South African Police Service

Draft Standard Operating Procedures

for the

Investigation, Search, Access or Seizure of Electronic Evidence in terms of Section 26 of the Cybercrimes Act, No. 19 of 2020

Table of Contents

1. Introduction

1.1 The Cybercrimes Act 19 of 2020 (CCA) ("the Act") came into partial operation on 1 December 2021 and the purpose of the Act is to:

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

1.2 Section 26 of the Cybercrimes Act (CCA) 19 of 2020 states that:

"(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 twelve (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."

1.3 The CCA creates a new legal mechanism for addressing cybercrime in South Africa, as well as creating a range of new cybercrime offences. It also provides for mechanisms to preserve electronic evidence[1] in the cyber domain, to conduct search and seizure operations in respect of an *article* e.g. computers, mobile devices, hardware and the gathering of data connected to both cyber and other crimes that are committed by means of or facilitated through the use of an *article*.

1.4 The scope of application of the SOPs includes 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*. An *article* is defined in Section 1 of the CCA as:

"(1) In this Act, unless the context indicates otherwise, ''article'' means any—

(a) data;[2]

(b) computer program;[3]

(c) computer data storage medium;[4] or

[1] The terms digital and electronic evidence are often used interchangeably and bear the same meaning.

[2] The CCA defines 'data' as electronic representations of information in any form and 'data message' as data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form.

[3] The CCA defines 'computer program' as data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function.

[4] The CCA defines 'computer data storage medium' as 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.

(d) computer system,[5] [6]

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."

1.5 The SOPs will furthermore serve as a common standard for exchanging electronic evidence in local and international investigations.

1.6 The basic principle to be followed for all activities set out in the SOPs is to ensure the integrity, reliability and authenticity of the data held on an article, such as computer systems, digital devices or other storage devices.

2. Jurisdiction and International Dimension of Cybercrime

2.1 In general, jurisdiction refers to the power or competence of a court or judicial entity to hear and determine an issue between persons or to try a person for an

[5] The CCA defines 'computer system' as-
(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.

[6] The CCA defines 'computer' as 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.

offence committed by him or her. Jurisdiction requires an assessment in respect of both the physical location of the suspect (is he or she within a specific court's area of jurisdiction) and the place where an offence was committed (is the offence committed within the area of a specific court's jurisdiction).

2.2 The CCA deals with jurisdiction for offences under Chapter 2 of the Act, but also applies to offences where an article was used in the commission of an offence under other laws of the Republic.[7]

2.3 Where an offence referred to in Part I or Part II of Chapter 2 was committed outside the Republic, the State may only institute a prosecution against a person with the written permission of the NDPP and such proceedings must commence before a court designated by the NDPP.[8]

2.4 The provisions of sections 48 to 51 of the CCA deal with Mutual Assistance and apply in addition to Chapter 2 of the International Co-operation in Criminal Matters Act, 1996. Unless specified otherwise, these provisions relate to the preservation of an article or other evidence in electronic format regarding the commission or suspected commission of:

2.4.1 an offence in terms of Part I or Part II of Chapter 2;

2.4.2 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

2.5 an offence in a foreign state which is similar to those contemplated in Part I or Part II of Chapter 2, or substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article.

2.6 These provisions apply pending a request in terms of section 2 or 7 of the International Co-operation in Criminal Matters Act, 1996.[9]

[7] Section 24 of the CCA
[8] Section 24(4) of the CCA
[9] Section 48 of the CCA

3. General Guidelines for the Investigation, Search, Access or Seizure of an Article

3.1 Introduction

3.1.1 The Criminal Procedure Act, No. 51 of 1977 (CPA) applies in addition to the provisions of Chapter 4 of the CCA (in so far that it is not inconsistent with the provisions of Chapter 4).

3.1.2 Chapter 4 of the CCA contains specific definitions relating to the access[10] and seizure[11] of an article.

3.1.3 Subject to the provisions of sections 31, 32, 33 and 40(1) and (2) of the CCA, 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.

3.1.4 An individual's right to privacy, as well as other fundamental rights, must always be respected and any infringement of these rights may only be justified in terms of the law.

3.1.5 The search, access and seizure of an article invoke specific processes and procedures to ensure compliance with the CCA. Electronic evidence should always be handled with care and the aim should always be to preserve such evidence in a way that ensures the integrity, reliability and eventual admissibility of the evidence in a court of law. This applies both to the physical devices such as a computer or digital device, but also the data and computer programs contained therein.

---

[10] "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.

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

3.1.6 Although electronic evidence shares properties with traditional forms of evidence, it also possesses unique characteristics such as:

3.1.6.1 It is invisible to the untrained eye

3.1.6.2 It is often volatile

3.1.6.3 It may be altered or destroyed through normal use

3.1.6.4 It can be copied without degradation

3.1.7 Principles for digital evidence have been developed and adapted over time:

3.1.7.1 **Principle 1- Data Integrity:** No action taken by law enforcement agencies, persons employed within those agencies or their agents should materially change any data, electronic device or media which may subsequently be used as evidence in court.

3.1.7.2 **Principle 2 - Audit Trail**: A record of all actions taken when handling electronic evidence should be created and preserved so that they can be subsequently audited. An independent third party should not only be able to repeat those actions, but also to achieve the same result.

3.1.7.3 **Principle 3 - Specialist Support:** If it is expected that electronic evidence may be found in the course of a planned operation, the person in charge of the operation should notify specialists/external advisers in time and to arrange their presence if possible.

3.1.7.4 **Principle 4 - Training and Experience:** Persons permitted by the CCA to search for, access or seize electronic evidence at a crime scene, should have basic training and/or experience to be able to search for and seize electronic evidence if no specialists are available at the scene.

3.1.7.5 **Principle 5 – Legality:** The person and agency in charge of the case are responsible for ensuring that the law, the evidential safeguards and the general forensic and procedural principles are followed. Legality forms the basis for the admissibility of evidence in judicial proceedings. In terms of section 35(5) of the Constitution of the Republic of South Africa, evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice.

3.1.8 No activity involving the search, access or seizure of an article should be undertaken without obtaining the requisite level of authorisation, such as obtaining lawful consent or a search warrant.[12]

3.1.9 The powers conferred upon a police official or an investigator in terms of section 29(2), 31, 32 or 33, must always be conducted with strict regard to decency and order and with due regard to the rights, responsibilities and legitimate interests of other persons. The powers so exercised must, furthermore, always be in proportion to the severity of the offence.[13]

3.1.10 The CCA provides for the following methods for the search, access and seizure of an article:

3.1.10.1 Written application for obtaining a search warrant in terms of section 29 of the CCA.

3.1.10.2 Oral application for obtaining a search warrant or amendment to a warrant.[14]

3.1.10.3 Search for, access to, or seizure of article without search warrant with consent of person who has lawful authority to consent.[15]

3.1.10.4 Search for, access to, or seizure of article involved in the commission of an offence without search warrant.[16]

3.1.10.5 Search for, access to, or seizure of article on arrest of person.[17]

3.1.11 The interception of an indirect communication or obtaining real-time communication-related information must be done in accordance with the provisions of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002.[18] [19]

[12] The CCA also provides for searches without a warrant in sections 32 and 33 of the Act, but there are strict conditions set out in the Act to be followed in each instance.
[13] Section 36 of the CCA
[14] Section 30
[15] Section 31
[16] Section 32
[17] Section 33
[18] Section 40(1) and (2) of the CCA
[19] Section 40(3) imposes additional obligations on electronic communications service providers.

3.2 Preparation for Search (With or Without Warrant)

3.2.1 The following considerations should be taken into account when preparing for the search, access and seizure of an article:

3.2.1.1 **Prevailing circumstances**: A search with or without a warrant can be conducted based on the specific circumstances of the case, such as e.g. the time available to act. The timing of the search and seizure is essential to, for instance, arrest a person whilst committing an offence.

3.2.1.2 **Purpose of the search and seizure**: The objectives of the search, access or seizure should be determined to ensure that evidence relevant to the investigation is gathered.

3.2.1.3 **Nature of the electronic evidence**: This will inform the equipment, instruments, tools and software which are required to search for, access or seize the electronic evidence and the level of expertise which is required during the operation and include considerations such as whether there will be a seizure of equipment or capturing of live data or a combination of both.

3.2.1.4 **Location of electronic evidence**: Electronic evidence may be found at various locations, which may impact on the judicial authority required, and the manner in which the search, access and seizure operation must be conducted.

3.2.1.5 **Logistical aspects:** It is essential that the logistical aspects of the investigation be considered, *inter alia*, sufficient available human resources and equipment.

3.2.1.6 **Other forensic examinations**: In gathering electronic evidence, the person permitted to conduct the search should take into consideration whether other forensic processes need to be performed, such as the collection of fingerprints or DNA samples during the search and seizure operation and to make appropriate arrangements to secure such evidence.

3.2.1.7 **Exhibits other than an article:** The person permitted to conduct the search has to ensure that the seizure of evidence other than an article[20] is carried out in accordance with applicable legislation.[21]

3.2.1.8 **Safety**: Consider safety of all persons at the scene and make appropriate arrangements to ensure their safety.

3.2.1.9 **Securing of location:** Appropriate arrangements should be made for securing the electronic evidence from unwanted access at location of the search, access and seizure and to maintain power to electronic devices.

3.2.2 Where circumstances permit, all persons involved in the search and seizure operation should be fully briefed and individual tasks should be assigned to the team members.

3.3 Persons Permitted to Search for, Access and Seize an Article

3.3.1 A police official[22] may, in accordance with the provisions of Chapter 4 of the CCA search for, access or seize any article located within the Republic.[23]

3.3.2 The CCA provides that a police official can request the assistance of an investigator during a search in terms of the CCA. The CCA defines an investigator as any fit and proper person, who is not a member of the South African Police Service. Such a person must be:

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

[20] As defined in the CCA

[21] Examples are seizures in terms of the CPA where e.g. drugs or firearms have to be seized or the Counterfeit Goods Act, 1997 where counterfeit goods are seized or the Precious Metals Act, 2005 where precious metals have to be seized.

[22] A 'police official' means a member of the South African Police Service as defined in section 1 of the South African Police Service Act, 1995.

[23] Section 28 of CCA.

3.3.2.2 requested by a police official in terms of section 31(2)[24], 32(3)[25] or 33(4)[26] to assist the police official with the search for, access or seizure of an article. Such assistance is always rendered subject to the direction and control of a police official.

3.3.3 A police official could thus request the assistance of a digital forensic expert or other person that could assist with any part of the search and seizure operations, but has to identify such person in the search warrant, or when searching with consent obtain written permission for such person to assist with the search. An investigator may also assist a police official to conduct a search where no warrant has been obtained[27] or during the arrest of a person[28], subject to the written authorisation of such a police official.

3.3.4 Where a police official makes use of the services of an investigator:

3.3.4.1 All articles seized in terms of activities under Chapter 4 of the CCA, must be handed over to a police official; and

3.3.4.2 The investigator is subject to the same standard operating procedures and guidelines applicable to a police official.

3.3.5 Where an article is obtained or seized by a person who is not a member of the SAPS and such article is handed to a police official all prescripts of the law must be followed by such police official to safeguard and store such exhibit. Should further investigation be required in relation to such article, the police official must ensure that there is compliance with Chapter 4 of the CCA before the article is accessed. The police official must furthermore ensure that the public prosecutor is briefed on how the article came into the possession of the police and the subsequent steps followed by the police to gain access to the device.

[24] Search with lawful consent and the consent for the investigator must be in writing.
[25] Section 32(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).
[26] Section 33(4): (Search on arrest of person): 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).
[27] Section 32
[28] Section 33

3.4 Specific Tools Used in the Investigation, Search, Access and Seizure of an Article

3.4.1 Any equipment, instruments, tools and software required for the processing of an article must be used in such a way as to ensure the integrity, reliability and admissibility of evidence in a court of law.

3.5 Publicly Available Data

3.5.1 A police official does not need to be specifically authorised in terms of the CCA to obtain publicly available data[29] 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.

3.5.2 A police official can also receive and use non-publicly available data where the data is disclosed to the police official by a person who is in control of, or in possession of the data. Such disclosure must be voluntarily and on such conditions regarding confidentiality and limitation of use which they deem necessary. It does not matter where the data is geographically located.[30]

3.6 Search, Access or Seizure of an Article with Consent

3.6.1 The CCA provides for the search, access or seizure of the equipment or data to be captured with the consent of a person who has the lawful authority to consent thereto. Such consent must be obtained in writing. When searching with lawful consent a police official can execute the same powers as set out in section 29(2) of the CCA. Should the police official require assistance from

[29] In terms of the CCA 'publicly available data' means data which is accessible in the public domain without restriction.

[30] Section 45(2)

an investigator, the person giving consent must also provide written consent for the investigator to assist with the search, seizure and access.[31]

3.7 Search with a Warrant

3.7.1 In terms of section 29 of the CCA, a police official can apply in writing for a search warrant relating to an article(s).

3.7.2 Section 30 of the CCA also makes provision for an oral application for a search warrant or amendment to an existing warrant. Such oral application is done with the assistance of a specifically designated police official[32], who will bring the application to the court on behalf of the police official that would normally have approached the court with a written application. The police official concerned must submit a written application to the magistrate or judge of the High court concerned within forty eight (48) hours after the issuing of the warrant or amended warrant under subsection 30(3).

3.7.3 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) must use it 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.[33]

3.7.4 If there is any change in the scope of the investigation or changes to the scope of a specific search warrant, a police official should bring a new application for a search warrant, or amendment to an already issued search warrant.

---

[31] Section 31 of the CCA. See also section 22(a) of the Criminal Procedure Act, No. 51 of 1977

[32] A specifically designated police official is defined in the CCA as a police official of the rank of captain or above referred to in section 33 of the SAPS Act, 1995, who has been designated in writing by the National Commissioner and the National Head of the Directorate, respectively, to make oral applications for a search warrant or an amendment of a warrant contemplated in section 30, issue expedited preservation of data directions contemplated in section 41; or serve or execute an order of the designated judge as contemplated in section 48(10).

[33] Section 37(2)(a)

3.8 Search for, Access, or Seizure of an Article Involved in the Commission of an Offence without a Search Warrant

3.8.1 Section 32 of the CCA provides for instances of a search without a warrant in terms of section 29(1)(a).[34] The police official can search any person, container, premises, vehicle, facility, ship or aircraft for a computer data storage medium or any part of a computer system, if they on reasonable grounds believe:

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

3.8.1.2 that the delay in obtaining such warrant would defeat the object of the search and seizure.

3.8.2 The police official and the investigator if one is used and authorised thereto in writing, can as a rule only perform limited activities without a search warrant:

3.8.2.1 It excludes access[35] (save for exclusions set out in paragraph 3.8.4 *infra*);

3.8.2.2 Can only perform the actions provided for in subsection (a) and (b) of the definition of seize;[36] and

3.8.2.3 Only in relation to a computer data storage medium or any part of a computer system.[37]

3.8.3 A police official may only access or perform the powers referred to in paragraphs (c) or (d) of the definition of *seize*, in respect of the computer data storage medium or a computer system referred to in subsection 32(1), in accordance with a search warrant issued in terms of section 29(1)(a).

3.8.4 Depending on the facts and nature of the case, a police official may only *access* and perform the powers referred to in paragraph (c) or (d) of the definition of seize in respect of the computer data storage medium or a computer system without a search warrant if they on reasonable grounds believe:

[34] See also section 22 (b) of the Criminal Procedure Act in this regard.
[35] See the definition of 'access' in the CCA
[36] See the definition of “seize” in the CCA
[37] Part (c) and (d) of the definition of *article.* Part (a) data and (b) computer programs are excluded.

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

3.8.4.2 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.

3.8.5 An investigator authorised in writing by a police official may assist the police official to seize an article as contemplated subsections 32(1) and 32(2) and to access the article as contemplated in subsection 32(2).

3.9 Search, Access, or Seizure of an Article on Arrest of a Person

3.9.1 A police official may without a warrant, as contemplated in section 40 of the CPA, arrest any person and section 33 of the CCA sets out the conditions for search, access and seizure of an article when a person is arrested.

3.9.2 On the arrest of a person contemplated in subsection 33(1) or in terms of section 40 or 43 of the CPA, a police official may search for and perform limited actions:

3.9.2.1 It excludes access[38] (save for circumstances a set out in paragraph 3.9.3 *infra*);

3.9.2.2 Can only perform the actions provided for in subsection (a) and (b) of the definition of seize;[39]

3.9.2.3 Only in relation to a computer data storage medium or any part of a computer system[40]; and

3.9.2.4 Which is found in the possession of or in the custody or under the control of the person.

3.9.3 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

[38] See the definition of “access” in the CCA
[39] See the definition of “seize” in the CCA
[40] Part (c) and (d) of the definition of article in the CCA. Part (a) data and (b) computer programs are excluded.

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).

3.9.4 If a police official may *access* and perform the powers referred to in paragraph (c) and (d) of the definition of seize without a search warrant if he/she on reasonable grounds believes:

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

3.9.4.2 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.

3.9.5 An investigator authorised in writing by a police official may assist the police official to seize an article as contemplated subsections 33(2) and 33(3) and to access the article as contemplated in subsection 33(3).

3.10 Preservation and Disclosure Provisions [Not in operation yet]

3.10.1 The CCA contains new procedures for the preservation and disclosure of data and electronic evidence. Preservation allows for a process where an article will be preserved i.e. the article is kept subject to circumstances that will ensure that the integrity of the evidence is maintained. In these circumstances the article is not handed over to a police official yet: the article will only be handed over subject to a search warrant in terms of section 29 of the CCA, or subject to a disclosure of evidence direction.

3.10.2 In terms of section 41 a specifically designated police official may, subject to certain conditions as set out in sections 41(1) and (2),[41] issue an expedited

[41] Section 41(1)(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.

preservation of data direction to a person, electronic communications service provider[42] or financial institution.[43]

3.10.3 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. The CCA also prescribes how the data must be preserved to maintain its integrity and availability and that such preservation is for a period of twenty one (21) days.[44]

3.10.4 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 of the CCA.[45]

3.10.5 The CCA also provides for a police official to make a written or oral application for a preservation of evidence direction to a magistrate or a judge of the high court.[46] The process is once again aimed at preserving the availability and integrity of the article in question.

3.10.6 Section 44 of the CCA sets out the procedure and prescripts under which 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)), apply to a magistrate or judge of the high court for the issuing of a disclosure of data direction to obtain:

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

---

[42] The CCA defines an "electronic communications service provider" as :
(1) 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
(2) 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.

[43] In terms of the CCA a financial institution as defined in section 1 of the Financial Sector Regulation Act, No 9 of 2017.

[44] The period of preservation can be extended subject to the provisions of section 41(6)

[45] See the provisions of section 41(7) and (8) for the process to object against an expedited preservation of data direction.

[46] Section 42 and 43 of the CCA

3.10.6.2 data as contemplated in paragraph (a) of the definition of article, which is held in a computer system or computer storage medium, or available to a computer system.

3.10.6.3 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).

3.10.6.4 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.[47]

4. Packaging, Transportation and Storage of Articles

4.1 Securing an Article

4.1.1 Computers and related devices are fragile electronic instruments that are sensitive to temperature, humidity, physical shock, static electricity, magnetic sources, and even to some operational functions (e.g. switching on/off). Special precautions should therefore be taken when packaging, transporting and storing devices that can contain electronic evidence. To maintain the chain of custody the packaging, transportation, and storage should be recorded and any change of custody or condition of the seized property should be timed and recorded.

4.1.2 If the computer data storage medium or any part of the computer system is damaged, this should be documented and recorded e.g. a cracked display monitor.

4.1.3 Note the location and circumstances where articles were found on the scene e.g. was the article concealed, found with all the other articles.

[47] Section 44(9) of the CCA

4.1.4 Inexpert handling can cause damage or destruction of electronic evidence, which can influence the eventual integrity, reliability and admissibility of such evidence in a court of law. Police officials and investigators have to ensure that they take the necessary precautions to ensure that articles are securely packaged, transported and stored.

4.2 Packaging

4.2.1 Ensure that all collected electronic evidence is properly documented and labelled before packaging.

4.2.2 Whenever possible, transport the collected electronic evidence in the original packaging.

4.2.3 If no original packaging is available, use appropriate packaging to secure and maintain the integrity of the article.

4.2.4 Do not fold, bend, or scratch storage media such as diskettes, CD-ROMs, and tapes.

4.2.5 Do not affix adhesive labels on the surface of the computer data storage medium or any part of a computer system. Use boxes or envelopes for packaging storage media whenever possible.

4.2.6 Ensure that all containers containing evidence are properly labelled.

4.2.7 If multiple computer systems are collected, label each system so that it can be reassembled as found.

4.2.8 Leave cellular, mobile, or smart phone(s) in the power state (on or off) in which they were found.

4.3 Transportation

4.3.1 Keep electronic evidence away from magnetic sources and protect the equipment from potential damage resulting from e.g. excessive shocks, bumps, heat and humidity.

4.3.2 Do not put heavy objects on top of smaller pieces of equipment/storage media.

4.3.3 Where practically possible, refrain from storing electronic evidence in vehicles for extended periods of time.

4.3.4 Document the transportation of the article from the scene to the storage facility and maintain the chain of custody for all evidence transported.

4.4 Storage

4.4.1 Articles must be booked into the SAPS13 register and the police official must ensure that the article is inventoried in accordance with the relevant SAPS National Instructions.[48]

4.4.2 Articles must be stored in a secure area, away from extreme temperatures and humidity and protected from magnetic sources, moisture, dust and other harmful particles or contaminants.

4.4.3 The storeroom must be secure and provide for the storage of articles in a way that maintains the integrity of the article.

5. Investigation of an Article that was Seized and Booked into Evidence

5.1 When investigating an article, the reason and extent of any actions must be done within the ambit of the underlying search warrant in terms of section 29 of the CCA or in terms of a disclosure of evidence direction in terms of section 44.

5.2 To preserve the chain of custody relating to a seized article, it must be booked out and handed to the person/s who will be required to perform the requisite digital forensic process(es).

5.3 Should evidence be found when investigating the article, and such evidence reveals criminality outside of the scope of the original investigation, the police official needs to obtain a new or amended search warrant in terms of section 29.

[48] See section 30(c) of the CPA. All articles/evidence seized under the provisions of the CCA must be given a distinctive identification mark and retained in police custody, or the police official must make such other arrangements with regard to the custody thereof as the circumstances may require.

5.4 Once the process of extraction and forensic analysis has been completed, the article must be resealed and re-packaged. The article is then handed back to the relevant police official who needs to book it back into the SAPS13 register for safekeeping. The chain of custody must always be maintained so as to insure the integrity, reliability and admissibility of the evidence in a court of law.

5.5 The provisions of the CPA apply to the subsequent handling of the article for availability in court proceedings, as well as the disposal of such articles.

6. Pornographic Images of Children and other Sensitive Evidence

6.1 A person performing an investigation must always be cognisant of any legal prescripts that could play a role during the extraction process.

6.2 Where electronic evidence is recovered which contains pornographic images[49] of children or other sensitive evidence, special care must be taken to restrict access to such evidence in order to prevent secondary victimisation of the victims and/or other persons. Viewing of such evidence should be restricted to persons who, in accordance with their official duties and responsibilities or in terms of an order of court, have to deal with the evidence in question.

[49] The Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007 defines "child pornography" as any image, however created, or any description or presentation of a person, real or simulated, who is, or who is depicted or described or presented as being, under the age of 18 years, of an explicit or sexual nature, whether such image or description or presentation is intended to stimulate erotic or aesthetic feelings or not, including any such image or description of such person:
(a) engaged in an act that constitutes a sexual offence;
(b) engaged in an act of sexual penetration;
(c) engaged in an act of sexual violation;
(d) engaged in an act of self-masturbation;
(e) displaying the genital organs of such person in a state of arousal or stimulation;
(f) unduly displaying the genital organs or anus of such person;
(g) displaying any form of stimulation of a sexual nature of such person's breasts;
(h) engaged in sexually suggestive or lewd acts;
(i) engaged in or as the subject of sadistic or masochistic acts of a sexual nature;
(j) engaged in any conduct or activity characteristically associated with sexual intercourse;
(k) showing or describing such person-
(i) participating in, or assisting or facilitating another person to participate in; or
(ii) being in the presence of another person who commits or in any other manner being involved in, any act contemplated in paragraphs (a) to (j); or
(l) showing or describing the body, or parts of the body, of such person in a manner or in circumstances which, within the context, violate or offend the sexual integrity or dignity of that person or any category of persons under 18 or is capable of being used for the purposes of violating or offending the sexual integrity or dignity of that person, any person or group or categories of persons.

6.3 A digital forensic examiner dealing with pornographic images of children and other sensitive evidence must ensure that:

6.3.1 access to evidence is strictly controlled and managed;

6.3.2 all evidence are exported as required and encrypted before it leaves the digital forensic laboratory;

6.3.3 items are sealed in an appropriate container, clearly marked that unauthorised access to the evidence is prohibited; and

6.3.4 the evidence is encrypted.

7. Data Held by Third Parties and Independent Data Holders

7.1 It may not always be possible to access a device physically or remotely. Data stored in large complex devices (such as those of large Internet Service Providers) may be all, but impossible to access without the cooperation and assistance of the relevant electronic communications service provider.

7.2 An alternative is to seek the cooperation of a third party (such as the hosting provider), who may be able to supply log files and service registration data.

7.3 Third parties may also collect electronic evidence on a provisional basis indicating that a cybercrime took place and prompting law enforcement to initiate an investigation.

7.4 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:

7.4.1 without undue delay and, where feasible, not later than seventy two (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

7.4.2 preserve any information which may be of assistance to the South African Police Service in investigating the offence.[50]

8. Evidence

8.1 Once the digital forensic analysis of an article has been completed, there must be a report[51] which should contain a description of the operations conducted, the tools used and the results obtained.

8.2 Section 53 of the CCA provides for instances where an affidavit or a solemn or attested declaration by a person can upon its mere production at such proceedings, *prima facie* proof of such fact.[52] It relates to any fact established by any examination or process requiring any skill in:

8.2.1 the interpretation of data;

8.2.2 the design or functioning of data, a computer program, a computer data storage medium or a computer system;

8.2.3 computer science;

8.2.4 electronic communications networks and technology;

8.2.5 software engineering; or

8.2.6 computer programming.

8.3 The facts should be 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.

8.4 Section 53 provides guidelines on the content of the affidavit or solemn attestation.[53]

8.5 The court may, in certain circumstances require oral evidence to be given.[54] [55]

---

[50] Section 54 of the CCA

[51] As provided for in section 53 of the CCA

[52] See section 53(1) for the relevant fields of study

[53] Section 53(1)(i)

[54] Section 54(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.

[55] Section 53(5)(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.

9. Prohibition on the Disclosure of Information

9.1 In terms of section 39 of the CCA, no person, investigator, police official, electronic communications service provider, financial institution or an employee of an electronic communications service provider or financial institution may 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 the CCA.

9.2 Section 39 does, however, contain exclusions[56] and also provides that the prohibition on disclosure of information contemplated in subsection (1) does not apply where the disclosure is authorised in terms of the CCA or any other Act of Parliament, or if it reveals a criminal activity.[57] Exceptions include:

9.2.1 For the performance of functions in terms of the CCA;

9.2.2 If a person of necessity supplies such information in the performance of their duties or functions in terms of this Act;

9.2.3 If it is information which is required in terms of any law or as evidence in any court of law;

9.2.4 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

9.2.5 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.

9.3 Sharing of information must always be duly authorised and be done subject to such conditions regarding confidentiality and limitation.[58]

---

[56] Subsection 39(2) of the CCA

[57] It is a criminal offence to unlawfully and intentionally contravene the provisions of section 39 and the sentence on conviction is a fine or imprisonment for a period not exceeding three years or to both a fine and such imprisonment.

[58] See also the provisions of section 47 of the CCA

10. Disposal of an Article

10.1 The provisions of section 30 to 36 of the CPA provide for the disposal of an article.

10.2 A police official or an investigator who obtains or uses any instrument, device, equipment, password, decryption key, data or other information contemplated in section 29(2)(h) of the CCA must only use it 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.[59] In addition, section 37(2)(a)(ii) of the CCA provides that a police official or investigator must destroy all passwords, decryption keys, data or other information if:

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

10.2.2 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

10.2.3 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.

11. Offences Relating to the Investigation, Search, Access or Seizure of an Article

11.1 It is an offence to unlawfully and intentionally obstruct or hinder a police official or an investigator in the exercise of their powers or the performance of their duties or functions in terms of Chapter 4, or to refuse or fail to comply with a

[59] Section 37(2)(a)(i) of the CCA

search warrant issued in terms of section 29(1).[60] A police official who may lawfully execute any power conferred upon them in terms of a search warrant under section 29(2), may use reasonably necessary force, which is proportional to all the circumstances, to exercise powers to execute the warrant.

11.2 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.[61] Where a police official is on reasonable grounds of the opinion that that an article which is the subject of the search may be destroyed, disposed of or tampered with, he/she would not have to audibly demand admission.

11.3 It is an offence for a police official or an investigator to unlawfully and intentionally act contrary to the authority of:

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

11.3.2 consent granted in terms of section 31(1).[62]

11.4 It is also an offence if a police official or investigator, without being authorised thereto under Chapter 4, or the provision of any other law which affords similar powers:

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

11.4.2 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.[63]

11.5 In terms of section 37(2)(b)(ii) it is a criminal offence if a police official or investigator fails to destroy all passwords, decryption keys, data or other information as contemplated in section 37(a)(ii).

11.6 In terms of section 38(1) of the CCA, it is an offence for a person to unlawfully or intentionally give false information under oath or by way of affirmation knowing it to be false or not knowing it to be true, and where such actions result in:

11.6.1 a search warrant being issued;

[60] Section 35 of the CCA
[61] Section 35(b) of the CCA
[62] Section 37(1)(a) of the CCA
[63] Section 37(1)(b) of the CCA

11.6.2 a search with consent taking pace on the basis of such information;

11.6.3 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;

11.6.4 an expedited preservation of data direction contemplated in section 41 being issued;

11.6.5 a preservation of evidence direction contemplated in section 42 being issued; or

11.6.6 a disclosure of data direction contemplated in section 44 being issued.

11.7 Any person who makes an affidavit or a solemn or attested declaration under subsection 53 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 (2) years or to both a fine and such imprisonment.[64]

12. The SAPS Designated Point of Contact [Not in operation yet]

12.1 The CCA provides for the creation of a Designated Point of Contact (DPoC) within SAPS structures.[65] The DPoC must ensure the provision of immediate assistance for the purpose of any proceedings or investigations regarding the commission or intended commission of:

12.1.1 an offence under Part I or Part II of Chapter 2 of the CCA;

12.1.2 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

12.1.3 an offence committed in a foreign state which is similar to the offences in Part 1 or Part II of Chapter 2 of the CCA, or which are substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article.

12.2 The assistance to be provided includes the following:

[64] Section 53(3) of the CCA
[65] Section 52 of the CCA

12.2.1 Provision of technical advice and assistance;

12.2.2 Facilitation or provision of assistance regarding anything which is authorised under Chapters 4 and 5 of the CCA;

12.2.3 Provision of legal assistance;

12.2.4 Identification and location of an article;

12.2.5 Identification and location of a suspect; and

12.2.6 Cooperation with appropriate authorities of a foreign State.

12.3 The National Director of Public Prosecutions must make members available to provide legal assistance to the DPoC as may be necessary or expedient for the effective operation of the DPoC.

12.4 The contact details of the DPoC are:

12.4.1 **[SAPS to provide the information]**

13. Glossary of Terms

Abbreviation/Term	Explanation
Availability	Property of being accessible and usable on demand by an authorised entity. The attribute of data that ensures it is always available to appropriate parties when required for use.
Browser (ECT Act)	A computer program which allows a person to read hyperlinked data messages.
Capturing Data	To copy data from a computer system or electronic media and store them on an external storage media before verifying the integrity of the data where possible (e.g. not possible for capturing RAM). Capturing data can also be possible for network data. In this context on machine in the network is used to capture the network packets and store their information to a file (e.g. in PCAP format).
Computer Forensics	Also known as Digital Forensics. In its strictest connotation, the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony.
Critical Data (ECT Act)	Data that is declared by the Minister in terms of section 53 to be of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens.
Critical Database (ECT Act)	A collection of critical data in electronic form from where it may be accessed, reproduced or extracted.
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
Cyber-Dependent Crime	Cyber-dependent crimes (or 'pure' cybercrimes) are offences that can only be committed using a computer, computer networks or other form of information communications technology (ICT). Cyber-dependent crime is often typified as the creation, dissemination and deployment of malware, ransomware, attacks on critical national infrastructure (e.g. the cyber-takeover of a power-plant by an organised crime group) and taking a website offline by overloading it with data (a DDOS attack).
Cyber-Enabled Crime	Cyber-enabled crimes are traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT). It is crimes that can occur in the offline world, but can also be facilitated by ICT. This

Abbreviation/Term	Explanation
	typically includes cyber frauds, cyber forgery and uttering and cyber extortion.
Cyber Event	Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.
Cyber Extortion (Cybercrimes Act)	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) of the Cyber-crimes Act, 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.
Cyber Fraud (Cybercrimes Act)	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 (Cybercrimes Act)	(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.
Cyber Incident	A cyber event that: (1) jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or (2) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.
Cyber Uttering (Cybercrimes Act)	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.
Damage to Property (Cybercrimes Act)	Damage to any corporeal or incorporeal property.

Abbreviation/Term	Explanation
Data Subject (POPIA)	The person to whom personal information relates.
Deleted Data	Files and folders that existed previously on the computer as active data but since have been deleted by the operating system or the end-user. Deleted data will remain in the storage unit until they are overwritten by another file.
Desktops	The term has been adopted as an adjective to distinguish office appliances (such as photocopiers and printers) which can be fitted on top of a desk, from larger equipment covering its own area on the floor. Desktop may also refer to Desktop computer, a personal computer designed to fit on a desk
Digital Forensics	A branch of forensic science related to the acquisition, processing, analysis and reporting of evidence that is stored on computer systems, digital devices and other storage media with the aim of admissibility in court.
Electronic /digital Evidence	Digital or electronic evidence is information generated, stored or transmitted using electronic devices that may be relied upon in court. To guarantee that the evidence is accepted in court, it is necessary to obtain the information following very well defined processes using specialised personnel and operating within an adequate legal framework.
Electronic Communications Service (Cybercrimes Act)	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.
Email	Electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication (ECT Act)
Faraday Isolation Bag	A dimensionless unit of electric charge quantity, equal to approximately 6.02 x 10 electric charge carriers. This is equivalent to one mole, also known as Avogadro´s constant. Faraday isolation bags are used to prevent mobile phones and devices from connecting to communication signals
Infrastructure (Critical Infrastructure Protection Act)	Any building, centre, establishment, facility, installation, pipeline, premises or systems needed for the functioning of society, the Government or enter-prises of the Republic, and includes any transport network or network for the delivery of electricity or water.
Internet Access	Means by which individual terminals, computers, mobile devices, and local area networks are connected to the global Internet. Internet access is usually sold by Internet Service

Abbreviation/Term	Explanation
	Providers (ISPs) that use many different technologies offering a wide range of data rates to the end user.
Internet Service Provider (ISP)	An organisation that provides access to the Internet. Internet service providers can be either community-owned and non-profit, or privately owned and for-profit.
Internet	Global network of data based on TCP/IP protocol that are utilised to interconnect computers and, as such, the transport of diverse services, the most popular being e-mail, web and FTP services.
Interception of Data (CCA)	The acquisition, viewing, capturing or copying of data of a non-public nature through the use of a hardware or software tool 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.
Interference with Data (CCA)	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.
Interreference with a Computer Data Storage Medium (CCA)	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.
Live Data Forensics	One part of computer forensics which is a branch of digital forensic science pertaining to legal evidence found in computers. Computer forensics deals with the examination of computer systems in a forensically sound manner with the aim of identifying, preserving, recovering, analysing and presenting facts that might become evidence in a trial. Live

Abbreviation/Term	Explanation
	data forensics follow this aim but is only focused on computer systems that are powered on. The main purpose is to acquire volatile data that would otherwise get lost if the computer system is turned off or would be overwritten if the computer system will stay turned on for a longer period.
Output of Data (CCA)	Having data displayed or in any other manner.
Output of a Computer Program (CCA)	Any: (a) data or output of the data; (b) computer program; or (c) instructions, generated by a computer program.
Password, Access Code or Similar Data or Device (CCA)	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.
Person (CCA)	A natural or a juristic person
Publicly Available Data (CCA)	Data which is accessible in the public domain without restriction.
Restricted Computer System (CCA)	Any data, computer program, computer data storage medium or computer system that is under the control of, or exclusively used by a financial institution or an organ of state as set out in section 239 of the Constitution (including a court) and which is protected by security measures against unauthorised access or use.
Software	Computer programs designed to perform specific tasks, such as word processing, accounting, network management, Website development, file management, or inventory management.
Storage Devices	A device for recording (storing) information (data). Recording can be done using virtually any form of energy, spanning from manual muscle power in handwriting, to acoustic vibrations in phonographic recording, to electromagnetic energy modulating magnetic tape and optical discs.
Traffic data (CCA)	Data relating to a communication indicating the communication's origin, destination, route, format, time, date, size, duration or type, of the underlying service.

Abbreviation/Term	Explanation
Unlawful Access (CCA)	Unlawful and intentional accessing a computer system or a computer data storage medium, which on its own is an offence. Or where such a person by gaining unlawful access enables himself/herself or another person to commit further cyber offences. **Access computer data storage medium:** Uses the data or a computer program stored on a computer data storage medium or stores data or a computer program **Access a computer system:** • Uses data or computer program • Stores data or a computer program on a computer data storage medium which forms part of a computer system • Instructs, communicates with or uses the computer system **Uses a computer program:** • Copies or moves the computer program to a different location • Causes a computer program to perform any function • Obtains the output of a computer program **Uses Data:** • Copies or moves the data to a different location • Obtains the output of the data.
Unlawful Interception of Data (CCA)	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. 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. 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. “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

Abbreviation/Term	Explanation
	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 Interference with Data or Computer Program (CCA)	Unlawfully and intentionally interfering with data or a computer program. ‘‘Interfere with data or a computer program’’ means to permanently or temporarily: (1) delete data or a computer program; (2) alter data or a computer program; (3) render vulnerable, damage or deteriorate data or a computer program; (4) render data or a computer program meaningless, useless or ineffective; (5) obstruct, interrupt or interfere with the lawful use of, data or a computer program; or (6) deny access to data or a computer program, held in a computer data storage medium or a computer system.
Unlawful Interference with a Computer Data Storage Medium or Computer System (CCA)	Any person who unlawfully and intentionally interferes with a computer data storage medium or a computer system, is guilty of an offence. 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 Possession of Data (CCA)	Unlawfully and intentionally possessing data or the output of data, with the knowledge that such data was intercepted unlawfully

Abbreviation/Term	Explanation
Unlawful Acts in Respect of Software or Hardware Tool (CCA)	Unlawful and intentional use or possession of any software or hardware tool for purposes of illegally accessing data, intercepting data, interfering with data or computer programme, interfering with data storage medium or computer system or acquiring, making available or use of a password, access code or similar data or device. "Software or hardware tool'' means any electronic, mechanical or other instrument, device, equipment, apparatus or a substantial component thereof or a computer program, which is designed or adapted primarily for the purpose to: (a) access as contemplated in section 2(1) or (2); (b) intercept data as contemplated in section 3(1); (c) interfere with data or a computer program as contemplated in section 5(1); (d) interfere with a computer data storage medium or a computer system as contemplated in section 6(1); or (e) acquire, make available or use a password, access code or similar data or device as defined in section 7(3).

Annexure A: Relevant Definitions in the Criminal Procedure Act and Cybercrimes Act

The Criminal Procedure Act, No 51 of 1977	The Cybercrimes Act, No 19 of 2020
19 Saving as to certain powers conferred by other laws The provisions of this Chapter shall not derogate from any power conferred by any other law to enter any premises or to search any person, container or premises or to seize any matter, to declare any matter forfeited or to dispose of any matter.	**27 Application of Criminal Procedure Act, 1977** The Criminal Procedure Act, 1977, applies in addition to the provisions of this Chapter in so far that it is not inconsistent with the provisions of this Chapter.
20 State may seize certain articles The State may, in accordance with the provisions of this Chapter, seize anything (in this Chapter referred to as an article)- (a) which is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within the Republic or elsewhere; (b) which may afford evidence of the commission or suspected commission of an offence, whether within the Republic or elsewhere; or	**28 Search for, access to, or seizure of certain articles** A police official may, in accordance with the provisions of this Chapter, search for, access or seize any article, within the Republic. Section 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-

(c) which is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence.	(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;
There is no definition of seize in the CPA	"**Seize**" includes to— (a) remove a computer data storage medium or any part of a computer system; (b) render inaccessible, data, a computer program, a computer data storage medium or any part of a computer system in order to preserve evidence; (c) make and retain a copy of data or a computer program; or (d) make and

	retain a printout of the output of data or a computer program.
Access is not defined in the CPA	For purposes of Chapter 4: "**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 1. (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;
There is no provision in the CPA for investigators	"**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;