Journal of Information, Law & Technology

Cyber Crime in South Africa – Hacking, cracking, and other unlawful online activities

Sizwe Snail
Attorney at Law
Couzyn Hertzog & Horak
SizweS@couzyn.co.za

This is a **refereed article** published on 28 May 2009.

Citation: Snail, S., 'Cyber Crime in South Africa – Hacking, cracking, and other unlawful online activities', 2009(1) *Journal of Information, Law & Technology (JILT)*, <http://go.warwick.ac.uk/jilt/2009_1/snail>

Abstract

This paper aims to give a broad overview of how South African law dealt with Cyber Crime from a common law perspective and also the new cyber crime provisions in the Electronic Communications Transactions Act, Act 25 of 2002. The paper focuses on the statutory defined crimes and then also gives provisions on the value and evidential weight of electronic data during criminal proceedings. The paper also covers the powers of 'Cyber inspectors' as well as discusses how the ECT has given our South African Court's broader jurisdiction when adjudicating Cybercrimes due to its borderless nature. The Article concludes with some brief comparative law from the EU and US and concluding remarks.

1. Introduction

Computer crime or commonly referred to as Cyber Crime or ICT Crime (van der Merwe, 2008, p.61) is a new type of criminal activity which started showing its ugly head in the early 90's as the Internet became a common place for online users worldwide. This is due to the fact that computer criminals now have the opportunity to gain access to sensitive information if they possess the necessary know-how. This generally causes huge problems in the economic sphere and results in companies and individuals having to take costly steps to ensure their safety and reduction in commission of cyber-crime (Gordon, 2000, p.423). Cyber crime or also known as computer crime can be defined as any criminal activity that involves a computer and can be divided into two categories .One, it deals with crimes that can only be committed which were previously not possible before the advent of the computer such as hacking, cracking, sniffing and the production and decimation of malicious code (Ibid) The other category of computer crimes are much wider and have been in existence for centuries but are now committed in the cyber environment such as internet fraud, possession and distribution of child pornography to name a few. It is clear from the above that ICT crime has to be tackled with a more sophisticated multi-disciplinary approach (van der Merwe, 2008, p.61). In modern times there is more focus from protecting the 'container' of valuables (the computer is merely the modern equivalent of a bank vault), only instead of money or gold it contains data) to protecting the real valuables in most ICT crimes, namely the data contained in the computer , the cell phone's GPS device and so on. (van der Merwe, 2008, p.63). The question then usually arises as to what types of criminal offences may be committed online and what laws one must apply to charge an offender to successfully get a prosecution.

2. Common law position: Prior to the ECT Act

It is submitted that prior to the enactment of the ECT, the common and statutory law at that time could be extended as widely as possible so as to cater for the arrest and successful prosecution of online offenders. One can easily apply the common law crimes of defamation, indecency (Online child pornography, decimation of child porn), *crimen iniuria* (also known as *Cyber-smearing*) fraud (Cyber fraud) (*S v. Van den Berg* 1991 (1) SACR 104 (T)), defeating the ends of justice, contempt of court (in the form of publishing any court proceedings without the court's permission online or by other electronic means), theft (*S v. Harper* 1981 (2) SA 638 (D) and *S v.*

Manuel 1953 (4) SA 523 (A) 526 where the court came to the conclusion that money which had been dematerialized could be stolen in its immaterial form) and forgery to the online forms of these offences. The applicability of the common law however has its own limitations and narrows significantly when dealing with online crimes involving assault, theft, extortion, spamming, phishing, treason, murder, breaking and entering into premises with the intent to steal and malicious damage to property.

When looking at the crimes of breaking and entering with intent to steal as well as the crimes of malicious damage to property two commonly known categories of Computer crimes come to mind. On the one hand, hacking and cracking and on the other hand the production and distribution of malicious code known as viruses, worms and Trojan Horses. In *S v. Howard* (unreported Case no. 41/ 258 / 02, Johannesburg regional magistrates court) as discussed by Van der Merwe, the court had no doubt whether the crime of malicious damage to property could apply to causing an entire information system to breakdown. The Court mentioned further that the crime no longer needed to be committed to 'physical property' but could also apply to data messages of data information. (van der Merwe, 2008, p.70).

The Interception and Monitoring Act, the Regulation of Interception of Communications and Provision of Communication Related Information Act (RICPCRIA) Act 70 of 2002, the Electronic Communications and Transactions Act and the Promotion of Access to Information Act (PROATIA) generally prohibits the unlawful interception or monitoring of any data message which could be used in prosecuting hacker and crackers.

2.1 Interception and Monitoring Prohibition Act

The Interception and Monitoring Prohibition Act specifically governs the monitoring of transmissions including e-mail.

Section 2 states that: no person shall –

> 'intentionally intercept or attempt to intercept or authorize, or procure any other person to intercept or to attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission'.

This means in simple terms that conduct that:

(a) Intentionally and without the knowledge or permission of the dispatcher to intercept a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line; or

(b) Intentionally monitor any conversations or communications by means of a monitoring device so as to gather confidential information concerning any person, body or organization, is unlawful and therefore prohibited. One must note that the attempt thereof is as sanctionable as the actual act of unlawfully intercepting and monitoring of a data communication. One must

however read the provision so as not to exclude any other accepted lawful grounds of justification such as, necessity, private defence, lawful interception, consent, court order or interception directive. In the English case of *R v. Secretary of State for Home Department, ex parte Rudduck and others* 1987 2 ALL ER 516, the court warned that the grounds of justification based on common law must be used sparingly and must not be readily available as a defence to the allegation of unlawful interception and monitoring of data communications. The learned judges made mention of the fact that there are provisions authorizing law enforcement officers to intercept and monitor data communication but the procedure for getting search warrants, interdict and/or interception and monitoring directives (as stated in the South African law) they must be strictly adhered to as this could cause an erosion to the individual's right to privacy (see section 3 (a) and (b) of the RICPCIRA on the provision regarding the execution and issuing of interception directives).

2.2 Dangerous Code

Now let us turn to the common law crime of malicious damage to property and how it could relate to dangerous code such as Viruses, Worms and Trojan horses. Dangerous refers to any computer programme that causes destruction or harm and has been programmed in such a way with malicious intent. Ebersoehn & Henning (2000, p.111) defines virus as:

> 'A piece of programming code usually disguised as something else that causes some unexpected and , for the victim usually undesirable event and which is often designed so that it is automatically spread to other computer users.'

They go on further and classify them as File infector viruses, system or boot record viruses and macroviruses. It must be noted that viruses can either be decimated or 'contracted' by exchange of various media or by receipt in an e-mail.

Ebersoehn & Henning (2000, p.112) define a worm as:

> 'a type of a virus….that situates itself in a computer system in a place where it can do harm'.

The difference between a virus and a worm is that the former has to be activated by the user and that worm on the other hand gains access to the computer and search for other internet locations infecting them in the process.

Ebersoehn & Henning define a Trojan as:

> 'A destructive computer programme disguised as a game, a utility or application. A

> Trojan horse does something devious to the computer system while appearing to do something useful' (ibid).

In my view, the court's inherent power to develop the common law relating to the creation and/or decimation of the above dangerous codes could have resulted in successful prosecution relating to malicious damage to property. The requirements of malicious intent and fault could easily be attributed in the form of *dolus directus, dolus indirectus* or even *dolus eventualis* and in some instances *luxuaria* (conscience negligence) could also be used where the author of such a programme failed to take precautions to ensure that it does not fall in the public domain (even if it was for research purposes).

2.3 Child Pornography

Crimes such as possession and distribution of child pornography can be prosecuted in terms of the Films and Publications Act, Act 65 of 1996 which defines 'publication as:

> '(i) any message or communication, including visual presentation, placed on any distributed network including, but not confined to , to the internet'.

The application of the previously codified and common law crimes was sometimes regarded as an academic expedition and caused great uncertainty as courts and prosecutors were not keen to do adventurous prosecutions. Gordon sates that in 1998 the then Eastern Cape Attorney General was loath to prosecute a man who had placed child pornography in his website as the said Act was not in force. This caused a general outcry in the community and the legislature was forced to bring the said Act into force in order to fill in the *lacunae* that were existed in the law. (Gordon, 2000, p.439) In terms of section 27 (1) and section 28 of the said legislation if anyone creates, produces, imports or is in possession of a publication or film which contains scenes of child pornography, he shall be guilty of an offense.[1] Gordon also notes that the Act may also extend to 'pseudo-pornography' as found in animated pornography (Gordon, 2000, p.439). Sections 25 and 26 also prohibit the decimation of child pornography in films or publications respectively.

3. Criminalizing Cyber-crime in the Electronic Communications and Transactions Act

In *Narlis v. South African Bank of Athens* 1976 (2) SA 573 (A), the Court held that a computer printout was inadmissible in terms of the Civil Procedure and Evidence Act 25 of 1965. It was also held that a computer is not a person. It was clear that the law regarding value of electronic data in legal proceedings required urgent redress. This resulted in the premature birth of the Computer Evidence Act 57 of 1983. Section 142 of the said Act made provision for an

[1] Section 27 (1) and Section 28 refer to child pornography publication and child pornography in films respectively.

authentication affidavit in order to authenticate a computer printout. The Computer Evidence Act seemed to make more provision for civil matters than criminal ones. It created substantial doubts and failed the mark for complimenting existing statutes and expansion of common principles (Kufa, 2008, pp.18-19)

After many years of legal uncertainty, Parliament enacted the Electronic Communications and Transactions Act[2] (ECT) which comprehensively deals with Cyber-crimes in Chapter XIII and has now created legal certainty as to what may and not constitute Cyber-crime. One must however, note section 3 of the ECT (its interpretation clause) does not exclude any statutory or common law from being applied to, recognizing or accommodating electronic transactions. In other words, the common law or other statutes in place wherever applicable is still in force and binding which has the result that wherever the ECT has not made specific provisions for criminal sanction such law will be applicable.

Section 85 defines 'cyber crime' as the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorized to access that data and still continues to access that data (Geredal, 2006, p.282) . Section 86(1) provides that, subject to the Interception and Monitoring Prohibition Act, 1992 (Act 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.

In the case of *R v. Douvenga* (District Court of the Northern Transvaal, Pretoria, case no 111/150/2003, 19 August 2003,unreported) the Court had to decide whether an accused employee GM Douvenga of Rentmeester Assurance Limited (Rentmeester) was guilty of a contravention of section 86(1) (read with sections 1, 51 and 85) of the ECT Act. It was alleged in this case that the accused, on or about 21 January 2003, in or near Pretoria and in the district of the Northern Transvaal, intentionally and without permission to do so, gained entry to data which she knew was contained in confidential databases and/or contravened the provision by sending this data per e-mail to her fiancée (as he then was) to 'hou' (keep). The accused was found guilty of contravening section 86(1) of the ECT Act and sentenced to a R1 000 fine or imprisonment for a period of three months (Geredal, 2006, p.282). It follows that the crime commonly known Hacking has now been entrenched in our law in section 86 (1) of the ECT which makes any unlawful access and interception of data a criminal offence.

This also applies to unauthorized interference with data as contained in section 86 (2) of the ECT (also see the provision of the RICPCRIA Act which prohibit unlawful data interference/monitoring of data). Section 86 (4) and 86(3) introduces a new form of crime known as the anti-cracking (or anti-thwarting) and hacking law. In terms of this law the provision and, or selling and/or designing and/or producing of anti-security circumventing (Ebersoehn, 2003, p.16) technology will be a punishable offence. In terms of section 86(4) a person is guilty of this offence if he uses and designs a programme to overcome copyright protection, with direct intent to overcome a specific data protection programme (Ebersoehn, 2003, p.17). E-mail bombing and spamming is now also a criminal offence as contained in sections 86 (5) and 45 of the ECT respectively.

[2] 25 of 2002

Denial of service (DOS) attacks also popularly known as Disk Operating System attacks, are attacks that cause a computer system to be inaccessible to legitimate users. Denials of service attacks disrupt service to legitimate users for a period of time (Kufa, 2008, p.20). Section 86(5) states that, 'any person who commits any act described in Section 86 with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial of services to legitimate users is guilty of an offence'. The act or conduct is fashioned in such a manner that it is widely defined and consist of any of the action criminalized in Sections 86(1) and Section 86(4). The actions include unauthorized access, unauthorized modification or utilizing of a program or device to overcome security measures (Kufa, 2008, p.20).

Section 87 of the ECT also has introduced the Cyber crimes of Extortion, Fraud & Forgery. Section 87 of the ECT also has introduced the Cyber crimes of E-Extortion as per section 87(1), E-Fraud as section 87(2) and E-Forgery as section 87(2). Section 87(1) provides an alternative to the common law crime of extortion. Kufa states that pressure is therefore exerted by threatening to perform any of the acts criminalized in section 86. Kufa also criticizes this section as 'wet behind the ears' as its common law equivalent applies to both forms of advantage of propriety and non-propriety form. He suggests that this proviso is wanting and will require redress (Kufa, 2008, p.21).

Cyber-crimes are not limited to the acts as contained in the ECT but there are also other statues that are applicable in the prosecution of Cyber crimes. For instance, in terms of the Prevention of Organized Crime Act (POCA) Act 121 of 1998 and The Financial Intelligence Centre Act (FICA) Act 38 of 2001 the prevention of all the crimes (as applicable to the cyber environment) listed is highlighted (but in an organized fashion) as well as the prohibition of money laundering and other financial related crimes which are these days done online may also contravene the Exchange Control Regulations. Also noteworthy is the National Gambling Act and Lotteries Act. In terms of section 89 of the National Gambling Act any form of unlicensed gambling is unlawful and may be imprisoned for period of 2 years. Similarly sections 57 and 59 of the Lotteries Act also state that 'any unlicensed lotteries or anyone participating in a foreign lottery is liable to a criminal offence'.

Notwithstanding Section 86(4) outlaws the cracking of anti-pirating and/or security software. It is also important to state that in the case of sale and/or making available of illegal copies of movies or music online (in formats such mpeg4, Divx, mov, mp3, wav, mwa etc) an individual may be in contravention of the Copyright Act as section 27 of the Copyright Act prohibits unlawful copying, decimation and/or distribution of copyrighted works. The provisions of the Counterfeit Goods Act may also be applied were the sale of such counterfeit goods (in this context reference to goods is the illegal copy of the movie or song) was concluded online.

4. Legal Aspects of the Enforcement of Cyber-crimes (Procedural and Evidential aspects of Cyber-crimes)

4.1 Admissibility and Evidential Weight of Data Messages (ECT Act, Section 15)

After much legal uncertainty as to the admissibility of a printout in Court in terms of the Old Computer Evidence Act, Section 15 of the ECT now states that the rules of evidence must not be used to deny admissibility of data messages on grounds that it's not in original form. A data message made in the ordinary course of business, or a printout correctly certified to be correct is admissible evidence. Section 15 of the ECT Act provides for the admissibility and evidential weight of a data message as electronic evidence. It is clear from the wording in section 1 that it sets out to facilitate rather than inhibit the admissibility of data messages as electronic evidence (Watney, 2008, p.3).

Section 1 defines that a data message means data generated, sent, received or stored by electronic means and includes (a) voice, where the voice is used in an automated transaction; and (b) a stored record. Data is defined as the electronic representation of information. It is in fact stated that a data message will not offend the best evidence rule on the ground that it is not in its original form (Ibid). It constitutes rebuttable proof of its contents when it is produced in the form of a print-out (compare the case of *S B Jafta v. Ezemvelo KZN Wildlife* (Case D204/07) where a e-mail used to accept an employment contract was regarded as conclusive proof that the said employment had been accepted).

The Act now states that Data messages shall be admissible giving due regard to reliability of manner of storage, generation and communication, reliability of admission manner of maintenance of message, manner in which originator is identified, and any other relevant factor. In other words the Act creates a rebuttable presumption of that data messages and/or printouts thereof are admissible in evidence (See also the controversial case of *S v. Motata* Johannesburg District Court case number 63/968/07 (unreported) at 622, where electronic information (data in the form of images and sound) from a cell phone was admitted into evidence in a trial within a trial).

4.2 Search and Seizure (ECT Act Section 81 – Section 83)

The ECTA has now created 'Cyber inspectors' who, with the authority of a warrant, may enter any premises or access information that has a bearing on an investigation (into possible Cyber-crime). These cyber police will be employees of the Department of Communications (Geredal, 2006, p.281). Their powers have been well defined in the Act in which includes the authority to search premises or information systems, search a person or premises if there is reasonable cause to believe they are in possession of article/document/record with bearing on investigation. Cyber inspectors may also demand the production of and inspection of any licences or registration certificates in respect of any law, take any extracts of books or documents on any premises or information system with a bearing investigation, and also the power to inspect any facilities on premises with a bearing on an investigation in terms of Section 82.

In terms of section 80(1) of the ECT Act, the director-general may appoint any employee of the department as a cyber inspector empowered to perform the functions provided for in the chapter. Subsection (2) further provides that a cyber inspector must be provided with a certificate of appointment signed by or on behalf of the director-general in which it is stated that he or she has

been appointed as a cyber inspector. Such a certificate provided for in subsection (2) may be in the form of an advanced electronic signature (Geredal, 2006, p.281).

To avoid issues of unnecessary red-tape which may hamper a prosecution, Cyber inspectors in terms of Section 83 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 with the operation of a computer to provide reasonable technical assistance. Van der Merwe however correctly points out that the said cyber inspector have not yet been introduced and suggest that the scorpions be the designated law enforcement agency to be blessed with these powers (Van der Merwe, 2008). However with the scorpions future in limbo maybe it would be better to look at the South Africa Police. Buys argues that there are constitutional concerns with regards to the search and seizure provisions (in particular section 14 of constitution-privacy) which still need to be addressed by the South African courts.

4.3 Jurisdiction (ECT Act s90)

Jurisdictional challenges are probably the main challenge that cyber prosecutors face in prosecution of cyber-crimes. Section 90 of the Act gives South African courts the jurisdiction to try offences arising from actions where an offence is committed in the republic, any act in preparation for the offence takes place in the republic, any part of the offence is committed in the republic, the result of the offence has effects in the republic, the offence is committed in the republic, by a person carrying on business in the Republic or when the offence is committed on board any ship or craft registered in republic. There is much legal debate however as to whether this provisions in line with International law and the effect of other international treaties on the prosecution of cyber-crimes

5. Lessons learnt from European Union and USA

5.1 European Union

In the European Union Cyber-crime law is primarily based on the Council of Europe's Convention on Cyber-crime (November 2001). South Africa has signed but did not ratify the Convention. South Africa has complied with the first part of the Convention (Van der Merwe, 2008, p.101) in terms of which member states are obliged to:

1. criminalise the illegal access to computer system,
2. illegal interception of data to a computer system,
3. interfering with computer system without right, intentional interference with computer data without right,
4. use of inauthentic data with intend to put it across as authentic (data forgery),
5. infringement of copyright related rights online,
6. interference with data or functioning of computer system,

7. child pornography related offences (possession/distribution/procuring/producing of child pornography).

The first part which is also known as the substantive part of the treaty has been dealt with in ECT Act in Section 86-87 as well as the Copyright Act and The Films and Publications Act. The Convention's broad coverage of offences has drawn extensive criticism. Critics argue that it should limit itself to protecting the global information infrastructure by criminalizing 'pure' cyber crimes. Fraud and forgery, they argue, are already covered in existing international agreements and should not be included in the Convention as 'computer-related fraud' and 'computer-related forgery' (Jones).

As far as enforcement mechanisms are concerned, the parties to the convention are obliged to co-operate with each other in order to facilitate the investigation of a computer system-related offence (Van der Merwe, 2008, p.101). There may also be insufficient international consensus on whether and how to criminalize 'content-related offences' like child pornography and copyright infringement- as well as the additional protocol on racist and xenophobic acts committed 'by means of a computer system' (Jones). Any measures taken by the parties to the convention should not infringe on fundamental human rights. These measures must include authorising authorities to access, search and seize computer systems as well as empowering authorities to order the production of computer data in a person's possession or control that has bearing on an investigation. Parties may also authorise the interception or collection of data reasonably believed to be related to the commission of an offence (Van der Merwe, 2008, p.101).

Parties to the convention shall be required to establish jurisdiction over Convention offences committed within their territory, on board a ship flying its flag by one of its nationals, if the offence is punishable where it was committed. Due to the borderless nature of Cyberspace it is necessary to have international co-operation if law relating to cyber crime enforcement is to get much success. Extradition is also possible as contained in Chapter 3 of the convention if an offence is punishable under the laws of both parties to the convention (ibid).

5.2 The United States of America

In principle, USA regulation and law enforcement of Cyber crime is similar to that of the EU. In the mid 1980 two important statutes were passed by UC Congress to combat computer-related crime in which federal interests are involved (Van der Merwe, 2008, p.90), the Counterfeit Access Device and Computer Fraud and Abuse Act (18USC § 1030-1984) as well as the Electronic Communication Privacy Act (18USC §§ 2500-2711-1986). Cyber fraud and making intentional false representations online, (that victims rely on) is a federal offence. Identity theft which happens in the form of unauthorised use of another person's social security number, driver's licence, work ID or credit card online is also a federal cyber-crime. In recent times there was a radical upward departure from sentencing guidelines in conviction for identity theft and obtaining of prescriptions among other things. Online gambling is generally prohibited; Nevada State is one of the states that approves of online gambling.

Federal law which targets senders of spam is limited to fraudulent telephonic solicitations or by

means of electronic form, but this is currently being revised. The Federal Trade Commission is not empowered to stop spamming, but it may stop fraudulent and/or deceptive marketing practices. However the state of Virginia has taken an initiative to specifically outlaw Spam.

The unlicensed sale of controlled items online is a cyber-crime in the USA. Non-prescriptive and prescriptive drugs (e.g. Viagra & Cipro), firearms, explosives, cigarettes, alcohol and even visas for sale on the internet should conform to the terms of the licensing. However this is very much an unsettled area of law. A Federal judge rejected New York's ban on online cigarette sales as it violates the Federal Commerce Clause.

Child pornography, in its various forms, is a federal crime. The offences include possession, production, procurement, or distribution or related materials. It is interesting to note the decision of *Ashcroft v. Free Speech Coalition* (2002) 535 U.S. 234 (2002) in which the Supreme Court judges were split over whether *virtual* pornographic images of children fell afoul of anti-child pornography provisions.

Under US law, Cyber-Stalking and Cyber-Harassment has also been outlawed. Reinhardt Buys quoted an example of how an offender assumed the identity of a woman in cyberspace and 'solicitated' rape on her behalf by stating online, 'how much she fantasised of being raped' and was guilty of accessory to rape due to his involvement in the rape. Crimes such as hate crimes, murder and murder threats are also punishable if certain of their elements are carried out online. The use of password sniffers, distribution and creation of worm programs as well as writing of virus programs and Trojan horses, website defacements, and web-spoofing are also well known federal offences.

The No Electronic Theft Act, in terms of which it is an offence to swap more than $2,500 in software, regulates normal copyright offences and copyright management offences. The Digital Millennium Copyright Act makes it a crime to traffic in devices primarily designed for purpose of circumventing technology protection measures (anti-piracy devices). Various trademark offences, economic extortion, money laundering which is carried out online is also regarded as cyber crime and means are currently being developed to create legislation that can sufficiently deal with these offences.

6. Conclusion

Most of the Cyber-crime provisions in the ECTA are noble endeavours and seem to cover the known types of cyber crime. It is refreshing to note that the legislature did not make cyber crimes an abstract concept of legal writing and logically created crimes that do not only cover crime after the advent of the computer but also before the advent of the computer. It is also refreshing that the mere attempt of these crimes also constitutes a criminal transgression. South Africa as well as countries like Nigeria and Egypt has taken legislative arms to deal with these new crimes. The crimes as stated in the ECTA are however not exempt from scrutiny. The enforceability of the ECTA provisions are still to be tested in our South African courts and some legal practitioners and adjudicators (magistrates and judges) need to be educated and mentally conditioned to embrace the cyber crime provisions of the ECTA. Given the borderless nature of

the internet and the challenges it poses in terms of jurisdictional questions, international co-operation and uniformity, it is of the utmost importance that States learn from each other's efforts to deal with Cyber-crime and create an international Cyber-crime code to be applied universally if any significant success is to be achieved in combating Cyber-crime.

References

Articles

Ebersohn, G J (2003), 'Catching Hackers' in Juta business Law, Vol. 12 Part 1

Gordon, B (2000), 'Internet Criminal Law' in Buys, R (ed.) Cyberlaw @ SA: The law of the Internet in South Africa

Henning, J J & Ebersohn, G J (2000), 'Insider trading, money laundering and computer crime, Transactions of the Centre for Business Law', Combating Economic Crime, 105

Geredal, S L (2006), 'The Electronic Communications and Transactions Act' in Thornton, L (ed.) Telecommunications Law in South Africa

Kufa, M (2008), 'Cybersurfing without boundaries', De Rebus, December, 20

Snail, S L (2008), 'Cyber Crime in context of the Electronic Communications Act', 16(2) Juta Business Law, 65

Books

Buys, R (2000), Cyberlaw @ SA: The law of the Internet in South Africa, Pretoria

Van der Merwe, D (2008), Information and Communication Technology Law (ed.), Pretoria

Cases

Narlis v. South African Bank of Athens 1976 (2) SA 573 (A),

R v. Douvenga (District Court of the Northern Transvaal, Pretoria, case no111/150/2003, 19 August 2003, unreported

R v. Secretary of State for Home Department, ex parte Rudduck and others 1987 2 ALL ER 516

S v. Harper 1981 (2) SA 638 (D)
S v. Howard (unreported Case no. 41/ 258 / 02, Johannesburg regional magistrates court)

S v. Manuel 1953 (4) SA 523 (A) 526

S v. Motata Johannesburg District Court case number 63/968/07 (unreported) at 622

S B Jafta v. Ezemvelo KZN Wildlife (Case D204/07)

Online Sources

Jones C., 'Convention on Cybercrime: Themes and Critiques', Berkeley University http://www.cyberlawenforcement.com/

Madziwa, S and Snail, S., 'Online Misdemeanour- Hacking, cracking, and other online activities', published online at: www.hg.org/article.sp?id=5351

Legislation

Copyright Act, Act 98 of 1978
Computer Evidence Act, Act 57 of 1983
European Convention on Cyber crime (ETS No 185).
Electronic Communication transaction Act, Act 25 of 2002
Evidence Act, Act 25 of 1965.
The Films and Publications Act, Act 65 of 1996

Conference Presentation

Van der Merwe, D., Criminal Law– Your partner in preventing information loss, Presented at the Lex Informatica 2008 , 23 May 2008 at the Innovation Hub.

Watney, M., Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position, Presented at Cyber Crime Africa 2008, 13 November 2008 at Monte Casino