THE SEARCH WARRANT PROVISIONS OF THE CYBERCRIMES ACT AND THEIR RELATIONSHIP WITH THE CRIMINAL PROCEDURE ACT

Pieter du Toit
Blur LLB LLM LLD
Faculty of Law, North-West University

SUMMARY

The recently enacted Cybercrimes Act 19 of 2020 regulates the powers of the police and investigators to investigate cybercrimes. Chapter 4 of the Act provides for the powers of the police and others in respect of search, access or seizure in the investigation of cybercrimes and other offences committed by means of cybertechnology. The provisions of the Criminal Procedure Act 51 of 1977 will continue to operate in addition to the provisions of the Cybercrimes Act, to the extent that the Criminal Procedure Act is not inconsistent with the Cybercrimes Act. The search and seizure provisions of the Criminal Procedure Act are object-based, as they do not deal explicitly with the specialised procedures that are required to investigate cybercrimes or other offences that involve the use of digital devices. The Cybercrimes Act attempts to address this shortcoming. The coexistence of the search and seizure provisions in these two Acts may cause difficulties in the fight against crime. In addition to the validity requirements of search warrants, as set out in the Acts, additional intelligibility requirements for the validity of search warrants have been developed by the courts.

1 INTRODUCTION

Section 14 of the Constitution of the Republic of South Africa of 1996 (the Constitution) guarantees the right to privacy. The first part of section 14 guarantees a general right to privacy, while the second part protects against the search and seizure of someone's person, property or possessions, and against infringements of communications.[1] The lawfulness of a search and seizure operation in the course of a criminal investigation is dependent on the citizen's legitimate expectation of privacy, as privacy extends "*a fortiori* only to those aspects in regard to which a legitimate expectation of privacy

[1] Currie and De Waal *The Bill of Rights Handbook* 6ed (2013) 294.

can be harboured".[2] It is a general principle of our law that a search and seizure operation may only be conducted on authority of a search and seizure warrant. The Constitutional Court has held that a search warrant is a mechanism employed to balance an individual's right to privacy with the public interest. A search warrant governs the time, place and scope of the search. This, the court held, "softens the intrusion on the right to privacy, guides the conduct of the inspection, and informs the individual of the legality and limits of the search".[3] The failure of the police or other law enforcement agencies to obtain a search warrant in circumstances where no swift action is required, and sufficient time is available to obtain such a warrant, will typically render a warrantless search illegal.[4] The informed consent of the person whose rights are affected by the search may also obviate the need for a search warrant.[5] Statutory prescripts providing for the power to conduct search and seizure operations generally infringe on the right to privacy, and must therefore comply with the limitations clause in the Constitution.[6]

The Criminal Procedure Act[7] is the primary criminal procedural code in South Africa, and Chapter 2 thereof provides for search and seizure operations in considerable detail. The provisions of the Criminal Procedure Act in respect of search and seizure do not derogate from the powers in respect of search and seizure conferred by any other law.[8] Section 21 of the Act regulates search warrants. The search and seizure provisions of the Criminal Procedure Act are object-based; they do not deal explicitly with any of the specialised procedures that are required to investigate cybercrimes or other offences that involve the use of digital devices.[9] A vast body of literature exists on the distinction between electronic or digital evidence on the one hand, and object-based evidence on the other, as well as the need for legal regimes to adopt criminal investigative procedures to deal more effectively with modern technological advances. These issues are not

---

2 *Bernstein v Bester* 1996 (2) SA 751 (CC) 75; *Minister of Police v Kunjana* 2016 (2) SACR 473 (CC) 26.

3 *Gaertner v Minister of Finance* 2014 (1) SA 442 (CC) 69.

4 *Gumede v S* (800/2015) [2016] ZASCA 148; *Ngqukumba v Minister of Safety and Security* 2014 (5) SA 112 (CC) 19. S 22(*b*) of the Criminal Procedure Act 51 of 1977 sets out the prerequisites for warrantless searches in matters of urgency.

5 S 22(*a*) of 51 of 1977. See *Buthelezi v Minister of Police* 2020 (2) SACR 21 (GJ) on the issue of "informed consent".

6 *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd In re: Hyundai Motor Distributors (Pty) Ltd v Smit NO* 2001 (1) SA 545 (CC) 20. S 36 of the Constitution "requires a weighing-up of the nature and importance of the right(s) that are limited together with the extent of the limitation, as against the importance and purpose of the limiting enactment. Section 36(1) of the Constitution spells out the factors that have to be considered in making a proportional evaluation of all the counterpoised rights and interests involved." See in this regard *Ex Parte Minister of Safety and Security: In Re S v Walters* 2002 (4) SA 613 (CC) 26–27.

7 51 of 1977.

8 S 19 of 51 of 1977. For various examples of such other legislation, see Kruger *Hiemstra's Criminal Procedure* (2008–SI 14) 2-1–2-2.

9 Department of Justice *Memorandum on the Cybercrimes and Cybersecurity Bill* 2017 [B 6–2017] 2. The clauses relating to cybersecurity were removed in later versions of the Cybercrimes Bill.

revisited in this contribution.[10] An attempt was made to address the shortcomings in the South African legal framework when the Electronic Communications and Transactions Act[11] (ECT Act) was enacted. This Act provided for the appointment of cyber inspectors.[12] These cyber inspectors were empowered to conduct search and seizure operations[13] and to apply for search and seizure warrants.[14] These provisions have been described as "more technical in nature" and catering for the electronic environment.[15] These provisions, however, have remained a dead letter as they have never come into operation in practice.[16]

Certain sections of the Cybercrimes Act,[17] including most of Chapter 4 thereof, came into operation on 1 December 2021.[18] In addition to creating offences that have a bearing on cybercrime,[19] the Cybercrimes Act regulates the powers of the police and investigators to investigate cybercrimes. Chapter 4 of the Act provides for the powers of the police and others in

---

10 See for instance, Kerr "Search Warrants in an Era of Digital Evidence" 2005 75(1) *Mississippi Law Journal* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=697541 (accessed 2022-01-21) 85 85–138; Basdeo "The Legal Challenges of Search and Seizure of Electronic Evidence in South African Criminal Procedure: A Comparative Analysis" 2012 25(2) *South African Journal of Criminal Justice* https://hdl.handle.net/10520/EJC127879 (accessed 2022-01-21) 195 195–212; Bouwer "Search and Seizure of Electronic Evidence: Division of the Traditional One-Step Process Into a New Two-Step Process in a South African Context" 2014 27(2) *South African Journal of Criminal Justice* https://hdl.handle.net/10520/EJC167857 (accessed 2022-01-21) 156 156–171; Nortjé and Myburgh "The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa" 2019 22(1) *Potchefstroom Electronic Law Journal* https://doi.org/10.17159/1727-3781/2019/v22i0a4886 (accessed 2022-01-21) 1 1–42. Digital evidence also brings about admissibility challenges. For comprehensive discussions regarding the issues of admissibility of, and weight to be afforded to, electronic evidence, see De Villiers "Old 'Documents', 'Videotapes' and New 'Data Messages': A Functional Approach to the Law of Evidence (Part 1)" 2010 3 *South African Law Journal* https://hdl.handle.net/10520/EJC55325 (accessed 2022-01-21) 558 558–575; De Villiers "Old 'Documents', 'Videotapes' and New 'Data Messages' – A Functional Approach to the Law of Evidence (Part 2)" 2010 4 *South African Law Journal* https://hdl.handle.net/10520/EJC55352 (accessed 2022-01-21) 720 720–735; Hofman "Electronic Evidence in Criminal Cases" 2006 19(3) *South African Journal of Criminal Justice* https://hdl.handle.net/10520/EJC52892 (accessed 2022-01-21) 257 257–275; Swales "An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part One" 2018 21(1) *Potchefstroom Electronic Law Journal* https://doi.org/10.17159/1727-3781/2018/v21i0a2916 (accessed 2022-01-21) 1 1–30; Swales 2018 *PELJ* 1–34; Theophilopoulos "The Admissibility of Data, Data Messages, and Electronic Documents at Trial" 2015 3 *Journal of South African Law* https://hdl.handle.net/10520/EJC-61acfb0f9 (accessed 2022-01-21) 461 461–481.

11 25 of 2002.

12 S 81 of the ECT Act.

13 S 82 of the ECT Act.

14 S 83 of the ECT Act.

15 Govender *A Critical Analysis of the Search and Seizure of Electronic Evidence Relating to the Investigation of Cybercrime in South Africa* (LLM dissertation, University of KwaZulu Natal) 2018 33. For a detailed analysis of the search and seizure provisions in terms of the ECT Act, see the same work at 30–35.

16 Govender *Search and Seizure of Electronic Evidence* 33.

17 19 of 2020

18 Proc R 42 in *GG* No 45562 of 2021-11-30.

19 Ch 2 of the Cybercrimes Act.

respect of search, access or seizure in the investigation of cybercrimes.[20] The provisions of the Criminal Procedure Act[21] continue to apply to the investigation of cybercrimes in that they operate in addition to the provisions of Chapter 4 of the Cybercrimes Act to the extent that the Criminal Procedure Act is not inconsistent with the Cybercrimes Act.[22] The aim of this article is to compare the search warrant provisions of the Cybercrimes Act to those of the Criminal Procedure Act in order to determine to what extent they differ. In the course of the discussion, problems that may arise in interpreting the search warrant provisions of the Cybercrimes Act as a result of the fact that they coexist with the provisions of the Criminal Procedure Act are also identified, and possible solutions are presented. The following matters are considered: the issuing official, the content of the application, the content of the warrant and the execution of the warrant. The issue of warrantless searches falls outside the scope of this contribution.

2 THE ISSUING OFFICIAL

The Constitutional Court regards the vesting of authority to issue search warrants in judicial officers as a significant tool to minimise the interference with personal liberties of individuals.[23] Judicial officers "possess qualities and skills essential for the proper exercise of this power, like independence and the ability to evaluate relevant information so as to make an informed decision".[24] It is of vital importance that the person issuing the warrant must have authority and jurisdiction to do so.[25] In terms of the Criminal Procedure Act, a pre-trial search warrant for investigative purposes must be issued by a magistrate or a justice of the peace.[26] The Act does not empower a judge of the High Court to issue a search warrant for investigative purposes. Furthermore, the definition of a "magistrate" in the Criminal Procedure Act excludes a regional magistrate.[27] Thus, where a provision of the Criminal Procedure Act empowers a magistrate to execute certain duties, a regional magistrate may not execute them. In instances where regional magistrates are empowered to execute duties, their office is explicitly named in the relevant provisions of the Criminal Procedure Act,[28] or reference is made to a broader term such as "judicial officer" in order to include them.[29] If a regional magistrate (and arguably a judge) issues a pre-trial search warrant contrary to the provisions of the Criminal Procedure Act, this does not, without more, render the evidence obtained in the subsequent search

---

20 In terms of s 28 of the Cybercrimes Act, a police official may, in accordance with Ch 4 of the Cybercrimes Act, search for, access or seize any article, within the Republic.

21 51 of 1977.

22 S 27 of the Cybercrimes Act.

23 *Minister for Safety and Security v Van der Merwe* 2011 (2) SACR 301 (CC) 37.

24 *Minister for Safety and Security v Van der Merwe supra* 38. Also, see South *African Association of Personal Injury Lawyers v Heath* 2001 (1) SA 883 (CC) 34.

25 *Minister for Safety and Security v Van der Merwe supra* 56.

26 S 21(1)(*a*) of the Criminal Procedure Act.

27 In terms of s 1 of the Criminal Procedure Act, the term magistrate includes "an additional magistrate and an assistant magistrate but not a regional magistrate".

28 See, for instance, s 205 of the Criminal Procedure Act.

29 See s 21(1)(*b*) of the Criminal Procedure Act.

inadmissible. In terms of section 35(5) of the Constitution, the trial court retains the discretion to admit the evidence obtained as a result of a technically deficient warrant, if the exclusion thereof would not be conducive to a fair trial or to the advancement of the administration of justice. Thus, where judicial approval for a search is sought from the wrong judicial officer in a *bona fide* fashion in order to protect individual rights, the defect in the warrant is not necessarily fatal for the admissibility of the evidence found as a result of the warrant in question.[30] In addition to magistrates, justices of the peace may also issue search warrants in terms of the Criminal Procedure Act. Justices of the peace are appointed in terms of the Justices of the Peace and Commissioners of Oaths Act.[31] Senior members of the prosecuting service and commissioned officers of the South African Police Service are among those who, *ex officio*, hold the office of justice of the peace.[32] They are most likely to issue search warrants. It is nevertheless submitted that a judicial officer ought to be the first port of call when an application is made for a search warrant, as justices of the peace may lack the measure of independence. The Criminal Procedure Act does, however, empower a judge or a "judicial officer presiding at criminal proceedings" to issue a search and seizure warrant (trial warrant) if required in evidence, subject to certain prerequisites.[33] Therefore, the warrant issued at the trial may clearly be issued by a judge, magistrate or regional magistrate presiding in a criminal trial.

The Cybercrimes Act extends the power to authorise search and seizure warrants to magistrates and judges of the High Court.[34] Unlike the Criminal Procedure Act, justices of the peace are not so empowered. The Cybercrimes Act empowers "a magistrate or a judge of the High Court presiding at criminal proceedings" to issue trial warrants. This provision thus differs from those of the Criminal Procedure Act in that the latter refers to a judge or a presiding officer in criminal proceedings. The Cybercrimes Act makes no explicit reference to regional magistrates in respect of the issuing of search and seizure warrants either at the pre-trial stage or at the trial. The question therefore arises whether regional magistrates are excluded. The present author submits that the Cybercrimes Act must be interpreted in a manner so as to include regional magistrates in issuing both these types of warrants. This is because, unlike the Criminal Procedure Act, the Cybercrimes Act neither defines the term "magistrate", nor specifically excludes regional magistrates from the meaning of "magistrate". The Magistrates Act,[35] which regulates the appointment and conditions of service of magistrates, defines a magistrate as "a judicial officer appointed under section 9 of the Magistrates' Courts Act,[36] read with section 10 of [the Magistrates] Act, excluding any person occupying that office in an acting or

30 *S v Dos Santos* 2010 (2) SACR 382 (SCA) 21–24.
31 16 of 1963. S 2 of the Act provides for their appointment by the Minister of Justice.
32 S 4 of 16 of 1963, read with the first schedule to the Act.
33 S 21(1)(*b*) of the Criminal Procedure Act.
34 S 29(1)(*a*) of the Cybercrimes Act.
35 90 of 1993.
36 32 of 1944.

temporary capacity and any assistant magistrate".[37] Section 9 of the Magistrates' Courts Act,[38] in turn, refers to the appointment of both district court magistrates and regional court magistrates.[39] The term "magistrate", therefore, also encompasses a regional magistrate for purposes of the two key pieces of legislation regulating the appointment of judicial officers in the lower courts. It would further be nonsensical if the legislator empowered both district court magistrates and judges of the High Court to issue search warrants (especially when presiding over a criminal trial), but excluded regional magistrates, who should be equally skilled to consider the authorisation of search warrants.

3 ARTICLES THAT MAY BE SEIZED

Section 20 of the Criminal Procedure Act provides for the articles that may be seized by the State. There must be some link between these articles and a criminal offence. Three categories of article may be seized. The first category is anything that is concerned, or is on reasonable grounds believed to be concerned, in the commission or suspected commission of an offence.[40] The second category refers to anything that may afford evidence of the commission or suspected commission of an offence.[41] The third category has to do with anything that is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence.[42] "Anything"[43] falling within one of these categories may be seized. A search and seizure warrant may authorise a search operation with reference to all three categories insofar as they are applicable.[44] Given the focus of the Cybercrimes Act on cybercrime and the fact that it caters for technological advances, the articles that may be seized in terms thereof are more precisely described. An "article" in this context refers to any data,[45] computer program,[46] computer data storage medium[47] or computer system.[48] Each of these articles is further defined in the definitions provisions.[49] The Cybercrimes Act, in very similar terms to the Criminal Procedure Act, also requires a link between the articles that may be seized and evidence of the suspected commission of a criminal offence. The offences are, however, further delimited under the definition of "article" in the Cybercrimes Act, namely:

---

37 S 1 of 90 of 1993.
38 32 of 1944.
39 S 9(1)(*a*) of 32 of 1944.
40 S 20(*a*) of the Criminal Procedure Act.
41 S 20(*b*) of the Criminal Procedure Act.
42 S 20(*c*) of the Criminal Procedure Act.
43 Introductory sentence of s 20 of the Criminal Procedure Act.
44 In *Polonyfis v Minister of Police* 2012 (1) SACR 57 (SCA) 10, the court held that the jurisdictional facts necessary for the issue of a single warrant may be found in all three sub-sections of section 20 of the Criminal Procedure Act.
45 S 1(1)(*a*) of the Cybercrimes Act.
46 S 1(1)(*b*) of the Cybercrimes Act.
47 S 1(1)(*c*) of the Cybercrimes Act.
48 S 1(1)(*d*) of the Cybercrimes Act.
49 S 1(1) of the Cybercrimes Act.

"(*aa*) an offence in terms of Part I and Part II of Chapter 2;
(*bb*) any other offence in terms of the law of the Republic; or
(*cc*) an offence in a foreign State that is substantially similar to an offence contemplated in Part I or Part II of Chapter 2 or another offence recognised in the Republic."[50]

Part I of Chapter 2 creates a number of cybercrimes,[51] while Part II criminalises "malicious communications".[52] It becomes clear that it is not only articles that are in some way or other involved in the commission of offences created by the Cybercrimes Act that are susceptible to seizure. The search and seizure operation may be in respect of any offence where data, a computer program, a computer data storage medium or a computer system is concerned in or may afford evidence of the commission of a crime. It will remain important that the articles to be seized are identified with sufficient particularity in both the application for the warrant and the search warrant itself.[53]

4 THE CONTENT OF THE APPLICATION

The Criminal Procedure Act requires that the information setting out the jurisdictional facts for the issuing of a search warrant be on oath.[54] The Cybercrimes Act, on the other hand, provides that the information may be presented either on oath or by way of affirmation.[55] The application for a pre-trial search warrant under the Criminal Procedure Act must satisfy the magistrate or justice of the peace, as the case may be, that there are reasonable grounds for believing that the article in question "is in the possession or under the control of or upon any person or upon or at any premises within the area of the jurisdiction" of the magistrate or justice of the peace.[56] It must be clear from the information made available to the magistrate that the article in question is covered by section 20 of the Criminal Procedure Act, which provides for the articles that may be seized by the State (as discussed under heading 3 above). The affidavit in support of the search warrant to be issued in terms of the Criminal Procedure Act must contain two important objective jurisdictional facts, namely: (i) the existence of a reasonable suspicion that a crime has been committed, and

50 *Ibid*.

51 These are: unlawful access to a computer system or a computer data storage medium (s 2); unlawful interception of data (s 3); unlawful acts in respect of software or hardware tool (s 4); unlawful interference with data or a computer program (s 5); unlawful interference with a computer data storage medium or computer system (s 6); unlawful acquisition, possession, provision, receipt or use of a password, access code or similar data or device (s 7); cyber fraud (s 8); cyber forgery and uttering (s 9); cyber extortion (s 10) and aggravated offences in respect of "restricted computer systems" (s 11). The Act also criminalises the theft of incorporeal property (s 12).

52 They are: data messages that incite damage to property or violence (s 14) and data messages that threaten persons with damage to property or violence (s 15).

53 *Minister for Safety and Security v Van der Merwe supra* 55.

54 S 21(1)(*a*) of the Criminal Procedure Act.

55 S 29(1)(*a*) of the Cybercrimes Act.

56 S 21(1)(*a*) of the Criminal Procedure Act.

(ii) the existence of reasonable grounds to believe that objects connected with the offence may be found on the premises or persons intended to be searched.[57]

In terms of the Cybercrimes Act, it must appear from the application that the article (a) is in the area of jurisdiction of the magistrate or judge,[58] *or* (b) is being used or is involved in or has been used or was involved in the commission of an offence and that there are reasonable grounds to believe that the article is within the area of the said jurisdiction.[59] The nature of cybercrimes or crimes involving the use of computers may present difficulties in establishing where precisely the offence was committed. A warrant may, therefore, also be issued if it appears to the issuing official that the article is within the Republic, but 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.[60] It is critical that these jurisdictional facts be placed before the judicial officer considering the warrant. A judicial officer authorising the warrant must satisfy himself or herself that the affidavit contains sufficient information on the existence of the jurisdictional facts. If not, the judicial officer should refuse to issue the warrant.[61] The affidavit in support of the application for a search warrant must be properly signed and sworn to before a commissioner of oaths, as set out in the Justices of the Peace and Commissioners of Oaths Act.[62] If the affidavit was already prepared and signed before it was presented to the commissioner of oaths for the administering of the oath, the warrant issued on the strength thereof will be invalid.[63]

5 ORAL APPLICATION FOR A SEARCH WARRANT

Both the Criminal Procedure Act[64] and the Cybercrimes Act[65] provide for warrantless searches in circumstances of urgency or where consent is given for the search. The Cybercrimes Act provides for a unique in-between procedure, namely an oral application for the warrant (or the amendment of the warrant) in matters of urgency or in other exceptional circumstances. Such an oral application may be made by a specifically designated police official in circumstances where "it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances to make a written application".[66] The application must indicate the particulars of urgency of the case or the other exceptional

57 *Minister of Safety and Security v Van der Merwe supra* 39.
58 S 29(1)(*a*)(i) of the Cybercrimes Act.
59 S 29(1)(*a*)(ii)(*aa*) of the Cybercrimes Act.
60 S 29(1)(*a*)(ii)(*bb*) of the Cybercrimes Act.
61 *Minister of Safety and Security v Van der Merwe supra* 39 and 56.
62 16 of 1963.
63 *Mogale v Minister of Safety and Security* 2016 (2) SACR 682 (GP). Also see *S v Malherbe* 2020 (1) SACR 227 (SCA).
64 S 22 of the Criminal Procedure Act.
65 S 32 of the Cybercrimes Act.
66 S 30(1) of the Cybercrimes Act.

circumstances,[67] and must also comply with any supplementary directives relating to oral applications that may be issued by the Chief Justice in terms of the Superior Courts Act.[68] The Act sets out the preconditions for the issuing of a warrant based on an oral application.[69] In addition to the normal requirements for the issuing of a warrant,[70] it must be evident that the warrant is immediately necessary in order to search for, access or seize an article,[71] and that it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application for the issuing of a warrant or to amend a warrant.[72] Furthermore, the police official concerned must submit a written application to the magistrate or judge of the High Court concerned, within 48 hours after the issuing of the warrant.[73] Such a warrant must, among other things, contain a summary of the facts that were considered, as well as the grounds upon which the warrant was issued.[74] Upon receipt of a written application, the issuing officer must reconsider that application, whereupon he or she may confirm, amend or cancel the warrant.[75]

6 THE CONTENT OF THE WARRANT

It is an essential requirement for the validity of a search warrant that its terms must be neither vague nor overbroad. The issue was summarised by the Supreme Court of Appeal as follows:

> "For where the warrant is vague it follows that it will not be possible to demonstrate that it goes no further than is permitted by the statute. If a warrant is clear in its terms a second, and different, question might arise, which is whether the acts that it permits go beyond what is permitted by the statute. If it does, then the warrant is often said to be 'overbroad' and will be invalid so far as it purports to authorise acts in excess of what the statute permits. A warrant that is overbroad might, depending upon the extent of its invalidity, be set aside in whole, or the bad might be severed from the good."[76]

The terms of the warrant must be reasonably intelligible to both the searcher and the person being searched, and the courts will construe the terms of a warrant with reasonable strictness.[77] The Criminal Procedure Act states that a search warrant should require a police official to seize the article in question. In order to achieve this, the warrant must authorise the police official to search any person identified in the warrant, or to enter any premises identified in the warrant and to search any person found on or at

---

67 S 30(2)(*a*) of the Cybercrimes Act.
68 10 of 2013. See s 30(2)(*b*) of the Cybercrimes Act.
69 S 30(4) of the Cybercrimes Act.
70 S 30(4)(*a*)(i) of the Cybercrimes Act.
71 S 30(4)(*a*)(ii) of the Cybercrimes Act.
72 S 30(4)(*a*)(iii) of the Cybercrimes Act.
73 S 30(4)(*b*) of the Cybercrimes Act.
74 S 30(5)(*c*) of the Cybercrimes Act.
75 S 30(6) of the Cybercrimes Act.
76 *Minister of Safety and Security v Van der Merwe supra* 14. Also see *Powell v Van der Merwe* [2005] 1 All SA 149 (SCA) 50–59.
77 *Minister of Safety and Security v Van der Merwe supra* 56.

such premises.[78] A search warrant issued in terms of the Cybercrimes Act must require a police official identified in the warrant to search for, access or seize the article in question, and to that end:

- search any person identified in the warrant;[79]
- enter and search any container, premises, vehicle, facility, ship or aircraft identified in the warrant;[80]
- search any person who is believed, on reasonable grounds, to be able to furnish any information of material importance concerning the matter under investigation and who is found near such container, on or at such premises, vehicle, facility, ship or aircraft;[81]
- search any person who is believed, on reasonable grounds, to be able to furnish any information of material importance concerning the matter under investigation and who (i) is nearby; (ii) uses; or (iii) is in possession or in direct control of, any data, computer program, computer data storage medium or computer system identified in the warrant to the extent set out in the warrant;[82]
- search for any article identified in the warrant to the extent set out in the warrant;[83]
- access an article identified in the warrant to the extent set out in the warrant;[84]
- seize an article identified in the warrant to the extent set out in the warrant;[85] or
- use or obtain any instrument, device, equipment, password, decryption key, data, computer program, computer data storage medium or computer system or other information that is believed, on reasonable grounds, to be necessary to search for, access or seize an article identified in the warrant to the extent set out in the warrant.[86]

It should be mentioned that the Act places certain restrictions on the use of the instrument, device, password or decryption key or information to gain access to the article defined in the warrant.[87]

The validity requirements laid out in the Cybercrimes Act must further be read with the common law intelligibility requirements for search warrants, as identified by the Constitutional Court in *Minister of Safety and Security v Van der Merwe*,[88] where it was found that a valid warrant: states the statutory

---

78 S 20(2) of the Criminal Procedure Act.

79 S 20(2)(*a*) of the Cybercrimes Act.

80 S 20(2)(*b*) of the Cybercrimes Act. A technically wrong address does not invalidate a warrant if it otherwise described the premises with sufficient particularity so that the police could ascertain and identify the place to be searched. See, in this regard, *Polonyfis v Minister of Police supra* 16.

81 S 20(2)(*c*) of the Cybercrimes Act.

82 S 20(2)(*d*) of the Cybercrimes Act.

83 S 20(2)(*e*) of the Cybercrimes Act.

84 S 20(2)(*g*) of the Cybercrimes Act.

85 S 20(2)(*h*) of the Cybercrimes Act.

86 S 20(2)(*a*) of the Cybercrimes Act.

87 S 37(2)(*a*) of the Cybercrimes Act.

88 *Supra* 55.

provision in terms of which it is issued;[89] is addressed to a specifically named police official; identifies the searcher; clearly mentions the authority it confers upon the searcher; identifies the person, container or premises to be searched; describes the article to be searched and seized with sufficient particularity; specifies the offence that triggered the criminal investigation; and names the suspected offender.[90]

There has been some academic and judicial debate on the question whether separate judicial authorisation is needed for the seizing of computer or device hardware, on the one hand, and accessing and retrieving data from the device on the other. Bouwer[91] argues that judicial authorisation is needed for each step. In *S v Miller,*[92] Gamble J analysed the relevant provisions of the Electronic Communications and Transactions Act and their relationship to the Criminal Procedure Act and concluded that such an approach is not necessary. In *Oosthuizen v the Magistrate, Hermanus*,[93] it was held that a warrant authorising the seizure of "all electronic equipment which include [sic] cell phones, desktop computers, laptops and Ipad's [sic]" was "strikingly broad" as the warrant did not distinguish between the electronic devices themselves and any material or information stored on them, neither did it identify the material to be seized as material that might have a bearing on the suspected offence. Norton AJ held:

> "What was required, in my view, was for the warrant, first, to specify that the object of the search (under this category of articles) would be material stored on the electronic devices, and second, to identify the relevant material by its connection to the suspected offences, and with reference to the types of electronically stored material (such as accounting records, invoices, correspondence, photographs or videos) which might evidence activities related to the suspected offences. This is the only way in which the police officers conducting the search would be able to distinguish between the electronically stored material subject to seizure, and material not subject to seizure."[94]

It is now clear from the wording of the Cybercrimes Act that, indeed, separate authorisations for the seizure of equipment and the accessing of data is required. In fact, even the method used to access the data must be

---

89 When a statutory offence is the subject of the investigation, the search warrant should refer to the specific statute and the section or subsection of the applicable legislation. This is necessary to enable both the person in charge of the premises to be searched and the police official authorised to execute the search warrant, to know precisely for which offences the search has been authorised. See, in this regard, *Goqwana v Minister of Safety and Security* 2016 (1) SACR 384 (SCA) 54–55.

90 Errors in the description of the offence may render a search and seizure warrant invalid on the grounds of vagueness and lack of reasonable intelligibility. See *Oosthuizen v Magistrate, Hermanus* 2021 (1) SACR 278 (WCC) 59.

91 Bouwer 2014 *South African Journal of Criminal Justice* 156–71.

92 2016 (1) SACR 251 (WCC).

93 *Supra* 69–70.

94 *Oosthuizen v Magistrate, Hermanus supra* 75. For a more detailed discussion of the case, see Du Toit 2021 2 *South African Journal of Criminal Justice* https://doi-org.nwulib.nwu.ac.za/10.47348/SACJ/v34/i2a11 (accessed 2022-12-31) 386 386–391. Also see *Craig Smith and Associates v Minister of Home Affairs* [2015] BCLR 81 (WCC). Also see *Beheersmaatschappij Helling I NV v Magistrate, Cape Town* 2007 (1) SACR 99 (C) 115f–h.

authorised. The authorisation for these different actions may, however, be contained in a single search and seizure warrant.

7 EXECUTION OF THE SEARCH AND SEIZURE WARRANT

7 1 Time of execution

The Criminal Procedure Act requires a search warrant to be executed by day, unless the person issuing the warrant in writing authorises the execution thereof by night.[95] The Cybercrimes Act, on the other, provides that a search warrant may be executed *at any time*, unless the person issuing the warrant in writing specifies otherwise.[96] It is submitted that judicial officers should give careful consideration to this issue and that authorisation for the search should not be lightly extended to night time, at least as far as the search of persons and premises are concerned. This consideration will be less concerning when "offsite" access is gained by experts to devices that had been seized earlier. It is preferable that the time of execution of the warrant also be delimited in a search warrant. One of the aims of a search warrant is to govern the time of a search, so as to limit the privacy intrusion.[97] Search and seizure must be carried out in the least intrusive and disruptive manner possible. The police may, for instance, not disrupt business more than is necessary, and may not act beyond the terms of the warrant.[98] Unless the affidavit in support of the application for the warrant makes out a case for the search and seizure of a person or premises at night, the warrant should preferably authorise day-time searches only.

7 2 Informational requirement

It is not necessary for persons whose rights are affected by a search and seizure operation to receive prior notice thereof as there is a risk that they would remove or destroy the evidence.[99] In terms of the Criminal Procedure Act, a police official executing a warrant must, after the execution thereof, upon demand of any person whose rights have been affected by the search, hand to him or her a copy of the warrant.[100] The Supreme Court of Appeal has held that it is not only the search and seizure warrant but also the affidavit in support of the application for the warrant that should accompany the warrant and be handed over if requested by the party affected by the search. The court found that this procedure would expedite any court application in which a person may wish to contend that his or her rights were

---

95 S 21(3)(*a*) of the Criminal Procedure Act. See, in this regard, *Young v Minister of Safety and Security* 2005 (2) SACR 437 (SE) 30.

96 S 29(4)(*a*) of the Cybercrimes Act.

97 *Magajane v Chairperson, North West Gambling Board* 2006 (2) SACR 447 74.

98 *Beheersmaatschappij Helling I NV v Magistrate, Cape Town supra* 115h–116e.

99 *Thint (Pty) Ltd v NDPP, Zuma v NDPP* 2008 (2) SACR 421 (CC) 98.

100 S 21(4) of the Criminal Procedure Act.

adversely affected by the search.[101] Ally[102] raises two objections against this provision. He is of the view, first, that a copy of the warrant should, whenever possible, be provided before the search and seizure operation. Secondly, the delivery of a copy should not depend on the request of the individual, as many subjects will not make such a request as a result of their lack of knowledge of the law.[103] Some of these concerns are addressed in the Cybercrimes Act, in terms of which the police official who executes a search warrant must hand a copy of the warrant and the written application of the police official to any person whose rights in respect of any search, or article accessed or seized under the warrant have been affected.[104] The handing over does not depend on the request of the individual whose rights are affected by the search. The provisions also give effect to the requirement that not only the warrant but also the application for the warrant be handed over. This, by implication, entails that the affidavit or affirmed statement in support of the application be handed over.

7 3 Assistance in the execution of the search

In terms of section 21(2) of the Criminal Procedure Act, only a police official may be authorised by a search warrant to conduct a search. Warrants authorising private individuals to search and seize are invalid.[105] In *Keating v Senior Magistrate*,[106] Kollapen J considered the question whether it is permissible for "outside persons" (for example, forensic investigators and computer experts) to be authorised to be present at a search and seizure for the limited purpose of the expertise they bring. The court held that one must take a realistic approach to the issue, while at the same time guarding against outsourcing the functions and powers of the police, or allowing private individuals or entities to usurp such powers. The court found that as technology and expertise become increasingly specialised and significant bodies of knowledge and expertise are developed in dedicated areas, it is unrealistic to expect the investigative agencies of the State, at any given time, to possess all of the expertise that may be required to conduct successful investigations. As such expertise may reside outside of the State, the use of such expertise may indeed be necessary.[107] The court concluded that there is nothing in the Criminal Procedure Act that finds the presence of private persons at a search and seizure offensive, provided, first, they are properly authorised to be there, and secondly, their role is clearly defined and does not relate to the actual execution of search and seizure activities.[108] The court also listed a number of issues to be placed before the authorising magistrate, including: the necessity for the presence of such

101 *Goqwana v Minister of Safety and Security supra* 31.
102 Ally "Search and Seizure" in Joubert (ed) *Criminal Procedure Handbook* 13ed (2020) 196.
103 Ally in Joubert (ed) *Criminal Procedure Handbook* 196.
104 S 29(5) of the Cybercrimes Act.
105 *Extra Dimensions v Kruger* 2004 (2) SACR 493 (T); *Smit & Maritz Attorneys v Lourens* 2002 (1) SACR 152 (W)).
106 2019 (1) SACR 396 (GP).
107 *Keating v Senior Magistrate supra* 37.
108 *Keating v Senior Magistrate supra* 39.

persons; whether they bring special expertise or knowledge to the search and seizure operation that do not ordinarily reside in police officials; the clearly defined role(s) the persons are required to play in the search operation; and under whose control and authority such persons will operate during the search and seizure operation. The affidavit should also indicate how the presence and assistance of such persons would render the search more effective and compliant, and possibly reduce or limit the incursion into the privacy and other rights of those who are the subject of the search.[109]

A search warrant issued in terms of the Cybercrimes Act may require an investigator or other person identified in the warrant to assist the police official identified in the warrant with the search for, access or seizure of the article in question, to the extent set out in the warrant.[110] It is submitted that in order for such an investigator or other person to be so authorised, the affidavit in support of the application should set out the need for their presence, as was described in *Keating v Senior Magistrate*. The Act also places an obligation on electronic communications service providers, financial institutions or persons who are "in control of any container, premises, vehicle, facility, ship, aircraft, data, computer program, computer data storage medium or computer system that is subject to a search authorised in terms of the Act" to provide assistance in the search, if required. The assistance includes "technical assistance" and "such other assistance as may be reasonably necessary" to a police official or investigator in order to search for, access or seize an article.[111] An "investigator" does not necessarily refer to an official appointed by the State, but rather to any fit and proper person who is not a member of the South African Police Service, and who is either identified and authorised in terms of a search warrant to assist the police official with the search operation, or is requested by the police officer to do so. Such a person remains subject to the direction and control of the police official.[112]

8 A SEPARATE WARRANT NECESSARY IN RESPECT OF ARTICLES NOT COVERED BY THE CYBERCIMES ACT?

As was pointed out earlier in this contribution, the Criminal Procedure Act continues to apply to the extent that its provisions are not incompatible with the Cybercrimes Act. It was also shown that the articles that may be seized in terms of the Cybercrimes Act are: any data; computer program; computer data storage medium; or computer system. It was further pointed out that the search and seizure provisions of the Cybercrimes Act are applicable not only to cybercrimes created by the Act but also to any offence committed in the Republic. The question arises whether it will be necessary to obtain a separate warrant in terms of the Criminal Procedure Act (or other relevant legislation) in respect of search and seizure of articles not covered by the

[109] *Keating v Senior Magistrate supra* 40.
[110] S 29(3) of the Cybercrimes Act.
[111] S 34(1) of the Cybercrimes Act.
[112] S 25 of the Cybercrimes Act.

Cybercrimes Act. For instance, an investigation in respect of a financial crime may require the search for and seizure of both computer data and handwritten documents. As the latter is not covered by the definition of "article" in the Cybercrimes Act, the situation would necessarily require that separate search warrants be issued in terms of the Cybercrimes Act and the Criminal Procedure Act. It must be recalled that one of the validity requirements for a search and seizure warrant is that it should state the statutory provision in terms of which it was issued. Such a fragmented approach seems to be quite inefficient and counterproductive to the investigation of crime. The Constitutional Court has held that our courts must take care that in ensuring protection for the right to privacy, they do not hamper the ability of the State to prosecute serious and complex crime, which is also an important objective in our constitutional scheme.[113] It is submitted that it should be quite acceptable for a single search warrant to be applied for and issued with reference to the provisions of both the Criminal Procedure Act and the Cybercrimes Act. Ultimately, the search warrant must be "reasonably intelligible", in the sense that it should be capable of being understood by the reasonably well-informed person who understands the relevant empowering legislation and the nature of the offences under investigation.[114]

9 CONCLUSION

Although the provisions of the Criminal Procedure Act have hitherto often been used to search for and seize articles now provided for in the Cybercrimes Act, the reality is that the search and seizure provisions of the Criminal Procedure Act have not kept pace with technological advancements. As such, the investigative tools provided for by the Cybercrimes Act must be welcomed. Not only should the requirements of search warrants, as set out in the Act, be strictly adhered to, but issuing officials should also bear in mind the additional requirements for the validity of search warrants that have been developed by our superior courts, so as to ensure that the validity of these warrants are upheld in either preliminary litigation or during the trial where the admissibility of evidence obtained pursuant to a search warrant may become an issue. It is imperative that the legislature incorporates the search and seizure provisions of the Cybercrimes Act into the Criminal Procedure Act in order to avoid the issuing various search warrants in respect of a single criminal investigation. The Criminal Procedure Act remains the primary criminal procedural code for the investigation of crime, and should, as such, reflect the social realities in respect of the use of electronic devices in criminal activities.

[113] *Thint (Pty) Ltd v NDPP, Zuma v NDPP supra* 80.
[114] *Thint (Pty) Ltd v NDPP, Zuma v NDPP supra* 154.