CHAPTER 10

COMPUTER-RELATED FRAUD

10.1 INTRODUCTION

The offence of fraud originates from Roman law[1] and covers a wide field. However with the advent of the computer and information technology, fraud is now increasingly perpetrated through new and sophisticated technology. Fraud can be perpetrated through the Internet and electronic mail and these types of actions are commonly referred to as *online fraud*. Internet banking is a relatively new phenomenon and has also recently been publicised to be the target of fraudulent actions.[2] Nowadays financial records and payment systems are computerised and the commission of fraud has become easier. *Data diddling* involves the changing of data before or during the input into a computer or system.[3] *Spoofing* involves the forgery of data. It often happens that an electronic mail message represents that it comes from a certain source, but instead it comes from a totally different source. This is called *e-mail spoofing* and the perpetrator can obtain credit card numbers and bank details in this manner.[4] *Phishing* scams direct victims to fake or bogus websites that trick victims into supplying personal information such as credit card

---

[1] There were two Roman Law crimes namely *stellionatus* and *crimina falsi*.(see Snyman Criminal Law (2002) 520 and C R Botha *Bedrog in die Suid-Afrikaanse Strafreg* (1988)).

[2] See for instance the Absa hacker case, discussed in more detail in the chapters above.

[3] Dana van der Merwe *Computers and the Law* (2000) 168; Irving J Sloan *The Computer and the Law* (1984) 9; David Davies *The Nature of Computer Crime* (1991) Computers and Law Vol. 2 Issue 3 9.

[4] H W K Kaspersen & Stuurman(ed) *Juridische Aspecten van E-mail* (2001) 11. See also G J Ebersöhn *A common law perspective on computer-related crimes (1)* (2004) 67 THRHR No. 1 25.

numbers and passwords. These websites look like ordinary respectable websites of known retailers but are in fact bogus or forged websites.

Bainbridge[5] distinguishes between four types of computer-related fraud:

- *Input fraud* which is the entry of an unauthorised instruction into a computer system;[6]
- The alteration of input data (data that is entered into the computer system) which in called *data fraud*;[7]
- *Output fraud* or the suppression of data such as the alteration of computer printouts;[8] and
- *Program fraud* where a computer program is altered to affect the fraud.[9]

Worldwide scholars have struggled with the question whether a misrepresentation can be made to a computer and whether a computer can be deceived.

10.2 INTERNATIONAL EXAMPLES

10.2.1 United States of America

In the United States there are various statutes that criminalises some form

[5] David I Bainbridge *Introduction to Computer Law* 2000.

[6] Bainbridge (footnote 5 *supra*) 292.

[7] Bainbridge (footnote 5 supra) 292 – 293.

[8] Bainbridge (footnote 5 *supra*) 293.

[9] Bainbridge (footnote 5 *supra*) 294.

of online fraudulent conduct.[10] Section 1030(a)(4) of the United States Criminal Code prohibits unauthorised access to a protected computer with the intent to defraud and obtaining something of value.[11] The United States Criminal Code contains provisions of wire fraud as well as certain unauthorised access offences with the intention to defraud or to obtain an advantage. The most well known case is that of Stanley Mark Rifkin that transferred 10.2 million dollars through the wire transfer system at Security Pacific National Bank.[12] Rifkin, a familiar face at the bank, obtained the computer security codes and from a public phone initiated the electronic fund transfer.[13] In the State of Alaska for example a specific provision is contained in the Alaska Statutes in relation to the deceiving of a machine.

10.2.2 United kingdom

Most fraudulent actions fall within the ambit of the Theft Act[14] for example theft[15], obtaining property by deception[16] and false accounting[17].

---

[10] See Emile Loza *Internet Fraud: Federal Trade Commission Prosecutions of Online Conduct* (2001) Communications and the Law Vol. 23 No. 2 55 *et seq*. for a discussion of the various statutes and cases pertaining to the Internet or online fraud. Also see Richard H Walker and David M Levine *"You've got jail": Current trends in civil and criminal enforcement of Internet securities fraud* (2001) American Criminal Law Review Vol. 38 No. 3 405.

[11] See paragraph 3.4.1.1 for the text of this provision. See Laura J Nicholson et al *Computer Crime* (2000) American Criminal Law Review Vol. 37 No. 2 209 *et seq*.

[12] Jay Becker *Rifkin, a documentary history* (1980) Computer Law Journal 471; Van der Merwe (footnote 3 *supra*) 169.

[13] David Davies *The Nature of Computer Crime* (1991) Computers and Law Vol. 2 Issue 3 10 – 11; David Davies *Computer crime risks and the impact of new technology* (1989-90) 6 Computer Law and Security Report 5.

[14] 1968.

[15] Section 1 of the Theft Act 1968.

[16] Section 15 of the Theft Act 1968.

[17] Section 17 of the Theft Act 1968.

The British Law Commission[18] identified the problem that a machine cannot be deceived and the fact that certain existing legislation is rendered less effective in relation to computers.[19] However, the Commission did not propose immediate legislative intervention.[20] According to Tapper it can be argued that the deception of a machine actually involves the deception of those who operate by means of the machine.[21] The common law offence of conspiracy to defraud is available when more than one person is involved. The Computer Misuse Act of 1990 does not contain any specific provisions in respect of computer-related fraud.

10.2.3 Australia

In the case of *Kennison v Daire*[22] the appellant was convicted of *larceny.* The appellant was a customer of the bank and was in possession of an ATM card. The appellant closed his account and on the next day drew $200 at an Automated Teller Machine. The ATM was off-line and therefore not connected to the central computer of the bank. The appellant was able to withdraw the money because the ATM was so programmed that when it was off-line and a person inserted a card and keyed in the correct pin number, it enabled a person to withdraw up to $200. When the ATM was off-line it couldn't establish whether the account was still in

---

[18] Law Commission Working Paper no 110, *Computer Misuse*, HMSO.

[19] Martin Wasik *Tackling technocrime: The Law Commission Report on Computer Misuse* (1989) Computer Law & Practice Vol. 6 No 1 26.

[20] See Stephen Saxby (ed) *The Law Commission working paper no 110 on computer misuse – The CBI submission Part 1* (1989-90) 1 The Computer Law and Security Report 15 *et seq*.; Richard Dedman *The Computer Misuse Bill 1990* (1990-91) The Computer Law and Security Report 14-15.

[21] Colin Tapper *Computer Law* (1989) 315.

[22] (1986) 60 ALJR 249 (HC).

operation or whether that account was in credit. It was not in dispute that the appellant had acted fraudulently with intent to permanently deprive the bank of the money. The appellant submitted that the bank consented to the taking of the $200, because the ATM had been programmed by the bank and gave effect to the intention of the bank. The Court decided that the Automated Teller Machine could not give consent on behalf of the bank. The ATM was a machine and not a human being and therefore did not have the ability to decide and to give consent.[23]

A similar defence was contended in the matter of *R v Evenett*[24] where an accused exceeded his credit limit when making a withdrawal at an ATM that was off-line. The ATM did not allow a person to withdraw funds in excess of the credit limit when on-line. The defence argued that the bank consented to the withdrawal because of the way in which the ATM had been programmed. This defence was rejected by the Court of Criminal Appeal, because the bank could not have consented through the ATM to the withdrawal.[25] In the case of *R v Baxter*[26] the accused made withdrawals through an ATM of funds that were available due to the deposit of fraudulent cheques. The accused submitted that there was no misrepresentation since an ATM is not a human being capable of thought with reference to the decisions in *Kennison v Daire* and *R v Evenett supra*. The Court found that in the *Kennison V Daire* and *R v Evenett*

---

[23] See Gordon Hughes *Mindless computers in Australia* (1988) 2 The Computer Law and Security Report 25 *et seq*.; David Brown et al *Criminal Laws; Material and commentary on criminal law and process in New South Wales* (1990) 1204 – 1206. Graham Greenleaf *Computers and crime – the hacker's new rules* (1990-91) 2 The Computer Law and Security Report; Gordon Hughes(ed) *Essays on Computer Law* (1990) 226 *et seq*.; Grabosky *et al Electronic Theft – Unlawful acquisition in Cyberspace* (2001) 4.

[24] (1987) 2 Qd. R. 753.

[25] Hughes (footnote 23 *supra*) 26.

[26] An unreported decision. See Hughes (footnote 23 *supra*) 26 – 27.

cases the issue at hand was the element of consent. The Court found that an ATM is a facility provided by the bank in the course of conducting its business. The misrepresentation is made to the bank that is a legal entity and capable of being deceived.[27]

Australia has various jurisdictions that operate locally and have legislation that govern the entire Australia. The Crimes Act of 1900 was amended to criminalise instances where unauthorised access is accompanied by an attempt to defraud, to obtain financial advantage or to cause loss or injury.[28] The Crimes Act was recently also amended by the Cybercrime Act[29].

10.3 INTERNATIONAL RESPONSES BY THE COUNCIL OF EUROPE

The Council of Europe released a report in 1990 entitled *computer-related crime.*[30] The Council of Europe suggested a minimum list of crimes that should be criminalised through legislative intervention, and an optional list that contains a list of offences of which the criminalisation is optional.[31] In many countries the deception of a human being is required in order to constitute fraud.[32] Certain criminal codes contain offences like

---

[27] Hughes (footnote 23 *supra*) 26 – 27.

[28] Section 309(2); See Gordon Hughes *Recent developments in Australian computer crime regulation* (1991) Computer Law & Practice 94.

[29] 2001.

[30] Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems, Strasbourg 1990.

[31] Hans G Nilsson *The Council of Europe fights computer crime* (1989) Computer Law & Practice Vol. 6 No. 1 8 *et seq*; Bernard P Zajac Jr *Transborder data flow and 1992* (1990-91) The Computer Law and Security Report.

[32] For a detailed discussion by South African writers see paragraph 10.4 *infra*.

embezzlement and credit card fraud. However, as pointed out in the Report, these offences have a limited scope of application.[33] The Council of Europe recommended that computer-related fraud should be on the so-called minimum list and suggested the following legislative text:

> "The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for himself or for another person (alternative draft: with the intent to unlawfully deprive that person of his property)."

The Report also proposed that computer forgery should be included on the minimum list and requires legislative intervention.[34] The falsification of data is therefore similar to the falsification of documents.

The Convention on Cybercrime[35] also deals with computer-related fraud and states in article 8 of the Convention as follows:

> "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:
> a) any input, alteration, deletion or suppression of computer data,
> b) any interference with the functioning of a computer system
> with fraudulent or dishonest intent of procuring, without right, an economic benefit for one self or for another."

---

[33] Council of Europe Report (footnote 30 *supra*) 37.

[34] Council of Europe Report (footnote 30 *supra*) 39 – 43.

[35] Convention on Cybercrime, ETS No. 185, Council of Europe, Budapest 2001 accessible at

The Convention focuses on economic benefit and loss of property. This limits the scope of application since computer fraud can be prejudicial in non-proprietary ways.

The Convention on Cybercrime also deals with computer-related forgery and states that the signatory countries should criminalise the "input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic".[36] It is irrelevant whether the data is directly intelligible.[37]

10.4 THE COMMON LAW CRIME OF FRAUD IN SOUTH AFRICA

10.4.1 Introduction

Snyman defines fraud as "the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another."[38] Hunt defines fraud as the "unlawful making, with intent to defraud, a misrepresentation which causes actual prejudice or which is potentially prejudicial to another".[39] Snyman, however, is of the view that the element of causation is no longer required.[40]

---

[36] Article 7 of the Convention on Cybercrime (footnote 35 *supra*).

[37] Article 7 of the Convention on Cybercrime (footnote 35 *supra*).

[38] Snyman *Criminal Law* (2002) 520.

[39] Hunt *South African Criminal Law and Procedure* (1970) 714.

[40] Snyman (footnote 38 *supra*) 526.

The elements of fraud consist of:

1.) a misrepresentation

2.) prejudice or potential prejudice

3.) unlawfulness

4.) intention to defraud. [41]

10.4.2 Misrepresentation

The act of fraud consists in the making of a misrepresentation. A misrepresentation is a distortion of the truth or something false. The misrepresentation can be made orally, in writing and through a persons conduct. One can imagine that fraud committed through the Internet would be in the form of written e-mails, websites and electronic documents. Writing would therefore include electronic digital data contained in computer systems and networks. Technology has become so advanced that one can have "telephone" conversations via the Internet and the misrepresentation can then be made orally. Furthermore the misrepresentation may be express or implied. The criminal action can be in the form of a *commission*[42] or can be perpetrated through an *omission* when there is a legal duty on the perpetrator to disclose certain facts.[43] According to Gordon it is easy to make misrepresentations *anonymously* through the Internet by creating false identities.[44] Many fraudulent acts by means of computers, computer networks and the Internet will therefore

---

[41] Snyman (footnote 38 *supra*) 520.

[42] A positive act.

[43] Snyman (footnote 38 *supra*) 522. A legal duty may be created through a statute (e.g. section 234 of the Companies Act) or where a court can find that a person should have acted positively to remove a misconception.

[44] Adv B Gordon *Fraud on the Internet – A growing challenge* (2002) Servamus 38.

easily fall within the common law element of making a misrepresentation to another person and computers or the Internet are just merely sophisticated technology tools with which these fraudulent acts are committed.[45]

An important question arises whether a misrepresentation can be made to a computer or with the intervention of a computer.[46] A computer is not a human being or a person.[47] Dreyer is of the view that the difficulty lies with the element of misrepresentation and that where the misrepresentation is made to a computer it is unlikely that the perpetrator can be convicted of fraud.[48] A similar view is held by Coetzee that a computer can't be equated to a human being and therefore can't be misled.[49] He states further that a misrepresentation to an Automated Teller Machine is not a misrepresentation to the bank since the transaction is concluded without intervention of a human being and therefore does not constitute a misrepresentation.[50]

Carstens and Trichardt advocate a different approach and submit that with ATMs the misrepresentation is made to the bank and not the computer.[51] A bank or building society is a legal person and therefore capable of

---

[45] See Barrie Gordon *Internet Criminal Law* in Buys(ed) *Cyberlaw @ SA* (2000) 430 – 431.

[46] M J F Coetzee *Kan 'n rekenaar bedrieg word* (1984) The Magistrate Vol. 19 No 3 101; J P G Eksteen *Die bydrae van akademici tot die regspleging* (1984) Obiter 4; G Horwitz *Computer abuse – the legal implications* (1986) De Rebus 506.

[47] *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A) at 577; *Ex Parte Rosch* [1998] 1 All SA 319 (W) at 327-328.

[48] J W Dreyer *Computer law in South Africa* (1983) De Rebus 537.

[49] M J F Coetzee (footnote 46 *supra*) 103-104.

[50] M J F Coetzee, footnote 49 *supra*.

[51] P Carstens & A Trichardt *Computer Crime by Means of the Automated Teller Machine – Just Another Face of Fraud?* (1987) SACC 131.

being misled. They state that the computer is merely the link to the bank records and funds and is therefore an instrument or conduit between the bank and the client. The Automated Teller Machine is programmed by the bank. The bank controls and monitors the Automated Teller Machines. The perpetrator is representing to the bank through the ATM that he is entitled to use the card or that he has sufficient funds in the account etc.

According to Botha a misrepresentation is made to a *person* because conceivably only a person can be misled or deceived.[52] Botha concludes with reference to *Narlis v South African Bank of Athens*[53] that a computer is not a person and can therefore not be deceived.[54] He is of the opinion that when a person uses a card fraudulently at an ATM and the entire transaction is concluded without the intervention of a human being or officer of the bank, an accused can't be convicted of fraud.[55]

In *S v Myeza*[56] it was decided that when a person places a counterfeit coin or object in a parking meter, the offence of fraud is committed.[57] In this instance a "misrepresentation" is made to the parking meter, which is not a person and can't be misled to believe that the object is real. However, the misrepresentation lies in the fact that the perpetrator represents to the

---

[52] C R Botha *Bedrog in die Suid-Afrikaanse Strafreg* (1988) 508 (Unisa doctorate dissertation); C R Botha *Sogenaamde 'rekenaarbedrog'*3 (1990) SACJ 231.

[53] 1976 (2) SA 573 (A). Holmes AR commented on page 577 that "Well, a computer perhaps fortunately is not a person".

[54] C R Botha (footnote 52 *supra*) 508; C R Botha (footnote 52 *supra*) 232.

[55] C R Botha (footnote 52 *supra*) 233.

[56] 1985 (4) SA 30 (T).

[57] In general see C R Snyman (footnote 38 *supra*) 526.

traffic department or authorities that his parking is legal and therefore misleads the authorities not to question the legality of the parking. In other words in this instance the misrepresentation is not made to the parking meter but to the traffic department and their employees.[58]

In the case of *S v Van den Berg*[59] the accused unlawfully through a computer terminal credited an account with an amount of R800. The Court held that this was a misrepresentation to the bank. The court decided further that the fact that the misrepresentation was introduced electronically into the computer system was not at all different from the instance where a clerk makes a written false entry into the accounting records.

A very common phenomenon in South Africa is the advance fee fraud schemes or better known as *419 scams.* In these cases the perpetrator would normally send an electronic mail message to another person in which certain misrepresentations are made, usually of a political nature, in which the victim is requested to keep certain money[60] in trust for the perpetrator. This would normally include a request for an advance or administration fee in order to facilitate the "transaction".[61] It could happen that an unsuspecting victim may so part with his money and this

[58] C R Botha *S v Myeza 1985 (4) SA 30 T: Oor blikringetjies en boetebessies – aspekte van bedrog* (1986) SACC 72.

[59] 1991 (1) SACR 104 (T).

[60] Usually large dollar amounts which in actual fact do not exist.

[61] See for example Paul Kirk *Brit police warn of lotto scam* The Citizen 10/02/2004 page 3. An electronic mail message is sent to a victim stating that the person won money in the lotto and that he should contact the "lotto prize agents" in the UK. Upon contacting the number provided, a "*handling fee*" is requested in order to receive the prize.

may well constitute fraud[62]. An intentional misrepresentation is made to the victim through the Internet that could cause prejudice or potential prejudice. These criminals usually send the misrepresentation through electronic mail messages and also make use of *spamming* (unsolicited e-mail) discussed in more detail below.[63]

10.4.3 Prejudice

Prejudice may consist of either actual prejudice or potential prejudice. Prejudice need not be in the form of financial loss and can be non-proprietary in nature.[64] The concept potential prejudice means that objectively there is reasonable possibility of prejudice. The prejudice must not be fanciful or too remote.[65] Prejudice in respect of a third party would be sufficient. It is irrelevant whether the person to whom the misrepresentation was made was not misled by the misrepresentation.[66] It would be sufficient if there was potential prejudice at the time the misrepresentation was made.

---

[62] The mere possession of such a letter or e-mail (therefore in electronic format) is a criminal offence in terms of the regulations published in the Government Gazette number 22459 Volume 433 dated 13 July 2001 and read with sections 15(c) and 16 of the Unfair Business Practices Act 71 of 1988.

[63] See Paul Kirk *SA has no 'cyber cops' to police cyber traffic* The Citizen 30/01/2004 page 4 and paragraph 10.6 *infra*.

[64] Snyman *Criminal Law* (2002) 526; *R v Heyne and others* 1956 (3) SA 604 (A).

[65] Snyman (footnote 64 *supra*) 526.

[66] Snyman (footnote 64 *supra*) 526; *S v Campbell* 1991 (1) SACR 503 (NM).

10.4.4 Unlawfulness and culpability

Grounds of justification may be found in compulsion or obeying of orders.[67] *Mens rea* in the form of intention is a requirement. The perpetrator must be aware that the misrepresentation is in fact false (intention to deceive). The perpetrator must also have the intention to defraud in that he or she must have the intention to induce someone to follow a course of action that is prejudicial as a result of the misrepresentation.[68] Intent in the form of *dolus eventualis* is sufficient to prove fraud. An intention to acquire an advantage is not a requirement.

10.4.5 Attempted fraud

Due to the fact that potential prejudice is sufficient to constitute fraud it was the view of many that there is no such offence as attempted fraud. In the matter of *R v Heyne*[69] the Appeal Court found that attempted fraud is possible. When a perpetrator sends an e-mail containing a misrepresentation to another person over the Internet but the e-mail is intercepted or sent to the wrong person, attempted fraud is committed.

10.5 SECTION 87(2) OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT

Section 87(2) of the Electronic Communications and Transactions Act 25 of 2002 states as follows:

---

[67] Snyman (footnote 64 *supra*) 527.

[68] Snyman (footnote 64 *supra*) 528.

[69] *R v Heyne and others* 1956 (3) SA 604 (A) at 622.

> "A person who performs any of the acts described in section 86 for the purpose of obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic, is guilty of an offence."

The legislator intervened in the debate amongst South African authors whether one can make a misrepresentation to a computer for the purposes of fraud. Section 87(2) criminalises computer-related fraud, forgery and uttering. Fraud and forgery are very similar. Forgery, however, requires that the misrepresentation take place through the falsification of a document.[70] Section 87(2) of the Act now provides that *data* should be falsified. The difference between fraud and forgery is that fraud is completed once the misrepresentation has come to the notice of the victim and forgery is completed once the document is forged.[71]

The illegal action consists in any of the actions mentioned in section 86 that cause fake data to be produced. Section 86 includes acts of unauthorised access to data, unauthorised interference with or alteration of data, unlawful possession of certain devices, unlawful use of these devices, and the lockout of legitimate users from access or service. The further requirement is that fake data needs to be produced. Data would include all information in digital or electronic form. *Fake data* means the data should be false or untrue. The legislator avoided the use of the word "misrepresentation" which involves the deceiving of a human being.

---

[70] Snyman *Criminal Law* (2002) 529.

[71] Snyman *Criminal Law* (2002) 529.

The next element is that the perpetrator should have *the purpose of obtaining any unlawful advantage.* It is interesting to note that contrary to the common law element of prejudice, the legislator use the term advantage. The Act does not prescribe that the perpetrator should in fact have obtained an advantage. It would seem that potential advantage by the perpetrator should be sufficient. The use of the term *advantage* may include some form of prejudice suffered by a third party. The question that should be asked is whether the term *advantage* limits the scope of the Act. Prejudice by the victim or a third party does not necessarily hold an advantage for the perpetrator. Watney also criticises the use of the term *advantage* by the legislator because fraud, forgery and uttering have always been viewed in the light of prejudice to the victim or a third party.[72]

The perpetrator should act unlawfully. It is possible that grounds of justification may exist. The legislator prescribed culpability in the form of intent. The perpetrator should intend that the fake data be considered or acted upon as if it were authentic. This intent is the same as the common law element in the form of intent to defraud.

Section 88(1) of the Act criminalises an attempt to commit the offence. Aiding and abetting the main perpetrator to commit the offence is an offence in terms of section 88(2) of the Act. Similarly would the conspiracy or enticement of another to commit this offence constitute offences in terms of the provisions of the Riotous Assemblies Act[73]. The

---

[72] M M Watney *Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 2)* (2003) 2 TSAR 241.

[73] Section 18(2) of Act 17 of 1956.

penalty clause is found in section 89(2) of the Act and provides that a person may be fined or imprisoned for a period not exceeding five years.

10.6 SPAMMING

Spam or unsolicited junk e-mail is increasingly being used in South Africa and has become a headache for Internet users.[74] This type of unsolicited electronic mail invites the recipient to for instance visit a certain website or to engage in some form of a business transaction.[75] Employees use valuable office time to clean e-mail boxes from unsolicited *spam*.[76] *Spam* could also cause the e-mail server to clog or even to crash.[77] Internet businesses that make use of junk e-mail sometimes forge their e-mail headings in order to hide the identity of the true sender. The forgery of the e-mail heading is called *spoofing*.[78] It was recently reported that a new form of Internet *spam* called *spim* is set to explode.[79] These messages are sent over instant messaging services run by companies such as MSN and Yahoo.

---

[74] In general see Gerrie Ebersöhn *The unfair business practices of spamming and spoofing* (2003) July De Rebus 25 *et seq*.; Philip de Wet *Damn that spam – and its R13bn whammy* This Day 22/10/2003 page 1; Philip de Wet *Spam summit to discuss growing problem* This Day 22/10/2003 page 19; Belinda Anderson *Spam clogs Internet and costs SA R13-bn/year* The Citizen 23/10/2003; Paul Kirk *SA has no 'cyber cops' to police cyber traffic* The Citizen 30/01/2004 page 4; Dennis W K Khong *The problem of spam law: a comment on the Malaysian communications and multimedia commission's discussion paper on regulating unsolicited commercial messages* (2004) Computer Law & Security Report Vol. 20 No. 3 206 *et seq*.; Mike Butler *Spam – the meat of the problem* (2003) Computer Law & Security Report Vol. 19 Issue 5 388 *et seq*.; John Christopher Anderson *Transmitting legal documents over the Internet: How to protect your client and yourself* (2001) Rutgers Computer and Technology Law Journal Vol. 27 No. 1 14.

[75] Ebersöhn (footnote 74 *supra*) 25.

[76] See footnote 74 *supra*. Also see Street & Grant *Law of the Internet* (1999) 153; Kevan & McGrath *E-Mail, The Internet and The Law* (2001) 111.

[77] Footnotes 74 and 76 *supra*.

[78] Ebersöhn (footnote 74 *supra*) 25.

[79] *'Spim' could flood Internet* The Citizen 01/04/2004 page 21.

The common law crime of fraud may be committed through this misrepresentation if it results in actual or potential prejudice.[80] After an evaluation of the provisions of section 86 of the Electronic Communications and Transactions Act, Ebersöhn is of the view that *spamming* and *spoofing* do not fall within the ambit of the provisions of section 86 of the Act.[81] The Act, however, provides for certain statutory offences in respect of unsolicited commercial communications.[82] Any person that sends unsolicited commercial communications to a consumer must give the consumer the option to cancel his or her subscription to the mailing list of that person.[83] In other words an "opt-out option" should be included in the communication.[84] The American State of Nevada for instance has similar provisions.[85] Upon request of the consumer, the sender of the unsolicited e-mail must provide the source from which the consumer's personal information was obtained.[86] A person who fails to comply with or contravenes these provisions is guilty of an offence.[87] A person that sends unsolicited commercial communications to a consumer after having been advised that these communications are unwelcome, is guilty of an offence.[88] A perpetrator may be sentenced to a fine or a term

[80] Also see Ebersöhn (footnote 74 *supra*) 26.

[81] Ebersöhn (footnote 74 *supra*) 25.

[82] See John Peter *The Electronic Communications and Transactions Act* (2003) April Advocate 30 *et seq*.

[83] Section 45(1) of Act 25 of 2002.

[84] Ebersöhn (footnote 74 *supra*) 26.

[85] Street & Grant (footnote 76 *supra*) 157.

[86] Section 45(1) of Act 25 of 2002. Also see Paul Kirk *SA has no 'cyber cops' to police cyber traffic* The Citizen 30/01/2004 page 4.

[87] Section 45(3) of Act 25 of 2002.

[88] Section 45(4) of Act 25 of 2002.

of imprisonment not exceeding 12 months.[89] However, as correctly pointed out by Ebersöhn, the provisions of section 45 do not criminalise *spoofing* or forgery.[90]

[89] Section 89(1) of Act 25 of 2002.

[90] Ebersöhn (footnote 74 *supra*) 26.