SEARCH FOR AND SEIZURE OF EVIDENCE IN CYBER ENVIRONMENTS: A LAW-ENFORCEMENT DILEMMA IN SOUTH AFRICAN CRIMINAL PROCEDURE

Vinesh M Basdeo
National Diploma (Pol Management),
BA Honours (Police Science),
LLB, LLM, LLD College of Law UNISA

Moses Montesh
National Diploma (Pol Management),
BA Honours (Police Science), MPA, PhD (Police Science)
College of Law UNISA

Bernard Khotso Lekubu
College of Law UNISA

This article is partially based on a thesis submitted by Vinesh Basdeo in fulfilment of the requirements for the degree Doctor of Laws at the University of South Africa.

Abstract

Investigating, deterring and imposing legal sanctions on cyber-criminals warrants an international legal framework for the investigation and prosecution of cybercrime. The real-world limits of local, state and national sovereignty and jurisdiction cannot be ignored by law-enforcement officials. It can be a strenuous task to obtain information from foreign countries, especially on an expedited basis – more specifically when the other country is in a different time zone, has a different legal system, does not have trained experts and uses different languages. In South Africa existing laws appear to be inadequate for policing the cyber realm. The effects and impact of information technology on the legal system have not yet received the attention they warrant. The challenges presented by the electronic realm cannot be solved merely by imposing existing criminal and criminal procedural laws which govern the physical world on cyberspace. The electronic realm does not necessarily demand new laws, but it does require that criminal actions be conceptualised differently and not from a purely traditional perspective. Sovereignty and the principle of non-interference in the domestic affairs of another state are fundamental principles grounding the relations between states; they constitute an important mechanism in the armoury of criminals. The harmonisation and enactment of adequate and appropriate transborder coercive procedural

Vol 1(1) 2014 pp 48–67
ISSN 2313-8289

measures consequently play a pivotal role in facilitating effective international cooperation. This article examines the efficacy of South African laws in dealing with the challenges presented by police powers to search for and seize evidence in cyber environments. It analyses the rudimentary powers that exist in South African criminal procedure regarding the search for and seizure of evidence in cyber environments, and compares them against the backdrop of the more systemic and integrated approach proposed by the Cybercrime Convention.

INTRODUCTION

The exponential growth of information communication technology infrastructure such as computer networks and information superhighways has created increasing opportunities for potential offenders as well as increasing risks for potential victims (Moore 2003, 1). In this regard, criminal offences assume various forms. These have been labelled, inter alia, computer crime, internet crime, information technology crime, high-tech crime, e-crime and cybercrime (Van der Merwe 2000, 187). Information technology crime does not require physical proximity between the victim and the perpetrator for the commission of the crime. Cybercriminals can virtually connect to information technology systems such as the internet from anywhere in the world. The real-world limits of local, state and national sovereignty and jurisdiction cannot be ignored by law-enforcement officials. It can be a daunting task to obtain information from foreign countries, especially on an expedited basis – more specifically when the other country is in a different time zone, has different legal systems, does not have trained experts and uses different languages.

The criminal justice field is not keeping pace with crime in the computing and electronic context (Moore 2003, 1). Today the policing of terrestrial space is very much a pluralistic pursuit. So too is the policing of cyberspace. Responsibilities for the control of cybercrime will be similarly shared between agents of the state, information security specialists in the private sector and individual users (Wall 2003, 80).

When an investigator harvests evidence from cyber environments, the primary goal is still to obtain evidence that is admissible as evidence in a court of law, and to preserve its evidential integrity. The essential characteristic of electronic evidence presents unique challenges with regard to its reliability because it can be easily destroyed, accurately copied or erased. The volatile character of the cyber realm necessitates exceptionally efficient search-and-seizure interventions as well as the power to control the environment for a certain period of time in order to maintain unimpeachable continuity, possession and integrity of electronic evidence. Searching for evidence in the cyber realm is generally more tedious and complicated than searching for tangible evidence in traditional investigative realms. Some of the idiosyncrasies of cyber environments include the fact that electronic files comprise electrical impulses that can be stored on the head of a pin and circulated around the world instantaneously. The search for and seizure of electronic evidence differs from general searches and seizures. The search for and seizure of electronic evidence compels law-enforcement officials to conduct

searches and seizures in non-traditional ways. Some of the essential characteristics of the cyber realm which warrant such measures include its global and borderless nature, its anonymity, its potential to reach vast audiences easily, its potential as a force multiplier of e-crime and the wealth of investigative information produced by the routine storage of information (United States Report of the President's Working Group on Unlawful Conduct on the Internet 2011, 14).

DEFINING CYBER SEARCH, SEIZURE AND RELATED PHENOMENA

The search for and seizure of electronic evidence does not merely entail transporting hardware from a crime scene to an evidence compound. Similarly, the production or preservation of information in electronic format does not merely entail the handing over of hardware. The search for and seizure of information from cyber environments entails browsing, busting the binary code in search of electronic evidence, and similar practices.

Cyber search and seizure

'Search' in terms of the Cybercrime Convention implies to seek, read, inspect or review data and it therefore permits both the searching for and the searching or examining of data (The Council of Europe's Explanatory Report to the Cybercrime Convention). Search and seizure in accordance with the Cybercrime Convention is directed at any computer data, including all forms of communication data, provided that such data is static, recorded and stored. Search and seizure of electronic evidence is concerned with data that has been recorded or registered in the past, either in tangible or in intangible form; and the gathering of this data takes place at a single moment in time, in other words, the period of the search, and in respect of data that exists at that time (Explanatory Report to the Cybercrime Convention). The term 'seize' means to take away the physical medium in which data or information is recorded, and includes the use or seizure of computer programs needed to access the data being seized (Explanatory Report to the Cybercrime Convention). The seizure of data includes both the gathering of evidence and the confiscation of data (Explanatory Report to the Cybercrime Convention).

Cyber data

Information consists of the organised and meaningful end product of data processing. Information is converted into evidence when it becomes admissible as evidence in a court of law. 'Data' in contemporary computing refers to information that has been translated into a form that is convenient to process (Whatis.com definitions).

Article 1(*b*) of the Cybercrime Convention defines 'computer data' as:

> … any representation of facts, information or concepts in a form suitable for processing on a computer system, including a program suitable to cause a computer system to perform a function.

The term 'cyber data' as introduced by the Cybercrime Convention should be understood as data in an electronic form, or in another directly processable form (Explanatory Report to the Cybercrime Convention 6). Section 1 of the Electronic Communications and Transactions Act (ECT Act) defines 'data' as electronic representations of information in any form.

Electronic evidence

'Electronic evidence' is generally defined as electronically stored information that can be used as evidence in a legal action (Volonino 2003, 1). This includes any information of probative value that is either stored or transmitted in a binary form by means of, for example, cellular telephones, digital audio and digital fax machines (Whitcomb 2002, 29). For the purposes of this article the terms 'electronic evidence' and 'digital evidence' are used interchangeably as they both include binary evidence accrued from cyber environments.

THE CYBERCRIME CONVENTION

The Convention on Cybercrime (hereinafter, 'the Convention' or 'the Cybercrime Convention') is a multilateral instrument directed specifically at addressing crimes committed in an electronic medium. The Convention was signed on 23 November 2001 by the Council of Europe member countries and four non-European countries, namely, South Africa, Canada, the United States and Japan. The United States ratified the Convention in September 2006 and it came into operation in January 2007. Approximately 43 countries have signed the Convention. The Convention is aimed at combating cybercrime by requiring signatory countries to establish certain substantive offences and to adopt domestic procedural laws to investigate cybercrime; and, furthermore, to address criminal and procedural law at an international level to ensure the harmonization of laws governing the criminal justice systems, and also to provide international cooperation and assistance in criminal investigations. The Convention criminalises certain computer actions, such as the interception of non-public transmission of computer data; establishes corporate liability; calls for the production of stored computer data; and recommends mutual assistance between countries in investigations. Although the Convention aims at international cooperation in prosecuting cybercrime, it contains no provision for cooperation in securing networks. The aim of the Convention to harmonise national laws in order to facilitate law enforcement's ability to act across national borders is a giant step in the right direction and

is highly laudable. However, it is difficult to implement in practice (Kumar 2010). The Cybercrime Convention constitutes the current internationally agreed-upon benchmark, inter alia, for the procedural powers aimed at the collection of electronic evidence. The Cybercrime Convention is inter alia aimed at accommodating flexible harmonisation in order to achieve law enforcement goals to support the timely eradication of electronic crime. The Convention is a potential tool for establishing hegemony in cyber regulation. Its overarching motivation was that virtual impunity from which criminal conduct in cyberspace has appeared to benefit could no longer be tolerated without jeopardising the future and the potential of electronic networks. The Convention is the only existing international tool that brings together nations of the world, so that the world can fight cybercrime as one (Marler 2002, 219). South Africa has signed but did not ratify the Convention; it has complied with the first part in terms of which member states are obliged to criminalise the illegal access to a computer system; the illegal interception of data to a computer system; the use of inauthentic data with the intention to expose it as authentic; the infringement of copyright related rights online; the interference with data or the functioning of a computer system, and child pornography-related offences (Van der Merwe 2008, 101).

The Cybercrime Convention is intended to be a binding international legal instrument; it is intended to supplement and not supplant existing multilateral and bilateral treaties and arrangements between parties (article 39(1)). However, in respect of specific matters dealt with only by the Convention, the rule of interpretation *lex specialis derogat legi generali* provides that the parties should give precedence to the rules contained in the Cybercrime Convention (article 30). Several articles of the Convention provide for the co-existence of domestic law and the treaty. For instance, article 15 incorporates the conditions and safeguards under the domestic law of the parties to the procedural powers and procedures provided for in section 2 of the Convention. Article 23 requires the parties to cooperate with each other to the widest possible extent, inter alia, by applying the domestic laws of the parties.

Search-and-seizure evidence in terms of the Cybercrime Convention

Requirements

Article 19 of the Cybercrime Convention provides for the procedural power at national level to search for and seize stored cyber data. Article 19 is primarily directed at establishing, in jurisdictions where stored cyber data *per se* is not considered to be a tangible object, an equivalent power of search and seizure, as opposed to tangible objects. Traditional search-and-seizure mechanisms remain relevant and applicable. However, additional procedural provisions are necessary to ensure that computer data can be obtained in the same manner as for the search and seizure of a tangible data carrier. Some of the reasons advanced

for the need for additional procedural provisions include the fact that the data is in an intangible form and to the physical medium in which the intangible data is stored must be seized and removed.

In terms of article 19(1)(*a*) of the Cybercrime Convention parties to it are required to empower law enforcement authorities to access and search cyber data which is either contained within a computer system or is part of it.

Article 19(2) of the Convention is directed at data that is physically stored in another system or storage device which can be legally accessed through the searched computer system by establishing a connection with other distinct computer systems. Article 19(3) empowers competent authorities to seize or secure cyber data that has been searched or accessed by seizing or similarly securing both computer systems. In certain circumstances when data is stored in unique operating systems that cannot be copied, it is unavoidable that the data carrier as a whole has to be seized. Article 19(3) also makes provision for alternative powers to make and retain a copy of accessed computer data, to maintain the integrity of the relevant stored computer data, and to render inaccessible and remove the computer data in the accessed computer system.

Article 19(4) makes provision for the cooperation of knowledgeable persons who could help to make searches more effective and cost-efficient for both the law enforcement agencies and the innocent individuals affected. Competent authorities are authorised to order any person with knowledge about the functioning of a computer system or measures employed to protect the computer data in it in order to provide as is reasonable the information needed to undertake the search measures provided in article 19(1) and (2).

The parameters of the search for and seizure of evidence

In terms of article 19(5) of the Convention measures of search and seizure are subject to article 14, which sets the parameters for the scope of all domestic procedural provisions contained in section 2 of the Cybercrime Convention.

Article 22 of the Convention obliges parties to establish jurisdiction over the criminal offences enumerated in articles 2 to 11 of the Convention. Article 22(1)(*a*) is based on the principle of territoriality. It requires parties to assert jurisdiction if these crimes are committed within their territory.

Safeguards for the search and seizure of electronic evidence

Article 19(5) of the Convention specifically provides that measures of search and seizure are subject to article 15, which specifies certain conditions and safeguards that must be provided for under domestic law in respect of all the domestic procedural provisions contained in section 2. In applying binding international obligations and established domestic principles, national legislatures must determine which of the procedural powers

and procedures are sufficiently intrusive to require the implementation of particular conditions and safeguards (Explanatory Report to the Cybercrime Convention 27). Article 15(1) of the Convention stipulates that the establishment, implementation and application of search-and-seizure mechanisms are subject to the conditions and safeguards provided for under the domestic law of each party. The safeguards include the right against self-incrimination, legal privileges and the specificity of individuals or places that are the object of the application of the measure (Explanatory Report to the Cybercrime Convention 27).

There are minimum safeguards to which parties to the Cybercrime Convention must comply with in balancing the interests of law enforcement and the protection of fundamental human rights. These safeguards must ensure the adequate protection of human rights and liberties. The safeguards may be provided for constitutionally, legislatively, judicially or otherwise (Explanatory Report to the Cybercrime Convention 27). Article 15(2) of the Convention requires that the conditions and safeguards include grounds justifying the application of the power or procedure and the limitation on the scope of the duration of such grounds. The principle of proportionality must be incorporated as a safeguard to the procedural powers of search and seizure in terms of article 19 of the Convention. Each party must implement proportionality in accordance with the relevant principles of its domestic law.

Transborder search and seizure of evidence

The Cybercrime Convention also makes provision for search-and-seizure mechanisms at an international level. In terms of article 31(1), each party must have the ability, for the benefit of another party, to search for or seize and disclose data stored by means of a computer system located within its national territory. This mechanism includes data that has been preserved pursuant to article 29. Article 31(2) stipulates that a mutual assistance request regarding the accessing of stored computer data should be responded to through the application of international instruments on international cooperation in criminal matters, arrangements agreed on on the basis of uniform or reciprocal legislation and domestic laws, referred to in article 23. Such cooperation must also comply with chapter III of the Convention. Article 31(3) of the Convention stipulates that a request for search and seizure must be responded to on an expedited basis where there are grounds to believe that the relevant data is particularly vulnerable to loss or modification or otherwise where the relevant treaties, arrangements or laws provide for such expedited cooperation.

Production orders in cyber environments

Article 18 of the Cybercrime Convention provides for a domestic production order directed at stored computer data. A production order provides for a flexible procedural measure which law enforcement can consider applying for in lieu of measures that are more intrusive or more onerous, such as search and seizure. Often, third parties as custodians of

data are willing to assist law-enforcement authorities voluntarily by providing data under their control. A production order provides an appropriate legal basis for such assistance, relieving such third parties of any contractual or non-contractual liability. In terms of article 18(1)(*a*) of the Convention, a party must ensure that its competent law-enforcement authorities have the power to order a party in its territory to submit specified computer data stored in a computer system, or a data storage medium that is in that person's possession or control.

Preservation and partial disclosure orders in cyber environments

Articles 16 and 17 of the Cybercrime Convention provide for domestic preservation and partial disclosure orders. Data preservation, which for the majority of countries is an entirely new legal phenomenon, is an important investigative tool in addressing crimes committed more specifically in the cyber environment. A preservation order may be less disruptive to the normal activities and the reputation of legitimate businesses than the execution of a search-and-seizure warrant on their premises. In situations where the custodian of the data is trustworthy, the integrity of the data can be secured more quickly and efficiently by means of an order to preserve the data (Explanatory Report to the Cybercrime Convention 29). Article 16 of the Convention is intended to ensure that national competent authorities are able to order or similarly obtain the expeditious preservation of specified stored computer data in connection with a specific criminal investigation or proceeding. Each party may determine the appropriate manner of preservation within the context of its domestic law (Explanatory Report to the Cybercrime Convention 29). Article 16(2) provides that a person who receives a preservation order in respect of specified stored computer data in the person's possession or under their control is obliged to preserve and maintain the integrity of that computer data for a maximum of 90 days in order to enable competent authorities to seek its disclosure.

Expedited preservation and partial disclosure of traffic data

Article 17 of the Cybercrime Convention imposes specific obligations with regard to the preservation of traffic data in terms of article 16 and provides for the expeditious disclosure of some traffic data so as to identify other service providers that were involved in the transmission of specified communications.

Transborder preservation and partial disclosure orders in cyber environments

Articles 29 and 30 of the Cybercrime Convention provide for the transborder expedited preservation of stored computer data and the transborder expedited disclosure of preserved traffic data. Article 29 ensures the availability of volatile computer data in the territory of

another party pending the longer and more involved process of executing a formal mutual assistance request that will facilitate its actual disclosure. Article 29(1) authorises a party to make a request for, and article 29(3) requires each party to have the legal ability to obtain, the expeditious preservation of data stored in the territory of the requested party. The intention is to prevent the data from being altered, removed, deleted or irretrievably lost during the period required to prepare, transmit and execute a request for mutual assistance to obtain the data (Explanatory Report to the Cybercrime Convention 29).

Article 30 provides that the international equivalent of the power established for domestic use in article 17 of the Convention. The international mechanism requires a party requested to preserve traffic data concerning a specific communication expeditiously to disclose to a requesting party a sufficient amount of traffic data to identify service providers, and the parts of the communication from other territories.

In South Africa

In South Africa domestic search for and seizure of electronic evidence is regulated by various legislative mechanisms. The first of these is chapter 2 of the Criminal Procedure Act 51 of 1977 (the CPA), which provides for search warrants, searches and seizures without a warrant, the entering of premises, and the forfeiture and disposal of property connected with offences.

Furthermore, sections 82 and 83 of the Electronic Communications and Transactions Act 25 of 2002 (the ECT Act) provide additional search and seizure powers to cyber inspectors that other statutory bodies with the powers of inspection or search and seizure could also draw from. In addition, section 205 of the CPA provides for the general production of information, and sections 17, 19, 23, 39(3) and 40(3) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICPCIA) make provision for certain categories of communication data to be made available.

No specific legislative provision is made for the expedited preservation and partial disclosure of stored computer data. The preservation and partial disclosure of stored computer data is currently facilitated by traditional powers of search and seizure. Section 30(2) of the RICPCIA is relevant in determining the expedited preservation of traffic data as required by the Cybercrime Convention, to the extent that communication-related information is preserved by default.

Transborder search and seizure and the preservation of electronic evidence are facilitated in terms of a broader mutual legal assistance framework. The International Co-operation in Criminal Matters Act 76 of 1996 is the enabling legislation that provides for the domestic legal basis for mutual legal assistance. This Act deals inter alia with the mutual provision of evidence and information. To a large extent, uncertainty exists as to whether the mutual facilitation of searches and seizures is enabled by this Act or by chapter 2 of the CPA.

Articles or things susceptible to search and seizure

Section 20 of the CPA prescribes the type of article which may be seized in terms of this Act. Section 20 is very wide. It stipulates that 'anything' may be seized, 'anything' being referred to as 'an article' in chapter 2 of the CPA. Although the specific nature of articles that may be seized in terms of section 20 is not clear, it is submitted that 'anything' should be susceptible to a wide enough interpretation to also include the search for and seizure of electronic data. The seizure of a particular computer would, however, be allowed in terms of chapter 2 of the CPA. Chapter 2 of the Act will, however, not apply to the search of a computer and the seizure of information located on that computer. It is submitted that these provisions of the Art should be restructured in order to reduce the restrictive interpretation of the word 'article' as a physical entity, as stipulated in sections 20 and 21 of the Act. In current law enforcement, the provisions of chapter 2 of the Act are widely interpreted and applied to facilitate a search for and seizure of electronic data. This practice has not yet been contested in a court of law (*Beheersmaatschappij Helling I NV v Magistrate Cape Town* 2007 (1) SACR 99 (C)).

In terms of section 82(3) of the ECT Act, the CPA applies, with the necessary changes, to searches and seizures in terms of the Act. It is questionable that section 82(4) of this Act specifically stipulates that any reference in the CPA to 'premises' and 'article' for the purposes of the ECT Act includes an information system as well as data messages.

Search and seizure in terms of the ECT Act

The ECT Act has now created 'cyber inspectors' who, with the authority of a warrant, may enter any premises or access information that is related to an investigation into possible cybercrime. Chapter XII of this Act provides for the appointment of cyber inspectors within the Department of Communications.

The powers of these cyber inspectors are well defined in the ECT Act and include the authority to search premises or information systems, or search a person or premises if there is reasonable cause to believe that they are in possession of an article, document or recording which is related to an investigation. Section 81(1) of the Act provides for the general powers of cyber inspectors. In the performance of any function in terms of the Act, a cyber inspector must be in possession of a certificate of appointment, which must be produced on demand to any person whose rights are affected.

In terms of the ECT Act, any statutory body with powers of inspection or powers of search and seizure in terms of any law, specifically referring to the South African Police Service, may apply for assistance from a cyber inspector. Such assistance may be authorised by the Department of Communications, subject to certain conditions. It is submitted that the reason for and intention behind these requirements is neither apparent nor clear and that in cases where cyber inspectors are approached to assist in a case, they

should do so in an advisory capacity and without taking over the investigation per se. It is further submitted that these requirements do not seem to allow other persons and entities who otherwise would not have been allowed to search or seize to approach the cyber inspectorate for assistance.

In terms of section 83 of the ECT Act cyber inspectors are also empowered to access and inspect the operation of any computer or equipment forming part of an information system used or suspected to have been used in an offence and require any person in control of, or otherwise involved in the operation of a computer, to provide reasonable technical assistance.

Section 83(1) of the ECT Act provides that any magistrate or judge may issue a warrant required by a cyber inspector, upon request from a cyber inspector, but subject to the provisions of section 25 of the CPA. It is interesting to note that section 83(1) of the ECT Act, unlike the CPA, does not include reference to a peace officer. The warrant must identify the premises or information system that may be entered and searched. In terms of section 83(3) of the ECT Act the warrant must specify the acts which may be performed under the warrant by the cyber inspector to whom the warrant is issued. Such a warrant to enter, search and seize may be issued at any time. The warrant is valid until it has been executed or for one month from the date on which it was issued. In terms of section 83(3) and (4) of the ECT Act a warrant is no longer valid if the purpose for issuing it has lapsed or if it is cancelled by the person who issued it or, in the case of that person's absence, by a person with similar authority. Section 83(5) provides that a warrant to enter and search premises may be executed only during the day, unless the judge or magistrate who issues the warrant authorises that it may be executed at any other time. A section 83(1) warrant empowers a cyber inspector to enter any premises without prior notice or to access an information system that is related to an investigation at any reasonable time. Section 82(1) empowers a cyber inspector to inspect, search and seize and mandates him or her to take certain steps.

Section 83(2) of the ECT Act provides that where a cyber inspector requests a magistrate or a judge to issue a warrant in terms of section 83(1), such a magistrate or judge may issue a warrant under certain circumstances.

Section 83(2) broadens the jurisdictional requirements, comparatively as set out in section 25 of the CPA, namely, the restrictive territorial requirement that the offence has been committed or is being committed within the jurisdiction of the issuing magistrate.

In terms of section 82 of the ECT Act a person who refuses to cooperate with or hinders a person conducting a lawful search shall be guilty of an offence. Further, section 80(5) stipulates that any person who hinders or obstructs a cyber inspector in the performance of his or her functions in terms of chapter XII of the Act (including section 82) shall be guilty of an offence. In terms of section 80(5)(*b*), a person who falsely claims to be a cyber inspector shall be guilty of an offence.

In terms of section 82(1)(*f*), a cyber inspector may have access to and inspect the operation of any computer or equipment that forms part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause

to suspect is or has been used in connection with any offence. It should be noted that section 82(1)(*f*) is the only section that does not refer to a specific investigation, but instead refers to 'any offence'. It is submitted that it appears that the legislature authorises cyber inspectors to conduct a search and seizure even in circumstances when such a search and seizure is not specifically authorised in a warrant. Such circumstances may arise where a cyber inspector, in the course of a search and seizure in terms of a warrant, develops a reasonable suspicion that an offence using computer equipment on the premises, where the investigation of the equipment was not specified in the warrant, has been or is being committed. It is submitted that it appears that section 82(1) provides for a practical arrangement to further the investigation of crime, in that the suspension of a search-and-seizure investigation to acquire a new or additional warrant may cause valuable evidence to be destroyed. It is submitted that the latter submission must be considered, taking cognisance of the fact that the general introduction to section 82(1) empowers cyber inspectors to enter any premises or access an information system that has a bearing on an investigation. It is further submitted that, in the first instance, section 82(1)(*f*) was initiated in the context of an initially specified investigation, but that the scope of such an investigation may be extended to access and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material reasonably suspected of being used or to have been used in connection with any offence.

Contrary to chapter 2 of the CPA, section 84 of the ECT Act specifically provides for the preservation of confidentiality. In terms of section 84(1) of the ECT Act a person who pursuant to any powers conferred under chapter XII of the Act has obtained access to any information may not disclose such information to any other person. Exceptions are provided for in that such information may be disclosed for the purposes of the ECT Act and for the prosecution of an offence or pursuant to a court order. In terms of section 84(2) unauthorised disclosure is criminalised.

Transborder search for and seizure of electronic evidence in cyber environments

Search-and-seizure investigations are coercive measures which infringe upon an individual's right to privacy and associated fundamental human rights. On the basis of the fact that the central doctrine of international law maintains that jurisdiction is strictly territorial in nature, an effective domestic legal mechanism is critically imperative (*Reuters Group PLC v Viljoen NNO* 2001 (12) BCLR 1265 (C) 127). In the domain of international cooperation, mutual legal assistance is the most rapidly growing component (Proust 2003, 295–310).

South Africa has progressed rapidly in making its legal processes available to the international community and in enhancing its own mechanisms for seeking legal assistance from abroad (D'Oliveira 2003, 323). There has been an explosion of

mechanisms providing for such assistance and substantial developments in the principles encompasses its application and practice. South Africa's current mutual legal assistance measures comply with the central requirements of international practice, although there are a number of aspects that warrant attention, predominantly in the area of role-player coordination and administrative arrangements. There are certain legislative and regulatory lacunae, however. For instance, in the International Co-operation in Criminal Matters Act no provision is made for the transfer of persons in custody to assist with investigations or to testify in a requesting state. No such enabling legislation has, as yet, been incorporated into domestic legislation with regard to correctional services.

In a case where coercive assistance is involved, it must first be ascertained whether South Africa is a convention or treaty partner with the requesting or requested state. Bilateral or multilateral treaties (section 27(1) of the International Co-operation in Criminal Matters Act and section 83(1), read together with section 231(1) of the South African Constitution), supported by domestic law, constitute an enhanced and flexible basis for international cooperation. The process of obtaining and providing evidential information with regard to extradition where criminal proceedings are pending constitutes one of the roots of mutual legal assistance. In treaties with other countries, South Africa has committed itself to the seizure and surrender of articles connected with the proving of an offence which is the subject of extradition (GN 292 of 1968 in *Government Gazette* 2179).

Chapter 2 of the International Co-operation in Criminal Matters Act provides for the mutual provision of evidence and information between states. A request from a foreign state for assistance in obtaining evidence in South Africa for use in such a foreign state must be submitted to the South African Director-General of Justice. If the director-general is satisfied, he or she must submit the request to the Minister of Justice and Constitutional Development for approval, upon whose approval the director-general must forward the request to the magistrate within whose area of jurisdiction the witness resides. The Act also provides for a subpoena, including *duces tecum*, an examination of witnesses, the rights and privileges of and offences by witnesses, which are indicative of the coercive element embedded in the provisions.

The International Co-operation in Criminal Matters Act also makes provision for a request to the authorities of a foreign state for obtaining not only evidence generated from proceedings in a court, but also information from a foreign agency via a judge in chambers or a magistrate. The procedure in section 2(1) of the Act is intended for hearings in which it appears to the court that the examination of a person in a foreign state is necessary in the interests of justice and that the attendance of such a person cannot be obtained without undue delay, expense or inconvenience. The court may then issue a letter of request for the evidence of the person for use in the proceedings. A letter of request is defined in s 1 of the Act as a letter requesting assistance of the nature contemplated in sections 2 (the provision of evidence or information), 13 (assistance in recovering a fine or compensation), 19 (assistance in enforcing a confiscation order) and 23 (assistance in enforcing a restraint order).

Section 2(2) of the Act makes provision for obtaining information prior to instituting proceedings, for use in an investigation related to an alleged offence. Upon application, a judge in chambers or a magistrate may issue an *ex parte* letter of request seeking to obtain information. Provision is made for the person in charge of the investigation to submit interrogatories to be attached to the letter of request, provided that this is permitted by the law of the requested state and, under the same *proviso*, to appear at the examination and question the person concerned.

In South Africa, the legal basis for search and seizure in mutual legal assistance practices is rather vague and unclear. In certain instances, chapter 2 of the CPA, together with section 31 of the International Co-operation in Criminal Matters Act, is relied upon to facilitate mutual search-and-seizure investigations. In other instances the provisions of sections 2 and 7 of the International Co-operation in Criminal Matters Act is used to enable mutual searches and seizures. It is submitted that the existing statutory criminal procedural arrangements for rendering search and seizure specific international assistance predates the International Co-operation in Criminal Matters Act. It is further submitted that this statute does not deal with search and seizure per se, but leaves existing law in place. And it is further submitted that the provisions of search and seizure and the specifics of assistance provided are not expressly limited, because section 31 of the International Co-operation in Criminal Matters Act stipulates that nothing contained in the Act shall be construed so as to prevent or to abrogate or derogate from any arrangement or practice for the provision or obtaining of international cooperation in criminal matters, otherwise than in the manner provided for by the said Act. However, in *Beheersmaatschappij Helling I NV v Magistrate Cape Town* 2007 (1) SACR 99 (C), the court held that where a foreign request for assistance entails intrusive, legally compulsive or coercive measures, such as an arrest, subpoena or search and seizure, legal mechanisms must be found in the domestic law of South Africa that authorise such measures. The court emphasised that the respondent's reliance on section 31 of the International Co-operation in Criminal Matters Act as justification for the application for an issue of search warrants was misplaced. The court advanced the view that, first, section 31 of the International Co-operation in Criminal Matters Act does not in itself confer any power on the State, that it merely preserves any pre-existing which must be derived from a legal source. The court maintained that neither the State nor the prosecuting authority enjoys a residual power in this regard, which is to be found in any other source. Secondly, the court advanced the view that there is no evidence of the existence of any arrangement or practice of the kind referred to in section 31. It does not necessarily mean that the Act is silent on the subject of searches and seizures, or that the legislature did not intend the Act to apply to evidence obtained by those means. The court also found no incompatibility between sections 20 and 21 of the CPA and section 7 of the International Co-operation in Criminal Matters Act.

Section 36(1) of the CPA provides for the delivery or disposal of a seized article with which an offence was committed or is on reasonable grounds suspected to have

been committed in a country outside South Africa. By implication, the International Co-operation in Criminal Matters Act does not limit other forms of assistance: indeed, the widest measure of assistance is to be provided. South Africa has positioned itself with the injunction to provide other jurisdictions with the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings with regard to criminal offences.

Section 16 of the International Co-operation in Criminal Matters Act provides for the express introduction of dual criminality of extradition law into the South African mutual assistance law by way of exception. Apart from the latter exception which enables the Minister of Justice and Constitutional Development to apply the dual criminality requirement, there is no statement of grounds for refusal in the International Co-operation in Criminal Matters Act. Despite the fact that section 16 begins with the words 'without limiting the Minister's discretion in any manner', nowhere is there any legislative indication of the components of such a discretion. South Africa's mutual assistance treaties generally contain suitable statements – for example, article 6 of the SADC Protocol and section 11 of the Extradition Act 67 of 1962 – in which provision is made for the minister's discretion in extradition matters, but this does not remedy the lacunae in the domestic legislation. Further, it is submitted that the International Co-operation in Criminal Matters Act is silent on aspects of confidentiality and use limitations, areas in which South African treaty-making is ahead of the Act. It is submitted that the legislature could draw from the formulations contained in South African treaties in remedying the lacunae.

CONCLUSION

Traditional investigation methods are generally ill-equipped to deal with cybercrime. The investigators are no longer dealing purely with tangible physical items situated on premises, but are required to investigate crimes perpetrated through highly sophisticated technology, and sometimes through borderless information networks.

The laws inherently governing the criminal justice system were developed in a physical world and the question arises whether the traditional law can accommodate the electronic medium, commonly referred to as 'cyberspace', whether the traditional law should be adapted to the electronic medium or whether new laws should be drafted? Cybercrime (commonly referred to as 'computer crime') is a new type of criminal activity which started presenting legal challenges in the early Nineties, as the internet became a common space for online users worldwide. Cybercrime can be defined as any criminal activity that involves a computer; it can be divided into two categories. First, it deals with crimes that were not possible to commit before the advent of the computer, such as hacking. The second category of computer crime is much broader: it has been in existence for centuries, but is now committed in the cyber environment. Such crimes include internet fraud and child pornography.

The Cybercrime Convention is a multilateral instrument directed specifically at addressing crimes committed in an electronic medium. The Convention is aimed at combating cybercrime by requiring signatory countries to establish certain substantive offences and to adopt domestic procedural laws to investigate cybercrime. Furthermore, it seeks to address criminal and procedural law at an international level to ensure the harmonisation of laws governing the various criminal justice systems, and to provide international cooperation and assistance in criminal investigations.

Although the Convention aims at international cooperation in prosecuting cybercrime, it contains no provision for cooperation in securing networks. The Convention's aim to harmonise national laws to facilitate the police's ability to act across national borders is a giant step in the right direction and is therefore laudable. However, it is difficult to implement in practice.

South Africa has signed but did not ratify the Convention. The country has complied with the first part of the Convention in terms of which member states are obliged to criminalise illegal access to a computer system; the illegal interception of data in a computer system; the use of inauthentic data with the intention of exposing it as authentic; the infringement of copyright-related rights online; the interference with the data or functioning of a computer system, and online child pornography.

The search-and-seizure mechanisms proposed by the Cybercrime Convention are subject to article 14 of the Convention. Article 22 requires parties to establish jurisdiction over the criminal offences created in articles 2 to 11, based on the principles of territoriality and nationality.

In terms of articles 23 and 25(1) international cooperation is to be provided among parties to the widest possible extent and impediments to it must be limited. The Convention does not create a separate general mutual assistance regime in lieu of existing mutual legal assistance frameworks. The grounds on which parties may refuse to cooperate are those provided for in the domestic law of the requested party and applicable mutual assistance treaties.

South African search and seizure mechanisms are provided for in chapter 2 of the CPA and chapter XII of the ECT Act. Article 19 of the Cybercrime Convention requires that domestic search-and-seizure mechanisms must be directed at stored computer data; furthermore, that such mechanisms aimed at computer data must be equivalent to the power to search for and seize tangible objects. Any statutory body conferred with powers of search and seizure in terms of any law may apply to a cyber inspector for assistance. Such a body cannot otherwise acquire a warrant issued in terms of section 83 of the ECT Act. The search-and-seizure mechanisms provided for in the CPA are the only mechanisms available to law enforcement officers. Article 19 also requires that domestic search-and-seizure mechanisms must be capable of inducing coerced cooperation for the purposes of enabling a search-and-seizure investigation. The ECT Act provides for cooperation in this regard.

The following specific conclusions are extracted from a comparative analysis of

South African search and seizure of electronic evidence approaches and those proposed by the Cybercrime Convention (where applicable, recommendations are provided):

1. Article 19 of the Cybercrime Convention stipulates that domestic search-and-seizure mechanisms directed at computer data must be equivalent to the power to search for and seize tangible objects. It is submitted that, where applicable, the provisions in chapter 2 of the CPA must be restructured in order to deal with conflict arising from a restrictive interpretation of the words 'premises' and 'article' as physical entities. This can be achieved by inserting in section 1 of the CPA a provision similar to section 82(4) of the ECT Act, which reads:

   'any reference in the Criminal Procedure Act to "premises" and "article" includes data messages as well as information communication systems.'

2. In terms of section 81(2) of the ECT Act any statutory body with powers of inspection or search and seizure in terms of any law may apply for assistance from a cyber inspector. Such a body cannot otherwise obtain a warrant issued in terms of section 83 of the ECT Act. The existing search-and-seizure mechanisms provided for in chapter 2 of the CPA are the only legal mechanisms available to law enforcement officers. It is submitted that there is uncertainty with regard to the applicability of the search-and-seizure mechanisms provided for in chapter 2 of the CPA with regard to computer data. It is submitted that chapter 2 of the CPA should be realigned to address these complications and challenges which hamper and challenge law-enforcement and investigative initiatives. It is also submitted that it is untenable, and that there is no substantive reason why all law-enforcement efforts pertaining to electronic evidence should be dealt with via a cyber inspectorate.
3. Article 19 of the Cybercrime Convention requires that domestic search-and-seizure mechanisms must allow for an extension of the search or access by establishing a connection from a legally accessed computer to other computer systems within the same national territory. Sections 21(1)*(a)* and 25(1) of the CPA provide that a magistrate may issue warrants only for articles within his or her specific area of jurisdiction; these provisions will render the tedious and cumbersome acquisition of multiple warrants a necessity in networked environments. It is submitted that the latter restrictive territoriality requirement is not conducive to effective law enforcement, and that the relevant sections should be readdressed. It is further submitted that this can be done by realigning sections 21 and 25 of the CPA with section 83(2) of the ECT Act.
4. Article 19 of the Cybercrime Convention stipulates that domestic search-and-seizure mechanisms must be capable of inducing coerced cooperation in order to enable a search-and-seizure investigation in circumstances where it is reasonably permissible. It is submitted that the use of reasonable force to overcome resistance,

as provided for in section 27 or the CPA, does not per se induce coerced cooperation in the execution of a search-and-seizure intervention. Further, section 205 of the CPA is not capable of an expedient enough application to address the dictates of a search-and-seizure intervention in a cyber context. It is submitted that these provisions of the CPA should be restructured in accordance with article 19 of the Cybercrime Convention by inserting an additional provision similar to the provision contained in section 82(1)(*h*) of the ECT Act.

5. The Cybercrime Convention specifically recommends the preservation of stored computer data and the preservation and partial disclosure of stored traffic data. The Convention stipulates that such preservation and/or partial disclosure should be facilitated by means of traditional mechanisms of search and seizure. In South Africa, however, no specific provision is made in the legislative framework for the expedited preservation of stored computer data or for the expedited preservation and partial disclosure of stored traffic data. It can be argued that the effect of the data retention requirement created by section 30 of the RICPCIA caters for this need by default. However, it should be noted that section 30 is not concerned with all categories of computer data, but is directed only at communication-related information. It is submitted that the creation of a criminal-law mechanism similar to an Anton Pillar order could protect the privacy of data and ensure its availability expediently.

6. In the South African legislative framework there is no prohibition on making and attending to urgent mutual assistance requests through expedited means of communication as provided for in article 25(3) of the Cybercrime Convention. It is submitted that it is necessary to lay down certain levels of security and authentication for such communications, and further prescribe what constitutes acceptable expedited means of formal confirmation of mutual legal assistance requests. It is submitted that the Minister of Justice should, by regulation under section 33 of the International Co-operation in Criminal Matters Act, direct the latter prescription.

7. In terms of article 27(9)(*a*)–(*d*) of the Cybercrime Convention pertaining to requests from foreign states to South Africa, South Africa must facilitate direct communication between judicial authorities or Interpol in urgent cases. In terms of article 27(9)(*e*) of the Convention South Africa must permit direct communication between the judicial authorities or Interpol with regard to mutual legal assistance requests that can be adhered to by the requested party without resorting to coercive action. It is submitted that it is doubtful and questionable whether a declaration under article 40, read together with article 27(9)(*e*) of the Convention, to direct that urgent mutual legal assistance requests from foreign states be addressed to the South African central authority, will be in the interests of efficiency and expediency. It is therefore submitted that South Africa should not avail itself of this reservation.

8. In addition, apart from the one exception in section 16 of the International Co-operation in Criminal Matters Act, which enables the Minister of Justice to apply the dual criminality in respect of the mutual execution of sentences and compulsory orders, there are no stated grounds for refusal in the International Co-operation in Criminal Matters Act. It is submitted that this is a vacuum or void in South African law that is required to be addressed. It is further submitted that the International Co-operation in Criminal Matters Act should contain specific substance that addresses both outgoing and incoming requests for all role-players.

REFERENCES

Publications

D'Oliveira, J. 2003. 'International co-operation in criminal matters: The South African contribution' *SA Journal of Criminal Justice*. 16(3):323–369.

Kumar. 2010. 'Africa could become the cybercrime capital of the world'. Available at http://www.psfk.com. Accessed 5 May 2011.

Marler, SL. 2002. 'The Convention on Cybercrime: Should the United States ratify?' *New England Law Review.* 11(1): 68–79.

Moore, RE. 2003. 'Search and seizure of digital evidence: An examination of constitutional and procedural issues'. PhD thesis University of Southern Mississippi. http://aquila.usm.edu/theses_dissertations

Nieman, A. 2006. 'Search and seizure, production and preservation of electronic evidence'. LLD thesis North-West University. http://dspace.nwu.ac.za/handle/10394/1367

Proust, R. 2003. 'International co-operation: A Commonwealth perspective'. *SA Journal of Criminal Justice* 16(3):295–310.

The Council of Europe 'Cybercrime Convention Budapest 23.X1.2001 CETS No: 185'. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=&CL=ENG. Accessed 10 June 2011.

United States Report of the President's Working Group on Unlawful Conduct on the Internet 'The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet.' Available at http://www.usdoj.gov/criminal/cybercrime/unlawful.htm. Accessed 27 January 2011.

Van der Merwe, DP. 2000. *Computers and the Law* (2 ed). Cape Town: Juta.

Volonino, P. 2003. 'Electronic evidence and computer forensics' *Communications of the Association for Information Systems;* 1.

Wall, DS. 2003. *Cyberspace Crime.* Washington: Ashgate Publishing.

Whatis.com Definitions 'Data'. Available at http://searchstorage.techtarget.com/Definition/0.sid5. Accessed 21 February 2011.

Whitcomb, CM. 2002. 'A historical perspective of digital evidence: A forensic scientist's view' *International Journal of Digital Evidence.* 1(1):19–23

Cases

Beheermaatschappij Helling I NV v Magistrate, Cape Town 2007 (1) SACR 99 (C)

Reuters Group PLC v Viljoen NNO 2001 (12) BCLR 1265 (C) 127

Statutes

Constitution of the Republic of South Africa, 1993 Act 200 of 1993, (interim Constitution)

Constitution of the Republic of South Africa, 1996, Act 108 of 1996

Criminal Procedure Act 51 of 1977

Electronic Communications and Transactions Act 25 of 2002

GN 292 of 1968 in *Government Gazette* 2179 (South Africa)

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002