



# **South African Police Service**

**Draft Standard Operating Procedures**

**for the**

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

# Table of Contents

1. Purpose .....	4
2. Scope and Application .....	8
3. Jurisdiction and International Dimension of Cybercrime .....	9
4. General Guidelines for the Investigation, Search, Access or Seizure of an Article.....	10
4.1 Introduction .....	10
4.2 Preparation for Search, Access or Seizure of an Article (With or Without Warrant).....	13
4.3 Persons Permitted to Search for, Access or Seize an Article .....	15
4.4 Specific Tools Used in the Investigation, Search, Access or Seizure of an Article.....	16
4.5 Publicly Available Data .....	16
4.6 Search, Access or Seizure of an Article with Consent .....	17
4.7 Search with a Warrant .....	17
4.8 Search for, Access, or Seizure of an Article Involved in the Commission of an Offence without a Search Warrant.....	18
4.9 Search, Access or Seizure of an Article on Arrest of a Person .....	20
4.10 Preservation and Disclosure Provisions.....	21
5. Packaging, Transportation and Storage of Articles .....	23
5.1 Securing an Article.....	23
5.2 Packaging .....	24
5.3 Transportation.....	24
5.4 Storage .....	25
6. Investigation of an Article that was Seized and Booked into Evidence .....	25

7.	Pornographic Images of Children and other Sensitive Evidence .....	26
8.	Data Held by Third Parties and Independent Data Holders .....	27
9.	Evidence .....	28
10.	Prohibition on the Disclosure of Information .....	29
11.	Disposal of an Article .....	30
12.	Offences in the CCA that relate to the Investigation, Search, Access or Seizure of an Article.....	32
13.	The SAPS Designated Point of Contact.....	36
14.	Glossary of Terms .....	37
	Annexure A: Relevant Definitions in the Criminal Procedure Act and Cybercrimes Act.....	45

# 1. Purpose

1.1 The Cybercrimes Act, No 19 of 2020 (CCA) (“the Act”) came into partial operation on 1 December 2021 and the purpose of the Act is to:

- provide for 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 The CCA thus provides 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<sup>1</sup> in the cyber domain, to conduct search, access and seizure operations in respect of an article as defined in the CCA 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.

---

<sup>1</sup> The terms digital and electronic evidence are often used interchangeably and bear the same meaning.

### 1.3 Definition of Article

1.3.1 The definition of article in the CCA relates to any of the following:

1.3.1.1 Data;<sup>2</sup>

1.3.1.2 Computer program;<sup>3</sup>

1.3.1.3 Computer data storage medium;<sup>4</sup> or

1.3.1.4 Computer system (one or more computers).<sup>5 6</sup>

1.3.2 Any of the four (4) types of articles will be relevant when it:

1.3.2.1 is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission of an offence;

1.3.2.2 may afford evidence of the commission or suspected commission of an offence; or

1.3.2.3 is intended to be used or is, on reasonable grounds believed to be intended to be used in the commission or intended commission of an offence.

1.3.3 The offences that are relevant to the definition are:

1.3.3.1 any offences in terms of Part I and Part II of Chapter 2 of the CCA;

1.3.3.2 any other offence in terms of the law of the Republic; or

---

<sup>2</sup> 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.

<sup>3</sup> 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.

<sup>4</sup> 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.

<sup>5</sup> 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.

<sup>6</sup> 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.

- 1.3.3.3 an offence in a foreign State that is substantially similar to an offence contemplated in Part I or Part II of Chapter 2 of the CCA or another offence recognised in the Republic.
- 1.3.4 Unless otherwise indicated, any reference to an article in the SOPs will bear the meaning of article as defined in the CCA.
- 1.4 Members of the SAPS, other law enforcement officials, prosecutors and members of the judiciary may become involved in the collection, analysis or decisions related to articles at some stage of a criminal investigation or court proceedings.
- 1.5 The basic principle to be followed for all digital forensic activities is to ensure the integrity, reliability, authenticity and eventual admissibility of evidence in a court of law, of processes and procedures relating to the data and computer programs held on computer systems and computer data storage mediums.
- 1.6 Since the ultimate goal is to use evidence to prove or disprove disputed facts, articles must be obtained and handled in compliance with existing South African legislation and best practice to ensure that the integrity of the evidence is maintained, that it is reliable and would be admissible in a court of law.
- 1.7 Amongst other provisions, Section 15 of the Electronic Communications and Transactions Act, No 25 of 2002 (ECT Act) states that information in the form of a data message<sup>7</sup> must be given due evidential weight. In assessing the evidential weight of a data message, the following factors must be considered:
- 1.7.1 the reliability of the manner in which the data message was generated, stored or communicated;
- 1.7.2 the reliability of the manner in which the integrity of the data message was maintained;
- 1.7.3 the manner in which its originator was identified; and
- 1.7.4 any other relevant factor.
- 1.8 Additional factors to consider when dealing with the admissibility of electronic evidence are:

---

<sup>7</sup> 'data' means electronic representations of information in any form and 'data message' means data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form

- 1.8.1 **Authenticity:** The evidence must establish facts in a way that cannot be disputed and is representative of its original state.
  - 1.8.2 **Completeness:** The analysis of or any opinion based on the evidence must tell the whole story and not be tailored to match a more favourable or desired perspective.
  - 1.8.3 **Reliability:** There must be nothing about the way in which the evidence was collected and subsequently handled that may cast doubt on its authenticity or veracity.
  - 1.8.4 **Evidentiary Weight:** The evidence must be persuasive as to the facts it represents and the finders of fact in the court process must be able to rely on it as the truth.
  - 1.8.5 **Proportionality:** The methods used to gather the evidence must be fair and proportionate to the interests of justice: the prejudice (i.e. the level of intrusion or coercion) caused to the rights of any party should not outweigh the “probative value” of the evidence (i.e. its value as proof).
- 1.9 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.
  - 1.10 The right to a fair trial is paramount, and the responsibility of the investigation and prosecution team in terms of gathering, preserving and presenting evidence to a court fairly and objectively, remain of utmost importance.
  - 1.11 Because cybercrime knows no geographical boundaries investigators and prosecutors have an increasing role in facilitating cross-border liaison and in obtaining digital evidence through mutual legal assistance. The CCA now also provides for a process of mutual assistance which provides for the preservation and disclosure of articles.
  - 1.12 The CCA has introduced new and specific definitions relating *inter alia* to the investigation, search, access or seizure of articles.
  - 1.13 Although the point of departure for the search, access and seizure of evidence lies *inter alia* within the Criminal Procedure Act, No 51 of 1977 (CPA), there is

thus a need to impose specific guidelines that deal with the search, access or seizure of an article as defined in the CCA.<sup>8</sup>

1.14 Chapter 2 of the CPA deals with search warrants, entering of premises, seizure, forfeiture and disposal of property connected with offences.<sup>9</sup>

1.15 Chapter 4 of the CCA also provides for the powers to investigate, search, access or seize and article.<sup>10</sup>

## 2. Scope and Application

2.1 Section 26 of the CCA provides for Standard Operating Procedures (SOPs) that must be published in the Government Gazette. These SOPs must be observed by:

2.1.1 the South African Police Service; or<sup>11</sup>

2.1.2 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.

2.2 Section 25 of the CCA also provides for 'investigators' that can assist a police official with search, access or seizure under Chapter 4.<sup>12</sup> Such investigators would also have to comply with the provisions of the SOPs.

2.3 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.

---

<sup>8</sup> Section 27 of the CCA provides that The Criminal Procedure Act, 1977, applies in addition to the provisions of Chapter 4 in so far that it is not inconsistent with the provisions of the Chapter.

<sup>9</sup> Sections 19 to 36

<sup>10</sup> Sections 25 to 45

<sup>11</sup> In terms of the CCA 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.

<sup>12</sup> "Investigator" is defined as 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.



- 2.4 The SOPs will furthermore serve as a common standard for exchanging electronic evidence in local and international investigations.
- 2.5 The basic principle to be followed for all activities set out in the SOPs is to maintain the integrity, reliability and authenticity of the data held in an article.

### **3. Jurisdiction and International Dimension of Cybercrime**

- 3.1 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 offence committed by him or her. Jurisdiction requires an assessment in respect of both the physical location of the article and/or suspect (is it, 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).
- 3.2 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.<sup>13</sup>
- 3.3 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.<sup>14</sup>
- 3.4 Section 29(1) of the CCA provides for the written application by a police official for a search warrant for an article. The section further states that a magistrate or judge of the High Court must consider information on oath or by way of affirmation in the application that deals with the location of such an article, namely that there are reasonable grounds for believing that the article:
- 3.4.1 is within the particular court's area of jurisdiction; or
- 3.4.2 is being used or is involved or has been used or was involved in the commission of an offence. Such offence must fall within:
- 3.4.2.1 the court's area of jurisdiction; or

---

<sup>13</sup> Section 24 of the CCA

<sup>14</sup> Section 24(4) of the CCA

- 3.4.2.2 the Republic, if the magistrate or judge 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.
- 3.4.3 An article can also be searched for, accessed or seized by virtue of a search warrant issued 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.<sup>15</sup>
- 3.5 The provisions of sections 48 to 51 of the CCA deal with Mutual Assistance and apply in addition to Chapter 2 of the International Cooperation 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:
- 3.5.1 an offence in terms of Part I or Part II of Chapter 2;
- 3.5.2 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
- 3.5.3 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.
- 3.6 These provisions apply pending a request in terms of section 2 or 7 of the International Cooperation in Criminal Matters Act, 1996.<sup>16</sup>

## **4. General Guidelines for the Investigation, Search, Access or Seizure of an Article**

### **4.1 Introduction**

- 4.1.1 A police official or investigator<sup>17</sup> may only search for, access or seize an article as provided for in Chapter 4 of the CCA. Subject to certain provisions, this

---

<sup>15</sup> Section 29(1)(b) of the CCA

<sup>16</sup> Section 48 of the CCA

<sup>17</sup> As defined in the CCA

will be done in terms of the provisions of section 29 of the CCA.<sup>18</sup> When a search is conducted for anything else but an article, such search must be conducted using the provisions of the CPA.

- 4.1.2 Chapter 4 of the CCA contains specific definitions relating to the access<sup>19</sup> and seizure<sup>20</sup> of an article.
- 4.1.3 Articles 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.
- 4.1.4 Although articles and the evidence contained therein share properties with traditional forms of evidence, it also possesses unique characteristics such as:
  - 4.1.4.1 It is invisible to the untrained eye
  - 4.1.4.2 It is often volatile
  - 4.1.4.3 It may be altered or destroyed through normal use
  - 4.1.4.4 It can be copied without degradation
- 4.1.5 Principles for digital evidence have been developed and adapted over time:
  - 4.1.5.1 **Principle 1- Data Integrity:** No action taken by law enforcement agencies, persons employed within those agencies or their agents should materially change any article which may subsequently be used as evidence in court.
  - 4.1.5.2 **Principle 2 - Audit Trail:** A record of all actions taken when handling an article 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.
  - 4.1.5.3 **Principle 3 - Specialist Support:** If it is expected that an article may be found in the course of a planned operation, the person in charge of the

---

<sup>18</sup> 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

<sup>19</sup> "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.

<sup>20</sup> 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.

operation should notify specialists/external advisers in time and to arrange their presence if possible.

- 4.1.5.4 **Principle 4 - Training and Experience:** Persons permitted by the CCA to search for, access or seize an article at a crime scene, should have basic training and/or experience to be able to search for, access and seize such articles without compromising the integrity of the evidence (if no specialists are available at the scene).
- 4.1.5.5 **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.
- 4.1.6 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.<sup>21</sup>
- 4.1.7 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.<sup>22</sup>
- 4.1.8 The CCA provides for the following methods for the search, access or seizure of an article:
- 4.1.8.1 Written application for obtaining a search warrant in terms of section 29 of the CCA.
- 4.1.8.2 Oral application for obtaining a search warrant or amendment to a warrant.<sup>23</sup>

---

<sup>21</sup> 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.

<sup>22</sup> Section 36 of the CCA

<sup>23</sup> Section 30

- 4.1.8.3 Search for, access, or seizure of article without search warrant with consent of person who has lawful authority to consent.<sup>24</sup>
- 4.1.8.4 Search for, access to, or seizure of article involved in the commission of an offence without search warrant.<sup>25</sup>
- 4.1.8.5 Search for, access to, or seizure of article on arrest of person.<sup>26</sup>
- 4.1.8.6 Preservation and disclosure of data and evidence.<sup>27</sup>
- 4.1.9 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.<sup>28 29</sup>

## 4.2 Preparation for Search, Access or Seizure of an Article (With or Without Warrant)

- 4.2.1 The following considerations should be taken into account when preparing for the search, access or seizure of an article:<sup>30</sup>
  - 4.2.1.1 **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, access or seizure is essential to, for instance, arrest a person whilst committing an offence.
  - 4.2.1.2 **Purpose of the search, access or seizure:** The objectives of the search, access or seizure should be determined to ensure that evidence relevant to the investigation is gathered.
  - 4.2.1.3 **Nature of the article:** This will inform the equipment, instruments, tools and software which are required to search for, access or seize the article(s) and the level of expertise which is required during the operation and include

---

<sup>24</sup> Section 31

<sup>25</sup> Section 32

<sup>26</sup> Section 33

<sup>27</sup> Section 40 to 44, and 48 to 51 of the CCA

<sup>28</sup> Section 40(1) and (2) of the CCA

<sup>29</sup> Section 40(3) imposes additional obligations on electronic communications service providers.

<sup>30</sup> See also Minister for Safety and Security v Van der Merwe and others [2011] JOL 27344 (CC) for provisions relating to search warrants

considerations such as whether there will be a seizure of equipment or capturing of live data or a combination of both.

- 4.2.1.4 **Location of article:** Articles may be found at various locations, which may impact on the judicial authority required, and the manner in which the search, access or seizure operation must be conducted.
- 4.2.1.5 **Logistical aspects:** It is essential that the logistical aspects of the investigation be considered, *inter alia*, sufficient available human resources and equipment.
- 4.2.1.6 **Other forensic examinations:** In the search, access or seizure of articles, the person permitted to conduct the actions should take into consideration whether other forensic processes need to be performed, such as the collection of fingerprints or DNA samples during the search, access or seizure operation and to make appropriate arrangements to secure such evidence.
- 4.2.1.7 **Exhibits other than an article:** The person permitted to conduct the search has to ensure that the seizure of evidence other than an article<sup>31</sup> is carried out in accordance with applicable legislation.<sup>32</sup>
- 4.2.1.8 **Safety:** Consider safety of all persons at the scene and make appropriate arrangements to ensure their safety.
- 4.2.1.9 **Securing of location:** Appropriate arrangements should be made for securing the article(s) from unwanted access at location of the search, access or seizure and to maintain power to electronic devices.
- 4.2.2 Where circumstances permit, all persons involved in the search, access or seizure operation should be fully briefed and individual tasks should be assigned to the team members.

---

<sup>31</sup> As defined in the CCA

<sup>32</sup> 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.

### 4.3 Persons Permitted to Search for, Access or Seize an Article

- 4.3.1 A police official<sup>33</sup> may, in accordance with the provisions of Chapter 4 of the CCA search for, access or seize any article located within the Republic.<sup>34</sup>
- 4.3.2 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:
- 4.3.2.1 identified and authorised in terms of a search warrant as contemplated in section 29(3); or
- 4.3.2.2 requested by a police official in terms of section 31(2)<sup>35</sup>, 32(3)<sup>36</sup> or 33(4)<sup>37</sup> 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.
- 4.3.3 A police official could thus request the assistance of a digital forensic expert or any other person that could assist with any part of the access, search or 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<sup>38</sup> or during the arrest of a person<sup>39</sup>, subject to the written authorisation of such a police official.
- 4.3.4 Where a police official makes use of the services of an investigator:
- 4.3.4.1 All articles seized in terms of activities under Chapter 4 of the CCA, must be handed over to a police official; and

---

<sup>33</sup> 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.

<sup>34</sup> Section 28 of CCA.

<sup>35</sup> Search with lawful consent and the consent for the investigator must be in writing.

<sup>36</sup> 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).

<sup>37</sup> 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).

<sup>38</sup> Section 32

<sup>39</sup> Section 33

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

4.3.5 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, such police official must follow all prescripts of the law to safeguard and store such article.<sup>40</sup> 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 article.

#### **4.4 Specific Tools Used in the Investigation, Search, Access or Seizure of an Article**

4.4.1 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.

#### **4.5 Publicly Available Data**

4.5.1 A police official does not need to be specifically authorised in terms of the CCA to obtain publicly available data<sup>41</sup> 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.

4.5.2 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

---

<sup>40</sup> As per the provisions of the CPA

<sup>41</sup> In terms of the CCA 'publicly available data' means data which is accessible in the public domain without restriction.



conditions regarding confidentiality and limitation of use which they deem necessary. It does not matter where the data is geographically located.<sup>42</sup>

## **4.6 Search, Access or Seizure of an Article with Consent**

- 4.6.1 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.
- 4.6.2 Should the police official require assistance from an investigator, the person giving consent must also provide written consent for the investigator to assist with the search, access or seizure.<sup>43</sup>

## **4.7 Search with a Warrant**

- 4.7.1 In terms of section 29 of the CCA, a police official can apply in writing for a search warrant relating to an article(s).
- 4.7.2 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<sup>44</sup>, 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).

---

<sup>42</sup> Section 45(2) of the CCA

<sup>43</sup> Section 31 of the CCA. See also section 22(a) of the Criminal Procedure Act, No. 51 of 1977

<sup>44</sup> 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).

- 4.7.3 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.<sup>45</sup>
- 4.7.4 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.

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

- 4.8.1 Section 32 of the CCA provides for instances of a search without a warrant in terms of section 29(1)(a).<sup>46</sup> 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<sup>47</sup>, if they on reasonable grounds believe:
- 4.8.1.1 that a search warrant will be issued to them under section 29(1)(a) if they apply for such warrant; and
  - 4.8.1.2 that the delay in obtaining such warrant would defeat the object of the search and seizure.
- 4.8.2 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:
- 4.8.2.1 It excludes access<sup>48</sup> (save for exclusions set out in paragraph 4.8.3 *infra*);
  - 4.8.2.2 Can only perform the actions provided for in subsection (a) and (b) of the definition of seize<sup>49</sup>, namely to:

---

<sup>45</sup> Section 37(2)(a)

<sup>46</sup> See also section 22 (b) of the Criminal Procedure Act, 1977 in this regard.

<sup>47</sup> Part (c) and (d) of the definition of an article

<sup>48</sup> See the definition of 'access' in the CCA

<sup>49</sup> See the definition of "seize" in the CCA

- (a) remove a computer data storage medium or any part of a computer system; or
  - (b) render the data, a computer program, a computer data storage medium or any part of a computer system inaccessible in order to preserve evidence; and
- 4.8.2.3 Only in relation to a computer data storage medium or any part of a computer system.<sup>50</sup>
- 4.8.3 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). A police official or investigator would therefore only be able to:
- 4.8.4 Depending on the facts and nature of the case, 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:
- 4.8.4.1 that a search warrant will be issued to them under section 29(1)(a) if they apply for such warrant; and
  - 4.8.4.2 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.
- 4.8.5 In terms of paragraph (c) and (d) of the definition of *seize* the police official or investigator would then be able to:
- 4.8.5.1 make and retain a copy of data or a computer program; or
  - 4.8.5.2 make and retain a printout of the output of data or a computer program.
- 4.8.6 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).

---

<sup>50</sup> Part (c) and (d) of the definition of *article*. Part (a) data and (b) computer programs are excluded.

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

- 4.9.1 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 or seizure of an article when a person is arrested.
- 4.9.2 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).
- 4.9.3 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 or investigator may search for and perform limited actions:
- 4.9.3.1 It excludes access<sup>51</sup> (save for circumstances a set out in paragraph 4.9.5 *infra*);
  - 4.9.3.2 Can only perform the actions provided for in subsection (a) and (b) of the definition of seize;<sup>52</sup>
  - 4.9.3.3 Only in relation to a computer data storage medium or any part of a computer system<sup>53</sup>; and
  - 4.9.3.4 Which is found in the possession of or in the custody or under the control of the person.
- 4.9.4 A police official or investigator 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).
- 4.9.5 A police official or investigator 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:
- 4.9.5.1 that a search warrant will be issued to them under section 29(1)(a), if they apply for such warrant; and

---

<sup>51</sup> See the definition of “access” in the CCA

<sup>52</sup> See the definition of “seize” in the CCA. A police official or investigator could therefore just:

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

(b) render inaccessible, data, a computer program, a computer data storage medium or any part of a computer system in order to preserve evidence.

<sup>53</sup> Part (c) and (d) of the definition of article in the CCA. Part (a) data and (b) computer programs are excluded.

- 4.9.5.2 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.<sup>54</sup>
- 4.9.6 In terms of paragraph (c) and (d) of the definition of seize the police official or investigator would then be able to:
  - 4.9.6.1 make and retain a copy of data or a computer program; or
  - 4.9.6.2 make and retain a printout of the output of data or a computer program.

## 4.10 Preservation and Disclosure Provisions

- 4.10.1 The CCA contains new procedures for the preservation and disclosure of data and other articles. Preservation allows for a process where data or an article will be preserved i.e. the data or other article is kept subject to circumstances that will ensure that the integrity of the evidence is maintained. In these circumstances the data or other article is not handed over to a police official yet: the data or other article will only be handed over subject to a search warrant in terms of section 29 of the CCA, or where data is concerned, subject to a disclosure of data direction.
- 4.10.2 In terms of section 41 a specifically designated police official may, subject to certain conditions as set out in sections 41(1) and (2),<sup>55</sup> issue an expedited

---

<sup>54</sup> In terms of (c) and (d) of the definition of *seize* the police official or investigator would be able to access and:  
(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.

<sup>55</sup> 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<sup>56</sup> or financial institution.<sup>57</sup>

- 4.10.3 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.<sup>58</sup>
- 4.10.4 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.<sup>59</sup>
- 4.10.5 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.<sup>60</sup> The process is once again aimed at preserving the availability and integrity of the article in question.
- 4.10.6 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, access or 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:
- 4.10.6.1 data which is subject to preservation in terms of an expedited preservation of data direction or a preservation of evidence direction; or

---

<sup>56</sup> 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 licenced in terms of the Electronic Communications Act, 2005.

<sup>57</sup> In terms of the CCA a financial institution as defined in section 1 of the Financial Sector Regulation Act, No 9 of 2017.

<sup>58</sup> The period of preservation can be extended subject to the provisions of section 41(6)

<sup>59</sup> See the provisions of section 41(7) and (8) for the process to object against an expedited preservation of data direction.

<sup>60</sup> Section 42 and 43 of the CCA

- 4.10.6.2 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.
- 4.10.6.3 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).
- 4.10.6.4 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.<sup>61</sup>

## **5. Packaging, Transportation and Storage of Articles**

### **5.1 Securing an Article**

- 5.1.1 Certain types of articles are fragile and could be 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 such articles. To maintain the chain of custody the packaging, transportation, and storage should be recorded and any change of custody or condition of the seized articles should be timed and recorded.
- 5.1.2 The chain of custody must be recorded in the form of an affidavit.
- 5.1.3 If the article is damaged, this should be documented and recorded e.g. a cracked display monitor on a laptop.
- 5.1.4 Note the location and circumstances where articles were found on the scene e.g. was the article concealed, found with all the other articles or other types of evidence.
- 5.1.5 Inexpert handling can cause damage or the destruction of an article, which can influence the eventual integrity, reliability and admissibility of such evidence in a court of law. Police officials and investigators have to ensure

---

<sup>61</sup> Section 44(9) of the CCA

that they take the necessary precautions to ensure that articles are securely packaged, transported and stored.

## **5.2 Packaging**

- 5.2.1 Ensure that all collected articles are properly documented and labelled before packaging.
- 5.2.2 Whenever possible, transport the collected articles in the original packaging.
- 5.2.3 If no original packaging is available, use appropriate packaging to secure and maintain the integrity of the article.
- 5.2.4 Do not fold, bend, or scratch storage media such as diskettes, CD-ROMs, and tapes.
- 5.2.5 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 articles whenever possible.
- 5.2.6 Ensure that all containers containing evidence are properly labelled.
- 5.2.7 If multiple computer systems are collected, label each system so that it can be reassembled as found.
- 5.2.8 Leave cellular, mobile, or smart phone(s) in the power state (on or off) in which they were found.

## **5.3 Transportation**

- 5.3.1 Keep articles away from magnetic sources and protect the equipment from potential damage resulting from e.g. excessive shocks, bumps, heat and humidity.
- 5.3.2 Do not put heavy objects on top of smaller pieces of equipment/storage media.
- 5.3.3 Where practically possible, refrain from storing articles in vehicles for extended periods of time.
- 5.3.4 Document the transportation of the article(s) from the scene to the SAPS storage facility and maintain the chain of custody for all evidence transported.



## 5.4 Storage

- 5.4.1 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.<sup>62</sup>
- 5.4.2 All articles 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.<sup>63</sup>
- 5.4.3 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.
- 5.4.4 Police officials should note that potential electronic evidence such as date, time and system configuration may be lost as a result of prolonged storage. Since batteries have a limited life, data could be lost if they fail. The appropriate personnel should be informed that a device powered by batteries requires immediate attention.
- 5.4.5 The storeroom must be secure and provide for the storage of articles in a way that maintains the integrity of the article.

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

- 6.1 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).
- 6.2 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.

---

<sup>62</sup> 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.

<sup>63</sup> See Section 30(c) of the Criminal Procedure Act, 1977.

- 6.3 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.
- 6.4 Once the process of investigation 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.
- 6.5 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.

## **7. Pornographic Images of Children and other Sensitive Evidence**

- 7.1 A person performing an investigation must always be cognisant of any legal prescripts that could play a role during the extraction process.
- 7.2 Where an article is recovered which contains pornographic images<sup>64</sup> 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

---

<sup>64</sup> 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.

persons, or which could for example be detrimental to state security. Viewing and/or handling 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.

- 7.3 A digital forensic examiner dealing with pornographic images of children and other sensitive evidence must ensure that:
  - 7.3.1 access to evidence is strictly controlled and managed;
  - 7.3.2 all evidence are exported as required and encrypted before it leaves the digital forensic laboratory;
  - 7.3.3 items are sealed in an appropriate container, clearly marked that unauthorised access to the evidence is prohibited; and
  - 7.3.4 the evidence is encrypted.

## **8. Data Held by Third Parties and Independent Data Holders**

- 8.1 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 third party, such as an electronic communications service provider.
- 8.2 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.
- 8.3 Third parties may also collect information on a provisional basis indicating that a cybercrime took place and prompting law enforcement to initiate an investigation.
- 8.4 In terms of section 54 of the CCA, 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:

- 8.4.1 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
- 8.4.2 preserve any information which may be of assistance to the South African Police Service in investigating the offence.<sup>65</sup>

## 9. Evidence

- 9.1 Once the digital forensic analysis of an article has been completed, there must be a report<sup>66</sup> which should contain *inter alia* a description of the operations conducted, the tools used and the results obtained.
- 9.2 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, be *prima facie* proof of such fact.<sup>67</sup> It relates to any fact established by any examination or process requiring any skill in:
  - 9.2.1 the interpretation of data;
  - 9.2.2 the design or functioning of data, a computer program, a computer data storage medium or a computer system;
  - 9.2.3 computer science;
  - 9.2.4 electronic communications networks and technology;
  - 9.2.5 software engineering; or
  - 9.2.6 computer programming.
- 9.3 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.
- 9.4 Section 53 furthermore provides guidelines on the content of the affidavit or solemn attestation.<sup>68</sup>

---

<sup>65</sup> Section 54 of the CCA

<sup>66</sup> As provided for in section 53 of the CCA

<sup>67</sup> See section 53(1) for the relevant fields of study

<sup>68</sup> Section 53(1)(i)

9.5 The court may, in certain circumstances require oral evidence to be given.<sup>69 70</sup>

## 10. Prohibition on the Disclosure of Information

- 10.1 In terms of section 39 of the CCA, no person, investigator, police official, electronic communications service provider, financial institution or its employees 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. This would include information obtained during the investigation, search, access, seizure, preservation or disclosure of an article and any activities relating to mutual assistance.
- 10.2 Section 39 does, however, contain exceptions<sup>71</sup> 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.<sup>72</sup> The exceptions include:
- 10.2.1 Where the information is required for the performance of functions in terms of the CCA;
  - 10.2.2 If a person has to supply such information in the performance of their duties or functions in terms of the CCA;
  - 10.2.3 If it is information which is required in terms of any law or as evidence in any court of law;
  - 10.2.4 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, is also allowed. The

---

<sup>69</sup> 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.

<sup>70</sup> 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.

<sup>71</sup> Subsection 39(2) of the CCA

<sup>72</sup> 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.

information-sharing may, however, not prejudice any criminal investigation or proceedings; or

- 10.2.5 Disclosure 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 where they are conducting an investigation with a view to institute criminal proceedings.
- 10.3 Sharing of information must always be duly authorised and be done subject to such conditions regarding confidentiality and limitation.<sup>73</sup>

## **11. Disposal of an Article**

- 11.1 A police official should as soon as practically possible, with due consideration to the investigation and in consultation with the prosecutor, return a seized article to the person from whom it was seized, provided such person may lawfully possess such an article.
- 11.2 Sections 30 to 36 of the CPA provide for the disposal of an article:
  - 11.2.1 Section 30, read with section 20 of the CPA provide for steps that a police official must take in relation to the disposal of an article after it has been seized.
  - 11.2.2 Section 30(c) provides that if the article is not disposed of or delivered under the provisions of section 30(a) or (b), it should be given a distinctive identification mark and retained in police custody or that such other arrangements be made with regard to the custody thereof as the circumstances may require.
  - 11.2.3 Where no criminal proceedings are instituted or where the article is not required for criminal proceedings, the provisions of section 31 of the CPA should be applied.
  - 11.2.4 Where criminal proceedings are instituted and an admission of guilt fine is paid the disposal of the article is governed by the provisions of section 32 of the CPA.

---

<sup>73</sup> See also the provisions of section 47 of the CCA

- 11.2.5 If criminal proceedings are instituted in connection with any article referred to in section 30(c) of the CPA and such article is required at the trial for the purposes of evidence or for the purposes of an order of court, the police official charged with the investigation, must deliver such article to the clerk of the court where the criminal proceedings are instituted.<sup>74</sup>
- 11.2.6 Section 33(2) and 33(3) of the CPA furthermore provide for measures where the article cannot be handed in at the clerk of the court or where the article has to be transferred to another court.
- 11.2.7 When criminal proceedings are concluded, the presiding judge or judicial officer must make an order on how to deal with an article that had been presented as evidence in such proceedings or had been used for purposes of an order of court.<sup>75</sup>
- 11.2.8 An article can also be forfeited to the State.<sup>76</sup>
- 11.2.9 Where an article is concerned in an offence committed outside Republic, the disposal of such article is governed by the provisions of section 36 of the CPA.
- 11.3 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) 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.<sup>77</sup> 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:
- 11.3.1 it is not required by a person who may lawfully possess the passwords, decryption keys, data or other information;
- 11.3.2 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 an order of court; or

---

<sup>74</sup> Section 33(1) of the CPA

<sup>75</sup> See section 34 of the CPA in this regard.

<sup>76</sup> See section 35 of the CPA in this regard.

<sup>77</sup> Section 37(2)(a)(i) of the CCA

- 11.3.3 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.

## **12. Offences in the CCA that relate to the Investigation, Search, Access or Seizure of an Article**

- 12.1 It is a criminal offence for an electronic communications service provider, financial institution or person to not provide technical or other assistance during a search when requested to do so by a police official. If found guilty, they could be liable to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment.<sup>78</sup>
- 12.2 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 search warrant issued in terms of section 29(1) of the CCA.<sup>79</sup> Upon conviction such person could be liable to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment.
- 12.3 A police official who may lawfully execute any power conferred upon them in terms of a search warrant under section 29(2) of the CCA, may use reasonably necessary force, which is proportional to all the circumstances, to exercise his/her powers to execute the warrant.
- 12.4 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 announced the purpose of their entry.<sup>80</sup> 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.

---

<sup>78</sup> Section 34 of the CCA

<sup>79</sup> Section 35 of the CCA

<sup>80</sup> Section 35(2)(b) of the CCA



- 12.5 It is an offence for a police official or an investigator to unlawfully and intentionally act contrary to the authority of:
- 12.5.1 a search warrant issued under section 29(1); or
  - 12.5.2 consent granted in terms of section 31(1).<sup>81</sup>
- 12.6 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:
- 12.6.1 searches for, accesses or seizes data, a computer program, a computer data storage medium or any part of a computer system; or
  - 12.6.2 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.<sup>82</sup>
- 12.7 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).
- 12.8 A police official or an investigator who contravenes or fails to comply with section 37(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. The Court may furthermore make a compensation order in terms of section 300 of the CPA.
- 12.9 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:
- 12.9.1 a search warrant being issued;
  - 12.9.2 a search with consent taking place on the basis of such information;
  - 12.9.3 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;

---

<sup>81</sup> Section 37(1)(a) of the CCA

<sup>82</sup> Section 37(1)(b) of the CCA

- 12.9.4 an expedited preservation of data direction contemplated in section 41 being issued;
- 12.9.5 a preservation of evidence direction contemplated in section 42 being issued; or
- 12.9.6 a disclosure of data direction contemplated in section 44 being issued.
- 12.10 If found guilty of a contravention of section 38, such a person could be liable to a fine or to imprisonment for a period not exceeding two years or to both such fine and imprisonment. The Court may furthermore make a compensation order in terms of section 300 of the CPA.
- 12.11 Any 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 discloses 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 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.<sup>83</sup>
- 12.12 In terms of section 41 a person, electronic communications service provider or financial institution commits a criminal offence in the following circumstances, and would be liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment:
  - 12.12.1 Failing to comply with an expedited preservation of data direction; or
  - 12.12.2 Disclosing data to a police official on the strength of an expedited preservation of data direction.
  - 12.12.3 Making a false statement in an application to amend or cancel the direction.
- 12.13 In terms of section 44 it is a criminal offence for a person, electronic communications service provider or a financial institution to:
  - 12.13.1 Fail to comply with a disclosure of data direction;
  - 12.13.2 Make a false statement in an application referred to cancel or amend a disclosure of data direction; or
  - 12.13.3 Make the data and an affidavit available to a police official.

---

<sup>83</sup> Section 39(3) of the CCA

- 12.14 If found guilty of a contravention of section 44(8) the person, electronic communications service provider or financial institution is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment.
- 12.15 In terms of section 49(4) it is a criminal offence for a person, electronic communications service provider or financial institution to:
- 12.15.1 Fail to comply with an order referred to in section 48 (6) which relates to the preservation of articles and expedited disclosure of traffic data; or
- 12.15.2 Make a false statement in an application to cancel or amend an order in terms of section 48.
- 12.16 If found guilty of a contravention of section 49(4) a person, electronic communications service provider or financial institution is liable to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment.
- 12.17 Failure to provide traffic data to the Designated Point of Contact, making false statements in the accompanying affidavit, or failing to comply with regulations in terms of section 59(1)(a)(xxii) are criminal offences and a person, electronic communications service provider or financial institution is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment.<sup>84</sup>
- 12.18 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.<sup>85</sup>

---

<sup>84</sup> Section 50(4)

<sup>85</sup> Section 53(3) of the CCA

## 13. The SAPS Designated Point of Contact

- 13.1 The CCA provides for the creation of a Designated Point of Contact (DPoC) within SAPS structures.<sup>86</sup>
- 13.2 The DPoC must ensure the provision of immediate assistance both locally and internationally for the purpose of any proceedings or investigations regarding the commission or intended commission of:
  - 13.2.1 an offence under Part I or Part II of Chapter 2 of the CCA;
  - 13.2.2 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
  - 13.2.3 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.
- 13.3 The assistance which will be provided by the DPoC includes the following:
  - 13.3.1 Provision of technical advice and assistance;
  - 13.3.2 Facilitation or provision of assistance regarding anything which is authorised under Chapters 4 and 5 of the CCA;
  - 13.3.3 Provision of legal assistance;
  - 13.3.4 Identification and location of an article;
  - 13.3.5 Identification and location of a suspect; and
  - 13.3.6 Cooperation with appropriate authorities of a foreign State.
- 13.4 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.

---

<sup>86</sup> Section 52 of the CCA

## 14. Glossary of Terms

Abbreviation/Term	Explanation
<b>Availability</b>	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.
<b>Browser (ECT Act)</b>	A computer program which allows a person to read hyperlinked data messages.
<b>Capturing Data</b>	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).
<b>Computer Forensics</b>	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.
<b>Critical Data (ECT Act)</b>	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.
<b>Critical Database (ECT Act)</b>	A collection of critical data in electronic form from where it may be accessed, reproduced or extracted.
<b>Cyber Attack</b>	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.
<b>Cyber-Dependent Crime</b>	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).
<b>Cyber-Enabled Crime</b>	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.
<b>Cyber Event</b>	Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.
<b>Cyber Extortion (Cybercrimes Act)</b>	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.
<b>Cyber Fraud (Cybercrimes Act)</b>	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.
<b>Cyber Forgery (Cybercrimes Act)</b>	(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.
<b>Cyber Incident</b>	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.
<b>Cyber Uttering (Cybercrimes Act)</b>	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.
<b>Damage to Property (Cybercrimes Act)</b>	Damage to any corporeal or incorporeal property.

<b>Abbreviation/Term</b>	<b>Explanation</b>
<b>Data Subject (POPIA)</b>	The person to whom personal information relates.
<b>Deleted Data</b>	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.
<b>Desktops</b>	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
<b>Digital Forensics</b>	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.
<b>Electronic /digital Evidence</b>	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.
<b>Electronic Communications Service (Cybercrimes Act)</b>	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.
<b>Email</b>	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)
<b>Faraday Isolation Bag</b>	A dimensionless unit of electric charge quantity, equal to approximately $6.02 \times 10^{23}$ 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
<b>Infrastructure (Critical Infrastructure Protection Act)</b>	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.
<b>Internet Access</b>	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.
<b>Internet Service Provider (ISP)</b>	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.
<b>Internet</b>	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.
<b>Interception of Data (CCA)</b>	<p>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:</p> <ul style="list-style-type: none"> <li>(a) examination or inspection of the contents of the data; and</li> <li>(b) diversion of the data or any part thereof from its intended destination to any other destination.</li> </ul>
<b>Interference with Data (CCA)</b>	<p>To permanently or temporarily:</p> <ul style="list-style-type: none"> <li>(a) delete data or a computer program;</li> <li>(b) alter data or a computer program;</li> <li>(c) render vulnerable, damage or deteriorate data or a computer program;</li> <li>(d) render data or a computer program meaningless, useless or ineffective;</li> <li>(e) obstruct, interrupt or interfere with the lawful use of, data or a computer program; or</li> <li>(f) deny access to data or a computer program, held in a computer data storage medium or a computer system.</li> </ul>
<b>Interference with a Computer Data Storage Medium (CCA)</b>	<p>Means to permanently or temporarily:</p> <ul style="list-style-type: none"> <li>(a) alter any resource; or</li> <li>(b) interrupt or impair— <ul style="list-style-type: none"> <li>(i) the functioning;</li> <li>(ii) the confidentiality;</li> <li>(iii) the integrity; or</li> <li>(iv) the availability,</li> </ul> </li> </ul> <p>of a computer data storage medium or a computer system.</p>
<b>Live Data Forensics</b>	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.
<b>Output of Data (CCA)</b>	Having data displayed or in any other manner.
<b>Output of a Computer Program (CCA)</b>	Any: (a) data or output of the data; (b) computer program; or (c) instructions, generated by a computer program.
<b>Password, Access Code or Similar Data or Device (CCA)</b>	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.
<b>Person (CCA)</b>	A natural or a juristic person
<b>Publicly Available Data (CCA)</b>	Data which is accessible in the public domain without restriction.
<b>Restricted Computer System (CCA)</b>	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.
<b>Software</b>	Computer programs designed to perform specific tasks, such as word processing, accounting, network management, Website development, file management, or inventory management.
<b>Storage Devices</b>	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.
<b>Traffic data (CCA)</b>	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
<p><b>Unlawful Access (CCA)</b></p>	<p>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.</p> <p><b>Access computer data storage medium:</b> Uses the data or a computer program stored on a computer data storage medium or stores data or a computer program</p> <p><b>Access a computer system:</b></p> <ul style="list-style-type: none"> <li>• Uses data or computer program</li> <li>• Stores data or a computer program on a computer data storage medium which forms part of a computer system</li> <li>• Instructs, communicates with or uses the computer system</li> </ul> <p><b>Uses a computer program:</b></p> <ul style="list-style-type: none"> <li>• Copies or moves the computer program to a different location</li> <li>• Causes a computer program to perform any function</li> <li>• Obtains the output of a computer program</li> </ul> <p><b>Uses Data:</b></p> <ul style="list-style-type: none"> <li>• Copies or moves the data to a different location</li> <li>• Obtains the output of the data.</li> </ul>
<p><b>Unlawful Interception of Data (CCA)</b></p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>“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</p>

Abbreviation/Term	Explanation
	<p>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:</p> <p>(a) examination or inspection of the contents of the data; and</p> <p>(b) diversion of the data or any part thereof from its intended destination to any other destination.</p>
<p><b>Unlawful Interference with Data or Computer Program (CCA)</b></p>	<p>Unlawfully and intentionally interfering with data or a computer program. “Interfere with data or a computer program” means to permanently or temporarily:</p> <p>(1) delete data or a computer program;</p> <p>(2) alter data or a computer program;</p> <p>(3) render vulnerable, damage or deteriorate data or a computer program;</p> <p>(4) render data or a computer program meaningless, useless or ineffective;</p> <p>(5) obstruct, interrupt or interfere with the lawful use of, data or a computer program; or</p> <p>(6) deny access to data or a computer program, held in a computer data storage medium or a computer system.</p>
<p><b>Unlawful Interference with a Computer Data Storage Medium or Computer System (CCA)</b></p>	<p>Any person who unlawfully and intentionally interferes with a computer data storage medium or a computer system, is guilty of an offence.</p> <p>For purposes of this section “interfere with a computer data storage medium or a computer system” means to permanently or temporarily:</p> <p>(a) alter any resource; or</p> <p>(b) interrupt or impair—</p> <p>(i) the functioning;</p> <p>(ii) the confidentiality;</p> <p>(iii) the integrity; or</p> <p>(iv) the availability,</p> <p>of a computer data storage medium or a computer system.</p>
<p><b>Unlawful Possession of Data (CCA)</b></p>	<p>Unlawfully and intentionally possessing data or the output of data, with the knowledge that such data was intercepted unlawfully</p>

Abbreviation/Term	Explanation
<b>Unlawful Acts in Respect of Software or Hardware Tool (CCA)</b>	<p>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.</p> <p>"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:</p> <ul style="list-style-type: none"> <li>(a) access as contemplated in section 2(1) or (2);</li> <li>(b) intercept data as contemplated in section 3(1);</li> <li>(c) interfere with data or a computer program as contemplated in section 5(1);</li> <li>(d) interfere with a computer data storage medium or a computer system as contemplated in section 6(1); or</li> <li>(e) acquire, make available or use a password, access code or similar data or device as defined in section 7(3).</li> </ul>

## 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
<p><b>19 Saving as to certain powers conferred by other laws</b></p> <p>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.</p>	<p><b>27 Application of Criminal Procedure Act, 1977</b></p> <p>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.</p>
<p><b>20 State may seize certain articles</b></p> <p>The State may, in accordance with the provisions of this Chapter, seize anything (in this Chapter referred to as an article)-</p> <p>(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;</p> <p>(b) which may afford evidence of the commission or suspected commission of an offence, whether within the Republic or elsewhere; or</p>	<p><b>28 Search for, access to, or seizure of certain articles</b></p> <p>A police official may, in accordance with the provisions of this Chapter, search for, access or seize any article, within the Republic.</p> <p>Section 1(1) In this Act, unless the context indicates otherwise-</p> <p><b>'Article'</b> means any-</p> <p>(a) data;</p> <p>(b) computer program;</p> <p>(c) computer data storage medium; or</p> <p>(d) computer system,</p> <p>which-</p>

<p>(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.</p>	<p>(i) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission;</p> <p>(ii) may afford evidence of the commission or suspected commission; or</p> <p>(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-</p> <p>(aa) an offence in terms of Part I and Part II of Chapter 2;</p> <p>(bb) any other offence in terms of the law of the Republic; or</p> <p>(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;</p>
<p>There is no definition of seize in the CPA</p>	<p><b>“Seize”</b> includes to—</p> <p>(a) remove a computer data storage medium or any part of a computer system;</p> <p>(b) render inaccessible, data, a computer program, a computer data storage medium or any part of a computer system in order to preserve evidence;</p> <p>(c) make and retain a copy of data or a computer program; or (d) make and</p>

	retain a printout of the output of data or a computer program.
Access is not defined in the CPA	<p>For purposes of Chapter 4:</p> <p>“<b>access</b>” includes without limitation to make use of:</p> <p>(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</p> <p>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;</p>
There is no provision in the CPA for investigators	<p>“<b>investigator</b>” means any fit and proper person, who is not a member of the South African Police Service and who is:</p> <p>(a) identified and authorised in terms of a search warrant as contemplated in section 29(3); or</p> <p>(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;</p>