Addressing the Challenges posed by Cybercrime: a South African Perspective

Fawzia Cassim
Associate Professor of Law
University of South Africa, Pretoria, South Africa
cassif@unisa.ac.za

Abstract: The South African common law has proven to be ineffective in addressing cybercrime. The Electronic Communications and Transactions Act, Act 25 of 2002 ("ECT") was introduced to address *inter alia* cybercrime in South Africa. Whilst the advent of the ECT is lauded, there is room for improvement. To illustrate this, section 15 of the ECT which facilitates the admission of information in electronic format is laudable, but the criminal sanctions in the Act appear to be inadequate. Recent case law also reveals that the courts are adopting a cautious approach towards cybercrime cases. A call for a more clear and concise judicial guidance is required. The South African banking sector is also vulnerable to cybercrime. However, the establishment of organisations such as SABRIC to combat cybercrime in the banking industry is welcomed. Although South Africa has adopted the Council of Europe's Convention in Cybercrime, it has not ratified the treaty. It is recommended that South Africa should ratify the treaty to avoid becoming an easy target for international cybercrime. This paper will deal with measures addressing cybercrime in South Africa and the way forward.

1 Introduction

Most of the so-called traditional crimes such as murder, rape, theft, malicious injury to property and housebreaking all originate from the South African common law namely, Roman-Dutch law. These traditional crimes only deal with tangibles, whereas cybercrime deals with intangibles. Before the commencement of the Electronic Communications and Transactions Act, Act 25 of 2002 (hereinafter, the "ECT"), the common law and statutory law applied to online forms of offences such as *inter alia*, indecency (child pornography), fraud (cyber fraud) and *crimen injuria* (cyber-smearing).[1] However, the common law was ineffective in addressing crimes such as theft, extortion, spamming and phishing. The perception thus arose that the common law cannot effectively deal with cybercrime.[2] The courts have also held that in terms of the 'prevailing law' they could not admit into evidence disputed documents, which contained information that has been processed and generated by a computer.[3] Thus, a need arose for the enactment of specific cyber legislation to address cybercrime.

[1] Prior to the inception of the ECT, crimes such as possession and distribution of child pornography could be prosecuted in terms of ss 27(1) and 28 of the Films and Publications Act 65 of 1996. It should be noted that we have a mixed or hybrid legal system in South Africa comprising the following sources of law : (1) statutory law (the Constitution 108 of 1996 is the supreme law in the land);
(2) common law comprising Roman Dutch authorities (inherited from our Dutch colonisers) and judicial authorities;
(3) African customary law and;
(4) foreign and international law.

[2] To illustrate this, the common-law crime of theft is not suitable for combating IT crime in South Africa. So too, the common-law crime of fraud. For further discussion about the inability of the common law to address cybercrime, see Burchell J "Criminal Justice at the crossroads" (2002) *South African Law Journal* 579 at 585.

[3] *S v Mashiyi* (2002) 2 SACR 387 at 393 C-D. This case considered the question of admissibility of computer-generated documents. The court held that documents which contain information that has been processed and generated by a computer are not admissible as evidence in a criminal trial. This case was decided before the inception of the ECT. For further discussion about case law addressing cybercrime crime before the inception of the ECT, see Van der Merwe DP *et al Information and Communications Technology Law* 70-74 (Lexis Nexis 2008).

2 The advent of the Electronic Communications and Transactions Act, Act 25 of 2002 (hereinafter, the "ECT")[4]

The main aim of the ECT is "to provide for the facilitation and regulation of electronic communications and transactions". However, the focus of the ECT is to protect "data" (electronic communications) or data messages. The ECT deals comprehensively with cybercrime in sections 85-89, Chapter X111. The following offences are punishable offences in the ECT: section 86(1) criminalises unauthorised access or interference with data, whereas section 86(2) prohibits unlawful modification of data; sections 86(3) and 86(4) introduce new forms of crimes called hacking law and anti-cracking (anti-thwarting) law (which prohibits the selling, designing or producing of anti-security circumventing technology); denial of service attacks is addressed in terms of section 86(5) whereas spamming is addressed in terms of section 45; the crimes of extortion, fraud and forgery are addressed in terms of section 87.[5] Section 3 of the ECT provides that in instances where the ECT has not made any specific provision for criminal sanctions, then the common law will prevail. However, other statutory remedies prevail in the prosecution of other cybercrime, for example, the Prevention of Organised Crime Second Amendment Act 38 of 1999 ("POCAA") addresses money laundering.[6]

The traditional requirement for documentary evidence is that it must be relevant and admissible, its authenticity must be proven and the original document must be produced.[7] This has now changed as a result of section 15 of the ECT which provides that the rules of evidence cannot be used to deny the admissibility of data messages on the mere ground that it is not in its original form.[8] The ECT thus creates a rebuttable presumption that data messages and printouts are admissible in evidence.[9] This facilitates the admission of information in electronic format which is commendable.

The Act has also created 'cyber-inspectors' who are authorised to enter premises and to obtain information that may impact on an investigation into cybercrime.[10] However, it is submitted that the provision in respect of search and seizure (namely, section 82) may infringe section 14 (right to privacy) and section 25 (right to property) of the Constitution 108 of 1996.[11] The criminal sanctions in the ECT have also been criticised for being inadequate.[12] To illustrate this, section 89(1) prescribes a maximum period of 1 year imprisonment for most crimes prohibited by section 86, whilst the crimes prohibited in sections 86(4) and (5) (denial of service attacks) and section 87 (extortion, fraud and forgery) prescribe a fine or imprisonment not exceeding 5 years. More stringent penalties are required to deter cyber criminals.

---

[4] It should be noted that this discussion deals only with certain provisions of the ECT.

[5] The creation of new crimes such as hacking is considered to be one of the greatest contributions by the ECT. It is submitted that any measure that protects the integrity of data is welcomed, as this is fundamental to successful electronic commerce. Also see Mndzima and Snail "Cybercrime in South Africa" 2009 available at http://www.hg.org/article (date of use 14 April 2009), Van der Merwe DP "Computer crime-recent national and international developments" (2003) 66 *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* (*THRHR)* 30 at 43-44 and Van der Merwe DP "Information technology crime – a new paradigm is needed" (2007) 70 *THRHR* 309 at 313 for further discussion about these provisions.

[6] It should be noted that POCAA targets organised crime, money laundering and criminal gang activities both nationally and internationally.

[7] See *inter alia*, *Seccombe v AG* (1919) TPD 270 at 277; *S v Mpumlo* (1986) 3 SA 485 (E) at 489. However, the exceptions to the general rule arise where the original document is destroyed, it cannot be located or its production is illegal. Secondary evidence is admissible in these circumstances. See *inter alia*, *Ex parte Ntuli* (1970) 2 SA 278 (W).

[8] Section 15 deals with the admissibility and evidential weight of data messages. Regarding the definition of a data message, see s 1 of the ECT. For further discussion about whether a data message constitutes hearsay, see Hofman J "Electronic evidence in criminal cases" (2006) 3 *South African Journal of Criminal Justice* 257 at 264. Regarding documentary evidence, see s 17 (production of evidence); s 14 (production of original evidence) and s 15(b)(exceptions) of the ECT respectively.

[9] According to Hofman (*ibid* at 262), the ordinary South African law on the admissibility of evidence will apply to data messages except where the ECT changes it. See *S v Motata* (Case number 63/968/07) where electronic information that is, data in the form of images and sound from a cell phone was admitted into evidence at the conclusion of a trial within a trial. Also see *Motata v Nair NO and Another* 2009 1 SACR 263 (T); 2009 2 SA 575 (T); (7023/2008)[2008] ZAFSHC 53 (11 June 2008) regarding the admissibility of playing the cellphone recordings (audio recording evidence) during the course of a trial-within-a trial.

[10] See s 82(1) of the ECT. The actions of the cyber inspectors are regulated by sections 80-84. It should be noted that very few cyber inspectors have been appointed since the inception of the ECT. Cyber inspectors don't work well in practice.

[11] Section 14 provides that everyone has a right to privacy which includes the right not to have their person or home searched, their property searched, their possession seized or the privacy of their communications infringed. Section 25 provides that no one may be deprived of property arbitrarily. However, these rights may be limited in terms of s 36 of the Constitution (limitation clause).

[12] However, the Regulation of Interception of Communication and Provision of Communications-Related Information Act 70 of 2002 ("RICA") prescribes harsher measures. Section 51 of RICA prescribes fines not exceeding R 2 000 000 or imprisonment not exceeding 10 years. Regarding juristic persons, fines may increase to a maximum of R 5 000 000. For further evaluation of the criminal provisions of the ECT, see Van der Merwe D *et al* (n 3 above) 75-78 (Lexis Nexis 2008).

Jurisdictional issues are regulated by section 90 of the ECT. [13] To illustrate this, section 90 of the ECT provides that a court in the Republic (SA) trying an offence in terms of this act committed elsewhere, will have jurisdiction in the following instances:

a) where the offence was committed in the Republic;
b) where part of the offence was committed in the Republic or the result of the offence had an effect in the Republic;
c) where the offence was committed by a South African citizen or a person with permanent residence in the Republic or a person carrying on business in the Republic;
d) or the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight from the Republic at the time that the offence was committed .[14]

It is submitted that section 90(b) facilitates the prosecution of perpetrators of viruses and hackers based abroad who may damage our local computer networks as a result of their unlawful cyber activities. A South African court will thus be vested with jurisdiction provided the above-mentioned offences "have an effect in the Republic". A South African court will also be vested with jurisdiction if a South African national commits a cybercrime abroad based solely on the nationality of the perpetrator.[15] However, the jurisdictional provisions have not escaped criticism. [16]

3 Recent case law

In *Ndlovu v Minister of Correctional Services and Another*[17] , the court had to consider *inter alia*, whether a computer print-out which was a copy, could not be admitted into evidence unless properly proved. The court found that as the print-out was generated by a computer, it was governed by the ECT. Thus, it examined section 15 of the ECT, and found that s 15(1)(a) prohibits the exclusion from evidence of a data message on the mere grounds that it was generated by a computer and not by a natural person, and s 15(1)(b) on the mere grounds that it is not in its original form. However, the court found that the print out was admissible into evidence not in terms of section 15 of the ECT, but in terms of the court's statutory discretion to admit hearsay evidence in terms of the Law of

[13] Jurisdiction refers to the competence of a court to hear a matter. Usually the courts will exercise jurisdiction regarding offences committed on South African territory only. See *inter alia*, *S v Maseki* 1981 4 SA 374 (T). The general rule regarding jurisdiction was that when a crime was committed outside the borders of South Africa, a South African court will not have jurisdiction to adjudicate on the case. However, there are a number of exceptions namely, high treason, charge of theft committed in a foreign country and offences committed on board ships or on aircrafts. For further information, see Bekker P *et al* "The criminal courts of the Republic" in *Criminal Procedure Handbook* 37-38 (Juta 2007).

[14] It is submitted that s 90 is more comprehensive than article 22 of the Council of Europe's Convention on Cybercrime ("COECC"). Article 22 provides that a country has jurisdiction when an offence is committed in:
its territory;
on board a ship flying a flag of that party;
on board an aircraft registered in that country;
by one of its nationals if the offence is punishable under criminal law where it was committed or if the offence was committed outside its territorial jurisdiction of any state.
The application of s 90 is, however, limited to crimes that can be committed under the ECT.

[15] Section 90(c) is regarded as being 'too broad'. It appears that where no country has jurisdiction in respect of the offence, then the nationality of the perpetrator should play an important role in deciding where he should be prosecuted. This conforms with article 22 of the COECC.

[16] Section 90(d) is also said to be problematic, because it differs from s 28(1)(d) of the Magistrate's Courts Act 32 of 1944, which requires the 'whole cause of action' to take place within a particular court or district (territorial borders), whilst s 90(d) provides for jurisdiction in terms of nationality rather than because the offence was committed within its territorial borders. It is also problematic if the cybercrime is committed beyond our borders but the offender is prosecuted in South Africa. Then the question arises as to which regional court or district court has jurisdiction to hear the matter. The ECT has also been criticised for "missing the opportunity to address some of the jurisdictional problems, particularly the regulation of jurisdictional connecting factors in e-contracts". In this regard, see OS Sibanda "Choice of law, jurisdiction and recognition and enforcement of judgments in South Africa" in *Cyber law, Security and Privacy* Kierkegaard SM (ed) 259-266 at 264 (International Association of IT lawyers 2007). Section 90 is also criticised for failing to address sexual crimes. See Van Zyl SP "Sexual offences and the Internet: Are we ready for 2010?" (2008) 71 *THRHR* 222 at 235 in this regard.

[17] (2006) 4 All SA 165 (W). The plaintiff sued the defendants for damages as a result of an alleged wrongful imprisonment and wrongful deprivation of privileges as an awaiting-trial detainee. The documents before the court comprised print-outs reflecting the monitoring of the plaintiff from the date of his release on parole.

Evidence Amendment Act 45 of 1988. This decision has been criticised for not providing clarity on the effect of section 15 of the ECT on the authenticity rule and the hearsay rule.[18]

In *S v Ndiki and Others*[19] the state sought to introduce certain documentary evidence consisting of computer-generated print-outs, designated as exhibits D1-D9, during the course of a criminal trial. The court held that if a computer print-out contained a statement of which an individual had personal knowledge and which was stored in the computer's memory, then its use in evidence would depend on the credibility of an identifiable individual and would therefore constitute hearsay. On the other hand, where the probative value of a statement in a print-out depended on the "credibility" of the computer, then section 3 of the Law of Evidence Amendment Act 45 of 1988 would not apply.[20] The court found that because certain individuals had signed exhibits D1 to D4, the computer had been used as a tool to create the relevant documentation. Therefore, these documents constituted hearsay. Exhibits D5 to D9 had been created without human intervention and such evidence constituted real evidence. Therefore, the admissibility of this evidence depended on the reliability and accuracy of the computer and its operating systems and processes. The duty to prove such accuracy and reliability lay with the state.[21] The court's progressive approach in regarding part of the computer-based evidence as real evidence has been lauded.[22]

The above discussion demonstrates that the South African courts are adopting a somewhat cautious approach in cybercrime cases. Although the *Ndiki* decision is encouraging, a clear and concise judicial guidance on the admissibility and evidential weight of electronic evidence is needed in future cases.

4. The South African banking sector

South African banks are also vulnerable to cybercrime.[23] Cybercrime is said to be increasing rapidly in the banking industry. Many banks and companies have underestimated threats emanating from phishing, data loss, identity theft, information leakage and other cyber activities. Banks have expressed concern about the increase in phishing schemes.[24] It is acknowledged that many of the phishing operators are part of the Nigerian 419 scam.[25] The recent bank SMS scam case has also raised serious questions about the security of online banking.[26] However, the establishment of organisations such as the South African Banking Risk Information Centre ("SABRIC") to combat cybercrime in the banking industry is lauded. SABRIC provides the banking industry with crime risk information management services and facilitates inter-bank initiatives to reduce the risk of organised bank-related crime through effective public private partnerships.[27] The Minister of Police has also recently indicated his willingness to work with banks and the IT industry via SABRIC by way of private-public partnerships to combat

[18] For a critical analysis about the case, see Collier D "Evidently no so simple: producing computer-outs in court" (2005) 13(1) *Juta's Business Law* 6-9.

[19] (2008) 2 SACR 252. The accused was charged with a number of counts of fraud and theft in connection with the delivery of medical supplies to the Department of Health and Welfare in the Eastern Cape. The problem arose when the state relied on the evidence of computer printouts which constituted necessary evidence to prove the fraudulent actions. The accused objected to the admissibility of such print-outs as the ECT had not come into operation at the time of the commission of the offence. The court found that since the documents in question were admissible in terms of the existing law, it was unnecessary to make a finding on the retrospective application of the ECT.

[20] It should be noted that s 3 gives the court a discretion to admit hearsay evidence if it is in the interests of justice.

[21] It was clear from the evidence that the computer was used as a tool with respect to exhibits D1 to D4. Although printed on a computer, the exhibits were signed by a functionary as envisaged by s 34(4) of the Civil Proceedings Evidence Act 25 of 1965. Therefore, this was 'made' by a functionary as envisaged by s 34(1). The court held that exhibits D5-D9 did not comply with the requirements of s 34 as these exhibits were not 'made' by a functionary.

[22] For further discussion about the case see Van der Merwe D *et al* (n 3 above) 121-123 (Lexis Nexis 2008), where Professor van der Merwe lauds the court's progressive approach. Van der Merwe's comments are supported.

[23] See *inter alia*, and Herselman M and Warren M "Cybercrime influencing businesses in South Africa" (2004) *Issues Informing Science and Technology Education* available at http://www.dealin.edu.au/dro/view (date of use 10 June 2009). It is advocated in the latter article that South Africa should learn from and apply the Organisation for Economic Co-operation and Development (OECD) guidelines (2002) to safeguard businesses against cybercrime.

[24] The major banks such as Absa, Standard Bank and FNB have confirmed breach of their clients' accounts by phishing schemes during 2007. See Anonymous 2007 http://www.iol.co.za/general/news (date of use 27 May 2007). Also see Van der Merwe D *et al* (n 3 above) 66-67 (Lexis Nexis 2008) for further discussion about the vulnerability of South African banks.

[25] The so-called "419" swindle is named after the article in the Nigerian penal code which outlaws it.

[26] It involved a Vodacom (South African cell phone service provider/ operator) employee who was working with a syndicate to intercept SMS notifications from banks to their customers. It has been reported that about R 7-million was siphoned off from customers' accounts as result of this scam. The case is pending. See Chelemu K "Banks open files for police in SMS scam case" *The Times* 23 2009 6.

[27] SABRIC was established in 2002 as a wholly owned subsidiary of the Banking Association. Its key stakeholders are the four major South African banks, namely, Standard Bank, Nedbank, Absa and First National Bank. For further information, see http://www.sabric.co.za/home (date of use 31 August 2009).

crime.[28] A close partnership between law enforcement agencies and the private sector is necessary to address bank-related crime and to ensure that cybercrime is not allowed to thrive in the country.

5. Concluding remarks

The global nature of computer technology presents a challenge to many countries to address cybercrime.[29] Domestic solutions are inadequate because cyberspace has no geographic or political boundaries, and many computer systems can be easily accessed from anywhere in the world. It is also difficult to obtain accurate cybercrime statistics because an unknown number of crimes go undetected and unreported. It is also costly to develop and maintain security and other preventative measures. International financial organisations are also common targets for computer fraud and embezzlement schemes.[30] Organised crime and terrorist groups are also using sophisticated computer technology to bypass government detection and carry out destructive acts of violence.[31] It is thus a continuous uphill battle to develop computer crime legislation that applies to both domestic and international audiences.

Multi-national international organisations, such as the International Criminal Police Organisation (Interpol), the Commonwealth of Nations, the Group of 8 (G8) and the Organisation for Economic Co-operation and Development (OECD) , all play pivotal roles in addressing cybercrime and their work encompasses a broader territorial environment. The Interpol has also provided technical guidance in cybercrime detection, investigation and evidence collection.[32] The enactment of the Council of Europe's Convention on Cybercrime ("COECC") is also lauded because it attempts to establish consistency in the cybercrime laws of many countries. However, many states still have to sign let alone ratify the Convention to serve as a deterrent.[33] The unanimous participation of all nations is thus required to achieve meaningful prosecution.

South Africa has adopted the COECC, but has not ratified it. The treaty contains important provisions to assist law enforcement (police) in their fight against transborder cybercrime. Therefore, South Africa needs to ratify the cybercrime treaty to avoid becoming an easy target for international cybercrime.[34] The South African government seems to be presently focused on basic service delivery and more traditional crimes given the current situation in the country where crime and poverty are rife. However, steps to establish the Computer Security Incident Response Team (CSIRT) indicate that the aim to tackle cybercrime is gathering momentum.[35] South Africa is also taking steps to address child pornography on the Internet. To this end, the South African government has launched a website to alert internet server providers of criminal activities relating to child pornography or images of sexual abuse hosted on their servers.[36] The South African Law Reform Commission has also recommended the introduction of legislation on the protection of personal information (so-called "information

[28] See "Sabric encouraged by police plans" available at http://www.moneyweb.co.za/mw/view (date of use 5 October 2009).

[29] The difficulties in addressing cybercrime are due to: the lack of tools by police to tackle the problem; 'old' laws do not fit the 'new' crimes being committed; new laws have not adjusted to the reality on the ground; there are few precedents to look for guidance; there are debates over privacy issues which hamper the ability of police officers to gather evidence needed to prosecute new cases; the distrust between police and computer professionals require close co-operation between the two parties to effectively address the cybercrime problem and make the Internet a safe place. See Singh T "Cybercrime and Information Technology" available at http://www.ind/ii.org/cyberlaw.aspx (date of use 6 May 2009) 1.

[30] See Bazelon DL *et al* (2006) 43 *American Criminal Law Review* 259 at 306.

[31] The case of Rami Yousef who orchestrated the 1993 World Trade Center bombing by using encryption to store details of his scheme on his laptop computer, is a case in point. *Ibid*.

[32] Interpol is also co-operating with credit card companies to combat payment fraud by building a database on Interpol's web site. Interpol is also making efforts to establish a network for collating information relating to illegal activities on the Internet.

[33] International co-operation is required to punish cyber crime offenders. However, international co-operation is limited to the particular participants and treaty signatories who have enacted domestic cybercrime legislation.

[34] It should be noted that South Africa does not need to introduce additional legislation to ensure compliance with the cybercrime treaty. We comply with the substantive obligations in the treaty by way of the ECT and the Films and Publications Act 65 of 1996. However, we would have a problem complying with the procedural obligations in the treaty. It would be difficult to establish a 24/7 contact centre due to financial constraints.

[35] A CSIRT strives to protect and secure the critical information assets of a country. See "Computer security gets its own response team" available at http://www.csir.co.za/enews/2009 (date of use 9 October 2009). Also see Anonymous 2009 http://www.ib/.com/internat.law-news (date of use 1 June 2009).

[36] See http://www.life.sitenews.com/ldn/2009/oct/ (date of use 7 October 2009). South Africa is also the first African country to join a global body of internet hotlines fighting against child pornography. The Films and Publications Board was granted full membership of the International Association of Internet hotlines (INHOPE) on 13 May 2009. See http://www.fpbprochild.org.za/ (date of use 7 October 2009).

protection legislation or information privacy legislation").[37] The promulgation of such legislation will impact on the ECT (chapter 8) as far as information protection is concerned.

6 The way forward

The advent of the ECT goes a long way towards addressing cybercrime in South Africa. However, there is room for improvement.[38] As stated earlier, South Africa needs to ratify the COECC to avoid becoming vulnerable to international cybercrime. A need also arises for the introduction of more specialised institutions such as specialised cyber tribunals or courts to facilitate the prosecution of cybercrime cases on a priority basis. Internet users should also be encouraged to share the burden of securing informational privacy where feasible. Computer ethics education should also be taught to children in schools to educate them about the negative consequences of committing cybercrime. Although technological advancement is welcomed, it has created numerous challenges. The possibility of new forms of cybercrime will emerge with rapidly evolving technology; therefore new cyber laws should be introduced to respond to these rapid changes. Thus there should also be continuous research and training of IT security personnel, finance service sector personnel, police officers, prosecutors and the judiciary to keep them abreast of evolving computer technology. At the end of the day, a balanced approach that considers the protection of fundamental human rights and the need for effective prosecution of cybercrime is the way forward.

[37] See SALRC Issue Paper (Project 124) *Privacy and Data Protection* 26 August 2009. It should be noted that information protection relates to the protection of a person's right to privacy. The right to privacy is protected in terms of s 14 of the Constitution 108 of 1996. The Protection of Personal Information Bill is regarded as a mechanism for the protection of the right to information protection and will be enacted sometime during 2009. South Africa needs to guarantee adequate protection of personal information of international travellers to contribute to a successful 2010 FIFA Soccer World Cup; hence the need for information protection legislation. Such legislation will also facilitate South Africa's future participation in the international information markets.

[38] The ECT is criticised for not having severe criminal penalties. It is recommended that the criminal jurisdictional limit and the wording in the anti-spam provision (namely s 86(5)) should be amended. See Van der Merwe (n 5 above) 319 in this regard.