat 'n beskermingsbevel uitgereik moet word en die besonderhede van die persoon in artikel 20(1)*(a)* bedoel, wat die betrokke databoodskap openbaar maak of die elektroniese kommunikasiediensver-skaffer, in artikel 20(1)*(b)* bedoel, wie se diens gebruik word om die databoodskap te huisves of gebruik was of word om die databoodskap openbaar te maak, is nie bekend nie, kan die hof—

(a) die verrigtinge verdaag tot enige tyd en datum op die bepalings en voorwaardes wat die hof doenlik ag; en
(b) 'n lasgewing in die voorgeskrewe vorm uitreik, wat 'n elektroniese kommunikasiediensverskaffer wat geglo word in staat te wees om daardie besonderhede te verskaf, gelas om die hof op die voorgeskrewe wyse deur middel van 'n beëdigde verklaring in die voorgeskrewe vorm te voorsien van—
  (i) die elektroniese kommunikasie-identiteitsnommer van waar die databoodskap afkomstig was;
  (ii) die naam, van, identiteitsnommer en adres van die persoon aan wie die elektroniese kommunikasie-identiteitsnommer toegeken is;
  (iii) enige inligting wat aandui dat die databoodskap vanaf die elektroniese kommunikasie-identiteitsnommer van die persoon na die elektroniese kommunikasie-identiteitsnommer van die applikant gestuur is al dan nie;
  (iv) enige inligting wat beskikbaar is aan 'n elektroniese kommunikasie-diensverskaffer wat die hof behulpsaam kan wees om die persoon bedoel

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

referred to in section 20(1)*(a)* or the electronic communications service provider referred to in section 20(1)*(b)*, which provides a service to that person;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) must consider the application;

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

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

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

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

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

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

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

in artikel 20(1)*(a)* of die elektroniese kommunikasiediensverskaffer bedoel in artikel 20(1)*(b)*, wat 'n diens aan daardie persoon verskaf, te identifiseer;

(v) enige inligting wat aan 'n elektroniese kommunikasiediensverskaffer beskikbaar is wat—

(aa) bevestig of hul elektroniese kommunikasiediens gebruik word om die betrokke databoodskap te huisves of gebruik was of word om dit openbaar te maak al dan nie; of

(bb) die hof behulpsaam kan wees om die elektroniese kommunikasiediensverskaffer te identifiseer wie se diens gebruik word om die betrokke databoodskap te huisves of gebruik was of word om dit openbaar te maak; of

(vi) 'n assessering of die elektroniese kommunikasiediensverskaffer in 'n posisie is, al dan nie, om—

(aa) die databoodskap of 'n skakel na daardie databoodskap te verwyder; of

(bb) toegang tot die databoodskap of 'n skakel tot daardie databoodskap te deaktiveer.

(2) Indien die hof 'n lasgewing ingevolge subartikel (1)*(b)* uitreik, moet die hof gelas dat die lasgewing op die voorgeskrewe wyse aan die elektroniese kommunikasiediensverskaffer beteken word: Met dien verstande dat indien die hof oortuig is dat die lasgewing nie op die voorgeskrewe wyse beteken kan word nie, die hof 'n bevel kan gee wat betekening in die vorm of op die wyse in daardie bevel gespesifiseer, toelaat.

(3) *(a)* Die inligting in subartikel (1)*(b)* bedoel, moet binne vyf gewone hofdae vanaf die tyd waarop die lasgewing aan 'n elektroniese kommunikasiediensverskaffer beteken is, aan die hof verskaf word.

(b) 'n Elektroniese kommunikasiediensverskaffer aan wie 'n lasgewing beteken is, kan op die voorgeskrewe wyse en deur middel van 'n beëdigde verklaring in die voorgeskrewe vorm by die hof aansoek doen om—

(i) 'n verlenging van die tydperk van vyf gewone hofdae in paragraaf *(a)* bedoel vir 'n verdere tydperk van vyf gewone hofdae op grond daarvan dat die inligting nie tydig voorsien kan word nie; of

(ii) die kansellasie van die lasgewing op gronde daarvan dat—

(aa) hulle nie 'n elektroniese kommunikasiediens aan die applikant of die persoon bedoel in artikel 20(1)*(a)*, lewer nie;

(bb) die inligting wat aangevra is, nie in die rekords van die elektroniese kommunikasiediensverskaffer beskikbaar is nie; of

(cc) hul diens nie gebruik word om die betrokke databoodskap te huisves nie of gebruik was of word om dit openbaar te maak nie.

(4) Ná ontvangs van 'n aansoek ingevolge subartikel (3)*(b)*—

(a) moet die hof die aansoek oorweeg;

(b) kan die hof, op die voorgeskrewe wyse, sodanige bykomende getuienis versoek by wyse van 'n beëdigde verklaring van die elektroniese kommunikasiediensverskaffer soos wat die hof goeddink;

(c) moet die hof daaroor beslis; en

(d) moet die hof die elektroniese kommunikasiediensverskaffer op die voorgeskrewe vorm en wyse van die uitslag van die aansoek verwittig.

(5) *(a)* Die hof kan, by ontvangs van 'n beëdigde verklaring van 'n elektroniese kommunikasiediensverskaffer wat die inligting bedoel in subartikel (1)*(b)*, bevat, die uitreiking van 'n beskermingsbevel ingevolge artikel 20(3) teen die persoon of elektroniese kommunikasiediensverskaffer oorweeg op die datum waartoe die verrigtinge verdaag is.

(b) Enige inligting wat ingevolge subartikel (1)*(b)* aan die hof verskaf is, maak deel uit van die getuienis wat 'n hof ingevolge artikel 20(3) kan oorweeg.

(6) Die Kabinetslid verantwoordelik vir die regspleging kan, by kennisgewing in die *Staatskoerant*, redelike tariewe voorskryf vir vergoeding betaalbaar aan elektroniese kommunikasiediensverskaffers vir die verskaffing van die inligting in subartikel (1)*(b)* bedoel.

(7) Enige elektroniese kommunikasiediensverskaffer of werknemer van 'n elektroniese kommunikasiediensverskaffer wat—

(a) versuim om die vereiste inligting binne vyf gewone hofdae vandat die lasgewing aan sodanige elektroniese kommunikasiediensverskaffer beteken

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

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

is guilty of an offence.

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

Orders on finalisation of criminal proceedings

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 provision of that Act must apply with the necessary changes as required by the context.

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

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

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

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

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

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

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

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

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

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

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

(a) attend or to remain in attendance;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

is, aan 'n hof te verskaf ingevolge subartikel (3)*(a)* of sodanige verlengde tydperk wat ingevolge subartikel (3)*(b)* deur die hof toegelaat word; of

(b) 'n vals verklaring in 'n wesenlike opsig in 'n beëdigde verklaring in subartikel (1)*(b)* of (3)*(b)* bedoel, maak,

is skuldig aan 'n misdryf.

(8) By die toepassing van hierdie artikel, beteken **"elektroniese kommunikasie-identiteitsnommer"** 'n tegniese identifikasie-etiket wat die oorsprong of bestemming van elektroniese kommunikasieverkeer verteenwoordig.

Bevele by afhandeling van strafregtelike verrigtinge

22. (1) Wanneer 'n persoon—

(a) aan 'n misdryf ingevolge artikel 14, 15 of 16 skuldig bevind word; of

(b) van 'n misdryf ingevolge artikel 14, 15 of 16 vrygespreek word,

maar getuienis bewys dat die persoon aan teistering meegedoen het of gepoog het om aan teistering mee te doen, soos beoog in die Wet op Beskerming teen Teistering, 2011, kan die verhoorhof, na afloop van 'n ondersoek, 'n beskermingsbevel soos beoog in artikel 9(4) van die Wet op Beskerming teen Teistering, 2011, teen die persoon uitreik, waarna die bepaling van daardie Wet, met die nodige veranderinge soos deur die samehang vereis, van toepassing sal wees.

(2) Die verhoorhof wat 'n persoon skuldig bevind aan 'n misdryf in artikel 14, 15 of 16 beoog, moet—

(a) daardie persoon beveel om te weerhou van die verdere beskikbaarstelling, openbaarmaking of verspreiding van die databoodskap beoog in artikel 14, 15 of 16, wat verband hou met die aanklag waaraan daardie persoon skuldig bevind is;

(b) daardie persoon of enige ander persoon beveel om die betrokke databoodskap of enige kopie van die databoodskap of enige uitset van die databoodskap te vernietig en 'n beëdigde verklaring in die voorgeskrewe vorm aan die aanklaer in die bevel geïdentifiseer, voor te lê dat die databoodskap aldus vernietig is; of

(c) 'n elektroniese kommunikasiediensverskaffer beveel om die betrokke databoodskap te verwyder of toegang daartoe te deaktiveer.

(3) Die bevel in subartikel (2)*(b)* bedoel, vir sover dit verband hou met 'n persoon, anders as die persoon wat aan die misdryf skuldig bevind is, en subartikel (2)*(c)*, moet in die voorgeskrewe vorm wees en moet op die voorgeskrewe wyse aan die persoon of elektroniese kommunikasiediensverskaffer beteken word: Met dien verstande dat, indien die verhoorhof oortuig is dat die bevel nie op die voorgeskrewe vorm en wyse beteken kan word nie, die hof 'n bevel kan gee wat betekening in die vorm of op die wyse in daardie bevel gespesifiseer, toelaat.

(4) Enige persoon beoog in subartikel (2)*(a)* of *(b)* of elektroniese kommunikasie-diensverskaffer beoog in subartikel (2)*(c)*, wat versuim om aan 'n bevel in subartikel (2) bedoel, te voldoen, is skuldig aan 'n misdryf.

(5) 'n Elektroniese kommunikasiediensverskaffer wat beveel word om die databoodskap te verwyder of toegang daartoe te deaktiveer, kan, binne 14 dae nadat die bevel ingevolge subartikel (3) aan hulle beteken is, by kennisgewing aan die betrokke verhoorhof, op die voorgeskrewe vorm en wyse, by die hof aansoek doen om die tersydestelling of wysiging van die bevel in subartikel (2)*(c)* bedoel.

(6) *(a)* Die verhoorhof moet so gou as redelikerwys moontlik 'n aansoek daaraan voorgelê ingevolge subartikel (5), oorweeg en kan vir daardie doel bykomende getuienis oorweeg wat die hof gepas ag, met inbegrip van mondelinge getuienis of getuienis by wyse van beëdigde verklaring, wat deel van die oorkonde moet uitmaak.

(b) Die verhoorhof kan, by die aanvoer van goeie gronde vir die wysiging of tersydestelling van die bevel, 'n bevel te dien effekte uitreik.

(7) Die hof kan, vir doeleindes van subartikel (6)*(a)*, op die voorgeskrewe vorm en wyse, enige persoon laat dagvaar as 'n getuie by daardie verrigtinge of om enige boek, dokument of voorwerp voor te lê, indien die getuienis van daardie persoon of boek, dokument of voorwerp vir die hof noodsaaklik blyk te wees vir die regverdige beslissing van die saak.

(8) Enige persoon wat ingevolge subartikel (7) gedagvaar word om verrigtinge by te woon en wat versuim om—

(a) dit by te woon of teenwoordig te bly;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(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.

Penalties

23. 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.

CHAPTER 3

JURISDICTION

Jurisdiction

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

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

(b) the person to be charged is—

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

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

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

(c) the offence was committed—

(i) in the territory of the Republic; or

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

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

(i) in the territory of the Republic; or

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

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

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(b) te verskyn by die plek en op die datum en tyd waarheen die betrokke verrigtinge verdaag kan word;

(c) teenwoordig te bly by daardie verrigtinge aldus verdaag; of

(d) enige boek, dokument of voorwerp in die dagvaarding gespesifiseer, voor te lê,

is skuldig aan 'n misdryf.

(9) By die toepassing van hierdie artikel beteken **"verhoorhof"**—

(a) 'n landdroshof ingestel kragtens artikel 2(1)*(f)*(i) van die Wet op Landdroshowe, 1944;

(b) 'n hof vir 'n streeksafdeling ingestel kragtens artikel 2(1)*(g)*(i) van die Wet op Landdroshowe, 1944; of

(c) 'n Hooggeregshof bedoel in artikel 6(1) van die Wet op Hoër Howe, 2013.

(10) Wanneer iemand aan 'n misdryf ingevolge artikel 14, 15 of 16 skuldig bevind word, moet die verhoorhof 'n bevel gee dat die persoon alle koste moet vergoed wat redelikerwys aangegaan is deur—

(a) 'n klaer na aanleiding van enige lasgewing ingevolge artikel 21(1)*(b)* uitgereik; of

(b) 'n elektroniese kommunikasiediensverskaffer om die betrokke databoodskap te verwyder of toegang tot die betrokke databoodskap te deaktiveer,

waarop die bepalings van artikel 300 van die Strafproseswet, 1977, met die nodige veranderinge deur die samehang vereis, daardie bevel van toepassing sal wees.

Strawwe

23. Enige persoon of elektroniese kommunikasiediensverskaffer wat aan 'n misdryf in artikel 20(9) of (10), 21(7) of 22(4) of (8) skuldig bevind word, is by skuldigbevinding strafbaar met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens twee jaar of met 'n boete sowel as sodanige gevangenisstraf.

HOOFSTUK 3

JURISDIKSIE

Jurisdiksie

24. (1) 'n Hof in die Republiek het jurisdiksie om enige misdryf in Deel I of Deel II van Hoofstuk 2 te bereg, indien—

(a) die beskuldigde gearresteer is binne die grondgebied van die Republiek, aan boord van 'n vaartuig, 'n skip, 'n aflandige installasie of vasstaande platform, of 'n lugvaartuig geregistreer of vereis om geregistreer te wees in die Republiek;

(b) die persoon wat aangekla staan te word 'n—

(i) burger van die Republiek is of gewoonlik in die Republiek woonagtig is;

(ii) 'n maatskappy, as sodanig ingelyf of geregistreer kragtens enige wet, in die Republiek is; of

(iii) enige liggaam van persone, ingelyf of oningelyf, in die Republiek is;

(c) die misdryf gepleeg is—

(i) in die grondgebied van die Republiek; of

(ii) aan boord van 'n vaartuig, 'n skip, 'n aflandige installasie of vaste platform, of 'n lugvaartuig geregistreer of vereis om geregistreer te wees in die Republiek toe die misdryf gepleeg is;

(d) enige handeling ter voorbereiding van die misdryf of enige optrede nodig om die misdryf of enige deel van die misdryf te pleeg, plaasgevind het—

(i) in die grondgebied van die Republiek; of

(ii) aan boord van 'n vaartuig, 'n skip, 'n aflandige installasie of vaste platform, of 'n lugvaartuig geregistreer of vereis om geregistreer te wees in die Republiek toe die handeling optrede, of deel van die misdryf plaasgevind het;

(e) die misdryf enige persoon, 'n beperkte rekenaarstelsel beoog in artikel 11(1)*(b)*, 'n openbare liggaam of enige besigheid in die Republiek raak;

(f) die misdryf buite die Republiek gepleeg is teen—

(i) enige persoon wat 'n burger van die Republiek is of gewoonlik in die Republiek woonagtig is;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

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

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

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

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

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

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

(b) that person—

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

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

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

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

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

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

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

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

CHAPTER 4

POWERS TO INVESTIGATE, SEARCH, ACCESS OR SEIZE

Definitions

25. In this Chapter, unless the context indicates otherwise—

"access" includes without limitation to make use of—

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

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

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

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

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

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

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

"seize" includes to—

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(ii) 'n beperkte rekenaarstelsel in artikel 11(1)*(b)* beoog;
(iii) 'n maatskappy, as sodanig ingelyf of geregistreer kragtens enige wet, in die Republiek;
(iv) enige liggaam persone, ingelyf of oningelyf, in die Republiek; of
(v) 'n regeringsfasiliteit van die Republiek, met inbegrip van 'n ambassade of ander diplomatieke of konsulêre perseel, of enige ander perseel van die Republiek; of

(g) die getuienis enige ander grondslag deur die reg erken, openbaar, ingevolge waarvan die hof jurisdiksie kan vestig om die misdryf te verhoor.

(2) Enige handeling wat na bewering 'n misdryf ingevolge Deel I of Deel II van Hoofstuk 2 daarstel en wat buite die Republiek gepleeg is deur 'n persoon, behalwe 'n persoon in subartikel (1) beoog, moet, ongeag of die handeling by die plek waar dit gepleeg is 'n misdryf daarstel, al dan nie, geag word in die Republiek gepleeg te wees indien—

(a) daardie persoon aan die Republiek uitgelewer word; of
(b) daardie persoon—
(i) in die Republiek gevind word; en
(ii) om een of ander rede nie deur die Republiek uitgelewer word nie of indien daar geen aansoek is om die persoon uit te lewer nie.

(3) Waar 'n persoon aangekla word van poging, sameswering, hulpverlening, aanstigting, uitlokking, aanhitsing, aanmoediging, aanraaiing, bevel, raadgewing of verkryging om 'n misdryf te pleeg of as 'n begunstiger by daardie misdryf, word die misdryf geag gepleeg te wees nie slegs by die plek waar die handeling gepleeg is nie, maar ook by elke plek waar die persoon as sodanig opgetree het.

(4) *(a)* 'n Vervolging van 'n misdryf bedoel in Deel I of Deel II van Hoofstuk 2, wat buite die Republiek gepleeg is—

(i) kan slegs teen 'n persoon ingestel word met die skriftelike toestemming van die Nasionale Direkteur van Openbare Vervolging; en
(ii) moet 'n aanvang neem voor 'n hof deur die Nasionale Direkteur vir Openbare Vervolging aangewys.

(b) 'n Afskrif van die skriftelike toestemming en aanwysing moet aan die beskuldigde beteken word en die oorspronklike daarvan moet by die hof waar die verrigtinge 'n aanvang neem, ingedien word.

(5) Die Nasionale Kommissaris en die Nasionale Hoof van die Direktoraat, in oorleg met die Nasionale Direkteur van Openbare Vervolging, moet voorskrifte uitreik, waaraan alle polisiebeamptes in die uitvoering van hul werksaamhede ingevolge hierdie Wet rakende die ondersoek van misdrywe wat buite die Republiek gepleeg is, moet voldoen.

HOOFSTUK 4

BEVOEGDHEDE VAN ONDERSOEK, DEURSOEKING, TOEGANG OF BESLAGLEGGING

Woordomskrywing

25. In hierdie Hoofstuk, tensy uit die samehang anders blyk, beteken—

"beslag lê" ook om—

(a) 'n rekenaardatabergingsmedium of enige deel van 'n rekenaarstelsel te verwyder;
(b) data, 'n rekenaarprogram, 'n rekenaardatabergingsmedium of enige deel van 'n rekenaarstelsel ontoeganklik te maak ten einde getuienis te bewaar;
(c) 'n kopie van data of 'n rekenaarprogram te maak en te behou; of
(d) 'n drukstuk van die uitset van data of 'n rekenaarprogram te maak en te hou;

"ondersoeker" enige gepaste en geskikte persoon, wat nie 'n lid van die Suid-Afrikaanse Polisiediens is nie, en wat—

(a) ingevolge 'n deursoekingslasbrief in artikel 29(3) beoog, geïdentifiseer en gemagtig is; of
(b) ingevolge artikel 31(2), 32(3) of 33(4) deur 'n polisiebeampte versoek is,

om, onderworpe aan die leiding en beheer van 'n polisiebeampte, die polisiebeampte by te staan met die deursoeking vir, toegang tot en beslaglegging op 'n item; en

"toegang" ook om sonder beperking gebruik te maak van—

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(a) remove a computer data storage medium or any part of a computer system;
(b) render inaccessible, data, a computer program, a computer data storage medium or any part of a computer system in order to preserve evidence;
(c) make and retain a copy of data or a computer program; or
(d) make and retain a printout of the output of data or a computer program.

Standard Operating Procedures

26. (1) The Cabinet member responsible for policing, in consultation with the National Commissioner, the National Head of the Directorate, the National Director of Public Prosecutions and the Cabinet member responsible for the administration of justice must, after following a process of public consultation, within 12 months of the commencement of this Chapter, issue Standard Operating Procedures which must be observed by—
(a) the South African Police Service; or
(b) any other person or agency who or which is authorised in terms of the provisions of any other law to investigate any offence in terms of any law,

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

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

Application of Criminal Procedure Act, 1977

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

Search for, access to, or seizure of certain articles

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

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

29. (1) Subject to the provisions of sections 31, 32, 33 and 40(1) and (2) of this Act, section 4(3) of the Customs and Excise Act, 1964, sections 69(2)*(b)* and 71 of the Tax Administration Act, 2011, and section 21*(e)* and *(f)* of the Customs Control Act, 2014, an article can only be searched for, accessed or seized by virtue of a search warrant issued—
(a) by a magistrate or judge of the High Court, on written application by a police official, if it appears to the magistrate or judge, from information on oath or by way of affirmation, as set out in the application, that there are reasonable grounds for believing that an article—
(i) is within their area of jurisdiction; or
(ii) is being used or is involved or has been used or was involved in the commission of an offence—
(aa) within their area of jurisdiction; or
(bb) within the Republic, if it is unsure within which area of jurisdiction the article is being used or is involved or has been used or was involved in the commission of an offence; or
(b) by a magistrate or judge of the High Court presiding at criminal proceedings, if it appears to such magistrate or judge that an article is required in evidence at such proceedings.

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(a) 'n rekenaardatabergingsmedium, of 'n rekenaarstelsel, of die toebehore en komponente of enige deel daarvan of enige bykomstige toestel of komponent daartoe; en
(b) data of 'n rekenaarprogram gehou in 'n rekenaardatabergingsmedium of 'n rekenaarstelsel,

vir sover dit nodig is om te deursoek vir en beslag te lê op 'n item.

Standaardbedryfsprosedures

26. (1) Die Kabinetslid verantwoordelik vir polisiëring, in oorleg met die Nasionale Kommissaris, die Nasionale Hoof van die Direktoraat, die Nasionale Direkteur van Openbare Vervolging en die Kabinetslid verantwoordelik vir die regspleging moet, na afloop van 'n proses van openbare oorlegpleging, binne 12 maande vanaf die inwerkingtreding van hierdie Hoofstuk, Standaardbedryfsprosedures uitreik wat nagekom moet word deur—

(a) die Suid-Afrikaanse Polisiediens; of
(b) enige ander persoon of agentskap wat ingevolge die bepalings van enige ander wet gemagtig is om enige misdryf ingevolge enige wet te ondersoek,

in die ondersoek van enige misdryf of vermeende misdryf ingevolge Deel I of Deel II van Hoofstuk 2 of enige ander misdryf of vermeende misdryf wat gepleeg is by wyse van, of gefasiliteer is deur die gebruik van, 'n item.

(2) Die Standaardbedryfsprosedures in subartikel (1) bedoel en enige wysiging daartoe moet in die *Staatskoerant* gepubliseer word.

Toepassing van bepalings van Strafproseswet, 1977

27. Die Strafproseswet, 1977, is van toepassing addisioneel tot die bepalings van hierdie Hoofstuk, vir sover dit nie onbestaanbaar is met die bepalings van hierdie Hoofstuk nie.

Deursoeking vir, toegang tot, of beslaglegging op sekere items

28. 'n Polisiebeampte kan, ooreenkomstig die bepalings van hierdie Hoofstuk, deursoek vir, toegang kry tot en beslag lê op enige item, binne die Republiek.

Deursoeking vir, toegang tot en beslaglegging op item kragtens deursoekingslasbrief

29. (1) Behoudens die bepalings van artikels 31, 32, 33 en 40(1) en (2) van hierdie Wet, artikel 4(3) van die Doeane- en Aksynswet, 1964, artikels 69(2)*(b)* en 71 van die Wet op Belastingadministrasie, 2011, en artikel 21*(e)* en *(f)* van die Wet op Doeanebeheer, 2014, kan deursoeking vir, toegang kry tot, of beslaglegging op, 'n item slegs plaasvind uit hoofde van 'n deursoekingsslasbrief uitgereik—

(a) deur 'n landdros of regter van die Hooggeregshof, by skriftelike aansoek deur 'n polisiebeampte, indien dit vir die landdros of regter uit inligting onder eed of by wyse van plegtige verklaring, soos in die aansoek uiteengesit, blyk dat daar redelike gronde is om te glo dat 'n item—
    (i) binne hul regsgebied is; of
    (ii) gebruik word of betrokke is of gebruik is of betrokke was in die pleging van 'n misdryf—
        (aa) binne hul regsgebied; of
        (bb) binne die Republiek, indien dit onseker is binne watter regsgebied die item gebruik word of betrokke is of gebruik is of betrokke was in die pleging van 'n misdryf; of
(b) deur 'n landdros of regter van die Hooggeregshof wat by strafregtelike verrigtinge voorsit, indien dit vir daardie landdros of regter blyk dat 'n item as getuienis by bedoelde verrigtinge benodig word.

(2) 'n Deursoekingslasbrief ingevolge subartikel (1) uitgereik, moet 'n polisiebeampte in die lasbrief geïdentifiseer gelas om te deursoek vir, toegang te kry tot of beslag te lê op die betrokke item en, vir daardie doel, moet dit die polisiebeampte magtig om—

(a) enige persoon in die lasbrief geïdentifiseer, te deursoek;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

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

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

(i) is nearby;

(ii) uses; or

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

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

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

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

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

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

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

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

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

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

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

Oral application for search warrant or amendment of warrant

30. (1) An application referred to in section 29(1)*(a)*, or an application for the amendment of a warrant issued in terms of section 29(1)*(a)*, may be made orally by a specifically designated police official, if it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application.

(2) An oral application referred to in subsection (1) must—

(a) indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the police official, justify the making of an oral application; and

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(b) enige houer, perseel, voertuig, fasiliteit, skip of lugvaartuig in die lasbrief geïdentifiseer, te betree en te deursoek;

(c) enige persoon te deursoek wat, op redelike gronde, geglo word in staat is om enige inligting van wesenlike belang aangaande die aangeleentheid wat ondersoek word, te voorsien en wat naby sodanige houer, op of by sodanige perseel, voertuig, fasiliteit, skip of lugvaartuig gevind word;

(d) enige persoon te deursoek wat, op redelike gronde, geglo word in staat is om enige inligting van wesenlike belang te voorsien aangaande die aangeleentheid wat ondersoek word en wat—

(i) in die nabyheid is;

(ii) gebruik maak; of

(iii) in besit of in direkte beheer is,

van enige data, rekenaarprogram, rekenaardatabergingsmedium of rekenaarstelsel in die lasbrief geïdentifiseer, tot die mate in die lasbrief uiteengesit;

(e) te deursoek vir enige item in die lasbrief geïdentifiseer tot die mate in die lasbrief uiteengesit;

(f) toegang te kry tot enige item in die lasbrief geïdentifiseer tot die mate in die lasbrief uiteengesit;

(g) beslag te lê op 'n item in die lasbrief geïdentifiseer tot die mate in die lasbrief uiteengesit; of

(h) enige instrument, toestel, toerusting, wagwoord, dekripteringsleutel, data, rekenaarprogram, rekenaardatabergingsmedium of rekenaarstelsel of ander inligting gebruik of verkry en gebruik wat, op redelike gronde, vermoed word nodig is om te deursoek vir, toegang te kry tot of beslag te lê op 'n item in die lasbrief geïdentifiseer tot die mate in die lasbrief uiteengesit.

(3) 'n Deursoekingslasbrief kragtens subartikel (1) uitgereik, kan vereis dat 'n ondersoeker of ander persoon in die lasbrief geïdentifiseer, die polisiebeampte in die lasbrief geïdentifiseer, bystaan in die deursoeking vir, toegang kry tot of beslaglegging op die betrokke item, tot die mate in die lasbrief uiteengesit.

(4) *(a)* 'n Deursoekingslasbrief kan te eniger tyd uitgevoer word, tensy die persoon wat die lasbrief uitreik skriftelik anders spesifiseer.

(b) 'n Deursoekingslasbrief kan op enige dag uitgereik word en is van krag totdat dit uitgevoer is of deur die persoon wat dit uitgereik het, of indien daardie persoon nie beskikbaar is nie, deur 'n persoon met soortgelyke gesag, gekanselleer word.

(5) 'n Polisiebeampte wat 'n lasbrief kragtens hierdie artikel uitvoer, moet 'n afskrif van die lasbrief en die skriftelike aansoek van die polisiebeampte beoog in subartikel (1)*(a)*, oorhandig aan enige persoon wie se regte geraak is ten opsigte van enige deursoeking, of item waartoe toegang gekry is of waarop beslag gelê is kragtens die lasbrief.

(6) Die bepalings van subartikels (1) tot (5) is van toepassing met die veranderinge deur die samehang vereis op 'n wysiging van 'n lasbrief ingevolge subartikel (1) uitgereik.

Mondelinge aansoek om deursoekingslasbrief of wysiging van lasbrief

30. (1) 'n Aansoek in artikel 29(1)*(a)* bedoel, of 'n aansoek om die wysiging van 'n lasbrief ingevolge artikel 29(1)*(a)* uitgereik, kan mondeling deur 'n spesifiek aangewese polisiebeampte gedoen word, indien dit nie redelikerwys prakties is, met inagneming van die dringendheid van die saak of die bestaan van buitengewone omstandighede, om 'n skriftelike aansoek te bring nie.

(2) 'n Mondelinge aansoek in subartikel (1) bedoel, moet—

(a) die besonderhede van die dringendheid van die saak of die ander buitengewone omstandighede aandui wat, na mening van die polisiebeampte, die doen van 'n mondelinge aansoek regverdig; en

(b) voldoen aan enige aanvullende voorskrifte aangaande mondelinge aansoeke wat ingevolge artikel 8(3) van die Wet op Hoër Howe, 2013, deur die Hoofregter uitgereik kan word.

(3) 'n Landdros of regter van die Hooggeregshof kan, by die bring van 'n mondelinge aansoek ingevolge subartikel (1) en behoudens subartikel (4), 'n lasbrief beoog in artikel 29(1)*(a)* uitreik of wysig.

This gazette is also available free online at www.gpwonline.co.za

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

(a) if the magistrate or judge of the High Court concerned is satisfied, on the facts alleged in the oral application concerned, that—
  (i) there are reasonable grounds to believe that a warrant or any amendment to a warrant applied for could be issued;
  (ii) a warrant or an amendment to a warrant is necessary immediately in order to search for, access or seize an article—
    (aa) within their area of jurisdiction; or
    (bb) within the Republic, if it is unsure within which area of jurisdiction the article is being used or is involved or has been used or was involved in the commission of an offence; and
  (iii) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application for the issuing of a warrant or to amend a warrant; and

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

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

(a) be in writing;

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

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

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

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

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

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

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

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

32. (1) A police official may without a search warrant referred to in section 29(1)*(a)* search any person, container, premises, vehicle, facility, ship or aircraft for the purposes of performing the powers referred to in paragraphs *(a)* and *(b)* of the definition of ''seize'' in respect of a computer data storage medium or any part of a computer system referred to in paragraph *(c)* or *(d)* of the definition of ''article'', if the police official on reasonable grounds believes—

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(4) 'n Lasbrief of enige wysiging aan 'n lasbrief kan slegs kragtens subartikel (3) uitgereik word—

(a) indien die landdros of regter van die betrokke Hooggeregshof, op grond van die feite in die betrokke mondelinge aansoek aangevoer, oortuig is dat—

(i) daar redelike gronde is om te glo dat 'n lasbrief of enige wysiging van 'n lasbrief waarom aansoek gedoen is, uitgereik kan word;

(ii) 'n lasbrief of 'n wysiging van 'n lasbrief onmiddellik noodsaaklik is ten einde te deursoek vir, toegang te kry tot of beslag te lê op 'n item—

(aa) binne hul regsgebied; of

(bb) binne die Republiek, indien hulle onseker is binne watter regsgebied die item gebruik word of betrokke is in die pleging van 'n misdryf; en

(iii) dit nie redelik moontlik is, met inagneming van die dringendheid van die saak of die bestaan van buitengewone omstandighede, om 'n skriftelike aansoek te bring vir die uitreiking van 'n lasbrief of om 'n lasbrief te wysig nie; en

(b) op voorwaarde dat die betrokke polisiebeampte 'n skriftelike aansoek aan die betrokke landdros of regter van die Hooggeregshof binne 48 uur ná die uitreiking van die lasbrief of gewysigde lasbrief kragtens subartikel (3), moet voorlê.

(5) 'n Lasbrief of enige wysiging van 'n lasbrief kragtens subartikel (3) uitgereik, moet—

(a) skriftelik wees;

(b) elektronies aan die polisiebeampte gestuur word of aan die spesifiek aangewese polisiebeampte voorsien word; en

(c) 'n opsomming bevat van die feite wat oorweeg is en die gronde waarop die lasbrief uitgereik is.

(6) 'n Landdros of regter van die Hooggeregshof wat 'n lasbrief uitgereik het of 'n lasbrief gewysig het kragtens subartikel (3) of, indien hulle nie beskikbaar is nie, enige ander landdros of regter van die Hooggeregshof, moet by ontvangs van 'n skriftelike aansoek ingevolge subartikel (4)*(b)*, daardie aansoek heroorweeg, waarna hulle daardie lasbrief kan bevestig, wysig of kanselleer.

(7) 'n Landdros of regter van die Hooggeregshof in subartikel (6) beoog, wat die lasbrief wysig of kanselleer, moet 'n bevel gee wat hulle gepas ag, oor hoe enige item wat deur hul beslissing geraak word, hanteer moet word.

Deursoeking vir, toegang tot, of beslaglegging op item sonder deursoekingslasbrief met toestemming van persoon met wettige magtiging om toe te stem

31. (1) Enige polisiebeampte kan, sonder 'n deursoekingslasbrief, die bevoegdhede bedoel in artikel 29(2) uitoefen, behoudens enige ander wetsbepaling, indien die persoon wat wettige magtiging het om toe te stem tot die deursoeking vir, toegang tot of beslaglegging op die betrokke item, skriftelik toestem tot sodanige deursoeking, toegang of beslaglegging.

(2) 'n Polisiebeampte wat ingevolge subartikel (1) optree kan, behoudens die regmatige skriftelike toestemming van die persoon wat wettige magtiging het om toestemming te verleen, 'n ondersoeker skriftelik magtig om hulle by te staan met die deursoeking vir, toegang tot of beslaglegging op die betrokke item.

Deursoeking vir, toegang tot of beslaglegging op item betrokke in pleging van misdryf sonder deursoekingslasbrief

32. (1) 'n Polisiebeampte kan sonder 'n deursoekingslasbrief in artikel 29(1)*(a)* bedoel, enige persoon, houer, perseel, voertuig, fasiliteit, skip of lugvaartuig deursoek met die doel om die bevoegdhede in paragrawe *(a)* en *(b)* van die omskrywing van ''beslag lê'' uit te oefen ten opsigte van 'n rekenaardatabergingsmedium of enige deel van 'n rekenaarstelsel bedoel in paragraaf *(c)* of *(d)* van die omskrywing van ''item'', indien die polisiebeampte op redelike gronde glo—

(a) dat 'n deursoekingslasbrief kragtens artikel 29(1)*(a)* aan hulle uitgereik sal word indien hulle om daardie lasbrief aansoek doen; en

(b) dat die vertraging in die verkryging van sodanige lasbrief die oogmerk van die deursoeking en beslaglegging sal verydel.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

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

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

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

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

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

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

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

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

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

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

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

Assisting police official or investigator

34. (1) An electronic communications service provider, financial institution or person, other than the person who is suspected of having committed the offence which is being investigated, who is in control of any container, premises, vehicle, facility, ship, aircraft,

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(2) 'n Polisiebeampte kan slegs toegang kry of die bevoegdhede in paragrawe *(c)* of *(d)* van die omskrywing van ''beslag lê'' uitoefen, ten opsigte van die rekenaardatabergingsmedium of rekenaarstelsel in subartikel (1) bedoel, ooreenkomstig 'n deursoekingslasbrief ingevolge artikel 29(1)*(a)* uitgereik: Met dien verstande dat 'n polisiebeampte kan, as hulle op redelike gronde glo—

(a) dat 'n deursoekingslasbrief kragtens artikel 29(1)*(a)* aan hulle uitgereik sal word as hulle om so 'n lasbrief aansoek doen; en

(b) dat dit nie redelikerwys moontlik is, met inagneming van die dringendheid van die saak of die bestaan van buitengewone omstandighede, om 'n skriftelike of mondelinge aansoek om 'n lasbrief te doen nie,

toegang kan kry en die bevoegdhede bedoel in paragraaf *(c)* of *(d)* van die omskrywing van ''beslag lê'' kan uitoefen, sonder 'n deursoekingslasbrief.

(3) 'n Ondersoeker wat skriftelik daartoe gemagtig is deur 'n polisiebeampte, kan die polisiebeampte bystaan in die beslaglegging op 'n item soos in subartikels (1) en (2) beoog en om toegang te kry tot die item soos in subartikel (2) beoog.

Deursoeking vir, toegang tot of beslaglegging op item by inhegtenisneming van persoon

33. (1) 'n Polisiebeampte kan sonder 'n lasbrief, soos beoog in artikel 40 van die Strafproseswet, 1977, enigiemand in hegtenis neem—

(a) wat enige misdryf ingevolge Deel I of Deel II van Hoofstuk 2 in hul teenwoordigheid pleeg;

(b) wat hul redelikerwys daarvan verdink dat hulle 'n misdryf ingevolge Deel I en Deel II van Hoofstuk 2 gepleeg het; of

(c) wat betrokke is by of teen wie 'n redelike klagte gebring is of geloofwaardige inligting ontvang is of 'n redelike verdenking bestaan dat hulle betrokke was by 'n misdryf—

(i) soortgelyk aan die misdrywe in Deel I of Deel II van Hoofstuk 2 beoog; of

(ii) wesenlik soortgelyk aan 'n misdryf in die Republiek erken, wat gepleeg kan word by wyse van, of gefasiliteer kan word deur die gebruik van, 'n item,

in 'n vreemde Staat, en waarvoor hulle, kragtens enige wetsbepaling in verband met uitlewering van voortvlugtige oortreders, in die Republiek gearresteer of in bewaring aangehou kan word.

(2) By die inhegtenisneming van 'n persoon in subartikel (1) beoog of ingevolge artikel 40 of 43 van die Strafproseswet, 1977, kan 'n polisiebeampte deursoek vir en die bevoegdhede bedoel in paragrawe *(a)* en *(b)* van die omskrywing van ''beslag lê'' uitoefen ten opsigte van 'n rekenaardatabergingsmedium of enige deel van 'n rekenaarstelsel in paragraaf *(c)* of *(d)* van die omskrywing van ''item'' bedoel, wat in die besit van of in die bewaring of onder beheer van die persoon gevind word.

(3) 'n Polisiebeampte kan slegs toegang kry of die bevoegdhede bedoel in paragraaf *(c)* of *(d)* van die omskrywing van ''beslag lê'' uitoefen, ten opsigte van 'n rekenaardatabergingsmedium of 'n rekenaarstelsel in subartikel (2) bedoel, ooreenkomstig 'n deursoekingslasbrief uitgereik ingevolge artikel 29(1)*(a)*: Met dien verstande dat 'n polisiebeampte, as hulle op redelike gronde glo—

(a) dat 'n deursoekingslasbrief kragtens artikel 29(1)*(a)* aan hulle uitgereik sal word, as hulle om daardie lasbrief aansoek doen; en

(b) dit nie redelikerwys moontlik is, met inagneming van die dringendheid van die saak of die bestaan van buitengewone omstandighede, om 'n skriftelike of mondelinge aansoek om 'n deursoekingslasbrief te doen nie,

toegang kan kry en die bevoegdhede in paragrawe *(c)* en *(d)* van die omskrywing van ''beslag lê'' kan uitoefen sonder 'n deursoekingslasbrief.

(4) 'n Ondersoeker wat skriftelik daartoe gemagtig is deur 'n polisiebeampte, kan die polisiebeampte bystaan in die beslaglegging op 'n item soos beoog in subartikels (2) en (3) en om toegang te kry tot die item soos in subartikel (3) beoog.

Bystand aan polisiebeampte of ondersoeker

34. (1) 'n Elektroniese kommunikasiediensverskaffer, finansiële instelling of persoon, anders as die persoon wat verdink word van die pleging van die misdryf wat ondersoek word, wat in beheer is van enige houer, perseel, voertuig, fasiliteit, skip, lugvaartuig,

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

data, computer program, computer data storage medium or computer system that is subject to a search authorised in terms of section 29(1) must, if required, provide—

(a) technical assistance; and

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

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

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

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

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

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

(i) reasonably necessary; and

(ii) proportional to all the circumstances,

relating to the execution of such powers.

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

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

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

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

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

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

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

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

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

(a) acts contrary to the authority of—

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

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

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

data, rekenaarprogram, rekenaardatabergingsmedium of rekenaarstelsel wat aan 'n deursoeking ingevolge artikel 29(1) gemagtig, onderwerp word, moet, indien dit vereis word—

(a) tegniese bystand; en

(b) sodanige ander bystand as wat redelikerwys nodig mag wees,

aan 'n polisiebeampte of ondersoeker verleen ten einde te deursoek vir, toegang te kry tot of beslag te lê op 'n item.

(2) 'n Elektroniese kommunikasiediensverskaffer, finansiële instelling of persoon wat versuim om aan die bepalings van subartikel (1) te voldoen, is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met 'n boete of gevangenisstraf vir 'n tydperk van hoogstens twee jaar of met beide 'n boete en sodanige gevangenisstraf.

Dwarsboming of belemmering van polisiebeampte of ondersoeker en magtiging om weerstand te oorkom

35. (1) Enige persoon wat wederregtelik en opsetlik 'n polisiebeampte of 'n ondersoeker dwarsboom of belemmer in die uitoefening van hul bevoegdhede of die verrigting van hul pligte of werksaamhede ingevolge hierdie Hoofstuk of wat weier of versuim om te voldoen aan 'n deursoekingslasbrief uitgereik ingevolge artikel 29(1), is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met 'n boete of gevangenisstraf vir 'n tydperk van hoogstens twee jaar of met beide 'n boete en daardie gevangenisstraf.

(2) *(a)* 'n Polisiebeampte wat wettig enige bevoegdheid ingevolge artikel 29(2) aan hulle opgedra, uitvoer, kan sodanige geweld gebruik wat—

(i) redelikerwys nodig; en

(ii) in verhouding tot al die omstandighede,

is, in verband met die uitvoering van daardie bevoegdhede.

(b) Geen polisiebeampte mag enige perseel, voertuig, fasiliteit, skip of lugvaartuig betree of deursoek nie tensy hul hoorbaar toelating tot die perseel, voertuig, fasiliteit, skip of lugvaartuig geëis het en die doel van hul betreding bekend gemaak het.

(c) Die bepalings van paragraaf *(b)* is nie van toepassing nie waar die polisiebeampte, op redelike gronde, van oordeel is dat 'n item ten opsigte waarvan die deursoeking geskied, vernietig, weggedoen of mee gepeuter kan word indien die bepalings van paragraaf *(b)* nagekom word.

Bevoegdhede aan polisiebeampte of ondersoeker opgedra moet op welvoeglike en ordelike wyse uitgevoer word met behoorlike inagneming van regte van ander persone

36. (1) Die bevoegdhede aan 'n polisiebeampte of 'n ondersoeker opgedra ingevolge artikel 29(2), 31, 32 of 33, moet uitgevoer word—

(a) met streng behoud van welvoeglikheid en orde; en

(b) met behoorlike inagneming van die regte, verantwoordelikhede en regmatige belange van ander persone in verhouding tot die erns van die misdryf.

(2) Indien 'n vrou ingevolge artikel 29(2)*(a)*, *(c)* of *(d)*, 32 of 33, fisiek deursoek moet word, moet daardie deursoeking deur 'n polisiebeampte wat ook 'n vrou is, gedoen word: Met dien verstande dat indien geen vroulike polisiebeampte beskikbaar is nie, die deursoeking deur enige vrou vir daardie doel deur 'n polisiebeampte aangewys, gedoen moet word.

Wederregtelike deursoeking, toegang of beslaglegging en beperking op gebruik van instrument, toestel, wagwoord of dekripteringsleutel of inligting om toegang te kry

37. (1) 'n Polisiebeampte of 'n ondersoeker wat wederregtelik en opsetlik—

(a) strydig optree met die magtiging van—

(i) 'n deursoekingslasbrief kragtens artikel 29(1) uitgereik; of

(ii) toestemming ingevolge artikel 31(1) gegee; of

(b) sonder om gemagtig te wees kragtens hierdie Hoofstuk of die bepaling van enige ander wet wat soortgelyke bevoegdhede aan 'n polisiebeampte of 'n ondersoeker verleen—

(i) deursoek vir, toegang kry tot of beslag lê op data, 'n rekenaarprogram, 'n rekenaardatabergingsmedium of enige deel van van 'n rekenaarstelsel; of

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

is guilty of an offence.

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

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

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

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

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

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

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

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

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

is guilty of an offence.

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

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

False information under oath or by way of affirmation

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

(a) a search warrant is issued;

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

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

(d) an expedited preservation of data direction contemplated in section 41 is issued;

(e) a preservation of evidence direction contemplated in section 42 is issued; or

(f) a disclosure of data direction contemplated in section 44 is issued,

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(ii) enige instrument, toestel, wagwoord, dekripteringsleutel of ander inligting wat nodig is om toegang te kry tot data, 'n rekenaarprogram, 'n rekenaardatabergingsmedium of enige deel van 'n rekenaarstelsel, te bekom of gebruik,

is skuldig aan 'n misdryf.

(2) *(a)* 'n Polisiebeampte of 'n ondersoeker wat enige instrument, toestel, toerusting, wagwoord, dekripteringsleutel, data of ander inligting beoog in artikel 29(2)*(h)* verkry of gebruik—

(i) moet die instrument, toestel, toerusting, wagwoord, dekripteringsleutel, data of inligting slegs ten opsigte van en tot die mate gespesifiseer in die deursoekingslasbrief gebruik om toegang te kry tot, of om data, 'n rekenaarprogram, 'n rekenaardatabergingsmedium of enige deel van 'n rekenaarstelsel te gebruik op die wyse en vir die doeleindes in die betrokke deursoekingslasbrief gespesifiseer; en

(ii) moet alle wagwoorde, dekripteringsleutels, data of ander inligting vernietig indien—

(aa) dit nie deur 'n persoon benodig word wat die wagwoorde, dekoderingsleutels, data of inligting wettig mag besit nie;

(bb) dit nie vir die doeleindes van enige strafregtelike verrigtinge of siviele verrigtinge beoog in Hoofstuk 5 of 6 van die Wet op Voorkoming van Georganiseerde Misdaad, 1998, of vir die doeleindes van getuienis of vir doeleindes van 'n hofbevel, benodig sal word nie; of

(cc) geen strafregtelike verrigtinge of siviele verrigtinge soos beoog in Hoofstuk 5 of 6 van die Wet op Voorkoming van Georganiseerde Misdaad, 1998, in verband met daardie inligting ingestel staan te word nie.

(b) 'n Polisiebeampte of ondersoeker wat wederregtelik en opsetlik—

(i) enige instrument, toestel, toerusting, wagwoord, dekripteringsleutel, data of inligting gebruik buite die magtiging van 'n lasbrief soos in paragraaf *(a)*(i) beoog; of

(ii) versuim om alle wagwoorde, dekripteringsleutels, data of ander inligting soos beoog in paragraaf *(a)*(ii) te vernietig,

is skuldig aan 'n misdryf.

(3) 'n Polisiebeampte of 'n ondersoeker wat subartikel (1) of (2) oortree of versuim om daaraan te voldoen, is by skuldigbevinding strafbaar met 'n boete of gevangenisstraf vir 'n tydperk van hoogstens twee jaar of met beide 'n boete en sodanige gevangenisstraf.

(4) Waar 'n polisiebeampte of 'n ondersoeker skuldig bevind word aan 'n misdryf in subartikel (1) of (2) bedoel, kan die hof wat daardie persoon skuldig bevind, op aansoek van enige persoon wat skade gely het of op die aansoek van die aanklaer wat in opdrag van daardie persoon optree, vergoeding ten opsigte van daardie skade toeken, waarop die bepalings van artikel 300 van die Strafproseswet, 1977, met die nodige veranderinge deur die samehang vereis, op daardie toekenning van toepassing is.

Vals inligting onder eed of deur plegtige verklaring

38. (1) Enige persoon wat wederregtelik en opsetlik vals inligting onder eed of deur plegtige verklaring gee, wetende dat dit vals is of nie wetende dat dit waar is nie, met die gevolg dat—

(a) 'n deursoekingslasbrief uitgereik word;

(b) 'n deursoeking in artikel 31 beoog op grond van daardie inligting plaasgevind het;

(c) 'n persoon, houer, perseel, voertuig, fasiliteit, skip of lugvaartuig deursoek of 'n rekenaardatabergingsmedium of enige deel van 'n rekenaarstelsel ingevolge artikel 32 op beslag gelê word of toegang gekry word daartoe;

(d) 'n lasgewing vir bespoedigde bewaring van data ingevolge artikel 41 uitgereik word;

(e) 'n lasgewing vir bewaring van getuienis beoog in artikel 42 uitgereik word; of

(f) 'n lasgewing vir openbaarmaking van data beoog in artikel 44 uitgereik word,

is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens twee jaar of met beide 'n boete en daardie gevangenisstraf.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

Prohibition on disclosure of information

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

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

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

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

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

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

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

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

(b) reveals a criminal activity.

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

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

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

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

(3) An electronic communications service provider who is—

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(2) Waar 'n persoon aan 'n misdryf bedoel in subartikel (1) skuldig bevind word, kan die hof wat daardie persoon skuldig bevind, op aansoek van enige persoon wat skade gely het of op die aansoek van die aanklaer wat in opdrag van daardie persoon optree, vergoeding ten opsigte van daardie skade toeken, waarop die bepalings van artikel 300 van die Strafproseswet, 1977, met die nodige veranderinge deur die samehang vereis, op daardie toekenning van toepassing is.

Verbod op openbaarmaking van inligting

39. (1) Geen persoon, ondersoeker, polisiebeampte, elektroniese kommunikasiediensverskaffer, finansiële instelling of 'n werknemer van 'n elektroniese kommunikasiediensverskaffer of finansiële instelling mag, behoudens subartikel (2), enige inligting wat hulle in die uitoefening van hul bevoegdhede of die verrigting van hul pligte ingevolge Hoofstuk 4 of 5 van hierdie Wet verkry het openbaar maak nie, behalwe—

(a) aan enige ander persoon wat dit uit noodsaak vereis vir die verrigting van hul werksaamhede ingevolge hierdie Wet;
(b) indien hul 'n persoon is wat daardie inligting uit noodsaak verskaf in die verrigting van hul pligte en werksaamhede ingevolge hierdie Wet;
(c) indien dit inligting is wat ingevolge enige wet as getuienis in enige geregshof benodig word;
(d) indien dit inligtingdeling tussen elektroniese kommunikasiediensverskaffers, finansiële instellings, die Suid-Afrikaanse Polisiediens, bevoegde owerhede of enige ander persoon of entiteit daarstel wat op die voorkoming, bespeuring, ondersoek of mitigasie van kubermisdaad gemik is: Met dien verstande dat sodanige inligtingdeling geen strafregtelike ondersoek of strafregtelike verrigtinge mag benadeel nie; of
(e) aan enige bevoegde owerheid in 'n vreemde Staat wat dit benodig vir die voorkoming, bespeuring of mitigasie van kubermisdaad, of die instelling van strafregtelike verrigtinge of 'n ondersoek met die oog op die instelling van strafregtelike verrigtinge.

(2) Die verbod op openbaarmaking van inligting in subartikel (1) beoog, is nie van toepassing nie waar die openbaarmaking—

(a) ingevolge hierdie Wet of enige ander Parlementswet gemagtig is; of
(b) 'n kriminele aktiwiteit onthul.

(3) 'n Persoon, ondersoeker, polisiebeampte, elektroniese kommunikasiediensverskaffer, finansiële instelling of 'n werknemer van 'n elektroniese kommunikasiediensverskaffer of finansiële instelling wat wederregtelik en opsetlik die bepalings van subartikel (1) oortree, is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met 'n boete of gevangenisstraf vir 'n tydperk van hoogstens drie jaar of met beide 'n boete en daardie gevangenisstraf.

Onderskepping van onregstreekse kommunikasie en verkryging van intydse kommunikasie-verwante inligting

40. (1) Die onderskepping van 'n onregstreekse kommunikasie soos omskryf in artikel 1 van die Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting, 2002, moet plaasvind ingevolge 'n lasgewing uitgereik ingevolge artikel 16(4) of 18(3) van daardie Wet en moet, behoudens subartikel (4), verder hanteer word op die wyse waarvoor daardie Wet voorsiening maak.

(2) Die verkryging van intydse kommunikasie-verwante inligting soos omskryf in artikel 1 van die Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting, 2002, op 'n deurlopende grondslag, soos dit beskikbaar word, moet plaasvind ingevolge 'n lasgewing uitgereik ingevolge artikel 17(3) of 18(3) van daardie Wet, en moet, behoudens subartikel (4), verder hanteer word op die wyse waarvoor daardie Wet voorsiening maak.

(3) 'n Elektroniese kommunikasiediensverskaffer wat—

(a) ingevolge artikel 30(1)*(b)* van die Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting, 2002, 'n elektroniese kommunikasiediens moet voorsien wat die vermoë het om kommunikasie-verwante inligting te bewaar; en

This gazette is also available free online at www.gpwonline.co.za

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

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

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

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

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

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

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

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

(bb) obtain and furnish traffic data.

(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.

Expedited preservation of data direction

41. (1) A specifically designated police official may—

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

(i) in possession of;

(ii) to receive; or

(iii) in control of,

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

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

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

(2) Subsection (1) also applies to—

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

(b) any other data which—

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

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(b) nie vereis word om kommunikasie-verwante inligting, ingevolge 'n voorskrif ingevolge artikel 30(2) van daardie Wet uitgereik, te bewaar nie,

moet, benewens enige ander verpligting deur enige wetsbepaling opgelê, voldoen aan—

(i) 'n intydse kommunikasie-verwante lasgewing in subartikel (2) beoog ingevolge waarvan die elektroniese kommunikasiediensverskaffer gelas word om intydse kommunikasie-verwante inligting te voorsien ten opsigte van 'n kliënt, op 'n deurlopende grondslag, soos dit beskikbaar word;

(ii) 'n lasgewing vir bespoedigde bewaring van data beoog in artikel 41, ingevolge waarvan die elektroniese kommunikasiediensverskaffer gelas word om intydse kommunikasie-verwante inligting ten opsigte van 'n kliënt te bewaar;

(iii) 'n lasgewing vir bewaring van getuienis in artikel 42 beoog, ingevolge waarvan die elektroniese kommunikasiediensverskaffer gelas word om intydse kommunikasie-verwante inligting ten opsigte van 'n kliënt te bewaar;

(iv) 'n lasgewing vir openbaarmaking van data in artikel 44 beoog, ingevolge waarvan die elektroniese kommunikasiediensverskaffer gelas word om intydse kommunikasie-verwante inligting ten opsigte van 'n kliënt wat deur die elektroniese kommunikasiediensverskaffer bewaar of andersins geberg is, te voorsien; of

(v) enige bevel deur die aangewese regter ingevolge artikel 48(6), ingevolge waarvan die elektroniese kommunikasiediensverskaffer beveel word om—

(aa) enige intydse kommunikasie-verwante inligting te verkry en te bewaar; of

(bb) verkeersdata te verkry en te verskaf.

(4) Enige onregstreekse kommunikasie wat onderskep moet word of enige intydse kommunikasie-verwante inligting of verkeersdata wat bekom moet word, op versoek van 'n owerheid, hof of tribunaal met jurisdiksie in 'n vreemde Staat, moet verder mee gehandel word op die wyse waarvoor in 'n bevel bedoel in artikel 48(6), deur die aangewese regter uitgereik, voorsiening gemaak word.

Lasgewing vir bespoedigde bewaring van data

41. (1) 'n Spesifiek aangewese polisiebeampte kan—

(a) as hul op redelike gronde glo dat enige persoon, 'n elektroniese kommunikasiediensverskaffer in artikel 40(3) bedoel, of 'n finansiële instelling—

(i) in besit is van data;

(ii) data gaan ontvang; of

(iii) in beheer is van data,

soos beoog in paragraaf (a) van die omskrywing van ''item''; en

(b) met behoorlike inagneming van die regte, verantwoordelikhede en regmatige belange van ander persone in verhouding tot die erns van die betrokke misdryf,

'n lasgewing vir bespoedigde bewaring van data aan daardie persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling uitreik.

(2) Subartikel (1) is ook van toepassing op—

(a) argief-bewaarde kommunikasie-verwante inligting wat 'n elektroniese kommunikasiediensverskaffer nie langer hoef te bewaar nie omdat die tydperk beoog in artikel 30(2)*(a)*(iii) van die Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting, 2002, gaan verstryk; of

(b) enige ander data—

(i) wat vir 'n sekere tyd geberg moet word ingevolge enige ander wetsbepaling en daardie tydperk gaan verstryk; of

(ii) wat deur 'n elektroniese kommunikasiediensverskaffer geberg word wat nie vir intydse kommunikasie-verwante inligting of argief-bewaarde kommunikasie-verwante inligting is soos beoog in artikel 1, gelees met artikel 30(2) en enige voorskrif uitgereik ingevolge daardie artikel, van die Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting, 2002, nie.

(3) 'n Lasgewing vir bespoedigde bewaring van data moet in die voorgeskrewe vorm wees en moet op die voorgeskrewe wyse deur 'n polisiebeampte aan die persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling daardeur geraak, beteken word.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

(a) to preserve the current status of;
(b) not to deal in any manner with; or
(c) to deal in a certain manner with,

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

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

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

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

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

(a) consider the application and may for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application;
(b) give a decision in respect of the application; and
(c) inform the applicant and specifically designated police official referred to in subsection (1) of the outcome of the application.

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

(a) fails to comply with an expedited preservation of data direction or contravenes the provisions of subsection (5); or
(b) makes a false statement in an application referred to in subsection (7),

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

Preservation of evidence direction

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

(a) upon written application by a police official;
(b) if it appears to the magistrate or judge upon consideration of the information provided under oath or by way of affirmation, as set out in the application, that there are reasonable grounds to believe that any person, electronic communications service provider or financial institution—
  (i) may receive;
  (ii) is in possession of; or
  (iii) is in control of,

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

issue a preservation of evidence direction.

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

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

(a) to preserve the current status of;
(b) not to deal in any manner with; or
(c) to deal in a certain manner with,

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(4) 'n Lasgewing vir bespoedigde bewaring van data moet die persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling daardeur geraak, gelas om van die tyd van betekening van die lasgewing en vir 'n tydperk van 21 dae—

(a) die huidige status te bewaar van;
(b) geensins op enige wyse te handel met; of
(c) op 'n sekere wyse te handel met,

die data in die lasgewing vermeld, ten einde die beskikbaarheid en integriteit van die data te bewaar.

(5) Geen data mag op grond van 'n lasgewing vir bespoedigde bewaring van data aan 'n polisiebeampte openbaar gemaak word nie, tensy dit ingevolge artikel 44 gemagtig word.

(6) Die tydperk van 21 dae in subartikel (4) bedoel, kan slegs eenmalig verleng word by wyse van'n lasgewing vir bewaring van getuienis in artikel 42 beoog, vir 'n bykomende tydperk wat nie 90 dae mag oorskry nie.

(7) 'n Persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling aan wie 'n lasgewing vir bespoedigde bewaring van data, in subartikel (1) bedoel, gerig is, kan skriftelik op die voorgeskrewe vorm en wyse, by 'n landdros in wie se regsgebied die persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling geleë is, aansoek doen om 'n wysiging of die kansellasie van die betrokke lasgewing op grond daarvan dat hulle nie tydig of op 'n redelike wyse aan die lasgewing kan voldoen nie.

(8) Die landdros by wie 'n aansoek ingevolge subartikel (7) gedoen word, moet, so gou moontlik ná ontvangs daarvan—

(a) die aansoek oorweeg en kan vir hierdie doel gelas dat mondelinge of skriftelike getuienis aangevoer word aangaande enige feit in die aansoek beweer;
(b) 'n beslissing ten opsigte van die aansoek gee; en
(c) die applikant en spesifiek aangewese polisiebeampte bedoel in subartikel (1) verwittig van die uitslag van die aansoek.

(9) 'n Persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling in subartikel (1) bedoel wat—

(a) versuim om aan 'n lasgewing vir bespoedigde bewaring van data te voldoen of die bepalings van subartikel (5) oortree; of
(b) 'n vals verklaring maak in 'n aansoek in subartikel (7) bedoel,

is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens twee jaar of met beide 'n boete en sodanige gevangenisstraf.

Lasgewing vir bewaring van getuienis

42. (1) 'n Landdros of regter van die Hooggeregshof kan—

(a) by skriftelike aansoek deur 'n polisiebeampte;
(b) indien dit vir die landdros of regter, by oorweging van die inligting onder eed of by wyse van plegtige verklaring verstrek, soos in die aansoek uiteengesit, blyk dat daar redelike gronde is om te glo dat enige persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling—
    (i) 'n item mag ontvang;
    (ii) in besit is van 'n item; of
    (iii) in beheer is van 'n item; en
(c) met behoorlike inagneming van die regte, verantwoordelikhede en regmatige belange van ander persone in verhouding tot die erns van die betrokke misdryf,

'n lasgewing vir bewaring van getuienis uitreik.

(2) 'n Lasgewing vir bewaring van getuienis moet in die voorgeskrewe vorm wees en moet op die voorgeskrewe wyse deur 'n polisiebeampte aan die persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling daardeur geraak, beteken word.

(3) Die lasgewing vir bewaring van getuienis moet die persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling gelas om, van die tyd van betekening van die lasgewing en vir die tydperk in die lasgewing gespesifiseer, wat nie 90 dae mag oorskry nie—

(a) die huidige status te bewaar van;
(b) nie op enige wyse te handel met; of
(c) op 'n sekere wyse te handel met,

'n item, ten einde die beskikbaarheid of integriteit van die item te bewaar.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

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

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

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

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

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

Oral application for preservation of evidence direction

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

(2) An oral application referred to in subsection (1) must—

(a) indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the police official, justify the making of an oral application; and

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

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

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

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

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

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

(iii) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application for the issuing of the preservation of evidence direction applied for; and

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

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(4) Enige persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling wat versuim om te voldoen aan 'n lasgewing vir bewaring van getuienis, is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens drie jaar of met beide 'n boete en sodanige gevangenisstraf.

(5) 'n Persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling aan wie 'n lasgewing vir bewaring van getuienis bedoel in subartikel (1) gerig is, kan skriftelik op die voorgeskrewe vorm en wyse, by 'n landdros of regter van die Hooggeregshof in wie se regsgebied die persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling geleë is, aansoek doen om 'n wysiging of die kansellasie van die betrokke lasgewing op grond daarvan dat hulle nie tydig of op 'n redelike wyse aan die lasgewing kan voldoen nie.

(6) Die landdros of regter van die Hooggeregshof by wie 'n aansoek ingevolge subartikel (5) gedoen word, moet, so gou moontlik ná ontvangs daarvan—

(a) die aansoek oorweeg en kan vir hierdie doel gelas dat mondelinge of skriftelike getuienis aangevoer word aangaande enige feit in die aansoek beweer;

(b) 'n beslissing ten opsigte van die aansoek gee; en

(c) die applikant en polisiebeampte verwittig van die uitslag van die aansoek.

Mondelinge aansoek om lasgewing vir bewaring van getuienis

43. (1) 'n Polisiebeampte kan 'n aansoek in artikel 42(1) bedoel, mondeling doen, indien hulle van mening is dat dit nie redelikerwys moontlik is, met inagneming van die dringendheid van die saak of die bestaan van buitengewone omstandighede, om 'n skriftelike aansoek te doen nie.

(2) 'n Mondelinge aansoek bedoel in subartikel (1) moet—

(a) die besonderhede van die dringendheid van die saak of die ander buitengewone omstandighede aandui wat, na mening van die polisiebeampte, die doen van 'n mondelinge aansoek regverdig; en

(b) voldoen aan enige aanvullende voorskrifte rakende mondelinge aansoeke wat ingevolge artikel 8(3) van die Wet op Hoër Howe, 2013 deur die Hoofregter uitgereik kan word.

(3) 'n Landdros of regter van die Hooggeregshof kan, by die ontvangs van 'n mondelinge aansoek aan hulle ingevolge subartikel (1) gedoen, die lasgewing vir bewaring van getuienis waarvoor aansoek gedoen word, uitreik.

(4) 'n Lasgewing vir die bewaring van getuienis kan slegs kragtens subartikel (3) uitgereik word—

(a) indien die betrokke landdros of regter van die Hooggeregshof oortuig is, op grond van die feite in die betrokke mondelinge aansoek aangevoer, dat—

(i) daar redelike gronde is om te glo dat 'n lasgewing vir die bewaring van getuienis waarom aansoek gedoen is, uitgereik kan word;

(ii) 'n lasgewing vir die bewaring van getuienis onmiddellik nodig is ten einde die beskikbaarheid of die integriteit van die item te verseker; en

(iii) dit nie redelikerwys moontlik is nie, met inagneming van die dringendheid van die saak of die bestaan van buitengewone omstandighede, om 'n skriftelike aansoek om die uitreiking van die lasgewing vir die bewaring van getuienis waarvoor aansoek gedoen word, te doen nie; en

(b) op voorwaarde dat die betrokke polisiebeampte 'n skriftelike aansoek aan die betrokke landdros of regter van die Hooggeregshof binne 48 uur ná uitreiking van die lasgewing vir die bewaring van getuienis kragtens subartikel (3), moet voorlê.

(5) 'n Lasgewing vir die bewaring van getuienis kragtens subartikel (3) uitgereik, moet skriftelik wees en moet elektronies versend word aan die polisiebeampte of vir 'n spesifiek aangewese polisiebeampte gegee word.

(6) 'n Landdros of regter van die Hooggeregshof wat 'n lasgewing kragtens subartikel (3) uitgereik het of, indien hulle nie beskikbaar is nie, enige ander landdros of regter van die Hooggeregshof, moet by ontvangs van 'n skriftelike aansoek ingevolge subartikel (4)*(b)*, daardie aansoek heroorweeg waarna hulle daardie lasgewing vir die bewaring van getuienis kan bevestig, wysig of kanselleer.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

(a) there are reasonable grounds for believing that—

- (i) data which is subject to preservation in terms of an expedited preservation of data direction or a preservation of evidence direction, is an article as contemplated in paragraph *(a)* of the definition of ''article''; or
- (ii) data, which is an article as contemplated in paragraph *(a)* of the definition of ''article'', is—
  - *(aa)* held in a computer system or computer data storage medium; or

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Lasgewing vir openbaarmaking van data en deursoeking vir, toegang tot en beslaglegging op items onderworpe aan bewaring

44. (1) *(a)* 'n Polisiebeampte kan, waar dit geleë is, anders as by wyse van 'n deursoeking en beslaglegging ingevolge 'n lasbrief in artikel 29(1) beoog, om—

(i) data te bekom wat onderworpe is aan bewaring ingevolge 'n lasgewing vir bespoedigde bewaring van data of 'n lasgewing vir die bewaring van getuienis; of

(ii) data soos beoog in paragraaf *(a)* van die omskrywing van ''item'' te bekom, wat—

(aa) in 'n rekenaarstelsel of rekenaardatabergingsmedium gehou word; of

(bb) aan 'n rekenaarstelsel beskikbaar is,

by 'n landdros of regter van die Hooggeregshof aansoek doen om die uitreiking van 'n lasgewing vir die openbaarmaking van data.

(b) 'n Aansoek in paragraaf *(a)*(i) bedoel, moet—

(i) die identiteit verstrek van die polisiebeampte wat om die lasgewing vir openbaarmaking van data aansoek doen;

(ii) die persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling identifiseer aan wie die lasgewing vir openbaarmaking van data, gerig moet word;

(iii) van 'n afskrif van die lasgewing vir bespoedigde bewaring van data of 'n lasgewing vir die bewaring van getuienis of enige wysiging daarvan vergesel gaan;

(iv) 'n beskrywing van die data bevat wat voorsien moet word en die formaat waarin dit voorsien moet word;

(v) die gronde spesifiseer waarom geglo word dat die data 'n item is soos beoog in paragraaf *(a)* van die omskrywing van ''item''; en

(vi) voldoen aan enige aanvullende voorskrifte wat verband hou met aansoeke om openbaarmaking van data, wat deur die Hoofregter uitgereik kan word ingevolge artikel 8(3) van die Wet op Hoër Howe, 2013.

(c) 'n Aansoek bedoel in paragraaf *(a)*(ii), moet—

(i) die identiteit verstrek van die polisiebeampte wat om die lasgewing vir openbaarmaking van data aansoek doen;

(ii) die persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling identifiseer aan wie die lasgewing vir openbaarmaking van data gerig moet word;

(iii) 'n beskrywing bevat van die data wat voorsien moet word en die formaat waarin dit voorsien moet word;

(iv) die gronde spesifiseer waarom geglo word dat die data 'n item is soos beoog in paragraaf *(a)* van die omskrywing van ''item'';

(v) die gronde spesifiseer waarom geglo word dat die betrokke data gehou word in 'n rekenaarstelsel of rekenaardatabergingsmedium of aan 'n rekenaarstelsel beskikbaar is wat onder beheer is van die persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling in subparagraaf (ii) bedoel, binne die regsgebied van die hof; en

(vi) voldoen aan enige aanvullende voorskrifte rakende aansoeke om die openbaarmaking van data, wat ingevolge artikel 8(3) van die Wet op Hoër Howe, 2013, deur die Hoofregter uitgereik kan word.

(2) 'n Landdros of regter van die Hooggeregshof kan, behoudens die bepalings van artikel 4(2) van die Doeane- en Aksynswet, 1964, artikels 69(2)*(b)* en 71 van die Wet op Belastingadministrasie, 2011, en artikel 21*(e)* en *(f)* van die Wet op Doeanebeheer, 2014, op skriftelike aansoek deur 'n polisiebeampte in subartikel (1) bedoel, indien dit vir die landdros of regter uit inligting onder eed of by wyse van plegtige verklaring, soos in die aansoek uiteengesit, blyk—

(a) dat daar redelike gronde is om te glo dat—

(i) data wat onderhewig is aan bewaring ingevolge 'n lasgewing vir bespoedigde bewaring van data of 'n lasgewing vir die bewaring van getuienis, 'n item is soos beoog in paragraaf *(a)* van die omskrywing van ''item''; of

(ii) data, wat 'n item is soos beoog in paragraaf *(a)* van die omskrywing van ''item''—

(aa) gehou word in 'n rekenaarstelsel of rekenaardatabergingsmedium; of

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(*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.

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

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(bb) aan 'n rekenaarstelsel beskikbaar is,

binne hul regsgebied; en

(b) dit in die belang van geregtigheid sal wees indien 'n lasgewing vir openbaarmaking van data uitgereik word,

die lasgewing vir openbaarmaking van data waarom aansoek gedoen is, uitreik.

(3) 'n Lasgewing vir openbaarmaking van data moet in die voorgeskrewe vorm wees en moet op die voorgeskrewe wyse deur 'n polisiebeampte aan die persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling daardeur geraak, beteken word.

(4) Die lasgewing vir openbaarmaking van data—

(a) moet die persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling gelas om die data in die lasgewing geïdentifiseer, tot die mate in die lasgewing uiteengesit, aan 'n geïdentifiseerde polisiebeampte te voorsien;

(b) moet die formaat spesifiseer waarin die data in paragraaf *(a)* geïdentifiseer, voorsien moet word;

(c) moet die tydperk uiteensit waarbinne die data in paragraaf *(a)* geïdentifiseer, voorsien moet word; en

(d) kan voorwaardes of beperkings in verband met die voorsiening van data daarin gemagtig, spesifiseer.

(5) 'n Persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling aan wie 'n lasgewing vir openbaarmaking van data in subartikel (3) bedoel, beteken word, kan, skriftelik op die voorgeskrewe vorm en wyse, by die landdros of regter aansoek doen om 'n wysiging of die kansellasie van die betrokke lasgewing op grond daarvan dat hulle nie tydig of op 'n redelike wyse aan die lasgewing kan voldoen nie.

(6) Die landdros of regter by wie die aansoek ingevolge subartikel (5) gebring word, moet so gou moontlik ná ontvangs daarvan—

(a) die aansoek oorweeg en kan, vir hierdie doel, beveel dat mondelinge of skriftelike getuienis aangebied word aangaande enige feit in die aansoek beweer;

(b) 'n beslissing gee ten opsigte van die aansoek; en

(c) indien die aansoek suksesvol is, die polisiebeampte en die applikant verwittig van die uitslag van die aansoek.

(7) Enige data wat ingevolge 'n lasgewing vir openbaarmaking van data beskikbaar gemaak moet word—

(a) aan die polisiebeampte in die lasgewing geïdentifiseer, voorsien word; en

(b) vergesel gaan van 'n beëdigde verklaring in die voorgeskrewe vorm deur die persoon of gemagtigde verteenwoordiger van 'n elektroniese kommunikasiediensverskaffer of finansiële instelling, wat die egtheid, integriteit en betroubaarheid van die data, wat voorsien word, bevestig.

(8) 'n Persoon, elektroniese kommunikasiediensverskaffer of 'n finansiële instelling wat—

(a) versuim om aan 'n lasgewing vir openbaarmaking van data te voldoen;

(b) 'n vals verklaring aflê in 'n aansoek in subartikel (5) bedoel; of

(c) versuim om aan subartikel (7) te voldoen,

is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met 'n boete of gevangenisstraf vir 'n tydperk van hoogstens twee jaar of tot beide 'n boete en sodanige gevangenisstraf.

(9) *(a)* Enige item wat onderhewig is aan 'n lasgewing vir die bewaring van getuienis, wat nie "data" is nie, moet op beslag gelê word ingevolge 'n lasbrief in artikel 29(1) bedoel.

(b) 'n Polisiebeampte kan, te eniger tyd, aansoek doen om 'n deursoekingslasbrief ingevolge artikel 29(1) om te deursoek vir, toegang te kry tot of beslag te lê op 'n item (wat "data" insluit) wat aan 'n lasgewing vir bespoedigde bewaring van data of 'n lasgewing vir die bewaring van getuienis onderhewig is of was.

Verkryging en gebruik van openbaar beskikbare data of ontvangs van data van persoon wat in besit is van data

45. 'n Polisiebeampte kan, sonder om uitdruklik ingevolge hierdie Hoofstuk daartoe gemagtig te wees, vir die ondersoek van enige misdryf of vermeende misdryf ingevolge Deel I of Deel II van Hoofstuk 2 of enige ander misdryf of vermeende misdryf ingevolge die wette van die Republiek, wat gepleeg kan word by wyse van, of gefasiliteer kan word deur die gebruik van, 'n item—

(a) openbaar beskikbare data ontvang, verkry of gebruik ongeag waar die data geografies geleë is; of

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

CHAPTER 5

MUTUAL ASSISTANCE

Application of provisions of Chapter

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

(a) an offence in terms of Part I or Part II of Chapter 2;
(b) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or
(c) an offence—
(i) similar to those contemplated in Part I or Part II of Chapter 2; or
(ii) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article,
in a foreign State,

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

Spontaneous information

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

(a) assist the foreign State in the initiation or carrying out of investigations; or
(b) lead to further cooperation with a foreign State to carry out an investigation,

regarding the commission or suspected commission of—

(i) an offence contemplated in Part I or Part II of Chapter 2, in the Republic;
(ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or
(iii) an offence—
(aa) similar to those contemplated in Part I or Part II of Chapter 2; or
(bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article,
in that foreign State.

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

(a) assist the South African Police Service in the initiation or carrying out of investigations; or
(b) lead to further cooperation with a foreign State to carry out an investigation,

regarding the commission or suspected commission of—

(i) an offence contemplated in Part I or Part II of Chapter 2, in the Republic;
(ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(b) nie-openbaar-beskikbare data ontvang en gebruik, ongeag waar die data geografies geleë is, indien 'n persoon wat in beheer is van, of in besit is van die data, vrywillig en op sodanige voorwaardes aangaande vertroulikheid en beperking van gebruik wat hulle nodig ag, die data aan 'n polisiebeampte openbaar maak.

HOOFSTUK 5

ONDERLINGE BYSTAND

Toepassing van bepalings van Hoofstuk

46. Die bepalings van artikels 48 tot 51 is van toepassing adissioneel tot Hoofstuk 2 van die Wet op Internasionale Samewerking in Strafregtelike Aangeleenthede, 1996, en het betrekking, tensy anders gespesifiseer, op die bewaring van 'n item of ander getuienis in elektroniese formaat aangaande die pleging of vermeende pleging van—

(a) 'n misdryf ingevolge Deel I of Deel II van Hoofstuk 2;

(b) enige ander misdryf ingevolge die wette van die Republiek, wat gepleeg kan word by wyse van, of gefasiliteer kan word deur die gebruik van, 'n item; of

(c) 'n misdryf—

(i) soortgelyk aan dié in Deel I of Deel II van Hoofstuk 2 beoog; of

(ii) wesenlik soortgelyk aan 'n misdryf erken in die Republiek, wat gepleeg kan word by wyse van, of gefasiliteer kan word deur die gebruik van, 'n item,

in 'n vreemde Staat,

hangende 'n versoek ingevolge artikel 2 of 7 van die Wet op Internasionale Samewerking in Strafregtelike Aangeleenthede, 1996.

Spontane inligting

47. (1) Die Nasionale Kommissaris of die Nasionale Hoof van die Direktoraat kan, op sodanige voorwaardes aangaande vertroulikheid en beperking van gebruik wat hulle mag bepaal, enige inligting tydens enige ondersoek verkry, verskaf aan 'n wetstoepassingsagentskap in 'n vreemde Staat wanneer die Nasionale Kommissaris of die Nasionale Hoof van die Direktoraat van mening is dat die openbaarmaking van daardie inligting—

(a) die vreemde Staat behulpsaam mag wees in die inisiëring of uitvoering van ondersoeke; of

(b) kan lei tot verdere samewerking met 'n vreemde Staat om 'n ondersoek uit te voer,

aangaande die pleging of vermeende pleging van—

(i) 'n misdryf in Deel I of Deel II van Hoofstuk 2 beoog, in die Republiek;

(ii) enige ander misdryf ingevolge die wette van die Republiek wat gepleeg kan word by wyse van, of gefasiliteer kan word deur die gebruik van, 'n item; of

(iii) 'n misdryf—

(aa) soortgelyk aan dié in Deel I of Deel II van Hoofstuk 2 beoog; of

(bb) wesenlik soortgelyk aan 'n misdryf in die Republiek erken wat gepleeg kan word by wyse van, of gefasiliteer kan word deur die gebruik van, 'n item,

in daardie vreemde Staat.

(2) Die Suid-Afrikaanse Polisiediens kan enige inligting van 'n vreemde Staat ontvang, behoudens voorwaardes rakende vertroulikheid en beperking van gebruik waarop ooreengekom mag word, wat—

(a) die Suid-Afrikaanse Polisiediens behulpsaam mag wees in die inisiëring of uitvoering van ondersoeke; of

(b) kan lei tot verdere samewerking met 'n vreemde Staat om 'n ondersoek uit te voer,

aangaande die pleging of vermeende pleging van—

(i) 'n misdryf in Deel I of Deel II van Hoofstuk 2 beoog, in die Republiek; of

(ii) enige ander misdryf ingevolge die wette van die Republiek, wat gepleeg kan word by wyse van, of gefasiliteer kan word deur die gebruik van, 'n item; of

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(iii) an offence—
(aa) similar to those contemplated in Part I or Part II of Chapter 2; or
(bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article,
in that foreign State.

Foreign requests for assistance and cooperation

48. (1) A request by an authority, court or tribunal exercising jurisdiction in a foreign State for the—
(a) preservation of data or other article;
(b) seizure of data or other article;
(c) expedited disclosure of traffic data;
(d) obtaining of real-time communication-related information or archived communication-related information; or
(e) interception of indirect communications,
must, subject to subsection (9), be submitted to the designated Point of Contact.

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

(3) *(a)* Upon receipt of a request referred to in subsection (2), the National Director of Public Prosecutions must satisfy himself or herself that—
(i) proceedings have been instituted in a court or tribunal exercising jurisdiction in the requesting foreign State; or
(ii) there are reasonable grounds for believing that an offence has been committed in the requesting foreign State or that it is necessary to determine whether an offence has been so committed and that an investigation in respect thereof is being conducted in the requesting foreign State; and
(iii) the offence in question is—
(aa) similar to those contemplated in Part I or Part II of Chapter 2; or
(bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article; and
(iv) the foreign State intends to submit a request in terms of section 7 of the International Co-operation in Criminal Matters Act, 1996, for obtaining the data, information, a communication or an article in the Republic for use in such proceedings or investigation in the foreign State.

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

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

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

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

(6) Subject to subsections (7) and (8), the designated judge may on receipt of a request referred to in subsection (4) or (5), issue any order they deem appropriate to ensure that the requested—
(a) data or other article is preserved in accordance with section 42;
(b) data or other article is seized on an expedited basis in accordance with section 29 and preserved;
(c) traffic data is disclosed on an expedited basis in terms of a disclosure of data direction in accordance with section 44;
(d) real-time communication-related information or archived communication related information, is obtained and preserved; or
(e) indirect communications are intercepted and preserved,
as is specified in the request.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(iii) 'n misdryf—
(aa) soortgelyk aan dié in Deel I of Deel II van Hoofstuk 2 beoog; of
(bb) wesenlik soortgelyk aan 'n misdryf in die Republiek erken, wat gepleeg kan word by wyse van, of gefasiliteer kan word deur die gebruik van, 'n item,

in daardie vreemde Staat.

Buitelandse versoeke om bystand en samewerking

48. (1) 'n Versoek deur 'n owerheid, hof of tribunaal wat regsbevoegdheid in 'n vreemde Staat uitoefen om die—
(a) bewaring van data of ander item;
(b) beslaglegging op data of ander item;
(c) bespoedigde openbaarmaking van verkeersdata;
(d) verkryging van intydse kommunikasie-verwante inligting of argief-bewaarde kommunikasie-verwante inligting; of
(e) onderskepping van onregstreekse kommunikasie,

moet, behoudens subartikel (9), aan die aangewese Kontakpunt voorsien word.

(2) Die aangewese Kontakpunt moet die versoek aan die Nasionale Direkteur vir Openbare Vervolgings voorlê vir oorweging.

(3) *(a)* By ontvangs van 'n versoek in subartikel (2) bedoel, moet die Nasionale Direkteur vir Openbare Vervolgings hulself tevrede stel—
(i) dat verrigtinge ingestel is in 'n hof of tribunaal wat regsbevoegdheid in die versoekende vreemde Staat uitoefen; of
(ii) dat daar redelike gronde is om te vermoed dat 'n misdryf in die versoekende vreemde Staat gepleeg is of dat dit nodig is om vas te stel of 'n misdryf aldus gepleeg is en dat 'n ondersoek ten opsigte daarvan in die versoekende vreemde Staat onderneem word; en
(iii) dat die betrokke misdryf—
(aa) soortgelyk is aan dié in Deel I of Deel II van Hoofstuk 2 beoog; of
(bb) wesenlik soortgelyk is aan 'n misdryf in die Republiek erken, wat gepleeg kan word by wyse van, of gefasiliteer kan word deur die gebruik van, 'n item; en
(iv) dat die vreemde Staat voornemens is om 'n versoek te rig ingevolge artikel 7 van die Wet op Internasionale Samewerking in Strafregtelike Aangeleenthede, 1996, vir die verkryging van die data, inligting, 'n kommunikasie of 'n item in die Republiek vir gebruik in daardie verrigtinge of ondersoek in die vreemde Staat.

(b) By die toepassing van paragraaf *(a)*, kan die Nasionale Direkteur van Openbare Vervolgings steun op 'n sertifikaat wat heet om uitgereik te wees deur 'n bevoegde owerheid in die betrokke vreemde Staat, waarin die feite in subartikel (3)*(a)* beoog, vermeld word.

(4) *(a)* Die Nasionale Direkteur van Openbare Vervolgings moet die versoek om bystand, tesame met hul aanbevelings, aan die Kabinetslid verantwoordelik vir die regspleging voorlê vir die Kabinetslid se goedkeuring.

(b) By verwittiging van die Kabinetslid se goedkeuring, moet die Nasionale Direkteur van Openbare Vervolgings die versoek in subartikel (1) beoog, na die aangewese regter stuur vir oorweging.

(5) Waar die versoek verband hou met die bespoedigde openbaarmaking van verkeersdata, is subartikels (3)*(a)*(iv) en (4) nie van toepassing nie, en die Nasionale Direkteur van Openbare Vervolgings moet die versoek om bystand, saam met hul aanbevelings, aan die aangewese regter voorlê.

(6) Behoudens subartikels (7) en (8), kan die aangewese regter by ontvangs van 'n versoek in subartikel (4) of (5) beoog, enige bevel uitreik wat hulle gepas ag om te verseker dat die aangevraagde—
(a) data of ander item ooreenkomstig artikel 42 bewaar word;
(b) data of ander item op beslag gelê word op 'n bespoedigde grondslag ooreenkomstig artikel 29 en bewaar word;
(c) verkeersdata op 'n bespoedigde grondslag openbaar gemaak word ingevolge 'n lasgewing vir openbaarmaking van data ooreenkomstig artikel 44;
(d) intydse kommunikasie-verwante inligting of argief-bewaarde kommunikasie-verwante inligting, verkry en bewaar word; of
(e) onregstreekse kommunikasie onderskep en bewaar word,

soos in die versoek gespesifiseer.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

(a) on the facts alleged in the request, there are reasonable grounds to believe that—
  (i) an offence substantially similar to the offences contemplated in Part I or Part II of Chapter 2 has been, is being, or will probably be committed; or
  (ii) any other offence substantially similar to an offence recognised in the Republic, has been, is being, or will probably be committed by means of, or facilitated through the use of, an article; and
  (iii) for purposes of the investigation it is necessary, in the interests of justice, to give an order contemplated in subsection (6);

(b) the request clearly identifies—
  (i) the person, electronic communications service provider or financial institution—
    (aa) who or which will receive, is in possession of, or is in control of, the data or other article that must be preserved; or
    (bb) from whose facilities the data, real-time communication-related information, archived communication-related information, indirect communications or traffic data must be obtained or intercepted;
  (ii) the data or other article which must be preserved;
  (iii) the data or other article which must be seized on an expedited basis and be preserved;
  (iv) the traffic data which must be disclosed on an expedited basis;
  (v) the real-time communication-related information or archived communication-related information, which is to be obtained; or
  (vi) the indirect communications, which are to be intercepted;

(c) the request is, where applicable, in accordance with—
  (i) any treaty, convention or other agreement to which that foreign State and the Republic are parties or which can be used as a basis for mutual assistance; or
  (ii) any agreement with any foreign State entered into in terms of section 57; and

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

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

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

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

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

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

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

(b) The specifically designated police official referred to in paragraph *(a)*, must inform—
  (i) the designated judge; and
  (ii) the National Director of Public Prosecutions,

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

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

Complying with order of designated judge

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

(2) A person, electronic communications service provider or financial institution to whom an order referred to in section 48(6) is addressed may, in writing, apply to the

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(7) Die aangewese regter kan slegs 'n bevel in subartikel (6) beoog gee, indien—

(a) daar, op die feite in die versoek beweer, redelike gronde is om te glo dat—

(i) 'n misdryf, wesenlik soortgelyk aan die misdrywe in Deel I of Deel II van Hoofstuk 2 beoog gepleeg is, gepleeg word of waarskynlik gepleeg sal word; of

(ii) enige ander misdryf wesenlik soortgelyk aan 'n misdryf in die Republiek erken, is, word of waarskynlik gepleeg sal word by wyse van, of gefasiliteer deur die gebruik van, 'n item; en

(iii) vir die doeleindes van die ondersoek, dit nodig is, in die belang van geregtigheid, om 'n bevel beoog in subartikel (6) te gee;

(b) die versoek identifiseer duidelik—

(i) die persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling—

(aa) wat die data of ander item wat bewaar moet word, sal ontvang, in besit is daarvan, of in beheer is daarvan; of

(bb) vanaf wie se fasiliteite die data, intydse kommunikasie-verwante inligting, argief-bewaarde kommunikasie-verwante inligting, onregstreekse kommunikasie of verkeersdata verkry of onderskep moet word;

(ii) die data of ander item wat bewaar moet word;

(iii) die data of ander item waarop beslag gelê moet word op 'n bespoedigde grondslag en wat bewaar moet word;

(iv) die verkeersdata wat op 'n bespoedigde grondslag openbaargemaak moet word;

(v) die intydse kommunikasie-verwante inligting of argief-bewaarde kommunikasie-verwante inligting, wat verkry moet word; of

(vi) die onregstreekse kommunikasie wat onderskep moet word;

(c) die versoek, waar van toepassing, in ooreenstemming is met—

(i) enige verdrag, konvensie of ander ooreenkoms waartoe daardie vreemde Staat en die Republiek partye is of wat as grondslag vir onderlinge bystand gebruik kan word; of

(ii) enige ooreenkoms met enige vreemde Staat aangegaan ingevolge artikel 57; en

(d) die bevel in subartikel (6) beoog in ooreenstemming is met enige toepaslike reg van die Republiek.

(8) Die aangewese regter kan, waar 'n versoek verband hou met die bespoedigde openbaarmaking van verkeersdata—

(a) voorwaardes of beperkings in verband met die openbaarmaking van verkeersdata spesifiseer soos hul gepas ag; of

(b) weier om 'n bevel bedoel in subartikel (6)*(c)* te gee, indien die openbaarmaking van die verkeersdata die soewereiniteit, sekuriteit, openbare veiligheid of ander noodsaaklike belange van die Republiek kan benadeel.

(9) *(a)* In die geval van dringendheid, kan 'n versoek deur enige owerheid, hof of tribunaal wat regsbevoegdheid in 'n vreemde Staat bedoel in subartikel (1) uitoefen, regstreeks aan die aangewese regter voorgelê word.

(b) By ontvangs van 'n versoek ingevolge paragraaf *(a)*, kan die aangewese regter enige bevel bedoel in subartikel (6) gee.

(10) *(a)* 'n Spesifiek aangewese polisiebeampte moet 'n bevel in subartikel (6) beoog, beteken of uitvoer.

(b) Die spesifiek aangewese polisiebeampte bedoel in paragraaf *(a)*, moet—

(i) die aangewese regter; en

(ii) die Nasionale Direkteur van Openbare Vervolgings,

skriftelik inlig van die feit dat 'n bevel beteken of uitgevoer is.

(11) Die Nasionale Direkteur van Openbare Vervolgings moet die toepaslike owerheid in 'n vreemde Staat skriftelik inlig van die feit dat 'n bevel gegee en uitgevoer is of nie gegee is nie.

Voldoening aan bevel van aangewese regter

49. (1) 'n Persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling moet aan 'n bevel van die aangewese regter wat ingevolge artikel 48(6) uitgevaardig is, voldoen.

(2) 'n Persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling aan wie 'n bevel bedoel in artikel 48(6) gerig is, kan skriftelik by die aangewese regter

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

designated judge for an amendment or the cancellation of the order concerned on the ground that they cannot timeously or in a reasonable fashion, comply with the order.

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

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

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

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

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

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

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

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

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

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

(a) the designated judge; and

(b) the applicable authority in a foreign State,

of the outcome of the request for assistance and cooperation.

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

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

(b) accompanied by—

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

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

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

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

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

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

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

Issuing of direction requesting assistance from foreign State

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

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

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

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

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

(aa) preserve data or other articles;

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

aansoek doen om 'n wysiging of die kansellasie van die betrokke bevel op grond daarvan dat hulle nie tydig of op 'n redelike wyse aan die bevel kan voldoen nie.

(3) Die aangewese regter by wie 'n aansoek ingevolge subartikel (2) gedoen is, moet, so gou moontlik ná ontvangs daarvan—

(a) die aansoek oorweeg en kan, vir hierdie doel, beveel dat mondelinge of skriftelike getuienis aangebied word aangaande enige feit in die aansoek beweer;

(b) 'n beslissing gee ten opsigte van die aansoek; en

(c) indien die aansoek suksesvol is, die Nasionale Direkteur van Openbare Vervolgings verwittig van die uitslag van die aansoek.

(4) 'n Persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling wat—

(a) versuim om aan 'n bevel bedoel in artikel 48(6) te voldoen; of

(b) 'n vals verklaring maak in 'n aansoek in subartikel (2) bedoel,

is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met 'n boete of gevangenisstraf vir 'n tydperk van hoogstens twee jaar of met beide 'n boete en sodanige gevangenisstraf.

Verwittiging van vreemde Staat van uitslag van versoek om onderlinge bystand en bespoedigde openbaarmaking van verkeersdata

50. (1) Die Nasionale Direkteur van Openbare Vervolgings moet—

(a) die aangewese regter; en

(b) die toepaslike owerheid in 'n vreemde Staat,

inlig van die uitkoms van die versoek om bystand en samewerking.

(2) Enige verkeersdata wat ingevolge 'n bevel bedoel in artikel 48(6)*(c)* beskikbaar gestel word, moet—

(a) op die voorgeskrewe wyse aan die aangewese Kontakpunt verskaf word vir voorlegging aan die toepaslike owerheid in 'n vreemde Staat; en

(b) vergesel gaan van—

(i) 'n afskrif van die bevel in artikel 48(6) bedoel; en

(ii) 'n beëdigde verklaring in die voorgeskrewe vorm deur die persoon of gemagtigde verteenwoordiger van 'n elektroniese kommunikasiediens-verskaffer of finansiële instelling, wat die egtheid, integriteit en betroubaarheid van die inligting wat voorsien word, bevestig.

(3) Die verkeersdata, tesame met die afskrif van die bevel en beëdigde verklaring in subartikel (2) bedoel, moet aan die toepaslike owerheid wat regsbevoegdheid uitoefen in 'n vreemde Staat wat die bystand ingevolge artikel 48(1) aangevra het, voorsien word.

(4) 'n Persoon, elektroniese kommunikasiediensverskaffer of finansiële instelling wat—

(a) versuim om aan subartikel (2) of enige regulasies beoog in artikel 59(1)*(a)*(xxii) te voldoen; of

(b) 'n vals verklaring maak in 'n beëdigde verklaring in subartikel (2)*(b)*(ii) bedoel,

is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met 'n boete of gevangenisstraf vir 'n tydperk van hoogstens twee jaar of met beide 'n boete en sodanige gevangenisstraf.

Uitreiking van lasgewing om onderlinge bystand van vreemde Staat te versoek

51. (1) Indien dit vir 'n landdros uit inligting onder eed of by wyse van plegtige verklaring blyk dat daar redelike gronde is om te vermoed dat—

(a) 'n misdryf beoog in Deel I of Deel II van Hoofstuk 2; of

(b) enige ander misdryf ingevolge die wette van die Republiek, wat gepleeg kan word by wyse van, of gefasiliteer kan word deur die gebruik van, 'n item,

gepleeg is of dat dit nodig is om vas te stel of die misdryf aldus gepleeg is en dat dit nodig is—

(i) hangende die uitreiking van 'n versoekbrief ingevolge artikel 2(2) van die Wet op Internasionale Samewerking in Strafregtelike Aangeleenthede, 1996, om—

(aa) data of ander items te bewaar;

(bb) op 'n bespoedigde grondslag op data of ander items beslag te lê;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

(dd) intercept indirect communications; or

(ii) to obtain traffic data,

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

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

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

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

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

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

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

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

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

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

within the area of jurisdiction of a foreign State.

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

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

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

which is requested to provide assistance and cooperation.

CHAPTER 6

DESIGNATED POINT OF CONTACT

Establishment and functions of designated Point of Contact

52. (1) The National Commissioner must—

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

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

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

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

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

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

(iii) an offence—

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

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

in a foreign State.

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

(i) the provision of technical advice and assistance;

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

(iii) the provision of legal assistance;

(iv) the identification and location of an article;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(cc) intydse kommunikasie-verwante inligting of argief-bewaarde kommunikasie-verwante inligting te verkry; of

(dd) onregstreekse kommunikasies te onderskep; of

(ii) om verkeersdata te verkry,

binne die regsgebied van 'n vreemde Staat, kan die landdros 'n lasgewing in die voorgeskrewe vorm uitreik waarin bystand van daardie vreemde Staat versoek word soos in die lasgewing uiteengesit word.

(2) 'n Lasgewing in subartikel (1) bedoel, moet spesifiseer dat—

(a) daar redelike gronde is om te glo dat 'n misdryf in subartikel (1)*(a)* of *(b)* in die Republiek gepleeg is of dat dit nodig is om vas te stel of so 'n misdryf gepleeg is;

(b) 'n ondersoek ten opsigte daarvan onderneem word; en

(c) dit vir die doeleindes van die ondersoek, in die belang van geregtigheid, nodig is dat—

(i) data of ander items in die lasgewing gespesifiseer, bewaar word;

(ii) data of enige ander item in die lasgewing gespesifiseer, op 'n bespoedigde grondslag op beslag gelê en bewaar moet word;

(iii) verkeersdata, in die lasgewing gespesifiseer, op 'n bespoedigde grondslag openbaargemaak moet word;

(iv) intydse kommunikasie-verwante inligting of argief-bewaarde kommunikasie-verwante inligting in die lasgewing gespesifiseer, verkry en bewaar moet word; of

(v) onregstreekse kommunikasie in die lasgewing gespesifiseer, onderskep en bewaar moet word,

binne die regsgebied van 'n vreemde Staat.

(3) Die lasgewing moet aan die Nasionale Direkteur van Openbare Vervolgings gestuur word vir oorsending aan—

(a) die gepaste owerheid in die vreemde Staat; of

(b) 'n aangewese Kontakpunt in die vreemde Staat,

waarvan bystand en samewerking versoek word.

HOOFSTUK 6

AANGEWESE KONTAKPUNT

Instelling en werksaamhede van aangewese Kontakpunt

52. (1) Die Nasionale Kommissaris moet—

(a) 'n kantoor instel of aanwys binne die bestaande strukture van die Suid-Afrikaanse Polisiediens, wat as die aangewese Kontakpunt vir die Republiek bekend sal staan; en

(b) die aangewese Kontakpunt toerus, bedryf en in stand hou.

(2) Die Nasionale Kommissaris oefen finale verantwoordelikheid oor die administrasie en funksionering van die aangewese Kontakpunt uit.

(3) *(a)* Die aangewese Kontakpunt moet die voorsiening van onmiddellike bystand verseker vir die doeleindes van verrigtinge of ondersoeke rakende die pleging of voorgenome pleging van—

(i) 'n misdryf kragtens Deel I of Deel II van Hoofstuk 2;

(ii) enige ander misdryf ingevolge die wette van die Republiek, wat gepleeg kan word by wyse van, of gefasiliteer kan word deur die gebruik van,'n item; of

(iii) 'n misdryf—

(aa) soortgelyk aan dié in Deel I of Deel II van Hoofstuk 2 beoog; of

(bb) wesenlik soortgelyk aan 'n misdryf in die Republiek erken, wat gepleeg kan word by wyse van, of gefasiliteer kan word deur die gebruik van, 'n item,

in 'n vreemde Staat.

(b) Die bystand beoog in subartikel (3)*(a)* sluit in—

(i) die voorsiening van tegniese advies en bystand;

(ii) die fasilitering of voorsiening van bystand aangaande enigiets wat kragtens Hoofstukke 4 en 5 gemagtig is;

(iii) die voorsiening van regsbystand;

(iv) die identifikasie en opsporing van 'n item;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(v) the identification and location of a suspect; and
(vi) cooperation with appropriate authorities of a foreign State.

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

(a) regulate any aspect provided for in subsection (3);
(b) impose additional duties on the designated Point of Contact; and
(c) regulate any aspect which is necessary or expedient for the proper implementation of this section.

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

(a) who have particular knowledge and skills in respect of any aspect dealt with in this Act; and
(b) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994, to the satisfaction of the National Director of Public Prosecutions,

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

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

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

(i) the number of matters in which assistance was provided in terms of subsection (3)*(a)*; and
(ii) the number of matters in which assistance was received from a foreign State.

CHAPTER 7

EVIDENCE

Proof of certain facts by affidavit

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

(a) the interpretation of data;
(b) the design or functioning of data, a computer program, a computer data storage medium or a computer system;
(c) computer science;
(d) electronic communications networks and technology;
(e) software engineering; or
(f) computer programming,

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

(i) *(aa)* fall within a category of persons within the Republic; or
(bb) are in the service of a body in the Republic or a foreign State,
designated by the Cabinet member responsible for the administration of justice, by notice in the *Gazette*;
(ii) possess relevant qualifications, expertise and experience which makes them competent to make the affidavit; and
(iii) have established such fact by means of an examination or process that is documented in the document,

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(v) die identifikasie en opsporing van 'n verdagte; en

(vi) samewerking met toepaslike owerhede van 'n vreemde Staat.

(4) Die Kabinetslid verantwoordelik vir polisiëring kan regulasies uitvaardig om verder—

(a) enige aspek waarvoor in subartikel (3) voorsiening gemaak word, te reël;

(b) bykomende pligte aan die aangewese Kontakpunt op te lê; en

(c) enige aspek wat noodsaaklik of raadsaam is vir die behoorlike implementering van hierdie artikel, te reël.

(5) Die Nasionale Direkteur van Openbare Vervolgings moet lede van die Nasionale Vervolgingsgesag beskikbaar stel—

(a) wat bepaalde kennis en vaardighede het ten opsigte van enige aspek wat in hierdie Wet hanteer word; en

(b) aan wie 'n sekerheidsklaring deur die Staatsveiligheidsagentskap ingevolge artikel 2A van die Wet op Nasionale Strategiese Intelligensie, 1994, uitgereik is, tot die tevredenheid van die Nasionale Direkteur van Openbare Vervolgings,

om regshulp aan die aangewese Kontakpunt te voorsien soos noodsaaklik of raadsaam mag wees vir die doeltreffende bedryf van die aangewese Kontakpunt.

(6) *(a)* Die Kabinetslid verantwoordelik vir polisiëring moet, aan die einde van elke boekjaar, 'n verslag aan die Voorsitter van die Gesamentlike Staande Komitee oor Intelligensie ingestel by artikel 2 van die Wet op Toesig oor Intelligensiedienste, 1994, voorlê oor die werksaamhede en aktiwiteite van die aangewese Kontakpunt.

(b) Die verslag in paragraaf *(a)* beoog, moet insluit—

(i) die getal aangeleenthede waar bystand ingevolge subartikel (3)*(a)* aan 'n vreemde Staat voorsien is; en

(ii) die getal aangeleenthede waar bystand van 'n vreemde Staat ontvang is.

HOOFSTUK 7

GETUIENIS

Bewys van sekere feite deur beëdigde verklaring

53. (1) Wanneer enige feit vasgestel deur enige ondersoek of proses wat enige vaardigheid vereis in—

(a) die vertolking van data;

(b) die ontwerp of funksionering van data, 'n rekenaarprogram, 'n rekenaardatabergingsmedium of 'n rekenaarstelsel;

(c) rekenaarwetenskap;

(d) elektroniese kommunikasienetwerke en tegnologie;

(e) sagteware-ingenieurswese; of

(f) rekenaarprogrammering,

tersaaklik is of kan word tot 'n aangeleentheid by strafregtelike verrigtinge of siviele verrigtinge soos in Hoofstuk 5 of 6 van die Wet op Voorkoming van Georganiseerde Misdaad, 1998, beoog, is 'n dokument wat voorgee om 'n beëdigde verklaring of plegtige of geattesteerde verklaring te wees soos afgelê deur 'n persoon wat, in daardie dokument, stel dat hulle—

(i) *(aa)* in 'n kategorie van persone in die Republiek val; of
(bb) in die diens staan van 'n liggaam in die Republiek of 'n vreemde Staat,
deur die Kabinetslid verantwoordelik vir die regspleging by kennisgewing in die *Staatskoerant* aangewys;

(ii) tersaaklike kwalifikasies, kundigheid en ervaring het wat hulle bevoeg maak om die beëdigde verklaring af te lê; en

(iii) daardie feit met behulp van 'n ondersoek of proses wat in die dokument gedokumenteer is, vasgestel het,

is by die blote voorlegging daarvan by sodanige verrigtinge, *prima facie* bewys van sodanige feit.

(2) Enige persoon wat kragtens subartikel (1) 'n beëdigde verklaring of plegtige of geattesteerde verklaring aflê en wat in sodanige beëdigde verklaring of plegtige of geattesteerde verklaring opsetlik enigiets stel wat vals is, is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met 'n boete of gevangenisstraf vir 'n tydperk van hoogstens twee jaar of met beide 'n boete en sodanige gevangenisstraf.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

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

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

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

(ii) authenticated—

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

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

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

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

CHAPTER 8

REPORTING OBLIGATIONS AND CAPACITY BUILDING

Obligations of electronic communications service providers and financial institutions

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

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

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

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

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

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(3) Die hof voor wie 'n beëdigde verklaring of plegtige of geattesteerde verklaring voorgelê word as *prima facie*-bewys van die tersaaklike inhoud daarvan kan, na goeddunke, die persoon wat die beëdigde verklaring of plegtige of geattesteerde verklaring afgelê het, laat dagvaar om mondelinge getuienis in die betrokke verrigtinge af te lê of kan skriftelike vraagpunte vir beantwoording aan sodanige persoon laat voorlê en sodanige vraagpunte en enige antwoord daarop wat voorgee om 'n antwoord van sodanige persoon te wees, is insgelyks as getuienis by sodanige verrigtinge toelaatbaar.

(4) Geen bepaling van hierdie artikel maak inbreuk op enige ander wetsbepaling waarkragtens enige sertifikaat of ander dokument as getuienis toelaatbaar is nie, en die bepalings van hierdie artikel word geag so 'n wetsbepaling aan te vul en nie te vervang nie.

(5) *(a)* By die toepassing van subartikel (1), is 'n dokument wat voorgee om 'n beëdigde verklaring of plegtige of geattesteerde verklaring afgelê deur 'n persoon wat in daardie beëdigde verklaring of plegtige of geattesteerde verklaring beweer dat hulle in die diens staan van 'n liggaam in die Republiek of 'n vreemde Staat aangewys deur die Kabinetslid verantwoordelik vir die regspleging by kennisgewing in die *Staatskoerant*, van nul en gener waarde tensy dit—

(i) ingevolge 'n bevel van 'n bevoegde hof of op gesag van 'n regeringsinstelling van die betrokke vreemde Staat, na gelang van die geval, verkry is; en

(ii) gewaarmerk is—

(aa) op die wyse voorgeskryf in die hofreëls vir die waarmerking van dokumente wat buite die Republiek verly is; of

(bb) deur 'n persoon, en op die wyse beoog in artikel 7 of 8 van die Wet op Vrederegters en Kommissarisse van Ede, 1963.

(b) Die toelaatbaarheid en bewyswaarde van 'n beëdigde verklaring in paragraaf *(a)* bedoel, word nie geraak deur die feit dat die vorm van die eed, bevestiging of attestasie daarvan verskil van die vorm van die eed, bevestiging of attestasie wat in die Republiek voorgeskryf word nie.

(c) 'n Hof voor wie'n beëdigde verklaring of 'n plegtige of geattesteerde verklaring in paragraaf *(a)* beoog, voorgelê word, kan ten einde enige onduidelikhede in die bedoelde beëdigde verklaring op te klaar, beveel dat 'n aanvullende beëdigde verklaring of plegtige of geattesteerde verklaring voorgelê word of dat mondelinge getuienis aangehoor word: Met dien verstande dat mondelinge getuienis slegs aangehoor kan word indien die hof van oordeel is dat dit in die belang van die regspleging is en dat 'n party tot die verrigtinge wesenlik benadeel sal word indien mondelinge getuienis nie aangehoor word nie.

HOOFSTUK 8

RAPPORTERINGSVERPLIGTINGE EN KAPASITEITSBOU

Verpligtinge van elektroniese kommunikasiediensverskaffers en finansiële instellings

54. (1) 'n Elektroniese kommunikasiediensverskaffer of finansiële instelling wat bewus is van of bewus word daarvan dat sy elektroniese kommunikasiediens of elektroniese kommunikasienetwerk betrokke is by die pleging van enige kategorie of klas misdrywe waarvoor in Deel I van Hoofstuk 2 voorsiening gemaak en wat ingevolge subartikel (2) bepaal word, moet—

(a) sonder onnodige vertraging en, waar moontlik, nie later nie as 72 uur ná bewuswording van die misdryf, die misdryf op die voorgeskrewe vorm en wyse by die Suid-Afrikaanse Polisiediens aanmeld; en

(b) enige inligting bewaar wat die Suid-Afrikaanse Polisiediens in die ondersoek van die misdryf behulpsaam kan wees.

(2) Die Kabinetslid verantwoordelik vir polisiëring, in oorleg met die Kabinetslid verantwoordelik vir die regspleging, moet—

(a) die kategorie of klas van misdrywe wat ingevolge subartikel (1) by die Suid-Afrikaanse Polisiediens aangemeld moet word; en

(b) die vorm en wyse waarop 'n elektroniese kommunikasiediensverskaffer of finansiële instelling misdrywe by die Suid-Afrikaanse Polisiediens moet aanmeld,

by kennisgewing in die *Staatskoerant* voorskryf.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

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

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

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

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

Capacity to detect, prevent and investigate cybercrimes

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

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

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

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

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

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

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

(b) the number of—

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

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

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

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

.

National Director of Public Prosecutions must keep statistics of prosecutions

56. (1) The National Director of Public Prosecutions must keep statistics of the number of prosecutions instituted for offences in terms of Part I or Part II of Chapter 2, the outcome of such prosecutions and any other information relating to such prosecutions, which is determined by the Cabinet member responsible for the administration of justice.

(2) The statistics or information contemplated in subsection (1) must be included in the report of the National Director of Public Prosecutions referred to in section 22(4)*(g)* of the National Prosecuting Authority Act, 1998.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(3) 'n Elektroniese kommunikasiediensverskaffer of finansiële instelling wat versuim om aan subartikel (1) te voldoen, is skuldig aan 'n misdryf en is by skuldigbevinding strafbaar met 'n boete van hoogstens R50 000.

(4) Behoudens enige ander wetsbepaling of verpligting, moet die bepalings van subartikel (1) nie sodanig uitgelê word nie dat dit verpligtinge aan 'n elektroniese kommunikasiediensverskaffer of finansiële instelling sou oplê om—

(a) die data wat die elektroniese kommunikasiediensverskaffer of finansiële instelling oorsend of berg te monitor; of

(b) aktief feite of omstandighede te soek wat aanduidend is van enige onwettige aktiwiteit.

(5) Hierdie Hoofstuk is nie op 'n finansiële sektor reguleerder of 'n werksaamheid verrig deur die Suid-Afrikaanse Reserwebank ingevolge artikel 10 van die Wet op die Suid-Afrikaanse Reserwebank, 1989, van toepassing nie.

Kapasiteit om kubermisdade te bespeur, te voorkom en te ondersoek

55. (1) Die Kabinetslid verantwoordelik vir polisiëring moet—

(a) genoegsame menslike hulpbron- en operasionele kapasiteit vestig en in stand hou om kubermisdade te bespeur, te voorkom en te ondersoek;

(b) verseker dat lede van die Suid-Afrikaanse Polisiediens basiese opleiding ontvang in aspekte wat verband hou met die bespeuring, voorkoming en ondersoek van kubermisdade; en

(c) in samewerking met enige inrigting vir hoër onderwys, in die Republiek of elders, geakkrediteerde opleidingsprogramme ontwikkel en instel vir lede van die Suid-Afrikaanse Polisiediens wat hoofsaaklik gemoeid is met die bespeuring, voorkoming en ondersoek van kubermisdade.

(2) Die Kabinetslid verantwoordelik vir polisiëring kan regulasies uitvaardig om enige aspek in subartikel (1) bedoel, verder te reël.

(3) Die Kabinetslid verantwoordelik vir polisiëring moet, aan die einde van elke boekjaar, 'n verslag aan die Parlement voorlê aangaande—

(a) vordering met die implementering van hierdie artikel;

(b) die getal—

(i) misdrywe waarvoor in Deel I of Deel II van Hoofstuk 2 voorsiening gemaak word, wat by die Suid-Afrikaanse Polisiediens aangemeld is;

(ii) sake wat, ingevolge subparagraaf (i), by die Suid-Afrikaanse Polisiediens aangemeld is, wat tot strafregtelike verrigtinge gelei het; en

(iii) sake waar geen strafregtelike vervolgings ingestel is nie ná 'n tydperk van 18 maande nadat 'n saak ingevolge subparagraaf (i) by die Suid-Afrikaanse Polisiediens aangemeld is; en

(c) die getal lede van die Suid-Afrikaanse Polisiediens wat opleiding soos beoog in subartikel (1)*(b)* en *(c)*, ontvang het.

Nasionale Direkteur van Openbare Vervolgings moet statistieke van vervolgings hou

56. (1) Die Nasionale Direkteur van Openbare Vervolgings moet statistieke hou van die getal vervolgings ingestel vir misdrywe ingevolge Deel I of Deel II van Hoofstuk 2, die uitslag van daardie vervolgings en enige ander inligting aangaande daardie vervolgings, wat deur die Kabinetslid verantwoordelik vir die regspleging bepaal word.

(2) Die statistieke of inligting in subartikel (1) beoog, moet in die verslag van die Nasionale Direkteur van Openbare Vervolgings bedoel in artikel 22(4)*(g)* van die Wet op die Nasionale Vervolgingsgesag, 1998, ingesluit word.

This gazette is also available free online at **www.gpwonline.co.za**

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

CHAPTER 9

GENERAL PROVISIONS

National Executive may enter into agreements

57. (1) The National Executive may enter into any agreement with any foreign State regarding—

(a) the provision of mutual assistance and cooperation relating to the investigation and prosecution of—
  (i) an offence under Part I or Part II of Chapter 2;
  (ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or
  (iii) an offence—
    (aa) similar to those contemplated in Part I or Part II of Chapter 2; or
    (bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article,

  in that foreign State;

(b) the implementation of cybercrime response activities;

(c) training, research, information and technology-sharing and the exchange of information on the detection, prevention, mitigation and investigation of cybercrimes;

(d) the establishment or designation of points of contact to facilitate the provision of mutual assistance and cooperation as contemplated in paragraph *(a)*;

(e) the implementation of emergency cross-border response mechanisms to mitigate the effect of cybercrimes; and

(f) the reciprocal implementation of measures to curb cybercrime.

(2) A member of the National Executive must, as soon as practicable after Parliament has agreed to the ratification of, accession to, amendment of, or revocation of, an agreement referred to in subsection (1), give notice thereof in the *Gazette*.

Repeal or amendment of laws

58. The laws mentioned in the Schedule are hereby repealed or amended to the extent reflected in the third column of the Schedule.

Regulations

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

(a) must make regulations to prescribe the—
  (i) form and manner of the application as contemplated in section 20(1);
  (ii) form of the order as contemplated in section 20(3);
  (iii) manner of serving the order as contemplated in section 20(4);
  (iv) form and manner of the application as contemplated in section 20(6);
  (v) form and manner in which the court may subpoena a person as contemplated in section 20(8);
  (vi) form of the direction and affidavit and manner to furnish information to a court as contemplated in section 21(1)*(b)*;
  (vii) manner of serving a direction as contemplated in section 21(2);
  (viii) manner and the form of the affidavit to apply for an extension of the time period or cancellation of the direction as contemplated in section 21(3)*(b)*;
  (ix) manner for requesting additional information as contemplated in section 21(4)*(b)*;
  (x) form and manner of informing an electronic communications service provider of the outcome of application as contemplated in section 21(4)*(d)*;
  (xi) tariffs of compensation payable to an electronic communications service provider as contemplated in section 21(6);
  (xii) form of the order and manner of service of the order as contemplated in section 22(3);

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

HOOFSTUK 9

ALGEMENE BEPALINGS

Nasionale Uitvoerende Gesag kan ooreenkomste aangaan

57. (1) Die Nasionale Uitvoerende Gesag kan enige ooreenkoms met enige vreemde Staat aangaan oor—

(a) die voorsiening van onderlinge bystand en samewerking aangaande die ondersoek en vervolging van—
   (i) 'n misdryf kragtens Deel I of Deel II van Hoofstuk 2;
   (ii) enige ander misdryf ingevolge die reg van die Republiek wat gepleeg kan word by wyse van, of gefasiliteer kan word deur die gebruik van, 'n item; of
   (iii) 'n misdryf—
      (aa) soortgelyk aan dié in Deel I of Deel II van Hoofstuk 2 beoog; of
      (bb) wesenlik soortgelyk aan 'n misdryf in die Republiek erken wat gepleeg kan word by wyse van, of gefasiliteer kan word deur die gebruik van, 'n item,

   in daardie vreemde Staat;

(b) die instelling van kubermisdaadreaksie-aktiwiteite;

(c) opleidings-, navorsings-, inligtings- en tegnologiedeling en die uitruil van inligting oor die bespeuring, voorkoming, mitigasie en ondersoek van kubermisdade;

(d) die instelling of aanwysing van kontakpunte om die voorsiening van onderlinge bystand en samewerking soos in paragraaf *(a)* beoog, te fasiliteer;

(e) die inwerkingstelling van oorgrensnoodreaksiemeganismes om die uitwerking van kubermisdade te mitigeer; en

(f) die wedersydse inwerkingstelling van maatreëls om kubermisdaad te bekamp.

(2) 'n Lid van die Nasionale Uitvoerende Gesag moet, so gou prakties moontlik nadat die Parlement ingestem het tot die bekragtiging van, toetreding tot, wysiging van of herroeping van 'n ooreenkoms in subartikel (1) bedoel, kennis daarvan in die *Staatskoerant* gee.

Herroeping of wysiging van wette

58. Die wette in die Bylae genoem word hierby herroep of gewysig tot die mate in die derde kolom van die Bylae aangedui.

Regulasies

59. (1) Die Kabinetslid verantwoordelik vir die regspleging—

(a) moet regulasies uitvaardig om die—
   (i) vorm en wyse van die aansoek soos in artikel 20(1) beoog;
   (ii) vorm van die bevel soos in artikel 20(3) beoog;
   (iii) wyse van betekening van die bevel soos in artikel 20(4) beoog;
   (iv) vorm en wyse van die aansoek soos in artikel 20(6) beoog;
   (v) vorm en wyse waarop die hof 'n persoon kan dagvaar soos in artikel 20(8) beoog;
   (vi) vorm van die lasgewing en beëdigde verklaring en wyse waarop inligting aan die hof voorsien moet word soos in artikel 21(1)*(b)* beoog;
   (vii) wyse van betekening van 'n lasgewing soos in artikel 21(2) beoog;
   (viii) wyse en die vorm van die beëdigde verklaring om aansoek te doen om 'n verlenging van die tydperk of kansellasie van die lasgewing soos in artikel 21(3)*(b)* beoog;
   (ix) wyse vir aanvra van bykomende inligting soos in artikel 21(4)*(b)* beoog;
   (x) vorm en wyse waarop 'n elektroniese kommunikasiediensverskaffer van die uitslag van die aansoek ingelig moet word soos in artikel 21(4)*(d)* beoog;
   (xi) tariewe van vergoeding betaalbaar aan 'n elektroniese kommunikasiediensverskaffer soos in artikel 21(6) beoog;
   (xii) vorm van die bevel en wyse van betekening van die bevel soos in artikel 22(3) beoog;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

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

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

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

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

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

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

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

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

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

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

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

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

(2) *(a)* The Cabinet member responsible for policing must make regulations in terms of section 54(2), prescribing the—

(i) category or class of offences which must be reported to the South African Police Service in terms of section 54(2)*(a)*; and

(ii) form and manner in which an electronic communications service provider or financial institution must report offences to the South African Police Service as contemplated in section 54(2)*(b)*.

(b) The Cabinet member responsible for policing may make regulations to further regulate aspects contemplated in section 52(4) and 55(2).

Short title and commencement

60. (1) This Act is called the Cybercrimes Act, 2020, and comes into operation on a date fixed by the President by proclamation in the *Gazette*.

(2) Different dates may be fixed under subsection (1) in respect of different provisions of this Act.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

(xiii) vorm en wyse van die aansoek soos in artikel 22(5) beoog;
(xiv) vorm en wyse waarop die hof 'n persoon kan dagvaar soos in artikel 22(7) beoog;
(xv) vorm van die lasgewing vir bespoedigde bewaring van data en wyse van betekening soos in artikel 41(3) beoog;
(xvi) vorm en wyse waarop 'n aansoek soos beoog in artikel 41(7) gedoen moet word;
(xvii) vorm van die lasgewing vir bewaring van getuienis en wyse van betekening soos in artikel 42(2) beoog;
(xviii) vorm en wyse waarop 'n aansoek om tersydestelling van 'n lasgewing vir bewaring van getuienis gedoen moet word, soos in artikel 42(5) beoog;
(xix) vorm van die lasgewing vir openbaarmaking van data en wyse van betekening soos in artikel 44(3) beoog;
(xx) vorm en wyse waarop 'n aansoek om die wysiging of tersydestelling van 'n lasgewing vir die openbaarmaking van data gedoen moet word soos in artikel 44(5) beoog;
(xxi) vorm van die beëdigde verklaring soos in artikel 44(7)*(b)* beoog;
(xxii) wyse waarop verkeersdata aan die aangewese Kontakpunt verskaf moet word soos in artikel 50(2) beoog;
(xxiii) vorm van die beëdigde verklaring soos in artikel 50(2)*(b)*(ii) beoog; en
(xxiv) vorm van die lasgewing soos in artikel 51(1) beoog,

voor te skryf; en

(b) kan regulasies uitvaardig wat nie met hierdie Wet of enige ander wetsbepaling onbestaanbaar is nie, om enige aangeleentheid voor te skryf wat ingevolge hierdie Wet voorgeskryf kan word of wat nodig of dienstig kan wees om voor te skryf ten einde die oogmerke van hierdie Wet te bereik of te bevorder.

(2) *(a)* Die Kabinetslid verantwoordelik vir polisiëring moet regulasies ingevolge artikel 54(2) uitvaardig, wat die—

(i) kategorie of klas van misdrywe wat by die Suid-Afrikaanse Polisiediens aangemeld moet word ingevolge artikel 54(2)*(a)*; en
(ii) vorm en wyse waarop 'n elektroniese kommunikasiediensverskaffer of finansiële instelling misdrywe by die Suid-Afrikaanse Polisiediens moet aanmeld soos in artikel 54(2)*(b)* beoog,

voorskryf.

(b) Die Kabinetslid verantwoordelik vir polisiëring kan regulasies uitvaardig om aspekte in artikel 52(4) en 55(2) beoog, verder te reël.

Kort titel en inwerkingtreding

60. (1) Hierdie Wet heet die Wet op Kubermisdade, 2020, en tree in werking op 'n datum deur die President by proklamasie in die *Staatskoerant* vasgestel.

(2) Verskillende datums kan kragtens subartikel (1) ten opsigte van verskillende bepalings van hierdie Wet vasgestel word.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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; or (ii) by a person or with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offence in question was committed; or *(c)* if it is proven that the offence was committed by any law enforcement officer— (i) involving amounts of more than R10 000; or (ii) as a member of a group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; or (iii) with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offence in question was committed. 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.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Bylae

(Artikel 58)
WETTE HERROEP OF GEWYSIG

Nommer en jaar van wet	**Kort titel**	**Omvang van herroeping of wysiging**
Wet No. 51 van 1977	Strafproseswet, 1977	Die volgende items word by Bylae 5 gevoeg: "'n Oortreding van artikel 8, 9 of 10 van die Wet op Kubermisdade, 2020— *(a)* waarby bedrae van meer as R500 000,00 betrokke is; *(b)* waarby bedrae van meer as R100 000,00 betrokke is, indien bewys word dat die misdryf gepleeg is— (i) deur 'n persoon, groep persone, sindikaat of enige onderneming handelende in die uitvoering of bevordering van 'n gemeenskaplike doel of sameswering; of (ii) deur 'n persoon of met die sameswering of bystand van iemand anders, wat as deel van sy of haar pligte, werksaamhede of wettige magtiging, toesig gehad het oor, in beheer was van, of toegang gehad het tot data, 'n rekenaarprogram, 'n rekenaardatabergingsmedium of 'n rekenaarstelsel van 'n ander persoon ten opsigte waarvan die betrokke misdryf gepleeg is; of *(c)* indien bewys word dat die misdryf deur enige wetstoepassingsbeampte gepleeg is— (i) waarby bedrae van meer as R10 000 betrokke is; of (ii) as 'n lid van 'n groep persone, sindikaat of enige onderneming handelende in die uitvoering of ter bevordering van 'n gemeenskaplike doel of sameswering; of (iii) met die sameswering of bystand van iemand anders, wat as deel van sy of haar pligte, werksaamhede of wettige magtiging toesig gehad het oor, in beheer was van, of toegang gehad het tot data, 'n rekenaarprogram, 'n rekenaardatabergingsmedium of 'n rekenaarstelsel van iemand anders ten opsigte waarvan die betrokke misdryf gepleeg is. 'n Oortreding van artikel 11(2) van die Wet op Kubermisdade, 2020.".
Wet No. 68 van 1995	Wet op Suid-Afrikaanse Polisiediens, 1995	Artikel 71 word geskrap.
Wet No. 65 van 1996	Wet op Films en Publikasies, 1996	Artikel 24B word geskrap.

This gazette is also available free online at **www.gpwonline.co.za**

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
Wet No. 105 van 1997	Strafregwysigings-wet, 1997	Die volgende item word by Deel II van Bylae 2 gevoeg: "'n Oortreding van artikel 8, 9 of 10 van die Wet op Kubermisdade, 2020— *(a)* waarby bedrae van meer as R500 000,00 betrokke is; *(b)* waarby bedrae van meer as R100 000,00 betrokke is, indien bewys word dat die misdryf gepleeg is— (i) deur 'n persoon, groep persone, sindikaat of enige onderneming handelende in die uitvoering of bevordering van 'n gemeenskaplike doel of sameswering; of (ii) deur 'n persoon of met die sameswering of bystand van iemand anders, wat as deel van sy of haar pligte, werksaamhede of wettige magtiging toesig gehad het oor, in beheer was van of toegang gehad het tot data, 'n rekenaarprogram, 'n rekenaar-databergingmedium of 'n rekenaarstelsel van iemand anders ten opsigte waarvan die betrokke misdryf gepleeg is; of *(c)* indien bewys word dat die misdryf deur enige wetstoepassingsbeampte gepleeg is— (i) waarby bedrae van meer as R10 000,00 betrokke is; of (ii) as 'n lid van 'n groep persone, sindikaat of enige onderneming handelende in die uitvoering of ter bevordering van 'n gemeenskaplike doel of sameswering; of (iii) met die sameswering of bystand van iemand anders, wat as deel van sy of haar pligte, werksaamhede of wettige magtiging toesig gehad het oor, in beheer was van of toegang gehad het tot data, 'n rekenaarprogram, 'n rekenaar-databergingsmedium of 'n rekenaarstelsel van iemand anders ten opsigte waarvan die betrokke misdryf gepleeg is.".
Wet No. 32 van 1998	Wet op die Nasionale Vervolgingsgesag, 1998	Artikels 40A en 41(4) word geskrap.
Wet No. 111 van 1998	Wet op Korrektiewe Dienste, 1998	Artikel 128 word geskrap.
Wet No. 38 van 2001	Wet op Finansiële Intelligensiesentrum, 2001	Artikels 65, 66 en 67 word geskrap.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
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 (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—

Reproduced by LexisNexis under Government Printer’s Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	**Kort titel**	**Omvang van herroeping of wysiging**
Wet No. 25 van 2002	Wet op Elektroniese Kommunikasies en Transaksies, 2002	*(a)* Artikels 85, 86, 87 en 88 word geskrap. *(b)* Artikel 89 word deur die volgende artikel vervang: “**Strawwe** **89.** **[(1)]** ’n Persoon wat skuldig bevind is aan ’n misdryf bedoel in artikels 37(3), 40(2), 58(2), 80(5)**[,]** of 82(2) **[of 86(1), (2) of (3)]** is strafbaar met ’n boete of gevangenisstraf vir ’n tydperk wat nie 12 maande oorskry nie. **[(2) ’n Persoon wat skuldig bevind is aan ’n misdryf bedoel in artikel 86(4) of (5) of artikel 87 is strafbaar met ’n boete of gevangenisstraf vir ’n tydperk wat nie vyf jaar oorskry nie.]**”.
Wet No. 70 van 2002	Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting, 2002	*(a)* Artikel 1 word gewysig deur paragraaf *(a)* van die omskrywing van “ernstige misdryf” deur die volgende paragraaf te vervang: “*(a)* misdryf vermeld in **[die]** Bylae 1; of”. *(b)* Artikel 4 word gewysig deur die volgende subartikel by te voeg: “(3) Ondanks subartikel (2), kan ’n wetstoepassingsbeampte of ’n persoon wat ingevolge die Strafproseswet, 1977, die Wet op Kubermisdade, 2020, of enige ander wetsbepaling, gemagtig is om ’n verdagte te betrek of in hegtenis te neem of om ’n perseel te betree ten opsigte van die pleging of vermeende pleging van enige misdryf, tydens die inhegtenisname van die verdagte of terwyl hy of sy wettig op die perseel is, opneem wat hy of sy waarneem of hoor indien— *(a)* die opname direk in verband staan met die doel waarvoor die verdagte in hegtenis geneem is of die wetstoepassingsbeampte of persoon die perseel betree het; en *(b)* die wetstoepassingsbeampte of persoon— (i) hom- of haarself as sodanig geïdentifiseer het; en (ii) enige betrokkene mondelings ingelig het dat sy of haar regstreekse kommunikasie opgeneem staan te word, voordat die opname gemaak word.”. *(c)* Subartikel (4) van artikel 17 word deur die volgende subartikel vervang: “(4) ’n Intydse kommunikasie-verwante lasgewing kan slegs uitgereik word indien dit vir die betrokke aangewese regter voorkom, op die feite in die betrokke aansoek beweer, dat daar redelike gronde is om te glo dat—

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		(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 an offence mentioned in Schedule II, or property which is or could probably be an instrumentality of a serious offence, or is or could probably be the proceeds of unlawful activities, is necessary, and that the provision of real-time communication-related information is necessary for purposes of investigating such offence or gathering such information.''. *(d)* The substitution for subsection (4) of section 19 of the following subsection: ''(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;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(a) 'n ernstige misdryf of 'n misdryf in Bylae II genoem, gepleeg is of word of waarskynlik gepleeg sal word; *(b)* die insameling van inligting aangaande 'n werklike bedreiging van die openbare gesondheid of veiligheid, nasionale sekuriteit of dwingende nasionale ekonomiese belang van die Republiek nodig is; *(c)* die insameling van inligting aangaande 'n potensiële bedreiging van die openbare gesondheid of veiligheid of nasionale sekuriteit van die Republiek nodig is; *(d)* die rig van 'n versoek vir die voorsiening, of die voorsiening aan die bevoegde owerhede van 'n land of gebied buite die Republiek, van enige hulp in verband met, of in die vorm van, die onderskepping van kommunikasies met betrekking tot georganiseerde misdaad, 'n misdryf in Bylae II genoem of enige misdryf met betrekking tot terrorisme of die insameling van inligting met betrekking tot georganiseerde misdaad of terrorisme— (i) ooreenkomstig 'n internasionale onderlinge hulpooreenkoms is; of (ii) in belang van die internasionale betrekkinge of verpligtinge van die Republiek is; of *(e)* die insameling van inligting aangaande 'n misdryf in Bylae II genoem, of eiendom wat 'n middel is of waarskynlik kan wees by 'n ernstige misdryf of die opbrengs is of waarskynlik kan wees van onwettige aktiwiteite nodig is, en dat die verstrekking van intydse kommunikasie-verwante inligting nodig is vir die doeleindes van die ondersoek van so 'n misdryf of die insameling van sodanige inligting.''. *(d)* Subartikel (4) van artikel 19 word deur die volgende subartikel vervang: "(4) 'n Argief-bewaarde kommunikasie-verwante lasgewing kan slegs uitgereik word indien dit vir die betrokke regter van die Hoë Hof, streekhoflanddros of landdros voorkom, op die feite in die betrokke aansoek beweer, dat daar redelike gronde is om te glo dat— *(a)* 'n ernstige misdryf of 'n misdryf in Bylae II genoem gepleeg is of word of waarskynlik gepleeg sal word;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		(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 an offence mentioned in Schedule II, or property which is or could probably be an instrumentality of a serious offence, or is or could probably be the proceeds of unlawful activities, is necessary, 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: ''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.''.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(b) die insameling van inligting aangaande 'n werklike bedreiging van die openbare gesondheid of veiligheid, nasionale sekuriteit of dwingende nasionale ekonomiese belang van die Republiek nodig is; *(c)* die insameling van inligting aangaande 'n potensiële bedreiging van die openbare gesondheid of veiligheid of nasionale sekuriteit van die Republiek nodig is; *(d)* die rig van 'n versoek vir die voorsiening, of die voorsiening aan die bevoegde owerhede van 'n land of gebied buite die Republiek, van enige hulp in verband met, of in die vorm van, die onderskepping van kommunikasies met betrekking tot georganiseerde misdaad, 'n misdryf in Bylae II genoem of enige misdryf met betrekking tot terrorisme of die insameling van inligting met betrekking tot georganiseerde misdaad of terrorisme— (i) ooreenkomstig 'n internasionale onderlinge hulpooreenkoms is; of (ii) in belang van die internasionale betrekkinge of verpligtinge van die Republiek is; of *(e)* die insameling van inligting aangaande 'n misdryf in Bylae II genoem, of eiendom wat 'n middel is of waarskynlik kan wees by 'n ernstige misdryf of die opbrengs is of waarskynlik kan wees van onwettige aktiwiteite nodig is, en dat die verstrekking van argiefbewaarde kommunikasie-verwante inligting nodig is vir die doeleindes om so 'n misdryf te ondersoek of sodanige inligting in te samel.''. *(e)* Die herbenoeming van die Bylae tot die Wet as ''Bylae I'' en die byvoeging van die volgende items: ''15 Enige misdryf in artikels 17, 18, 19A of 20 van die Wysigingswet op die Strafreg (Seksuele Misdrywe en Verwante Aangeleenthede), 2007 (Wet No. 32 van 2007), beoog. 16 Enige misdryf beoog in— *(a)* artikel 8, 9(1) of (2) of 10 waarby 'n bedrag van R200 000,00 of meer betrokke is; of *(b)* artikel 11(1) of (2) of 17 (vir sover die artikel in verband staan met die misdrywe bedoel in artikel 11(1) of (2)), van die Wet op Kubermisdade, 2020.''.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		(f) The addition of the following Schedule after Schedule I: "**Schedule II** 1 Any offence referred to in— *(a)* section 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— (i) by 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 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) by the substitution for the heading to Part 2 of Chapter 3 of the following heading: "*Sexual exploitation and sexual grooming of children, exposure or display of or causing exposure or display of child pornography or pornography to children, child pornography and using children for pornographic purposes or benefiting from child pornography*"; and

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	**Kort titel**	**Omvang van herroeping of wysiging**
		(f) Die volgende Bylae word ná Bylae I bygevoeg: "**Bylae II** 1 Enige misdryf bedoel in— *(a)* artikels 3(1), 5, 6, 7(1), 8, 9(1) of (2), of 10; of *(b)* artikel 17 (vir sover die artikel in verband staan met die misdrywe in paragraaf *(a)* bedoel), van die Wet op Kubermisdade, 2020, waarby 'n bedrag van R50 000,00 of meer betrokke is. 2 Enige misdryf wat wesenlik soortgelyk is aan 'n misdryf in item 1 bedoel wat in 'n vreemde Staat gepleeg word of was, waarby 'n bedrag van R50 000,00 of meer betrokke is.".
Wet No. 32 van 2007	Wysigingswet op die Strafreg (Seksuele Misdrywe en Verwante Aangeleenthede), 2007	*(a)* Die Inhoudsopgawe tot die Wysigingswet op die Strafreg (Seksuele Misdrywe en Verwante Aangeleenthede), 2007, word hierby gewysig— (i) deur die volgende Deel en items ná item 11 in te voeg: "***Deel 3A*** "*Persone 18 jaar of ouer: Skadelike openbaarmaking van pornografie en bevele om klaer teen die skadelike uitwerking van openbaarmaking van pornografie te beskerm* 11A Skadelike openbaarmaking van pornografie 11B Bevele om klaer teen skadelike openbaarmaking van pornografie te beskerm hangende afhandeling van strafregtelike verrigtinge 11C Elektroniese kommunikasiediensverskaffer moet besonderhede aan hof verskaf 11D Bevele by afhandeling van strafregtelike verrigtinge"; (ii) deur die opskrif tot Deel 2 van Hoofstuk 3 deur die volgende opskrif te vervang: "*Seksuele uitbuiting en seksuele aanvoring van kinders, blootstelling of vertoon van of veroorsaking van blootstelling of vertoon van kinderpornografie of pornografie aan kinders, kinderpornografie en gebruikmaking van kinders vir pornografiese doeleindes of voordeeltrekking uit kinderpornografie*"; en

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		(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 definitions: " '**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; '**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—

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(iii) deur die volgende item ná item 19 in te voeg: "19A. Misdrywe in verband met kinderpornografie". *(b)* Artikel 1 word gewysig— (i) deur die volgende omskrywings ná die omskrywing van "Direkteur van Openbare Vervolgings" in te voeg: " **'elektroniese kommunikasiediens'** enige diens wat in die geheel of hoofsaaklik bestaan uit die oordrag, op enige wyse, van elektroniese kommunikasies oor 'n elektroniese kommunikasienetwerk, met uitsondering van uitsaaidienste soos omskryf in artikel 1 van die Wet op Elektroniese Kommunikasie, 2005; **'elektroniese kommunikasiediensverskaffer'**— *(a)* enige persoon wat 'n elektroniese kommunikasiediens verskaf aan die publiek, dele van die publiek, die Staat, of die intekenaars tot sodanige diens, kragtens en ooreenkomstig 'n elektroniese kommunikasiedienslisensie aan daardie persoon uitgereik ingevolge die Wet op Elektroniese Kommunikasie, 2005, of wat geag word gelisensieer of vrygestel van lisensiëring as sodanig te wees ingevolge daardie Wet; en *(b)* 'n persoon wat wettige magtiging het om die bedryf of gebruik van 'n private elektroniese kommunikasiediensnetwerk te beheer wat hoofsaaklik gebruik word vir voorsiening van elektroniese kommunikasiedienste vir die eienaar se eie gebruik en wat van lisensiëring vrygestel is ingevolge die Wet op Elektroniese Kommunikasie, 2005; **'elektroniese kommunikasie-identiteitsnommer'** 'n tegniese identifikasie-etiket wat die oorsprong of bestemming van elektroniese kommunikasieverkeer verteenwoordig; **'elektroniese kommunikasienetwerk'** 'n 'elektroniese kommunikasienetwerk' soos omskryf in artikel 1 van die Wet op Elektroniese Kommunikasie, 2005, en sluit 'n rekenaarstelsel in;".

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		(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;''.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(ii) deur die volgende omskrywing ná die omskrywing van ''hof vir seksuele misdrywe'' in te voeg: '' **'huisves'** om inligting op 'n elektroniese kommunikasienetwerk te berg wat gebruik word om 'n elektroniese kommunikasiediens te verskaf, waar dit besigtig, gekopieer of afgelaai kan word;''; (iii) deur die volgende omskrywing ná die omskrywing van ''Nasionale Direkteur van Openbare Vervolgings'' in te voeg: '' **'openbaar maak'** en **'openbaarmaking'**, in verband met die skadelike openbaarmaking van pornografie in artikel 11A beoog, ook om— *(a)* die pornografie aan 'n persoon wat die bedoelde ontvanger van die elektroniese kommunikasie is of enige ander persoon te stuur; *(b)* die pornografie op 'n elektroniese kommunikasienetwerk te berg, waar die pornografie besigtig, gekopieer of afgelaai kan word; of *(c)* 'n skakel na die pornografie wat op 'n elektroniese kommunikasiediensnetwerk geberg is, aan 'n persoon te stuur of andersins beskikbaar te stel waar die pornografie besigtig, gekopieer of afgelaai kan word;''; (iv) deur die volgende omskrywing ná die omskrywing van ''pornografie'' in te voeg: '' **'regstreekse uitvoering wat kinderpornografie behels'** 'n geleentheid waar 'n kind gebruik word om kinderpornografie te skep, te maak of te vervaardig;''; en (v) deur die volgende omskrywing ná die omskrywing van ''sorggewer'' in te voeg: '' **'Wet op Elektroniese Kommunikasie'** die Wet op Elektroniese Kommunikasie, 2005 (Wet No. 36 van 2005).''.

This gazette is also available free online at www.gpwonline.co.za

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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 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. **Orders to protect complainant against harmful disclosure of pornography pending finalisation of criminal proceedings**

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(c) Die volgende Deel en artikels word hierby ná artikel 11 in Hoofstuk 2 ingevoeg: "**Deel 3A** ***Persone 18 jaar of ouer: Skadelike openbaarmaking van pornografie en bevele om klaer teen skadelike uitwerking van openbaarmaking van pornografie te beskerm*** **Skadelike openbaarmaking van pornografie** **11A.** (1) Iemand ('A') wat wederregtelik en opsetlik pornografie waarin 'n persoon ('B') verskyn of beskryf word, openbaar maak of veroorsaak dat dit openbaar gemaak word, en sodanige openbaarmaking— *(a)* vind plaas sonder B se toestemming; en *(b)* veroorsaak enige leed, met inbegrip van geestelike, psigologiese, fisieke, maatskaplike of ekonomiese leed, aan B of enige lid van B se familie of enige ander persoon in 'n noue verwantskap met B, is skuldig aan die misdryf van skadelike openbaarmaking van pornografie. (2) Iemand ('A') wat wederregtelik en opsetlik dreig om pornografie soos bedoel in subartikel (1) openbaar te maak of dreig om die openbaarmaking daarvan te veroorsaak, en sodanige dreigement enige leed, of sodanige openbaarmaking redelikerwys verwag kan word om enige leed, bedoel in subartikel (1)*(b)* te veroorsaak, is skuldig aan die misdryf van dreigement om pornografie openbaar te maak wat leed sal veroorsaak. (3) Iemand ('A') wat wederregtelik en opsetlik dreig om pornografie in subartikel (1) bedoel openbaar te maak of dreig om die openbaarmaking daarvan te veroorsaak ten einde enige voordeel van B of enige familielid van B of enige ander persoon in 'n noue verwantskap met B, te verkry, is skuldig aan die misdryf van skadelike openbaarmaking van pornografie verwante afpersing. **Bevele ter beskerming van klaer teen skadelike openbaarmaking van pornografie beskerm hangende afhandeling van strafregtelike verrigtinge**

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		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— *(a)* is *prima facie* evidence that an offence referred to in section 11A(1), (2) or (3), has allegedly been committed against the applicant; and *(b)* are reasonable grounds to believe that a person referred to in subsection (1)*(a)*, disclosed or caused the disclosure or threatened the applicant with the disclosure or causing the disclosure of such pornography; or *(c)* are reasonable grounds to believe that the electronic communications service of the electronic communications service provider referred to in subsection (1)*(b)*, is used to host or disclose such pornography, 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.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		11B. (1) 'n Klaer (hierna die applikant genoem) wat 'n klag by die Suid-Afrikaanse Polisiediens indien dat 'n misdryf in artikel 11A(1), (2) of (3) beoog na bewering teen hom of haar gepleeg is, kan op 'n *ex parte*-grondslag op die voorgeskrewe vorm en wyse, by 'n landdroshof aansoek doen om 'n beskermingsbevel hangende die afhandeling van die strafregtelike verrigtinge om— *(a)* enige persoon te belet om pornografie wat met die klag verband hou, openbaar te maak, of veroorsaak dat dit openbaar gemaak word of die applikant te dreig met die openbaarmaking of veroorsaking van die openbaarmaaking daarvan; of *(b)* 'n elektroniese kommunikasiediens-verskaffer wie se elektroniese kommunikasiediens gebruik word om die pornografie te huisves of openbaar te maak wat met die klag verband hou, te beveel om daardie pornografie te verwyder of toegang daartoe te deaktiveer. (2) Die hof moet 'n aansoek ingevolge subartikel (1) aan die hof voorgelê, so gou as redelik moontlik oorweeg en kan, vir daardie doel, enige bykomende getuienis wat die hof gepas ag, oorweeg, met inbegrip van mondelinge getuienis of getuienis by wyse van beëdigde verklaring, wat deel van die oorkonde van die verrigtinge moet uitmaak. (3) Indien die hof oortuig is dat daar— *(a)* *prima facie* getuienis is dat 'n misdryf in artikel 11A(1), (2) of (3) bedoel, na bewering teen die applikant gepleeg is; en *(b)* redelike gronde is om te glo dat 'n persoon in subartikel (1)*(a)* bedoel, daardie pornografie openbaar gemaak het of openbaarmaking veroorsaak het of die applikant gedreig het met die openbaarmaking of veroorsaaking van die openbaarmaking van die pornografie; of *(c)* redelike gronde is om te glo dat die elektroniese kommunikasiediens van die elektroniese kommunikasiediens-verskaffer in subartikel (1)*(b)* bedoel, gebruik word om daardie pornografie te huisves of openbaar te maak, kan die hof, onderworpe aan sodanige voorwaardes wat die hof gepas ag, die bevel bedoel in subartikel (1) in die voorgeskrewe vorm uitreik.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(4) Die bevel in subartikel (3) bedoel, moet aan die persoon in subartikel (1)*(a)* of elektroniese kommunikasiediensverskaffer in subartikel (1)*(b)* bedoel, op die voorgeskrewe wyse beteken word: Met dien verstande dat indien die hof oortuig is dat die bevel nie op die voorgeskrewe wyse beteken kan word nie, die hof 'n bevel kan gee wat betekening in die vorm of op die wyse in daardie bevel gespesifiseer, toelaat. (5) 'n Bevel in subartikel (3) bedoel, is van krag vanaf die oomblik wat dit deur die hof uitgereik word en die bestaan daarvan onder die aandag van die persoon bedoel in subartikel (1)*(a)* of elektroniese kommunikasiediensverskaffer bedoel in subartikel (1)*(b)*, gebring is. (6) Iemand in subartikel (1)*(a)* bedoel, anders as die persoon wat van die pleging van die betrokke misdryf beskuldig word, of 'n elektroniese kommunikasiediensverskaffer in subartikel (1)*(b)* bedoel kan, binne 14 dae nadat die bevel ingevolge subartikel (4) aan hom of haar beteken is, of binne sodanige verdere tydperk wat die hof mag toelaat, by kennisgewing aan die betrokke landdroshof, op die voorgeskrewe vorm en wyse, by die hof aansoek doen om die tersydestelling of wysiging van die bevel in subartikel (3) bedoel. (7) *(a)* Die hof moet 'n aansoek ingevolge subartikel (6) aan die hof voorgelê, so gou as redelik moontlik oorweeg en kan vir daardie doel sodanige bykomende getuienis soos die hof gepas ag, oorweeg, met inbegrip van mondelinge getuienis of getuienis by wyse van beëdigde verklaring, wat deel van die oorkonde van die verrigtinge moet uitmaak. *(b)* Die hof kan, by die aanvoer van goeie gronde vir die wysiging of tersydestelling van die beskermingsbevel, 'n bevel te dien effekte uitreik. (8) Die hof kan, vir doeleindes van subartikels (2) en (7), op die voorgeskrewe vorm en wyse enige persoon laat dagvaar as 'n getuie by daardie verrigtinge of om enige boek, dokument of voorwerp voor te lê, indien die getuienis van daardie persoon of boek, dokument of voorwerp vir die hof noodsaaklik blyk te wees vir die regverdige beslissing van die saak.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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), apply 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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(9) Iemand in subartikel (1)*(a)* bedoel, of 'n elektroniese kommunikasiediensverskaffer in subartikel (1)*(b)* bedoel, wat versuim om aan 'n bevel in subartikel (3) bedoel of enige wysiging daarvan, te voldoen, is skuldig aan 'n misdryf. (10) Enige persoon wat ingevolge subartikel (8) gedagvaar is om verrigtinge by te woon en wat versuim om— *(a)* dit by te woon of teenwoordig te bly; *(b)* te verskyn by die plek en op die datum en die tyd waarheen die betrokke verrigtinge verdaag mag word; *(c)* teenwoordig te bly by daardie verrigtinge aldus verdaag; of *(d)* enige boek, dokument of voorwerp in die dagvaarding gespesifiseer voor te lê, is skuldig aan 'n misdryf. (11) Die bepalings ten opsigte van appèl en hersiening soos in die Wet op Landdroshowe, 1944, en die Wet op Hoër Howe, 2013, voor voorsiening gemaak, is van toepassing op verrigtinge ingevolge hierdie artikel. (12) Artikels 8 en 9(3) van die Wet op Beskerming teen Teistering, 2011 (Wet No. 17 van 2011), is van toepassing met die nodige veranderinge deur die samehang vereis op verrigtinge in subartikels (2) en (7) beoog. **Elektroniese kommunikasiediensverskaffer moet besonderhede aan hof verskaf** **11C.** (1) Indien daar ingevolge artikel 11B(1) om 'n beskermingsbevel aansoek gedoen word en die hof is ingevolge artikel 11B(3) oortuig dat 'n beskermingsbevel uitgereik moet word en die besonderhede van die persoon in artikel 11B(1)*(a)* bedoel, of die elektroniese kommunikasiediensverskaffer in artikel 11B(1)*(b)* bedoel, wie se diens gebruik is om daardie pornografie te huisves of openbaar te maak, is nie bekend nie, kan die hof— *(a)* die verrigtinge verdaag tot enige tyd en datum op die bepalings en voorwaardes wat die hof doenlik ag; en

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		(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 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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	**Kort titel**	**Omvang van herroeping of wysiging**
		(b) 'n lasgewing in die voorgeskrewe vorm uitreik, wat 'n elektroniese kommunikasiediensverskaffer, wat geglo word in staat te wees om daardie besonderhede te verskaf, gelas om die hof op die voorgeskrewe wyse deur middel van 'n beëdigde verklaring in die voorgeskrewe vorm te voorsien van— (i) die elektroniese kommunikasie-identiteitsnommer van waar daardie pornografie afkomstig was; (ii) die naam, van, identiteitsnommer en adres van die persoon aan wie die elektroniese kommunikasie-identiteitsnommer toegeken is; (iii) enige inligting wat aandui dat daardie pornografie vanaf die elektroniese kommunikasie-identiteitsnommer van die persoon na die elektroniese kommunikasie-identiteitsnommer van die applikant gestuur is al dan nie; (iv) enige inligting wat beskikbaar is aan 'n elektroniese kommunikasiediensverskaffer wat die hof behulpsaam kan wees om die persoon bedoel in artikel 11B(1)*(a)* of die elektroniese kommunikasiediensverskaffer bedoel in artikel 11B(1)*(b)*, wat 'n diens aan daardie persoon verskaf, te identifiseer; (v) enige inligting wat aan 'n elektroniese kommunikasiediensverskaffer beskikbaar is wat— *(aa)* bevestig of hul elektroniese kommunikasiediens gebruik word om daardie pornografie te huisves of gebruik was of word om daardie pornografie openbaar te maak al dan nie; of *(bb)* die hof behulpsaam kan wees om die elektroniese kommunikasiediensverskaffer te identifiseer wie se diens gebruik word om die betrokke pornografie te huisves of gebruik was of word om dit openbaar te maak; of

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		(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. (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 to disclose such pornography. (4) After receipt of an application in terms of subsection (3)(*b*), the court— *(a)* must consider the application;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(vi) 'n assessering of die elektroniese kommunikasiediensverskaffer in 'n posisie is, al dan nie, om— (*aa*) daardie pornografie of 'n skakel na daardie pornografie te verwyder; of (*bb*) toegang tot daardie pornografie of 'n skakel na daardie pornografie te deaktiveer. (2) Indien die hof 'n lasgewing ingevolge subartikel (1)*(b)* uitreik, moet die hof gelas dat die lasgewing op die voorgeskrewe wyse aan die elektroniese kommunikasiediensverskaffer beteken word: Met dien verstande, dat indien die hof oortuig is dat die lasgewing nie op die voorgeskrewe wyse beteken kan word nie, die hof 'n bevel kan gee wat betekening in die vorm of op die wyse in daardie bevel gespesifiseer, toelaat. (3) *(a)* Die inligting in subartikel (1)*(b)* bedoel, moet binne vyf gewone hofdae vanaf die dag waarop die lasgewing aan 'n elektroniese kommunikasiediensverskaffer beteken is, aan die hof verskaf word. *(b)* 'n Elektroniese kommunikasiediensverskaffer aan wie 'n lasgewing beteken is, kan op die voorgeskrewe wyse en deur middel van 'n beëdigde verklaring in die voorgeskrewe vorm by die hof aansoek doen om— (i) 'n verlenging van die tydperk van vyf gewone hofdae in paragraaf *(a)* bedoel vir 'n verdere tydperk van vyf gewone hofdae op grond daarvan dat die inligting nie tydig voorsien kan word nie; of (ii) die kansellasie van die lasgewing op grond daarvan dat— (*aa*) dit nie 'n elektroniese kommunikasiediens aan die applikant of die persoon bedoel in artikel 11B(1)*(a)* lewer nie; (*bb*) die inligting wat aangevra is, nie in die rekords van die elektroniese kommunikasiediensverskaffer beskikbaar is nie; of (*cc*) hul diens nie gebruik word om daardie pornografie te huisves nie of nie gebruik was of word om daardie pornografie openbaar te maak nie. (4) Ná ontvangs van 'n aansoek ingevolge subartikel (3)*(b)*— *(a)* moet die hof die aansoek oorweeg;

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		(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. (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—

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(b) kan die hof, op die voorgeskrewe wyse, sodanige bykomende getuienis versoek by wyse van beëdigde verklaring van die elektroniese kommunikasiediensverskaffer soos wat die hof goeddink; *(c)* moet die hof daaroor beslis; en *(d)* moet die hof die elektroniese kommunikasiediensverskaffer op die voorgeskrewe vorm en wyse van die uitslag van die aansoek verwittig. (5) *(a)* Die hof kan, by ontvangs van 'n beëdigde verklaring van 'n elektroniese kommunikasiediensverskaffer wat die inligting bedoel in subartikel (1)*(b)* bevat, die uitreiking van 'n beskermingsbevel ingevolge artikel 11B(3) teen die persoon of elektroniese kommunikasiediensverskaffer oorweeg op die datum waarheen die verrigtinge verdaag is. *(b)* Enige inligting wat ingevolge subartikel (1)*(b)* aan die hof verskaf is, maak deel uit van die getuienis wat 'n hof ingevolge artikel 11B(3) kan oorweeg. (6) Die Kabinetslid verantwoordelik vir die regspleging kan, by kennisgewing in die *Staatskoerant*, redelike tariewe voorskryf vir vergoeding betaalbaar aan elektroniese kommunikasiediensverskaffers vir die verskaffing van die inligting in subartikel (1)*(b)* bedoel. (7) Enige elektroniese kommunikasiediensverskaffer of werknemer van 'n elektroniese kommunikasiediensverskaffer wat— *(a)* versuim om die vereiste inligting binne vyf gewone hofdae vanaf die dag waarop die lasgewing aan daardie elektroniese kommunikasiediensverskaffer beteken is, aan 'n hof te verskaf ingevolge subartikel (3)*(a)* of sodanige verlengde tydperk wat ingevolge subartikel (3)*(b)* deur die hof toegelaat word; of *(b)* 'n vals verklaring in 'n wesenlike opsig in 'n beëdigde verklaring bedoel in subartikel (1)*(b)* of (3)*(b)* maak, is skuldig aan 'n misdryf. **Bevele by afhandeling van strafregtelike verrigtinge** **11D.** (1) Die verhoorhof, wat 'n persoon skuldig bevind aan enige misdryf in artikel 11A(1), (2) of (3) bedoel, moet—

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		(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. (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 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.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(a) daardie persoon beveel om die pornografie te vernietig en om 'n beëdigde verklaring in die voorgeskrewe vorm aan die aanklaer in die bevel geïdentifiseer, voor te lê, dat die pornografie aldus vernietig is; of *(b)* 'n elektroniese kommunikasiediensverskaffer wie se diens gebruik word om daardie pornografie te huisves of openbaar te maak, beveel om daardie pornografie te verwyder of toegang daartoe te deaktiveer. (2) Die bevel in subartikel (1)*(b)* bedoel, moet in die voorgeskrewe vorm wees en moet op die voorgeskrewe wyse aan die elektroniese kommunikasiediensverskaffer beteken word: Met dien verstande dat, indien die verhoorhof oortuig is dat die bevel nie op die voorgeskrewe wyse beteken kan word nie, die hof 'n bevel kan gee wat betekening in die vorm of op die wyse in daardie bevel gespesifiseer, toelaat. (3) Enige persoon of elektroniese kommunikasiediensverskaffer wat versuim om aan 'n bevel in subartikel (1) bedoel te voldoen, is skuldig aan 'n misdryf. (4) 'n Elektroniese kommunikasiediensverskaffer kan, binne 14 dae na die bevel bedoel in subartikel (1)*(b)*, ingevolge subartikel (2) daaraan beteken is, by kennisgewing aan die betrokke verhoorhof, op die voorgeskrewe vorm en wyse, by die verhoorhof aansoek doen om die tersydestelling of wysiging van die bevel. (5) *(a)* Die verhoorhof moet so gou as redelikerwys moontlik 'n aansoek ingevolge subartikel (4) daaraan voorgelê, oorweeg en kan vir daardie doel sodanige bykomende getuienis oorweeg wat die hof gepas ag, met inbegrip van mondelinge getuienis of getuienis by wyse van beëdigde verklaring, wat deel van die oorkonde moet uitmaak. *(b)* Die hof kan, by die aanvoer van goeie gronde vir die wysiging of tersydestelling van die bevel, 'n bevel te dien effekte uitreik.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		(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— (*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 2 of Chapter 3 of the following heading:

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(6) Die verhoorhof kan, by die toepassing van subartikel (5)*(a)*, enige persoon op die voorgeskrewe vorm en wyse laat dagvaar as getuie by daardie verrigtinge of om enige boek, dokument of voorwerp voor te lê, indien die getuienis van daardie persoon of boek, dokument of voorwerp vir die hof noodsaaklik blyk te wees vir die regverdige beslissing van die saak. (7) Enige persoon wat ingevolge subartikel (6) gedagvaar is om verrigtinge by te woon en wat versuim om— *(a)* dit by te woon of teenwoordig te bly; *(b)* te verskyn by die plek en op die datum waarheen die betrokke verrigtinge verdaag kan word; *(c)* teenwoordig te bly by daardie verrigtinge aldus verdaag; of *(d)* enige boek, dokument of voorwerp in die dagvaarding gespesifiseer, voor te lê, is skuldig aan 'n misdryf. (8) By die toepassing van hierdie artikels, beteken **'verhoorhof'—** *(a)* 'n landdroshof ingestel kragtens artikel 2(1)*(f)*(i) van die Wet op Landdroshowe, 1944; *(b)* 'n hof vir 'n streeksafdeling ingestel kragtens artikel 2(1)*(g)*(i) van die Wet op Landdroshowe, 1944; of *(c)* 'n Hooggeregshof bedoel in artikel 6(1) van die Wet op Hoër Howe, 2013. (9) Wanneer 'n persoon ook al aan 'n misdryf in artikel 11A(1), (2) of (3) skuldig bevind word, moet die verhoorhof 'n bevel gee dat die persoon wat aldus skuldig bevind is, alle koste moet vergoed wat redelikerwys aangegaan is deur— *(a)* 'n klaer na aanleiding van enige lasgewing ingevolge artikel 11C(1)*(b)* uitgereik; of *(b)* 'n elektroniese kommunikasiediensverskaffer om daardie pornografie te verwyder of toegang daartoe te deaktiveer, waarop die bepalings van artikel 300 van die Strafproseswet, 1977, met die nodige veranderinge deur die samehang vereis, by daardie bevel van toepassing sal wees.''. *(d)* Hoofstuk 3 word hierby gewysig— (i) deur die opskrif by Deel 2 van Hoofstuk 3 deur die volgende opskrif te vervang:

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

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, 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. (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—

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	**Kort titel**	**Omvang van herroeping of wysiging**
		"***Seksuele uitbuiting en seksuele aanvoring van kinders, blootstelling of vertoon van of veroorsaking van blootstelling of vertoon van kinderpornografie of pornografie aan kinders, misdrywe in verband met kinderpornografie en gebruikmaking van kinders vir pornografiese doeleindes of voordeeltrekking uit kinderpornografie***"; (ii) deur die volgende subartikel by artikel 17 te voeg: "(7) Enige persoon wat wederregtelik en opsetlik op enige wyse die seksuele uitbuiting van 'n kind verkondig, adverteer, aanmoedig of bevorder, is skuldig aan 'n misdryf."; (iii) deur die volgende artikel ná artikel 19 van die Wet in te voeg: "**Misdrywe in verband met kinderpornografie** **19A.** (1) Iemand wat wederregtelik en opsetlik kinderpornografie skep, maak of vervaardig, op enige wyse, anders as om 'n kind vir kinderpornografie te gebruik soos in artikel 20(1) beoog, is skuldig aan 'n misdryf. (2) Iemand wat wederregtelik en opsetlik, op enige wyse behulpsaam is met die skepping, maak of vervaardiging van kinderpornografie of dit fasiliteer, is skuldig aan 'n misdryf. (3) Iemand wat wederregtelik en opsetlik kinderpornografie besit, is skuldig aan 'n misdryf. (4) Iemand wat wederregtelik en opsetlik, op enige wyse — *(a)* kinderpornografie versprei; *(b)* kinderpornografie beskikbaar stel; *(c)* kinderpornografie oorsend; *(d)* kinderpornografie te koop aanbied; *(e)* kinderpornografie verkoop; *(f)* aanbied om kinderpornografie te verkry; *(g)* kinderpornografie verkry; *(h)* toegang kry tot kinderpornografie; *(i)* kinderpornografie aflaai; of *(j)* kinderpornografie besigtig, is skuldig aan 'n misdryf. (5) Iemand wat wederregtelik en opsetlik op enige wyse met die—

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		(a) distribution; *(b)* making available; *(c)* transmission; *(d)* offering for sale; *(e)* selling; *(f)* offering to procure; *(g)* procuring; *(h)* accessing; *(i)* downloading; or *(j)* viewing, of child pornography, is guilty of an offence. (6) Any person who unlawfully and intentionally 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. (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.''.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(a) verspreiding van kinderpornografie; *(b)* beskikbaarstelling van kinderpornografie; *(c)* oorsending van kinderpornografie; *(d)* te koop aanbieding van kinderpornografie; *(e)* verkoop van kinderpornografie; *(f)* aanbieding om kinderpornografie te verkry; *(g)* verkryging van kinderpornografie; *(h)* verkryging van toegang tot kinderpornografie; *(i)* aflaai van kinderpornografie; of *(j)* besigtiging van kinderpornografie, bystand verleen of dit fasiliteer, is skuldig aan 'n misdryf. (6) Iemand wat wederregtelik en opsetlik 'n finansiële transaksie verwerk of fasiliteer, wetende dat daardie transaksie 'n oortreding van subartikels (1) tot (5) sal fasiliteer, is skuldig aan 'n misdryf.''; en (iv) artikel 20 word gewysig, deur die volgende subartikels by te voeg: ''(3) Iemand wat wederregtelik en opsetlik 'n regstreekse uitvoering wat kinderpornografie behels— *(a)* bywoon; *(b)* besigtig; of *(c)* daaraan deelneem, is skuldig aan die misdryf van bywoning, besigtiging of deelname aan 'n vertoning wat kinderpornografie behels. (4) Iemand ('A') wat wederregtelik en opsetlik 'n klaer of klaagster wat 'n kind is ('B'), met of sonder die toestemming van B, werf, hetsy vir finansiële of ander beloning, guns of vergoeding aan B of 'n derde persoon ('C') al dan nie, ten einde— *(a)* kinderpornografie te skep, te maak of te vervaardig, is skuldig aan die misdryf van werwing van 'n kind vir kinderpornografie; of *(b)* deel te neem aan 'n regstreekse uitvoering wat kinderpornografie behels, soos in subartikel (3) beoog, is skuldig aan die misdryf van werwing van 'n kind vir deelname aan 'n regstreekse uitvoering wat kinderpornografie behels.''.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		(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: "(3) *(a)* Any person who contravenes the provisions of section 11A(1) or (2), is liable on conviction to a fine or to imprisonment for a period not exceeding five years or to both such fine and imprisonment. *(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 two years or to both such fine and imprisonment.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(e) Artikel 54 van die Wet word gewysig deur die volgende subartikels by te voeg: "(3) Iemand wat, met kennis van die pleging van enige misdryf in artikel 19A bedoel, of wat rede het om te vermoed dat so 'n misdryf gepleeg is of gepleeg word of waarskynlik gepleeg sal word en wederregtelik en opsetlik versuim om— *(a)* daardie kennis of vermoede so gou moontlik by die Suid-Afrikaanse Polisiediens aan te meld; of *(b)* op versoek van die Suid-Afrikaanse Polisiediens, alle besonderhede van daardie kennis of vermoede, te verskaf, is skuldig aan 'n misdryf. (4) 'n Elektroniese kommunikasiediensverskaffer wat bewus is of bewus word dat hul elektroniese kommunikasiediens of elektroniese kommunikasienetwerk gebruik word of betrek is by die pleging van enige misdryf in artikel 19A bedoel, moet— *(a)* die misdryf onmiddellik by die Suid-Afrikaanse Polisiediens aanmeld; *(b)* enige inligting bewaar wat die Suid-Afrikaanse Polisiediens behulpsaam kan wees in die ondersoek van die misdryf; en *(c)* alle redelike stappe neem om toegang deur enige persoon tot die kinderpornografie te voorkom.". *(f)* Artikel 56A word gewysig deur die volgende subartikels by te voeg: "(3) *(a)* Iemand wat die bepalings van artikel 11A(1) of (2) oortree, is strafbaar by skuldigbevinding met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens 5 jaar of met beide daardie boete en gevangenisstraf. *(b)* Iemand wat die bepalings van artikel 11A(3) oortree, is strafbaar by skuldigbevinding met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens 10 jaar of met beide daardie boete en gevangenisstraf. *(c)* Iemand of 'n elektroniese kommunikasiediensverskaffer wat aan 'n misdryf bedoel in subartikel 11B(9) of (10) skuldig bevind word, is strafbaar by skuldigbevinding met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens 2 jaar of met beide daardie boete en gevangenisstraf.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		(d) Any person or electronic communications service provider that is convicted of an offence referred to in section 11C(7), is liable, on conviction to a fine or to imprisonment for a period not exceeding two years or to both such fine and imprisonment. *(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 five years or to both such fine and imprisonment; *(b)* in the case of a second conviction, to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment; or *(c)* in the case of a third and 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 *(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

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(d) Iemand of 'n elektroniese kommunikasiediensverskaffer wat aan 'n misdryf bedoel in artikel 11C(7) skuldig bevind word, is strafbaar by skuldigbevinding met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens 2 jaar of met beide daardie boete en gevangenisstraf. *(e)* 'n Elektroniese kommunikasiediensverskaffer of persoon wat aan 'n misdryf bedoel in artikel 11D(3) of (7) skuldig bevind word, is strafbaar by skuldigbevinding met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens 2 jaar of met beide daardie boete en gevangenisstraf. (4) Iemand wat die bepalings van artikel 19A(3), (4)*(f)*, *(g)*, *(h)*, *(i)* of *(j)*, of (5)*(f)*, *(g)*, *(h)*, *(i)* of *(j)* oortree, is strafbaar— *(a)* in die geval van 'n eerste skuldigbevinding, met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens 5 jaar of met beide sodanige boete en gevangenisstraf; *(b)* in die geval van 'n tweede skuldigbevinding, met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens 10 jaar of met beide daardie boete en gevangenisstraf; of *(c)* in die geval van 'n derde en daaropvolgende skuldigbevinding, met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens 15 jaar of met beide daardie boete en gevangenisstraf. (5) Iemand wat die bepalings van artikel 17(7), 19A(1), (2), (4)*(a)*, *(b)*, *(c)*, *(d)* of *(e)*, (5)*(a)*, *(b)*, *(c)*, *(d)* of *(e)* of 20(3) of (4) oortree, is strafbaar— *(a)* in die geval van 'n eerste skuldigbevinding, met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens 10 jaar of met beide daardie boete en gevangenisstraf; of *(b)* in die geval van 'n tweede en daaropvolgende skuldigbevinding, met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens 15 jaar of met beide daardie boete en gevangenisstraf. (6) Iemand wat die bepalings van artikel 19A(6) oortree, is strafbaar— *(a)* in die geval van 'n eerste skuldigbevinding, met 'n boete van R1 000 000 of met gevangenisstraf vir 'n tydperk van hoogstens 5 jaar of met beide daardie boete en gevangenisstraf; of

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Number and year of law	Short title	Extent of repeal or amendment
		(b) in the case of a second or subsequent conviction, to a fine of R2 000 000 or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment. (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 *(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.''.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Nommer en jaar van wet	Kort titel	Omvang van herroeping of wysiging
		(b) in die geval van 'n tweede en daaropvolgende skuldigbevinding, met 'n boete van R2 000 000 of met gevangenisstraf vir 'n tydperk van hoogstens 10 jaar of met beide daardie boete en gevangenisstraf. (7) Iemand wat die bepalings van artikel 54(3) oortree, is strafbaar by skuldigbevinding met 'n boete of met gevangenisstraf vir 'n tydperk van hoogstens vyf jaar of met beide daardie boete en gevangenisstraf. (8) 'n Elektroniese kommunikasiediensverskaffer wat die bepalings van artikel 54(4) oortree, is strafbaar by skuldigbevinding met 'n boete van hoogstens R1 000 000 of met gevangenisstraf vir 'n tydperk van hoogstens vyf jaar of met beide daardie boete en gevangenisstraf.''.
Molao 75 wa 2008	Molao wa Bosiamisi wa Ngwana,	*(a)* Go tsenngwa ga ntlha e e latelang mo èejuleng 2: "26. Tlolomolao nngwe le nngwe e e umakilweng mo— *(a)* karolong 2, 3 kgotsa 4 ya *Cybercrimes Act*, 2020; *(b)* dikarolong 5, 6, 7 kgotsa 11(1) tsa *Cybercrimes Act*, 2020, fa tshenyegelo e e dirilweng e le kwa tlase ga bokana ka R5000; *(c)* karolo 14, 15 kgotsa 16 ya *Cybercrimes Act*, 2020; kgotsa *(d)* karolo 8, 9 kgotsa 10 ya *Cybercrimes Act*, 2020, fa tlhotlhwa e e amegang e le kwa tlase ga R1500. 27. Tlolomolao nngwe le nngwe e e umakilweng mo karolong 11A (1) le (2) ya Criminal *Law (Sexual Offences and Related Matters) Amendment Act, 2007*.''. *(b)* Go tsenngwa ga ntlha e e latelang mo èejuleng 3: "23. Tlolomolao nngwe le nngwe e e umakilweng mo— *(a)* karolong 5, 6, 7 kgotsa 11(1) ya *Cybercrimes Act*, 2020, fa tshenyegelo e e dirilweng e le kwa godimo ga bokana ka R5000; *(b)* karolo 8, 9 kgotsa 10 ya *Cybercrimes Act*, 2020, fa tlhotlhwa e e amegang e le kwa godimo ga R1500; kgotsa *(c)* karolo 11(2) ya *Cybercrimes Act*, 2020. 24. Tlolomolao e e umakilweng mo karolong 11A(3) ya *Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007*.''.

Reproduced by LexisNexis under Government Printer's Authorisation (Authorisation No. 11802) dated 13 November 2018

Printed by and obtainable from the Government Printer, Bosman Street, Private Bag X85, Pretoria, 0001
Contact Centre Tel: 012-748 6200. eMail: info.egazette@gpw.gov.za
Publications: Tel: (012) 748 6053, 748 6061, 748 6065