South African Police Service

Standard Operating Procedures

in terms of

Section 26 of the Cybercrimes Act, No 19 of 2020 for the Investigation, Search, Access or Seizure of Articles

Acknowledgements

The Standard Operating Procedures (SOPs) have been drafted by an interdepartmental team, composed of representatives from the South African Police Services (SAPS), Directorate for Priority Crime Investigation (DPCI), National Prosecuting Authority (NPA) and the Department of Justice and Constitutional Development (DoJ&CD).

The Committee acknowledges the inputs of all parties that have been received during the time the SOPs were drafted.

Table of Contents

1. Background

1.1 The Cybercrimes Act, No 19 of 2020 ("CCA") came into partial operation on 1 December 2021. The CCA *inter alia* provides for a new and improved legal mechanism to address cybercrime in South Africa.

1.2 The CCA provides for offences in Chapter 2, Part I and II. Part I deals with specific categories of cybercrimes. Part II deals with malicious communications. Chapter 2 Part III provides for attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence in terms of Chapter 2 Part I and II and Part IV for competent verdicts. The CCA also provides for interim protection orders in Chapter 2 Part VI.

1.3 Chapter 3 regulates jurisdiction in respect of cybercrimes.

1.4 Chapter 4 of the CCA further regulates the powers to investigate cybercrimes, as well as those criminal offences that are committed by means of or facilitated through the use of an article. Chapter 4 furthermore contains new provisions relating to the search, access and seizure of articles. It also provides for mechanisms to preserve articles as defined in the CCA (and the electronic evidence[1] contained therein), to conduct search, access and seizures in respect of such articles, which relate to the investigation of offences in the CCA, as well as to other criminal offences that are committed by means of or facilitated through the use of an article.

1.5 Chapter 5 regulates aspects relating to mutual assistance (as opposed to mutual legal assistance) in respect of the investigation of cybercrimes. Because cybercrime knows no geographical boundaries, investigators and prosecutors have an increasing role in facilitating cross-border liaison and in obtaining electronic evidence through mutual legal assistance. The process of mutual assistance provides for *inter alia* the preservation of an article or other evidence in electronic format relating to certain offences, pending a request in terms of section 2 or 7 of the International Co-operation in Criminal Matters Act, 1996.

[1] The terms digital and electronic evidence are often used interchangeably and for purposes of this document bear the same meaning.

1.6 Chapter 6 provides for the establishment and functioning of a Designated Point of Contact.

1.7 Chapter 7 contains provisions for the proof of certain facts by affidavit.

1.8 Section 54 imposes obligations to report cybercrimes under certain conditions.

1.9 Section 55 provides for building capacity to detect, prevent and investigate cybercrimes.

1.10 Chapter 9 provides for general provisions such as that the Executive may enter into agreements with foreign States to promote measures aimed at the detection, prevention, mitigation and investigation of cybercrimes, the deletion and amendment of provisions of certain laws, and to provide for matters connected therewith.

1.11 For ease of reference, an article as defined in the CCA, will be referred to as a **cyber article** in this document.[2]

2. Scope and Application of the Standard Operating Procedures

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;[3] or

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] This is also aimed at avoiding confusion with the term “article” as defined in the Criminal Procedure Act, No. 51 of 1977 where “article” is defined as “anything”.

[3] The CCA defines a 'police official' as a member of the South African Police Service, as defined in section 1 of the South African Police Service Act, No. 68 of 1995

2.2 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, a cyber article.

2.3 Section 25 of the CCA also provides for 'investigators' that can assist a police official with search, access or seizure under Chapter 4.[4] Such investigators would also have to comply with the provisions of the SOPs.

2.4 The SOPs aim to ensure that the way in which a police official obtains evidence from cyber articles for purposes of investigating a criminal offence, complies with South African legislation and that due regard is given to an individual's right to privacy and the right to a fair trial.

2.5 In the case of victims and witnesses, the SOPs aim to ensure that cyber articles are generally obtained with their informed consent.[5]

2.6 The SOPs can assist with the exchange of electronic evidence in local and international investigations.

2.7 Where personal information is processed during any activity under Chapter 4 of the CCA, the relevant principles in the Protection of Personal Information Act, No. 4 of 2013 (POPIA) applies. In cases where the responsible party[6], being either the NPA, SAPS or DPCI, uses a third party or service provider to assist in the search, access and seizure of a cyber article, such other party would be regarded as an operator[7].

---

4 "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.

5 See section 31 of the CCA in this regard.

6 In POPIA ''responsible party'' means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

7 In POPIA an ''operator'' means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party

3. Principles for the Search, Access or Seizure of a Cyber Article for Purposes of Conducting an Investigation

3.1 These principles have been developed based on the provisions of the CCA, considering other relevant South African legislation, as well as similar international guidelines.

3.2 The principles also take account of inputs received from the SAPS, the DPCI, the NPA and the DoJ&CD, as well as feedback received during the process of public consultation.

3.3 The main aim is to balance the fundamental rights of victims and witnesses with the right of a suspect(s) to a fair trial.[8]

3.4 The principles should also be practical to implement.

3.5 The following seven (7) principles apply to this document:

PRINCIPLE	APPLICATION
Principle 1: **Conducting activities with due regard to an individual's fundamental rights, including the right to a fair trial**	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 South African legislation. 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.

[8] . In accordance with the CCA, any breach of the eight conditions for lawful processing of personal information should be dealt with in terms of Chapter 10 of POPIA and not in terms of the CCA.

PRINCIPLE	APPLICATION
Principle 2: **Maintaining the integrity, reliability and authenticity of a cyber article**	The basic principle to be applied in all activities relating to the investigation, search, access or seizure of a cyber article is to ensure that all actions, processes and procedures relating thereto are aimed at maintaining the integrity, reliability, authenticity and eventual admissibility of such evidence in a court of law. Any search, access or seizure of a cyber article will always be conducted in accordance with South African legislation and case law. It is also necessary to maintain adequate security measures to protect personal information that is processed as part of any activity in Chapter 4 of CCA. Persons expect that information they create and store in an electronic format should be afforded the same privacy protections as information they previously held in a paper format.[9] POPIA does not apply to the processing of personal information where it is performed by or on behalf of a public body for the purpose of the investigation or proof of offences, provided that adequate safeguards have been established in legislation for the protection of such personal information.

[9] See sections 19 and 22 of POPIA in this regard.

PRINCIPLE	APPLICATION
Principle 3: **Proportionate and necessary for purpose of conducting an investigation**	Any investigation, search, access or seizure of a cyber article should be aimed at gathering relevant evidence for a criminal investigation and be proportionate to the scope thereof. Cyber articles can be searched, accessed or seized by means of a search warrant, without a warrant, on arrest, or with consent. In most instances, a cyber article of a cooperative witness or innocent third party should be obtained by means of consent.
Principle 4: **Legality**	The police official in charge of an investigation is 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, 1996, 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. Police officials and investigators, where they are used, must always perform their functions/ duties under Chapter 4 with strict regard to decency and order, giving due regard to the rights, responsibilities and legitimate interests of other persons.

PRINCIPLE	APPLICATION
Principle 5: **Adequate, relevant and not excessive for the purpose for which it was searched, accessed or seized**	Police officials and where applicable investigators must conduct any search, access or seizure of a cyber article to the extent specified in the search warrant, within the scope of consent, or where a search is conducted without a warrant, within the confines of the provisions of the CCA. If it is necessary to obtain evidence from a cyber article, police officials and investigators should consider whether there is a less intrusive method to obtain the evidence. The method must maintain the integrity, reliability and authenticity of the cyber article.
Principle 6: **Audit Trail**	A record of all actions taken when handling a cyber article should be created and preserved so that it can subsequently be audited. An independent third party should not only be able to repeat those actions, but should also be able to achieve the same result.
Principle 7: **Secure appropriate advice and support**	If it is expected that a cyber article may be found in the course of an operation, and depending on the nature and circumstances of the particular investigation, the police official(s) conducting the search can for example approach the Designated Point of Contact for assistance, or secure the assistance of an investigator as defined in the CCA.

4. Cyber Articles in the CCA

4.1 For ease of use the definition of a cyber article is divided into three (3) parts:

4.1.1 **Type of cyber article:** The definition of a cyber article in the CCA relates to any of the following and it is imperative to remember the order in which the four (4) types of articles are stated as only certain types of articles can be searched for, accessed and seized without a search warrant:

(a) Data.[10] Examples of data include video, graphics, text and images. The data may be in any form, whether readable only by a computer, only by a human, or by either;

(b) Computer program.[11] Examples of computer programs include operating systems, Microsoft Office programs such as Word and Excel, mobile applications and cloud services;

(c) Computer data storage medium.[12] Examples include hard drive disks (HDDs), solid-state drives (SSDs), tapes, compact discs (CDs), USB flash drives, secure digital cards (SD cards) and cloud storage; or

(d) Computer system.[13] A computer system can consist of one or more computers.[14] For example, a computer system can be all the computers

---

10 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.

11 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.

12 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.

13 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.

14 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,

in a particular business, all the hardware and software which is needed for the functioning of that computer system, which provides for input from users and also creates information for storage and output. This would also for example include all the hardware, central processing unit (CPU), the operating system the computer uses and any peripheral equipment the computer needs to function. Other examples of a computer system include a cell phone, a notepad, tablet, smart devices, desktop or laptop.

4.1.2 **When is it relevant?** Any or all of the four (4) types of cyber articles will be relevant when it:

4.1.2.1 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;

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

4.1.2.3 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.

4.1.3 **Which offences?** The offences that are relevant to the definition are:

4.1.3.1 any offences in terms of Part I and Part II of Chapter 2 of the CCA. These are the so-called cybercrime offences which are contained in the CCA;

4.1.3.2 any other offence in terms of the law of the Republic. This would mean that where, for example, a cyber article can afford evidence or is used in the commissioning of a corruption or murder case, it could also fall within the definition of a cyber article; or

4.1.3.3 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.

---

computer program or computer data storage medium that are related to, connected with or used with such a device.

4.2 The definition of cyber article has a wider application than just the offences defined in Chapter 2 of the CCA. It also applies to all types of offences that involve a cyber article, for example where crimes such as murder, corruption or money laundering are committed by means of, or facilitated using a computer or cell phone and the data and computer programs on such devices can afford evidence in the investigation. In most instances it is all about the electronic evidence (data or computer programs) contained on a computer data storage medium or computer system that can be used in the investigation of criminal offences.

5. Distinguishing between Articles as defined in the CCA and CPA

5.1 It is crucial to have a proper understanding of what is defined as an article in the CCA and the application thereof. In terms of the Criminal Procedure Act, No. 51 of 1977 (CPA), article has a much wider meaning namely "anything" that can be seized by the State, subject to the conditions set out in section 20 of the CPA. The definition in the CCA is narrower and a reading of these two Acts can thus cause confusion – especially as it applies to search and seizure.

5.2 As stated above for purposes of this document the term **cyber article** will be used to describe an article as defined in the CCA.

5.3 Chapter 2 of the CPA deals with search warrants, entering of premises, seizure, forfeiture and disposal of property connected with offences.[15]

5.4 Chapter 4 of the CCA also provides for the powers to investigate, search, access or seize cyber article.[16] The CCA has also introduced new and specific

[15] Sections 19 to 36 of the CPA
[16] Sections 25 to 45 of the CCA

definitions relating *inter alia* to the investigation, search, access or seizure of cyber articles.[17]

5.5 Although the point of departure for the search, access and seizure of evidence lies *inter alia* within the CPA, there is a need to impose specific guidelines that deal with the search, access or seizure of a cyber article as defined in the CCA.[18]

5.6 Members of the SAPS, other law enforcement officials and some prosecutors may become involved in the collection, analysis or decisions related to cyber articles at some stage of a criminal investigation or court proceedings. The judiciary is for example, responsible for authorising search warrant applications and can also issue a search warrant where they are presiding at criminal proceedings and a cyber article is required in evidence at such proceedings.

5.7 It is also important to note that the SOPs do not only apply to police officials (members of SAPS), but to all other agencies and persons that are conducting investigations of offences in terms of their (own) enabling legislation, as well as investigators that assist a police official with the search, seizure or access of a cyber article.

6. Extra-territorial Jurisdiction and Scene of Crime

6.1 Jurisdiction of a Court to Try an Offence

6.1.1 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 they committed. Chapter 3 of the CCA deals with jurisdiction and provides for circumstances where the courts in the Republic have jurisdiction to try any offence referred to in Part I or Part II of Chapter 2.

---

17 There are definitions specifically relating to “access” for the purposes of search, an “investigator”, as well as a definition of “seize” for the purposes of conducting activities under Chapter 4 of the CCA

18 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.

6.1.2 Jurisdiction requires an assessment in respect of both the physical location of the cyber article and/or suspect (is the cyber article, or the suspect/person 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).

6.2 The Scene of Crime

6.2.1 There can be confusion between what is meant by jurisdiction as opposed to what is meant by a scene of crime. A scene of crime is commonly defined as the place where a crime was committed. It is sometimes difficult to establish where a cybercrime has been committed e.g. as the crime might have been committed in "cyberspace", across multiple jurisdictions or at an unknown location. For this purpose and to assist police officials to register case dockets, the SAPS have provided the following guidelines:

6.2.1.1 If the victim or complainant is a natural person, the home address of such a person should be used as the "scene of crime" to open a docket on Crime Administration System (CAS) or Integrated Case Docket Management System (ICDMS).

6.2.1.2 Where the victim or complainant is a juristic person such as a business, the business address should be used as the "scene of crime" to open a docket on CAS/ICDMS.

6.3 Jurisdiction and Application for a Search Warrant

6.3.1 In terms of section 29(1) of the CCA a police official can only search for, access or seize a cyber article by virtue of a search warrant. A police official must submit a written application for a search warrant to the court that has jurisdiction to hear such an application.

6.3.2 The 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 a cyber article, namely that there are reasonable grounds for believing that the cyber article:

6.3.2.1 is within the particular court's area of jurisdiction; or

6.3.2.2 is being used or is involved or has been used or was involved in the commission of an offence. Such offence must fall within:

6.3.2.3 the court's area of jurisdiction; or

6.3.2.4 the Republic, if the magistrate or judge is unsure within which area of jurisdiction the cyber article is being used or is involved or has been used or was involved in the commission of an offence.

6.3.3 The CCA does not only provide for instances where a police official can apply for a search warrant. Where it appears to a magistrate or judge of the High Court that an article can provide evidence in a criminal trial, a search warrant can also be issued by the presiding officer in criminal proceedings.[19]

6.4 Other Relevant Provisions

6.4.1 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.[20]

6.4.2 Any cross-border transfer of personal information must be done with due consideration of the provisions of section 72 of the POPIA.[21]

---

19 Section 29(1)(b) of the CCA

20 Section 24(4) of the CCA

21 Section 72 of POPIA deals with the transfer of personal information outside of the Republic. For purposes of the functions in Chapter 4 of the CCA, this will mostly refer to the condition that personal information can only be transferred to a country where the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that:
(i) effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and

6.4.3 The provisions of sections 48 to 51 of the CCA deal with mutual assistance and these provisions apply pending a request in terms of section 2 or 7 of the International Cooperation in Criminal Matters Act, 1996. It also applies to certain offences as set out in section 46 (a) to (c) of the CCA.[22]

7. Guidelines for the Investigation, Search, Access or Seizure of a Cyber Article[23]

7.1 Introduction

7.1.1 Police officials and investigators should always consider the possibility that any electronic device or equipment that they might encounter during the course of an investigation could potentially yield evidence, which includes electronic evidence. By way of example, a mobile device or keyboard could yield DNA or fingerprints, but the mobile device could also contain electronic evidence, which is contained in the device (e.g. data).

7.1.2 In the technological era we are living in, electronic evidence is a fundamental component of most criminal investigations. With the advent of the smartphone, social media and various internet services, a suspect leaves a digital trail and it is important that the digital trail is captured and analysed for investigation purposes. The search and seizure phase of an investigation is critical as it will safeguard the devices and the data held on them. If cyber articles are not

(ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country.

[22] Unless specified otherwise, these provisions relate to the preservation of a cyber article or other evidence in electronic format regarding the commission or suspected commission of:
(a) an offence in terms of Part I or Part II of Chapter 2;
(b) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, a cyber article; or
(c) 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, a cyber article

[23] According to ISO/IEC 27037 there are four phases involved in the initial handling of electronic evidence: identification, collection, acquisition, and preservation.

searched for, accessed and seized correctly, valuable evidence can be lost or it can also lead to such evidence being inadmissible in a court of law.

7.1.3 Cyber articles can hold important evidence that has been created either automatically by the device itself, or by the user. User-generated data could include documents, photos, image files, e-mails and their attachments, databases and financial information. Computer-generated data can include the Internet browsing history, chat logs, event logs and data about other services, computers and networks to which the device has been connected.

7.1.4 Cyber articles should always be handled with care and the aim should be to preserve such evidence in a way that ensures the integrity, reliability and eventual admissibility of the evidence in a court of law.

7.1.5 Although a cyber article(s) and the electronic evidence contained therein share properties with traditional forms of evidence, it also possesses unique characteristics such as:

7.1.5.1 It is invisible to the untrained eye

7.1.5.2 It is often volatile

7.1.5.3 It may be altered or destroyed through normal use

7.1.5.4 It can be copied without degradation

7.1.6 Similar to other types of forensic evidence, such as fingerprints and DNA, the correct acquisition and handling of electronic evidence are vital to the outcome of a criminal investigation. The Association of Chief Police Officers (ACPO) has provided a set of principles for electronic evidence, which has been revised and adapted over time and has also been incorporated into the Principles set out in Clause 3 above.

7.1.7 The search, access and seizure of a cyber article generally involves two steps, which in most cases need to be considered simultaneously:

7.1.7.1 the seizure of the device itself, namely the computer data storage medium or computer system; and[24]

[24] Part (a) and (b) of the definition of seize

7.1.7.2 the seizure of data and computer programs contained in the device, namely copying or making a printout of the data and computer programs on the computer data storage medium or computer system.[25]

7.1.8 Circumstances may differ from case to case. In some instances the police official will have to remove the article from the scene and any digital forensic processes will be completed off-scene. In other instances the analysis can or has to be done on site. In some instances the police official or investigator would not be able to make and retain a copy of data or a computer program, and will only be able to make and retain a printout of the output of data or a computer program.

7.1.9 Selecting which cyber article to seize and which evidence to collect or capture at a crime scene can be complicated. Difficulties on site can be avoided by careful planning and advance preparation.

7.1.10 The first consideration in planning for any activity relating to the investigation, search, access or seizure of a cyber article is to ascertain what type of legal permission or authorisation to use in a particular case. This could for example, include applying for a search warrant in terms of section 29 of the CCA, or obtaining written consent in terms of section 31 of the CCA.[26]

7.1.11 A police official or investigator[27] may only search for, access or seize a cyber article as provided for in Chapter 4 of the CCA.[28]

7.1.12 If and when a search is conducted for anything else but a cyber article, such search must be conducted using the provisions of the CPA.

---

25 Part (c) and (d) of the definition of seize

26 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.

27 As defined in the CCA

28 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

7.2 Use of the Correct Legal Instrument to Obtain Evidence

7.2.1 Police officials must ascertain which the correct legal instrument is to use in a particular scenario.

7.2.2 It is important to distinguish when to use section 205 of the CPA and when to apply for a search warrant - be it an application for a search warrant in terms of either the CCA or the CPA:[29]

7.2.2.1 Search warrants in terms of the CCA did not replace the use of a section 205 subpoena under the CPA.

7.2.2.2 When requesting historical information such as bank records and cell phone records, this should be done using a section 205 subpoena. Remember that this is information that is held by e.g. the bank or the mobile network operator. It is extracts from their business records demonstrating what transactions their client has performed. For ease of reference, when requesting records from a mobile network operator, the police official would be able to request the records relating to an action that depleted the airtime or data that the client paid for: such as making a call to another number, using data to access social media, or to browse the internet.

7.2.3 It is also important to establish which search warrant to use, namely a search warrant in terms of the CCA or in terms of the CPA:

7.2.3.1 A search warrant in terms of the CCA is used when any of the four (4) items under the definition of a cyber article needs to be seized. By way of example, a police official needs to search, seize and access the cell phone of a suspect. The aim is not to obtain call data records (CDRs) which are the records kept by the mobile network operator, but to see what is contained in the cell phone. The police official will then obtain a search warrant and a person skilled in copying and analysing the data and computer programs in the device can then extract the information from the

[29] See also section 15(4) of the ECT Act in this regard: A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law. admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

cell phone. The information on the cell phone could be emails, SMS messages, photos, screenshots, voice notes etc.

7.2.3.2 In all other instances where an article does not meet the definition of a cyber article as set out in the CCA, a search warrant in terms of the CPA must be obtained.

7.2.4 Each search, access and seizure of a cyber article should be evaluated and done based on the particular circumstances of the case.

7.2.5 In some instances it might be possible to seize, access and copy the cyber article(s) on the scene,[30] and in others the cyber article e.g. the cell phone or computer, will be seized at the scene, sealed, marked and booked into the SAPS13. The analysis of the device e.g. obtaining a copy of the data and computer programs on the device[31] will be done off site.

7.2.6 There are also instances where the cyber article e.g. a big server cannot be seized and booked into evidence. It is imperative to obtain expert assistance from persons that are skilled to deal with these types of scenarios and who can assist to obtain the data and computer programs on the scene. An example of this is where a live forensic acquisition has to be made on the scene because the server/computer cannot be transported from the scene, and if it were powered off, valuable evidence would be lost. The server will not be booked into evidence, only the e.g. hard drive that the copy was made to. The copy becomes the original.

7.2.7 Where a printout of the output of data and computer program is made[32] the printout is also evidence and the integrity thereof should be maintained. By way of example no notes, marks etc can be made on the printout.

7.2.8 In the instance of imaging a cyber article that is in possession of or belongs to a witness, victim or innocent third party the police official will endeavour to follow a process that ensures the least possible intrusion to such a person and proportionate to the acquisition of such evidence.

---

30 All or any of the four actions set out in the definition of seize
31 Part (c) of the definition of seize
32 Part (d) of the definition of seize

7.2.9 When dealing with the search, access and seizure of a cyber article it is also imperative to distinguish between instances when the powers are performed with, or without a warrant.

7.2.10 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.[33] The powers so exercised must always be proportional to the severity of the offence.

7.2.11 The interception of an indirect communication or obtaining real-time communication-related information must still be done in accordance with the provisions of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002.[34] [35]

7.3 Definitions in Chapter 4 of CCA

7.3.1 Chapter 4 of the CCA contains specific definitions namely “access”, “investigator” and “seize”.

7.3.2 The definition of “access” includes certain actions that can be taken for the purpose of searching for, accessing or seizing a cyber article.[36] The police official or investigator can make use of the following to search for a cyber article:

7.3.2.1 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

---

33 Section 36 of the CCA

34 Section 40(1) and (2) of the CCA (once in operation)

35 Once in operation, section 40(3) will impose additional obligations on electronic communications service providers.

36 “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.

7.3.2.2 data or a computer program held in a computer data storage medium or a computer system.

7.3.3 In both instances access will typically include the use of certain software applications and tools that are used by digital forensic investigators to gain access to a cyber article and for example copy the data and computer programs contained on a particular device to an external hard drive.

7.3.4 As with the definition of a cyber article, the definition of "seize" includes four (4) distinctive actions. It is also important to refer to the four actions in the order it is stated in the CCA, as only certain actions can be performed when a search is conducted without a search warrant. [37] Seize includes to:

(a) remove a computer data storage medium or any part of a computer system. Examples include removing the hardware such as a cell phone and properly packaging, transporting and booking it into evidence;

(b) render inaccessible, data, a computer program, a computer data storage medium or any part of a computer system in order to preserve evidence. Examples of actions include depriving the suspect of use of a cell phone and removing the battery or SIM cards. When seizing a desktop computer it can include removing the hard drive;

(c) make and retain a copy of the data or a computer program. Examples are to use forensic tools to copy the data and computer programs from a cell phone; or

(d) make and retain a printout of the output of data or a computer program. Examples include to print out the information that is displayed on the screen/print screen.

[37] In the instances of section 32 and 33 of the CCA

7.4 Preparation for Search, Access or Seizure of a Cyber Article (with or without a Search Warrant)

7.4.1 The planning and preparation for a search and seizure operation for cyber articles is an essential part of any search and seizure operation and should take into account a range of considerations such as the following:[38]

7.4.1.1 **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.

7.4.1.2 **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.

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

7.4.1.4 **Location of article**: Articles may be found at various locations and it is not unusual for data to be hosted in a location other than where the equipment is present e.g. cloud storage or at an offsite data storage warehouse. This may impact on the judicial authority required and the manner in which the search, access or seizure operation must be conducted.

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

7.4.1.6 **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

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

collection of fingerprints or DNA samples during the search, access or seizure operation and to make appropriate arrangements to secure such evidence.

7.4.1.7 **Exhibits other than a cyber article:** The person permitted to conduct the search has to ensure that the seizure of evidence other than a cyber article[39] is carried out in accordance with applicable legislation.[40] A cyber article must be seized in terms of the CCA. Any other article must be seized in terms of other applicable legislation, such as the CPA.

7.4.1.8 **Safety**: Consider the safety of the members of the search team and the scene by making appropriate arrangements.

7.4.1.9 **Securing of cyber article(s) at location:** Appropriate arrangements should be made for securing the cyber article(s) from unnecessary access at the scene and to maintain power to electronic devices. All location access routes need to be secured prior to commencing with the search to mitigate the risk of suspect's discarding/destroying important evidence or leaving the scene.

7.4.2 In completing the procedural requirements, the final objectives of the search must be in compliance with South African law, be appropriate in the particular circumstances of a case, be clear and specific with regards to:

7.4.2.1 The authorisation for the seizure of cyber articles

7.4.2.2 Obtaining forensic copies or printouts ("on-site" or not)

7.4.2.3 Analysis of the devices "on-site"

7.4.2.4 Using or obtaining any instrument, device, equipment, password, decryption key, data, computer program, computer data storage medium or computer system or other information that is necessary to search for, access or seize a cyber article

---

39 As defined in the CCA

40 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.

7.4.3 Where a cyber article is dealt with in terms of Chapter 4 of the CCA and personal information is subsequently processed, section 13(1) of POPIA would be relevant.

8. Execution of Search, Access or Seizure of a Cyber Article

8.1 General Provisions

8.1.1 When conducting a search, the police official must ensure the integrity of all evidence, both traditional and electronic. Potential evidence on cyber articles can be easily altered, modified, deleted, or destroyed. Traditional forensic evidence also has a role to play and is susceptible to cross-contamination.

8.1.2 Digital evidence is highly volatile and the speed of entry to the scene must be considered. It is important that a suspect is prevented from deleting/ wiping/destroying a cyber article at the time of entry and steps should be taken to isolate the suspect from any device which may contain electronic evidence.

8.1.3 Whether cyber articles are searched for, accessed or seized with or without a search warrant, the technical rules for their identification, sealing, transport and subsequent analysis remain the same.

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

8.2 Securing the Scene

8.2.1 In the case of the search, access or seizure of cyber articles, the aim is to avoid the loss, alteration, modification or destruction of any possible evidence.

The following is some of the aspects that can be taken into consideration when securing the scene:

8.2.1.1 Forbid and remove unauthorised persons from the scene.

8.2.1.2 Quickly locate the most obvious cyber articles such as computers and mobile phones, especially those that are connected to the Internet and those that need special assurance measures to prevent data loss.

8.2.1.3 Check the existence of any connections that could allow access and modification of data and/or computer programs from outside.

8.2.1.4 Complete the necessary documentation of the scene, such as noting all sources of electronic evidence that might be the target of seizure, as well as their status and connections. This can include taking photographs or drawing a map of the scene to identify the location of cyber articles.

8.2.1.5 Assess the volatility of electronic evidence that is present at the location in order to take steps to prevent potential loss of critical data which is of temporary nature. It is imperative that volatile electronic evidence be seized first in order to prevent loss of data.

8.2.1.6 Use gloves when handling cyber articles to avoid damaging latent prints and ensure successful collection of fingerprint/DNA evidence, where applicable.

8.2.1.7 A thorough search of the scene can provide other data and information to support the subsequent analysis of cyber articles that may be useful during an investigation, such as searching for written passwords, handwritten notes, hardware and software manuals, calendars or diaries, text or graphical computer printouts, photographs.

8.2.1.8 Any annotation related to the use of passwords, settings, email accounts, etc., as well as in the case of e.g. cellular phones, the SIM cardholders with their Integrated Circuit Card Identification Number (ICCID), original Personal Identification Number (PIN), Personal Unblocking Key (PUK) and any other relevant information will be searched and documented. They can be used in the subsequent analysis of the cyber articles.

8.2.1.9 Refuse any help offered from unauthorised persons in the investigation.

9. Seizure Phase

9.1 Persons Permitted to Search for, Access or Seize a Cyber Article

9.1.1 Only a police official[41] may, in accordance with the provisions of Chapter 4 of the CCA, search for, access or seize any article located within the Republic.[42]

9.1.2 A police official can be assisted by an investigator where so required. If a police official uses an investigator, the person must be identified and authorised to assist with the search, access or seizure of a cyber article. In all instances an investigator assists subject to the direction and control of a police official.[43]

9.1.3 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[44] or during the arrest of a person[45], subject to the written authorisation of such a police official.

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

---

41 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

42 Section 28 of CCA

43 The CCA defines an investigator as any fit and proper person, who is not a member of the SAPS. Such a person must be:
(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 assist the police official with the search for, access or seizure of a cyber article. Such assistance is always rendered subject to the direction and control of a police official.

44 Section 32

45 Section 33

9.1.4.1 When any physical cyber articles[46] are seized, such articles must be handed over to the police official immediately after finalisation of the search and booked into the SAPS13. This also applies where a copy(ies) of the data and/or computer programs are made, or where a printout of the output of data or computer programs is made.

9.1.5 The investigator is subject to the SOPs set out in this document.

9.1.6 As a rule, all seized cyber articles must be booked into the SAPS13. Where a cyber 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, the police official must follow all prescripts of the law to safeguard and store such a cyber article.[47]

9.1.7 Should further investigation be required in relation to such cyber article, the police official must ensure that there is compliance with Chapter 4 of the CCA before the cyber article is accessed.

9.1.8 The police official must furthermore ensure that the public prosecutor is briefed by means of an affidavit, filed in the case docket, on how the cyber article came into the possession of the police official and the subsequent steps followed by the police official to gain access to the cyber article. Where a police official makes use of an investigator, this should also be clearly stated in the affidavit.

9.2 Specific Tools Used in the Search, Access or Seizure of a Cyber Article

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

[46] Part (c) and (d) of the definition of a cyber article
[47] As per the provisions of the CPA

9.3 Actions to Secure a Cyber Article

9.3.1 The CCA provides for the following actions to secure a cyber article:

9.3.1.1 Written application for obtaining a search warrant.[48]

9.3.1.2 Oral application for obtaining a search warrant or amendment to a warrant.[49]

9.3.1.3 Search for, access, or seizure of article without search warrant with the written consent of person who has lawful authority to consent.[50]

9.3.1.4 Search for, access to, or seizure of article involved in the commission of an offence without search warrant.[51]

9.3.1.5 Search for, access to, or seizure of article on arrest of person.[52]

9.3.1.6 Preservation and disclosure of data and evidence.[53]

9.4 Search, Access or Seizure of a Cyber Article with Consent

9.4.1 The CCA provides for the search, access or seizure of article(s) 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.

9.4.2 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.[54]

9.5 Searching with a Warrant: Sections 29 and 30 of the CCA

9.5.1 There is a plethora of factors relating to search and seizure, case law etc that covers the requirements for search warrants.

---

48 Section 29 of CCA
49 Section 30 of CCA
50 Section 31 of CCA
51 Section 32 of CCA
52 Section 33 of CCA
53 Section 40 to 44, and 48 to 51 of the CCA
54 Section 31 of the CCA. See also section 22(a) of the Criminal Procedure Act, No. 51 of 1977

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

9.5.3 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, 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).

9.5.4 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.[55]

9.5.5 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.

9.6 Documents to Complete for a Section 29 Search Warrant

9.6.1 In order to apply for a search warrant in terms of section 29 of the CCA, the applicant must compile the following set of documents:

9.6.1.1 Supporting affidavit of the applicant (this can be used for both application under CCA and CPA where searching for different "articles").

9.6.1.2 Draft search and seizure warrant stating what cyber articles, their location, what type of actions on access/seizure needs to be taken, reference to passwords, access codes etc and other provisions under section 29.

9.6.1.3 First attachment to draft search warrant – List of articles to be seized.

[55] Section 37(2)(a) of the CCA

9.6.1.4 Second attachment to draft search and seizure warrant – List of SAPS officials who may execute the search warrant, which, where applicable, include investigators where such persons will be used during the search, access and seizure.

9.7 Search for, Access, or Seizure of a Cyber Article Involved in the Commission of an Offence Without a Search Warrant

9.7.1 Section 32 of the CCA provides for instances of a search without a warrant in terms of section 29(1)(a) of the CCA.[56] A 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,[57] if such police official on reasonable grounds believes:

9.7.1.1 that a search warrant will be issued under section 29(1)(a) if applied for; and

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

9.7.2 The police official and the investigator (where applicable and where such an investigator is authorised thereto in writing by the police official), can only execute limited powers when conducting a search without a search warrant:

9.7.2.1 It excludes access[58] (save for exclusions set out in paragraph 4.8.3 *infra*);

9.7.2.2 Can only execute the powers provided for in subsection (a) and (b) of the definition of seize[59], namely to:

(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

---

56 See also section 22 (b) of the Criminal Procedure Act, 1977 in this regard.
57 Part (c) and (d) of the definition of an article
58 See the definition of 'access' in the CCA
59 See the definition of “seize” in the CCA

(c) only in relation to a computer data storage medium or any part of a computer system.[60]

9.7.3 A police official would only be authorised to access the data and computer programs contained in the seized cyber article and e.g. make a copy of such data or computer program, by obtaining a search warrant in terms of section 29 of the CCA. A police official or investigator would therefore:

9.7.3.1 Depending on the facts and nature of the case, only be able to *access* and perform the powers referred to in paragraph (c) or (d) of the definition of seize[61] in respect of the computer data storage medium or a computer system without a search warrant if they, on reasonable grounds, believe:

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

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

9.7.4 In terms of paragraph (c) and (d) of the definition of seize the police official or investigator would then be able to:

9.7.4.1 make and retain a copy of data or a computer program; or

9.7.4.2 make and retain a printout of the output of data or a computer program.

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

9.8 Search, Access or Seizure of a Cyber Article on Arrest of a Person

9.8.1 As contemplated in section 40 of the CPA, a police official may arrest any person without a warrant.

---

60 Part (c) and (d) of the definition of *article.* Part (a) data and (b) computer programs are excluded.

61 As defined in section 25 of the CCA

9.8.2 Section 33 of the CCA sets out the conditions for search, access or seizure of a cyber article when a person:

9.8.2.1 commits any offence in terms of Part I or Part II of Chapter 2 of the CCA in the presence of a police official;

9.8.2.2 whom the police official reasonably suspects of having committed any offence in terms of Part I and part II of Chapter 2; or

9.8.2.3 where it relates to an offence that has been committed in a foreign state, such person is concerned with or against whom a reasonable complaint has been made, or credible information has been received, or a reasonable suspicion exists that they have been concerned with an offence which is:

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

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

9.8.3 An investigator who is authorised in writing by a police official, may assist the police official to seize a cyber article as contemplated subsections 33(2) and 33(3) and to access the article in exceptional circumstances (as contemplated in subsection 33(3)).

9.8.4 Section 33(2) of the CCA provides that, where a person is arrested as contemplated in subsection 33(1) of the CCA, or arrested in terms of section 40[62] or 43[63] of the CPA, a police official or investigator may only search for and perform the powers provided for in subsection (a) and (b) of the definition of "seize";[64]

9.8.4.1 It excludes access[65] (save for circumstances a set out in paragraph 9.8.6 *infra*);

---

62 Section 40 of the CPA: Arrest by peace officer without warrant

63 Section 43 of CPA: Warrant of arrest may be issued by magistrate or justice

64 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.

65 See the definition of "access" in the CCA

9.8.4.2 Only in relation to a computer data storage medium or any part of a computer system[66]; and

9.8.4.3 Where the computer data storage medium or any part of a computer system is found in the possession of, in the custody or under the control of the person.

9.8.5 As a rule a police official or investigator that has seized a computer data storage medium or computer system without a warrant, would first have to obtain a search warrant in terms of section 29(1)(a) of the CCA, before the police official may access or perform the powers referred to in paragraph (c) or (d) of the definition of "seize". By way of example the police official would not be able to access the data and computer programs on a cell phone to make a copy thereof, before obtaining a search warrant in terms of section 29(1)(a).

9.8.6 Where urgency or exceptional circumstances exists in the case, 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 the police official on reasonable grounds believes:

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

9.8.6.2 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.[67]

9.8.7 In terms of paragraph (c) and (d) of the definition of seize the police official or investigator would then be able to:

9.8.7.1 make and retain a copy of data or a computer program; or

9.8.7.2 make and retain a printout of the output of data or a computer program.

---

66 Part (c) and (d) of the definition of article in the CCA. Part (a) data and (b) computer programs are excluded.

67 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.

10. Packaging, Transportation and Storage of Cyber Articles

10.1 Securing a Cyber Article

10.1.1 Certain types of cyber articles are fragile and are sensitive to temperature, humidity, physical shock, static electricity, magnetic sources and some operational functions, such as power interruptions. Special precautions should be taken when packaging, transporting and storing such cyber articles. To maintain the chain of custody the packaging, transportation and storage should be recorded. Any change of custody or condition of the seized articles should also be timed and recorded.[68]

10.1.2 The chain of custody must be recorded in an affidavit.

10.1.3 If the cyber article is damaged, this should be documented and recorded e.g. a cracked display monitor on a laptop.

10.1.4 Note the location and circumstances where the cyber articles were found on the scene e.g. was the cyber article concealed, found with all the other articles or other types of evidence, etc.

10.1.5 The principle is to limit interaction with a cyber article. Inexpert handling can cause damage or the destruction of a cyber article, which in turn can influence the integrity, reliability and eventual admissibility of such evidence in a court of law. Police officials and investigators have to ensure that they take the necessary precautions to ensure that cyber articles are securely packaged, transported and stored.

[68] The chain of custody is defined in ISO 27037 as a document or series of related documents that details the chain of custody and records who was responsible for handling potential digital evidence, either in the form of digital data or other formats (such as paper notes). The purpose of maintaining a chain of custody record is to enable the identification of access and movement of potential digital evidence at any given point in time.

10.2 Packaging

10.2.1 Ensure that all collected cyber articles are properly secured, documented and labelled before packaging it.

10.2.2 Whenever possible, transport the collected cyber articles in the original packaging.

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

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

10.2.5 Do not affix any mark the cyber article itself, such as affixing an adhesive label on the surface of the computer data storage medium or any part of a computer system. Depending on the size and nature of the cyber article and the prevailing circumstances, the cyber article must be placed in an evidence bag upon seizure or as soon as possible thereafter. Ensure that all evidence bags containing evidence are properly labelled.

10.2.6 If multiple cyber articles are seized, the evidence bag must be sealed and labelled. Where appropriate and in instances where multiple cyber articles are packed and sealed in one bag, a detailed inventory should be included in the evidence bag.

10.2.7 Leave cellular, mobile, or smart phone(s) in the power state (on or off) in which they were found, unless otherwise directed by a digital forensic specialist.

10.3 Transportation

10.3.1 The police official should make use of an official vehicle to transport cyber articles. Where no appropriate official vehicle is available, the use of another vehicle must be authorised and documented.

10.3.2 Cyber articles should be packed and transported in such a way that it does not damage any of the cyber articles.

10.3.3 Where practically possible, refrain from storing cyber articles in vehicles for extended periods of time.

10.3.4 Document the transportation of the cyber article(s) from the scene to the SAPS storage facility and maintain the chain of custody for all evidence transported.

10.4 Storage

10.4.1 Cyber articles must be booked into the SAPS13 register and the police official must ensure that the cyber article is inventoried.

10.4.2 All cyber articles seized under the provisions of the CCA must be given a distinctive identification mark and be retained in police custody, or the police official must make such other arrangements with regard to the custody thereof as prevailing circumstances may require.[69]

10.4.3 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.

10.4.4 The storeroom must be secure and provide for the storage of cyber articles in a way that maintains its integrity.

[69] See Section 30(c) of the Criminal Procedure Act, 1977

11. Investigation of a Cyber Article that was Searched for, Accessed or Seized and Booked into Evidence

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

11.2 When investigating a cyber 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 of the CCA.

11.3 Once the process of investigation has been completed, the cyber article must be resealed and re-packaged. The cyber 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.

11.4 Where the copying of data and computer programs, and/or obtaining a printout[70] has been performed by an investigator: Both police officials and investigators must at all times apply adequate safeguards in relation to the cyber articles as it might contain personal information (as defined in POPIA), as well as to ensure compliance with section 39 of the CCA.[71]

11.5 Where an investigator has performed the actions under (c) and (d) of the definition of seize, any and all cyber articles should be returned to the police official.

11.6 When performing digital forensic processes such as copying data from a cyber article, the rule is that an independent third party should not only be able to

[70] Actions in the actions in (c) or (d) of the definition of seize

[71] In terms of POPIA, SAPS or any other person or agency investigating criminal offences should ensure adequate safety measures for the protection of personal information. This should be read with section 39 of the CCA.

repeat the same actions the digital forensic investigator performed, but also be able to achieve the same result.

11.7 The provisions of the CPA apply to the subsequent handling of the cyber article for availability in court proceedings, as well as to the disposal of a cyber article.[72]

12. Preservation and Disclosure Provisions

12.1 The CCA contains new procedures for the preservation and disclosure of data and other cyber articles. The provisions are not in operation yet. Preservation allows for a process where data or other cyber articles will be preserved i.e. the data or other cyber article is kept subject to circumstances that will ensure that the integrity of the evidence is maintained. There is also a process for the expedited preservation of data.

12.2 Preservation is always done with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence in question.

12.3 When a cyber article is preserved, it is not handed over to a police official: it 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.

12.4 In terms of section 41 of the CCA a specifically designated police official may, subject to certain conditions as set out in sections 41(1) and (2),[73] issue an

---

[72] See also section 37(2)(a)(ii) of the CCA, which deals with the disposal of articles seized in terms of the CCA.

[73] 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.

expedited preservation of data direction to a person, electronic communications service provider[74] or financial institution.[75]

12.5 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.[76]

12.6 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.[77]

12.7 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.[78] The process is once again aimed at preserving the availability and integrity of the cyber article in question.

12.8 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:

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

---

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

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

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

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

78 Section 42 and 43 of the CCA

12.8.2 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.

12.9 Any cyber 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).

12.10 A police official may, at any time, apply for a search warrant in terms of section 29(1) to search for, access or seize a cyber article (which includes data) that is or was subject to an expedited preservation of data direction or a preservation of evidence direction.[79]

13. Salient Points on the Investigation, Search, Access or Seizure of a Cyber Article

13.1 Police officials must determine which the correct legal instrument(s) is to use in a particular scenario. It is important to distinguish between using a search warrant and a section 205 subpoena in terms of the CPA. For example, section 205 of the CPA will still be used to obtain information such as banking and cell phone records.

13.2 Searching with Consent

13.2.1 When searching, accessing or seizing a cyber article with consent, the effect of performing such powers is the same as if a search warrant in terms of section 29 had been obtained.[80] Where the police official makes use of an investigator, the police official needs to obtain written consent from a

[79] Section 44(9) of the CCA
[80] Section 31 of the CCA

person who is in a position to give lawful consent, for an investigator to take part in such a search.

13.2.2 Although a police official can ask for assistance from persons at the premises that needs to be searched, this should never include asking assistance from a person that is a possible suspect.[81]

13.2.3 Police officials and investigators must always conduct search operations in an orderly and decent manner with respect to the parties concerned.[82]

13.2.4 Where cyber articles have to be obtained from third parties or witnesses, the first point of call should be to obtain such a cyber article with consent. It is only when no consent is given that a legal instrument such as a search warrant should be used.

13.3 When the Search, Access or Seizure Takes Place with a Search Warrant in terms of the CCA[83]

13.3.1 Police officials and other persons or agencies bound by the SOPs should always ensure that their actions are aimed at preserving the integrity, reliability and authenticity of the evidence, so as to provide for the admissibility of such evidence in a court of law.

13.3.2 Police officials should plan for each search operation, depending on the particular circumstances of the case. It might not always be possible to do so, in for example cases of urgency.

13.3.3 The chain of custody must be preserved and all steps and actions taken when executing the search, access or seizure of a cyber article, must be documented. These type of documents are of significant importance in the subsequent court trial where e.g. it must be proven that the particular evidence is reliable and had not been tampered with.

---

81 Section 34 of the CCA
82 Section 36 of the CCA
83 Sections 29 and 30 of the CCA

13.3.4 Search warrants should be carefully drafted, utilising the applicable legislation.

13.4 Searching Without a Warrant and on Arrest[84]

13.4.1 **The layby principle**: In South Africa the principle of layby is well-known. It is an agreement whereby a person requests that the retailer remove the item from the floor and that it be kept in safekeeping until such time as a person has paid in full for the item. The item will only be handed to the purchaser once full payment had been received. The same principle is useful when understanding the practical implications of searching without a warrant, or in instances where a cyber article is preserved[85]:

13.4.1.1 Thus just as with a layby agreement, the data and computer programs contained in the cyber article can only be accessed with a warrant in terms of section 29 of the CCA. Where the cyber article has been preserved, the police official will only be placed in possession thereof after the appropriate legal instrument has been served on the party concerned. [86]

13.4.1.2 By way of example: A police official will only be able to seize the computer data storage medium or computer system[87] such as a cell phone, computer or memory stick of the suspect. The police official can therefore not perform all four (4) actions contained in the definition of "seize", but only those in (a) and (b) of the definition of "seize" that deal with securing the (physical) cyber article. Part (c) and (d) of the definition involves actions that require access to the data and computer programs contained on a device e.g. a cell phone. For this a police official would require a search warrant in terms of section 29 of the CCA.

---

84 Sections 32 and 33 of the CCA
85 Sections 41 to 44 of the CCA
86 Or where applicable, a disclosure of data direction has been obtained.
87 Part (c) and (d) of the definition of article in the CCA. It can conveniently be referred to as the hardware

13.4.2 There are, however, exceptions: Both sections 32 and 33 of the CCA provide for urgent cases and exceptional circumstances where it would be possible for a police official or investigator to access the data and computer programs on the seized cyber article without having obtained a search warrant. Note that what is urgent or exceptional circumstances will vary from case to case. Besides having reasonable grounds for believing that a search warrant would have been issued if the police official had applied for it, the police official must also be able to motivate that it was not reasonably practical as a result of urgency, to approach the court for a search warrant[88], as well as that the police official could not make an oral application for a warrant.

14. Publicly Available Data

14.1 A police official does not need to be specifically authorised in terms of the CCA to obtain publicly available data[89] 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, a cyber article.[90]

14.2 Examples is the use of data that is available on the internet, dark web, deep web and which can be obtained without having to overcome any restriction.[91]

---

88 In terms of section 29 of e CCA

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

90 It is important to note that POPIA only applies to the processing of personal information. If the information being processed is not of a personal in nature, then POPIA does not apply.

91 In respect of non-publicly available data, regard should be had to section 12(2)(d)(i) of POPIA. This particular section indicates that personal information need not be collected directly from the data subject, if the collection of the information from another source is necessary to avoid prejudice to the maintenance of the law by any public body, including the investigation, prosecution and punishment of offences. The personal information must be kept confidential and retain its integrity, as per section 19(1) of POPIA. Section 13(1) indicates that the personal information must be collected for a specific purpose. This must be read in conjunction with section 18(4)(c)(i), which says that the responsible party (for example the SAPS) do not have to inform the data subject when collecting personal information, if it is to avoid prejudice to the maintenance of the law by any public body, which includes the investigation, prosecution and punishment of offences.

14.3 A police official can also receive and use non-publicly available data where the data is disclosed to the police official by a person who is in control of, or in possession of the data. Such disclosure must be voluntarily and on such conditions regarding confidentiality and limitation of use which they deem necessary.

14.4 It does not matter where the data is geographically located.[92]

15. Pornographic Images of Children and Other Classified Information

15.1 A person performing a digital forensic investigation must always be cognisant of any legal impediments that could play a role during the process of seizing a cyber article in terms of the CCA.

15.2 Where a cyber article is recovered which contains pornographic images[93] of children or other sensitive evidence, special care must be taken to restrict access to such evidence in order to e.g. prevent secondary victimisation of the

---

92 Section 45(2) of the CCA

93 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.

victims and/or other 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.

15.3 A digital forensic examiner dealing with pornographic images of children and classified information must ensure that:

15.3.1 access to evidence is strictly controlled and managed;

15.3.2 all evidence are exported as required and encrypted before it is handed over; and

15.3.3 items are sealed in an appropriate container, clearly marked that unauthorised access to the evidence is prohibited.

16. Data Held by Third Parties and Independent Data Holders

16.1 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 difficult to access without the cooperation and assistance of the relevant third party.

16.2 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.

16.3 In certain instances some, or even all of a company's network resources will be managed by external companies and hosted in remote locations. In such cases the cooperation of the remote system administrator can be invaluable. The administrator's cooperation is only needed for information about the infrastructure and to grant access rights to certain areas of a server, workstation or software functions. A big company might also have e-discovery solutions in place.

16.4 By way of example: It is practice for police officials to approach third parties that have CCTV footage of a crime that took place. In instances where evidence such as the CCTV footage has to be obtained from persons other than the person(s) suspected of committing the offence under investigation, police officials should endeavour to first obtain such evidence by means of consent. Where no consent is granted, the police official can seize the evidence using a legal instrument such as a search warrant.

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

16.6 Once in operation, section 54 of the CCA will provide that 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:

16.6.1 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

16.6.2 preserve any information which may be of assistance to the South African Police Service in investigating the offence.

17. Cloud Service Providers

17.1 Cloud services and online storage is a topic that has become of significant importance. Cloud services are able to replace almost every part of a company's IT infrastructure, such as software applications and even employee workstations.

17.2 Instances may arise where cloud service (electronic communication service) providers will be required to preserve or disclose data.

17.3 A police official should endeavour to obtain data and computer programs which are stored in the cloud by means of a search warrant, unless in instances where there are exceptional circumstances present that warrant access to data and computer programs without a search warrant. Access to cloud data can also be obtained with consent, which is preferred where access is sought from an innocent third party. Where such efforts are not successful, the police official can proceed to obtain such data from the electronic communications service provider by means of a search warrant. Any business records, such as the client and account details should be obtained using a section 205 subpoena in terms of the CPA.

18. Evidence

18.1 Once the digital forensic analysis of a cyber article has been completed, there must be a report[94] which should contain *inter alia* a description of the operations conducted, the tools used and the results obtained.

18.2 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.[95] It relates to any fact established by any examination or process requiring any skill in:

18.2.1 the interpretation of data;

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

18.2.3 computer science;

[94] As provided for in section 53 of the CCA
[95] See section 53(1) for the relevant fields of study

18.2.4 electronic communications networks and technology;

18.2.5 software engineering; or

18.2.6 computer programming.

18.3 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.

18.4 Section 53 furthermore provides guidelines on the content of the affidavit or solemn attestation.[96]

18.5 In certain circumstances the court may require that oral evidence be given in relation to the affidavit or solemn or attested declaration.[97] [98]

18.6 Admissibility and Evidential Weight relating to Cyber Articles

18.6.1 The intangible nature of data messages makes it much easier to manipulate and more prone to alteration than traditional forms of evidence. This has created special challenges for the justice system which requires that such data be handled in a specific manner to ensure the reliability and integrity of the evidence it provides.[99]

18.6.2 There is a common misconception that the CCA repealed the Electronic Communications and Transactions Act, No 25 of 2002 (ECT Act) in totality.[100] Within the context of the SOPs, the ECT Act still *inter alia* provides for the legal recognition, as well as the admissibility and evidential weight of data messages. [101]

---

96 Section 53(1)(i)

97 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.

98 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.

99 The court will then inter alia use the provisions of section 15(3) of the ECT Act to consider the evidential weight of the data messages.

100 Only sections 85, 86, 87 and 88 of the ECT Act were deleted and there was a substitution of section 89.

101 Note the different definitions of data message in the ECT and CCA respectively

18.6.3 In terms of section 15 of the ECT Act the factors to consider when assessing the evidential weight of data messages are:

18.6.3.1 The reliability of the manner in which the data message was generated, stored or communicated;[102]

18.6.3.2 the reliability of the manner in which the integrity of the data message was maintained;[103]

18.6.3.3 the manner in which its originator was identified.[104] This would also include the concept of non-repudiation which indicates a measure of assurance that the originator of the data/message/electronic evidence is in fact the originator;[105] and

18.6.3.4 any other relevant factor.[106]

18.6.4 Such other relevant factors to consider can include:

18.6.4.1 **Authenticity**: The evidence must establish facts in a way that cannot be disputed and is representative of its original state.

18.6.4.2 **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.

18.6.4.3 **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).

---

102 Section 15(3)(a) of ECT Act
103 Section 15(3)(b) of ECT Act
104 Section 15(3)(c) of ECT Act
105 NIST defines non-repudiation as assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
106 See in this regard case law such as S v Brown 2016 (1) SACR 206 (WCC); Ndlovu v Minister of Correctional Services 2006 4 All SA 165 (W) 172

19. Prohibition on the Disclosure of Information

19.1 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 a cyber article and any activities relating to mutual assistance.

19.2 Section 39 does, however, contain exceptions[107] 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.[108] The exceptions include:

19.2.1 Where the information is required for the performance of functions in terms of the CCA;

19.2.2 If a person has to supply such information in the performance of their duties or functions in terms of the CCA;

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

19.2.4 Information-sharing between electronic communications service providers, financial institutions, the SAPS, competent authorities or any other person or entity which is aimed at preventing, detecting, investigating or mitigating cybercrime, is also allowed. The information-sharing may, however, not prejudice any criminal investigation or proceedings; or

19.2.5 Disclosure to any competent authority in a foreign State which requires it for the prevention, detection, or mitigation of cybercrime, or the institution

---

107 Subsection 39(2) of the CCA

108 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.

of criminal proceedings or where they are conducting an investigation with a view to institute criminal proceedings.

19.3 Sharing of information must always be duly authorised and be done subject to such conditions regarding confidentiality and limitation.[109]

20. Disposal of a Cyber Article

20.1 As the CCA does not contain provisions on the disposal of cyber articles, the provisions of the CPA will apply.[110]

20.2 A police official should as soon as practically possible, with due consideration to the investigation and in consultation with the prosecutor, return a seized cyber article to the person from whom it was seized, provided such person may lawfully possess such a cyber article.[111]

20.3 Section 30, read with section 20 of the CPA provide for steps that a police official must take in relation to the disposal of a cyber article after it has been seized and the same will apply to a cyber article.

20.4 In terms of section 30(c) of the CPA, if the cyber 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 such other arrangements must be made with regard to the custody thereof as the circumstances may require.

20.5 Where no criminal proceedings are instituted or where the cyber article is not required for criminal proceedings, the provisions of section 31 of the CPA should be applied.

---

109 See also the provisions of section 47 of the CCA

110 Section 27 of the CCA. Sections 30 to 36 of the CPA provide for the disposal of an article as defined in that Act.

111 When disposing of an article that contains personal information, due regard be given to the provisions of section 14 of POPIA.

20.6 Where criminal proceedings are instituted and an admission of guilt fine is paid the disposal of the cyber article is governed by the provisions of section 32 of the CPA.

20.7 If criminal proceedings are instituted in connection with any cyber article referred to in section 30(c) of the CPA and such cyber 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 cyber article to the clerk of the court where the criminal proceedings are instituted.[112]

20.8 Section 33(2) and 33(3) of the CPA furthermore provide for measures where the cyber article cannot be handed in at the clerk of the court or where the cyber article has to be transferred to another court.

20.9 When criminal proceedings are concluded, the presiding judge or judicial officer must make an order on how to deal with a cyber article that had been presented as evidence in such proceedings or had been used for purposes of an order of court.[113]

20.10 A cyber article can also be forfeited to the State.[114]

20.11 Where a cyber article is concerned in an offence committed outside Republic, the disposal of such cyber article is governed by the provisions of section 36 of the CPA.

20.12 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.[115]

---

[112] Section 33(1) of the CPA
[113] See section 34 of the CPA in this regard.
[114] See section 35 of the CPA in this regard.
[115] Section 37(2)(a)(i) of the CCA

20.13 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:

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

20.13.2 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

20.13.3 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.

21. Offences in the CCA that relate to the Investigation, Search, Access or Seizure of a Cyber Article

21.1 It is a criminal offence for an electronic communications service provider, financial institution or person to not provide technical or other assistance as may be reasonably necessary 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.[116]

21.2 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.[117] 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.

[116] Section 34 of the CCA
[117] Section 35 of the CCA

21.3 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.[118] Where a police official is on reasonable grounds of the opinion that that a cyber article which is the subject of the search may be destroyed, disposed of or tampered with, the police official would not have to audibly demand admission.

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

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

21.4.2 consent granted in terms of section 31(1).[119]

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

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

21.5.2 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.[120]

21.6 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).

21.7 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 two (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.

---

[118] Section 35(2)(b) of the CCA
[119] Section 37(1)(a) of the CCA
[120] Section 37(1)(b) of the CCA

21.8 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:

21.8.1 a search warrant being issued;

21.8.2 a search with consent taking place on the basis of such information;

21.8.3 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;

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

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

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

21.9 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 (2) years or to both such fine and imprisonment. The Court may furthermore make a compensation order in terms of section 300 of the CPA.

21.10 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.[121]

21.11 In terms of section 41 a person, electronic communications service provider or financial institution commits a criminal offence in the following

[121] Section 39(3) of the CCA

circumstances, and would be liable on conviction to a fine or imprisonment for a period not exceeding two (2) years or to both a fine and such imprisonment:

21.11.1 Failing to comply with an expedited preservation of data direction; or

21.11.2 Disclosing data to a police official on the strength of an expedited preservation of data direction.

21.11.3 Making a false statement in an application to amend or cancel the direction.

21.12 In terms of section 44 it is a criminal offence for a person, electronic communications service provider or a financial institution to:

21.12.1 Fail to comply with a disclosure of data direction;

21.12.2 Make a false statement in an application referred to cancel or amend a disclosure of data direction; or

21.12.3 Fail to make the data and an affidavit available to a police official.

21.13 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.

21.14 In terms of section 49(4) it is a criminal offence for a person, electronic communications service provider or financial institution to:

21.14.1 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

21.14.2 Make a false statement in an application to cancel or amend an order in terms of section 48.

21.15 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.

21.16 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.

21.17 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.[122]

22. The Designated Point of Contact

22.1 Once in operation, the CCA will provide for the creation of a Designated Point of Contact (DPoC) within SAPS structures.[123]

22.2 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:

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

22.2.2 any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of a cyber article; or

22.2.3 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 a cyber article.

22.3 The assistance which will be provided by the DPoC includes the following:

22.3.1 Provision of technical advice and assistance;

[122] Section 53(3) of the CCA
[123] Section 52 of the CCA

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

22.3.3 Provision of legal assistance;

22.3.4 Identification and location of a cyber article;

22.3.5 Identification and location of a suspect; and

22.3.6 Cooperation with appropriate authorities of a foreign State.

22.4 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.

23. Glossary of Terms

Abbreviation/Term	Explanation
Chain of Custody	The chain of custody is defined in ISO 27037 as a document or series of related documents that details the chain of custody and records who was responsible for handling potential digital evidence, either in the form of digital data or other formats (such as paper notes). The purpose of maintaining a chain of custody record is to enable the identification of access and movement of potential digital evidence at any given point in time
Cloud Service Provider	A cloud service provider is an information technology (IT) company that provides its customers with computing resources over the internet and delivers them on-demand (www.technopedia.com)
Cyber-Dependent Crime	Cyber-dependent crimes (or 'pure' cybercrimes) are offences that can only be committed using a computer, computer networks or other form of information communications technology (ICT). Cyber-dependent crime is often typified as the creation, dissemination and deployment of malware, ransomware, attacks on critical national infrastructure (e.g. the cyber-takeover of a power-plant by an organised crime group) and taking a website offline by overloading it with data (a DDOS attack).
Cyber-Enabled Crime	Cyber-enabled crimes are traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT). It is crimes that can occur in the offline world, but can also be facilitated by ICT. This typically includes cyber frauds, cyber forgery and uttering and cyber extortion.
Data Subject (POPIA)	The person to whom personal information relates.
Digital Forensics	Also called Computer Forensics. A branch of forensic science related to the acquisition, processing, analysis and reporting of evidence that is stored on computer systems, digital devices and other storage media with the aim of admissibility in court. In its strictest connotation, it can also be defined as 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.

Abbreviation/Term	Explanation
	A digital or computer forensic specialist is a person who performs the activities listed above.
Electronic /digital Evidence	Digital or electronic evidence is information generated, stored or transmitted using electronic devices that may be relied upon in court. To guarantee that the evidence is accepted in court, it is necessary to obtain the information following very well defined processes using specialised personnel and operating within an adequate legal framework.
Electronic Communications Service (Cybercrimes Act)	Means any service which consists wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services as defined in section 1 of the Electronic Communications Act, 2005.
Electronic Communications Service Provider (CCA)	a) any person who provides an electronic communications service to the public, sections of the public, the State, or the subscribers to such service, under and in accordance with an electronic communications service licence issued to that person in terms of the Electronic Communications Act, 2005, or who is deemed to be licenced or exempted from being licenced as such in terms of that Act; and b) a person who has lawful authority to control the operation or use of a private electronic communications network used primarily for providing electronic communications services for the owner's own use and which is exempted from being licensed in terms of the Electronic Communications Act, 2005
Financial Institution	In terms of the CCA a financial institution bears the same meaning as the definition in section 1 of the Financial Sector Regulation Act, No 9 of 2017. It would thus mean any of the following, other than a representative: a) a financial product provider; b) a financial service provider; c) a market infrastructure; d) a holding company of a financial conglomerate; or e) a person licensed or required to be licensed in terms of a financial sector law
Internet Service Provider (ISP)	An organisation that provides access to the Internet. Internet service providers can be either community-owned and non-profit, or privately owned and for-profit.
Operator (POPIA)	A person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party'.

Abbreviation/Term	Explanation
Person (CCA)	A natural or a juristic person
Publicly Available Data (CCA)	Data which is accessible in the public domain without restriction.
Responsible Party (POPIA)	The public or private body or any other person, which alone or in conjunction with others, determines the purpose of and means for processing personal information'.

24. Bibliography

24.1 CoE: Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors And Judges

24.2 ACPO Good Practice Guide for Digital Evidence, March 2012

24.3 Interpol: Guidelines for Digital Forensics First Responders, March 2021

24.4 Cybercrime Programme Office of the Council of Europe: Standard Operating Procedures for the collection, analysis and presentation of electronic evidence

24.5 UK College of Policing, Authorised Professional Practice Extraction of material from digital devices, May 2021

Annexure A: Comparison of Provisions relating to Search and Seizure in the Criminal Procedure and Cybercrimes Acts

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

The Criminal Procedure Act, No 51 of 1977	The Cybercrimes Act, No 19 of 2020
commission of an offence, whether within the Republic or elsewhere; or (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.	
An article is defined as “anything”	Section 1(1) In this Act, unless the context indicates otherwise- **'Article'** means any- (a) data; (b) computer program; (c) computer data storage medium; or (d) computer system, which- (i) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission; (ii) may afford evidence of the commission or suspected commission; or (iii) is intended to be used or is, on reasonable grounds believed to be intended to be used in the commission or intended commission, of- (aa) an offence in terms of Part I and Part II of Chapter 2;

The Criminal Procedure Act, No 51 of 1977	The Cybercrimes Act, No 19 of 2020
	(bb) any other offence in terms of the law of the Republic; or (cc) an offence in a foreign State that is substantially similar to an offence contemplated in Part I or Part II of Chapter 2 or another offence recognised in the Republic
Jurisdiction of court to issue search warrant: Section 21(1): Subject to the provisions of sections 22, 24 and 25, an article referred to in section 20 shall be seized only by virtue of a search warrant issued- (a) by a magistrate or justice, if it appears to such magistrate or justice from information on oath that there are reasonable grounds for believing that any such article is in the possession or under the control of or upon any person or upon or at any premises within his area of jurisdiction; or (b) by a judge or judicial officer presiding at criminal proceedings, if it appears to such judge or judicial officer that any such article in the	**Jurisdiction of court to issue search warrant:** Section 29(1): Subject to the provisions of sections 31, 32, 33 and 40 (1) and (2) of this Act, section 4 (3) of the Customs and Excise Act, 1964, sections 69 (2) (b) and 71 of the Tax Administration Act, 2011, and section 21 (e) and (f) of the Customs Control Act, 2014, an article can only be searched for, accessed or seized by virtue of a search warrant issued: (a) by a magistrate or judge of the High Court, on written application by a police official, if it appears to the magistrate or judge, from information on oath or by way of affirmation, as set out in the application, that there are reasonable grounds for believing that an article-

The Criminal Procedure Act, No 51 of 1977	The Cybercrimes Act, No 19 of 2020
possession or under the control of any person or upon or at any premises is required in evidence at such proceedings.	(i) is within their area of jurisdiction; or (ii) is being used or is involved or has been used or was involved in the commission of an offence- (aa) within their area of jurisdiction; or (bb) within the Republic, if it is unsure within which area of jurisdiction the article is being used or is involved or has been used or was involved in the commission of an offence; or (b) by a magistrate or judge of the High Court presiding at criminal proceedings, if it appears to such magistrate or judge that an article is required in evidence at such proceedings.
Provisions relating to what a police official is authorised to do in terms of a search warrant is set out in section 21, but differ from that set out in section 29 of the CCA	Provisions relating to what a police official is authorised to do in terms of a search warrant as set out in section 29 is more comprehensive than the provisions in the CPA.
Section 21(4): A police official executing a warrant under this section or section 25 shall, after such execution, upon demand of any person whose rights in respect of any search or article seized	Section 29(5): A police official who executes a warrant under this section must hand to any person whose rights in respect of any search, or article accessed or seized under the warrant

The Criminal Procedure Act, No 51 of 1977	The Cybercrimes Act, No 19 of 2020
under the warrant have been affected, hand to him a copy of the warrant.	have been affected, a copy of the warrant and the written application of the police official contemplated in subsection (1) (a).
No provision for oral application for a search warrant by specifically designated police official	Section 30 provides for an oral application for a search warrant or amendment thereof by a specifically designated police official
No limitations specified as to what actions can be taken in respect of an article that is searched and seized without a warrant or during arrest	Limitation of what actions can be performed in relation to an article when it is searched, accessed or seized without a search warrant or during arrest.
There is no definition of " seize" in the CPA	"**Seize**" includes to: (a) remove a computer data storage medium or any part of a computer system; (b) render inaccessible, data, a computer program, a computer data storage medium or any part of a computer system in order to preserve evidence; (c) make and retain a copy of data or a computer program; or (d) make and retain a printout of the output of data or a computer program.

The Criminal Procedure Act, No 51 of 1977	The Cybercrimes Act, No 19 of 2020
Access is not defined in the CPA	For purposes of Chapter 4: "**Access**" includes without limitation to make use of: (a) a computer data storage medium, or a computer system, or their accessories and components or any part thereof or any ancillary device or component thereto; and (b) data or a computer program held in a computer data storage medium or a computer system, to the extent necessary to search for and seize an article;
There is no definition in the CPA for "investigator"	"**Investigator**" means any fit and proper person, who is not a member of the South African Police Service and who is: (a) identified and authorised in terms of a search warrant as contemplated in section 29(3); or (b) requested by a police official in terms of section 31(2), 32(3) or 33(4), to, subject to the direction and control of a police official, assist the police official with the search for, access or seizure of an article;
There is no definition of "access" in the CPA	"**Access**" includes without limitation to make use of- (a) a computer data storage medium, or a computer system, or their

The Criminal Procedure Act, No 51 of 1977	The Cybercrimes Act, No 19 of 2020
	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
There is no definition of "seize" in the CPA	"**Seize**" includes to- (a) remove a computer data storage medium or any part of a computer system; (b) render inaccessible, data, a computer program, a computer data storage medium or any part of a computer system in order to preserve evidence; (c) make and retain a copy of data or a computer program; or (d) make and retain a printout of the output of data or a computer program.
Contains provisions relating to the disposal of an article	The CCA contains no provisions relating to the disposal of an article and the provisions of the CPA would thus apply
'peace officer' includes any magistrate, justice, police official, correctional official as defined in section 1 of the Correctional Services Act, 1959 (Act 8 of 1959), and, in relation to any area, offence, class of offence or power	CCA contains no reference to a "peace officer"

The Criminal Procedure Act, No 51 of 1977	The Cybercrimes Act, No 19 of 2020
referred to in a notice issued under section 334 (1), any person who is a peace officer under that section	
Contains no provisions relating to the preservation and disclosure of an article	CCA contains specific provisions relating to the preservation and disclosure of a cyber article
Contains no provision for Standard Operating Procedures relating to the search, access and seizure of articles	Section 26 provides for Standard Operating Procedures