CHAPTER 1

INTRODUCTION

1.1 THE ELECTRONIC FRONTIER

> " The revolution in information technologies has changed society fundamentally and will probably continue to do so in the foreseeable future. Many tasks have become easier to handle. Where originally only some specific sectors of society had rationalized their working procedures with the help of information technology, now hardly any sector of society has remained unaffected. Information technology has in one way or the other pervaded almost every aspect of human activities"[1]

People have been using calculating devices[2] for at least a thousand years. Although some of these early devices were information processors, they were not programmable.[3] The first successfully built[4] computer was designed by Herman Hollerith.[5] In 1939 John V Atanashoff constructed the first special purpose electronic digital computer.[6] The first general purpose electronic (digital) computer was built in 1946 by Eckert[7] and

---

[1] Explanatory Report to the Convention of Cybercrime, ETS No. 185, Council of Europe, Budapest 2001 (accessible at http://conventions.coe.int/Treaty/en/Reports/Html/185.htm).

[2] Such as the *abacus.* See *The New Encyclopedia Britannica* (1975) Vol. 4 on page 1046.

[3] *The New Book of Knowledge* (1992) Vol. 3 490; *The New Encyclopedia Brittanica* (1975) Vol. 4 1046.

[4] In the 1800's Charles Babbage designed the *analytical engine,* but was unable to construct the machine (*The World Book Encyclopedia* (1996) Vol. 4 on page 264).

[5] Hollerith devised a punching card system (*The World Book Encyclopedia* (1996) Volume 4 264 – 265).

[6] *The World Book Encyclopedia* (1996) Vol. 4 265.

[7] J Presper Eckert junior who was an engineer at the University of Pennsylvania USA.

Mauchly[8]. In 1951 these two engineers designed a more advanced computer[9] that subsequently became the first computer that was commercially available.[10] In 1975 the first personal computer was introduced and in 1977 two American students[11] founded the Apple Computer Company and introduced the Apple II personal computer.[12]

The computer evolved from a machine with enormous components that filled an entire room to smaller personal computers with digital chips that are hardly visible.[13] It was said that already in the 1970s the entire working of a computer could be placed on merely a handful of digital chips.[14] Computer technology evolved to one of the most advanced technical fields. Computers will still become more powerful and advanced and will increasingly be used in all fields of society.

In this exciting cyber era information technology and computers have invaded our every day lives to such an extent that we can't cope without them. Traditional shopping malls have been replaced by virtual shopping malls and one can acquire almost anything through the Internet.[15] Information superhighways have made a virtual borderless world

---

[8] John William Mauchly who also was an engineer at the University of Pennsylvania USA.

[9] This computer was called UNIVAC1 (*Universal Automated Computer*).

[10] *The World Book Encyclopedia* (1996) Vol. 4 266.

[11] Steven P Jobs and Stephan G Wozniak.

[12] *The World Book Encyclopedia* (1996) Vol. 4 266. In 1981 IBM entered the personal computer market with a more successful computer. In 1984 Apple introduced the Macintosh, a powerful and easy-to-use desktop computer.

[13] Miniaturisation of computer parts and components was aided by the invention of the transistor (*The World Book Encyclopedia* (1996) Vol. 4 266).

[14] *The World Book Encyclopedia* (1996) Vol. 4 266.

[15] For example Kalahari.net sells a wide range of books.

possible. One can have access to information located anywhere in the world within seconds and with the mere click of a mouse. Computers and information technology are used in business, industry, medicine, science, engineering, education and government, to name but a few fields.[16] It is hard to imagine what the world would be like without information technology. The advantages of computers are countless and they have a profound effect on society.

Unfortunately advanced technology also impact negatively on society. Computers and computer networks are targeted by highly sophisticated criminals and have become the playground of computer fanatics.[17] With the advent of new technology, new types of crime surfaced and traditional crimes are now being perpetrated by means of sophisticated technology.[18] Traditional boundaries have fallen away and a virtual borderless world has become the scene of crime.

---

[16] In a newspaper clipping entitled *Computers can predict crime* it is reported that a team of researchers from Carnegie Mellon University in the United States has developed a computer program that can predict crime. It is reported that the program was able to predict monthly crime rates with a 10 to 50 % error margin depending on certain factors (The Citizen 14/08/2003 page 15).

[17] The *I love you* virus, created by a student in the Philippines, wreaked havoc on computers worldwide and caused damage estimated at approximately $15 billion. See Reinhardt Buys *Love Hurts… Computer, network and e-mail security* (2000) July De Rebus 33 and Claire Coleman *Securing cyberspace – new laws and developing strategies* (2003) Computer Law and Security Report Vol. 19 No. 2 131 *et seq.* where it is reported that in May 2000 the *I love you* virus infected nearly 60 million computers worldwide. See further *Hacker cleans out bank accounts* Sunday Times 20/07/2003 and *Hacker hits Absa accounts* The Citizen 21/07/2003. At the time of writing there was fear that online banking was not safe and subsequently the *Absa hacker* was arrested and charged. See *Suspect charged in hacker case* Sunday Times 27/07/2003; *Hacker suspect's 46 charges* The Citizen 17/09/2003; *Alleged Absa hacker's secrets revealed in court* Sunday Times 21/09/2003; *Suspect granted bail in R629 000 Absa hacking case* The Citizen 08/10/2003. The Citizen (14/08/2003) reported in *Worst virus attack of year* that a virus infected various computers worldwide. The newest viruses, at the time of writing, included the *Sobig.F* virus that was described as the fastest spreading virus over the Internet (*Sobig.F virus: now brace for the second wave* The Citizen 25/08/03 page 2; *SoBig virus – "may have commercial motivation"* The Citizen 26/08/2003 page 2 as well as the *Swen* virus (The Citizen 23/09/2003).

[18] This distinction was also made by K Burden and C Palmer *Cyber Crime – A new breed of criminal?* Computer Law and Security Report (2003) Vol. 19 No. 3. The authors distinguished on page 222 between "true" cyber crime (i.e. dishonest or malicious acts which would not exist outside an online environment) and a crime that is simply e-enabled (i.e. a criminal act known to the world before the advent of the worldwide web, but which is now increasingly perpetrated over the Internet).

1.2 DEFINING THE PROBLEM

> "Throughout history law has struggled to keep pace with social, cultural, economic and technological change"[19]

South African criminal law originates from Roman law and legal principles were developed centuries ago. The founders of our legal principles could hardly have imagined the way the world has evolved and the revolutionary and continuous emergence of new technology. Legal concepts that were developed many centuries ago are struggling to cope with advanced technology. Traditional methods of detection, investigation and prosecution of crime are somewhat strained in the light of new and advanced cyber crimes. The question has been asked whether South African law is going to cope with new and advanced technology.[20] In an article entitled *Crimes committed by computer* A st Q Skeen stated: "the question that arises is whether our criminal law, which evolved before the space and electronic age, is supple enough to meet the onslaught of the white collar criminal who specialises in computer crime".[21] His Honourable Judge J P G Eksteen at the official opening of the academic year of the University of Port Elizabeth stated:

---

[19] Arkin *et al Prevention and prosecution of computer and high technology crime* (1990) p 1-1. Also see Peter Grabosky *et al Electronic Theft – Unlawful Acquisition in Cyberspace* (2001) 3.

[20] See A st Q Skeen *Computer and Crime* (1984) 8 SACC 262; D P van der Merwe *Computer crime* (1983) Obiter 124 *et seq*.; D P van der Merwe *Diefstal van Onliggaamlike Sake met Spesifieke Verwysing na Rekenaars* (1985) 9 SACC 129; D P van der Merwe *Onlangse ontwikkelinge op die raakvlak tussen Rekenaars en die Reg* (1991) 54 THRHR 95; C R Botha *Sogenaamde "Rekenaarbedrog"* (1990) 3 SACJ 231; J W Dreyer *Computer law in South Africa* (1983) De Rebus 535; D J le Roux *Diefstal deur middel van die rekenaar* (1985) De Rebus 401; G Horwitz *Computer abuse – the legal implications* (1986) De Rebus 503; F R Malan *Oor inligting, rekenaarmisbruik en die strafreg* (1989) 2 De Jure 211; M M Watney *Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 1)* (2003) 1 TSAR 68; DP van der Merwe *Computers* in WA Joubert LAWSA (1998) Vol. 5; D P van der Merwe *Computer crime – recent national and international developments* (2003) 66 THRHR 30.

[21] Businessman's Law (1984/1985) Vol. 14 page 9.

> "The computer is such a novel concept in itself and one so far removed from the contemplation of the founders of our legal system, that the application of the principles framed by them often presents considerable difficulty when seeking to apply them to the behaviour of people using computers"[22].

Prior to the enactment of the Electronic Communications and Transactions Act[23] some authors argued that there was a *lacuna*[24] in our law as far as computer crimes and related fields are concerned.[25] It was questioned whether legislation would be necessary to effectively deal with this issue.[26] It was apparent at the time, prior to 31 July 2002, that our law was hopelessly insufficient and ill equipped to deal with the revolution in information technology.[27]

The problem was exacerbated by the principle of *nullum crimen sine lege* which provides that no action shall be punishable as a crime unless it constitutes an offence in terms of existing laws and crimes.[28] In terms of the Constitution of South Africa every accused person has the right to a fair trial, which includes the right "not to be convicted for an act or omission that was not an offence under either national or international

---

[22] J P G Eksteen *Die bydrae van akademici tot die regspleging* (1984) Obiter 1.

[23] Act 25 of 2002.

[24] A gap or defect.

[25] Footnote 20 *supra*.

[26] D P van der Merwe *Computers and the Law* (2000) 200. The author was of the opinion that legislation was the only way to criminalise certain computer crimes. Also see Barrie Gordon *Criminal law* in Buys(ed) *Cyberlaw @ SA* (2000) 445.

[27] The helplessness of the business community at the time was reflected in Greg Gordon *Hackers can tap into computers, steal data and get off scot-free* at http://www.btimes.co.za/97/0601/tech/tech6.htm.

[28] The principle of legality. See Snyman *Criminal Law* (2002) 39 *et seq.*

law at the time it was committed or omitted".[29] The extension of the scope of application of certain existing common law and statutory crimes by means of analogy to include cyber offences would have been extremely difficult due to this constitutionally entrenched right[30]. Certain South African authors and legal scholars therefore called for legislation to criminalise cyber crimes[31] and our law relating to the subject changed dramatically with the enactment of the Electronic Communications and Transactions Act 25 of 2002.

Jonathan Burchell, however, warns against the so-called *blunderbuss* approach to simply resort to the enactment of new offences rather than improving on the detection and investigation of existing crimes.[32] He states:

> "Before succumbing to the crime-control model of criminal justice and developing new crimes to counter the ingenuity of the criminal mind, we need to answer two questions: (a) has a thorough and creative examination been done to determine whether the existing common or statutory law is inadequate to deal with the new or revived nefarious manifestation; and (b) does the cost in human and financial terms warrant the intervention of legislation, diverting already limited resources from the detection and prosecution of common-law crimes of violence to special and costly forms of law enforcement and to defending potentially time-consuming constitutional challenges to the legislation?"[33]

---

[29] Section 35(3)(l) of Act 108 of 1996. See Snyman *Criminal Law* (2002) 41 *et seq.*

[30] Footnote 29 *supra*.

[31] Footnote 20 *supra*.

[32] Jonathan Burchell *Criminal Justice at the Crossroads* (2002) SALJ Vol. 119 579 at 580.

[33] Burchell (footnote 32 *supra*) 585.

At first computer crime consisted of theft of electronic money and unauthorised access and alteration of data. Subsequently, with the advent of viruses and other forms of malicious software a clear need for international conformity and legislative intervention emerged. The creators of the *I love you* virus, students from the Philippines, whose virus infected approximately 60 million computers worldwide and caused considerable damage, could not be prosecuted of a crime due to the lack of a sanctioning provision in the Philippine Criminal Code that criminalised their actions.[34] This situation again emphasised the fact that many countries did not have legislation that criminalise such offending actions (cyber crimes).

Internationally many countries have enacted legislation to deal with cyber crime and the problems associated therewith.[35] The United States of America was probably the first country to enact legislation at federal as well as state level. Some of these statutes were enacted before the emergence of viruses and malicious software and were subsequently criticised as ineffective. Some of these statutes have since been amended or repealed.[36]

International organisations such as the European Union released reports on computer crime and conventions were held.[37] Some of these international developments as well as local efforts changed our law on

---

[34] Claire Coleman *Securing cyberspace – new laws and developing strategies* (2003) Computer Law and Security Report Vol. 19 No. 2 132.

[35] Dana van der Merwe *Computer crime – recent national and international developments* (2003) 66 THRHR 30.

[36] See paragraph 3.4.1 and paragraph 4.4.1 *infra*.

[37] Van der Merwe (footnote 35 *supra*) 33 *et seq*.

this subject dramatically.[38] The Council of Europe's Convention on Cybercrime was opened for signature on 23 November 2001 at Budapest.[39] The preamble states:

> "Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia* by adopting appropriate legislation and fostering international co operation…"

The Convention aims to harmonise laws in respect of cyber offences, procedure, investigation and prosecution thereof. South Africa became a signatory on 23 November 2001.

Early in 2001 the South African Law Commission released a discussion paper entitled "Computer related crime: Preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects" (hereinafter referred to as the Law Commission Report).[40] The Law Commission as well as its recommendations focused on the criminalisation of unauthorised access to and the modification of data. The Law Commission recommended that legislation should be considered to introduce new cyber offences.[41] A draft Computer Misuse Bill, with

---

[38] Van der Merwe (footnote 35 *supra*) 30 *et seq*.

[39] Convention on Cybercrime, ETS No. 185, Council of Europe, Budapest 2001 (Hereinafter referred to as the Convention on Cybercrime) at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm See in general Debbie Collier *Criminal Law and the Internet* in Buys(ed) *Cyberlaw @ SA II* (2004) 338 – 341; Claire Coleman *Securing cyberspace – new laws and developing strategies* (2003) Computer Law and Security Report Vol. 19 No. 2 131 *et seq*.

[40] Discussion Paper 99 Project 108 (hereinafter referred to as the SA Law Commission Report). The discussion paper was released for comment in May 2001 and the project leader was Prof D P van der Merwe. See Debbie Collier *Criminal Law and the Internet* in Buys(ed) *Cyberlaw @ SA II* (2004) 320 – 321 and 329 – 333; John Kuhn *New SA law pins down cyber criminals* at http://www.gal.co.za/planetgal/specfeat/01-11-15specrep-1.htm

[41] SA Law Commission Report (footnote 40 *supra*) 12. See Burchell (footnote 32 *supra*) 585.

the purpose of preventing unlawful access to computer material was recommended by the Law Commission.[42]

A green paper on Electronic Commerce was released by the Department of Communications.[43] The green paper focused on the regulation of electronic commerce ("e-commerce"). The Electronic Communications and Transactions Bill came to light.[44] It was amended after much comment[45] and then enacted. The Act was assented to on 31 July 2002 by Mr. Thabo Mbeki[46] using his own digital signature.[47] The Act has been in operation since 30 August 2002.[48]

---

[42] Page 61 – 68 of the SA Law Commission Report (footnote 40 *supra*). Also see Bobby Jordan *Hackers set to get the chop* at http://www.sundaytimes.co.za/2001/05/20/politics/pol01.htm

[43] Accessible at http://docweb.pwv.gov.za/Ecomm-Debate/myweb/greenpaper/execsummary.html.

[44] See Deloitte & Touche Legal e-Law Division *Guide to the Electronic Communication & Transactions Bill* accessible at www.deloitte.co.za; Derick Swart *The Electronic Communications and Transactions Bill, 2002* at http://www.markotter.co.za/ectbill.htm

[45] In an article entitled *The good things about the Electronic Communications and Transactions Bill…*Wim Mostert sets out some of the positive aspects in the bill including the criminalisation of computer and cyber offences (Without Prejudice April/May 2002 Vol. 2 No. 3 1). In the same periodical Doug Franke deals with the criticism against the bill in an article entitled *…and this is what some think is bad* (Without Prejudice April/May 2002 Vol. 2 No. 3 4). Adverse comment was directed at the powers of newly created cyber inspectors as well as domain name and cryptography registration. In *Comment on just introduced Electronic Communications & Transactions Bill* Gaye de Villiers refers to comment by Wayne Lurie, Garlicke & Bousfield's IT specialist that a positive move is that cyber crime such as fraud, forgery, computer-related extortion and interference with data will be criminal offences and punishable by law (http://www.webtelegraph.co.za/mainstories/26-03-2002/article002.htm). Also see *Experts say bill offers exciting opportunities* Sanchia Temkin Business Day 1st Edition 05/03/02; Phillip de Wet *The ECT Bill will fail and it's all your fault* at http://www.itweb.co.za/sections/columnists/doubletake/dewet020403.asp; Charl Bergkamp *ECT is a strange mix of forwards and backwards* at http://www.computingsa.co.za/Gifs/020415off01.htm; *Bill Gates risk* in The Citizen 04/07/2002 page 3; *New Bill opens Net to all* in The Citizen 07/08/2002; *Send bad Bill back* in The Citizen 31/07/2002.

[46] The President of South Africa.

[47] The Citizen 01/08/2002. This is advantageous since new legislation is enacted and assented to by using new technology. This places confidence in the legislator and its abilities.

[48] Government Gazette number 23809, 30 August 2002. In general see John Peter *The Electronic Communications and Transactions Act* (2003) Advocate April 30 *et seq*.; Danie Olivier *Wet op Elektroniese Kommunikasie en Transaksies* (2003) Society News 4.

The Regulation of Interception of Communications and Provision of Communication-Related Information Act[49] was assented to on 30 December 2002 and regulates certain communications. Criminal offences are also enacted.[50] The Act is not in operation yet and will repeal the Interception and Monitoring Prohibition Act[51] when it comes into operation.

The Electronic Communications and Transactions Act created new offences in our law, which, to a certain extent, filled the *lacuna* that previously existed. Since legislation in terms of the South African Constitution[52] may not have retrospective effect, it is important to deal with the position prior to the enactment of the Electronic Communications and Transactions Act. The position before and after the Electronic Communications and Transactions Act will be discussed. In this paper it will also be investigated whether the various forms of new legislation sufficiently deal with the issue of cyber crime or whether there still exist a need for improvement. It will be argued that certain "criminal" actions do not fall within the ambit of the definitions of common law crimes, statutory offences nor within the Electronic Communications and Transactions Act and that there still is a need for further development.

One should not lose sight of the fact that technology and cyber crime are still evolving and that the possibility of new forms or types of cyber

[49] Act 70 of 2002.

[50] Chapter 9 of Act 70 of 2002.

[51] Act 127 of 1992.

[52] The Constitution of the Republic of South Africa, Act 108 of 1996.

crime cannot be ruled out.[53] Cyber criminals will use more inventive and technologically advanced methods to commit cyber crimes. Will the various criminal offences in the Act encompass all forms of technologically advanced cyber crimes? Differently stated: will our current legislation survive the onslaught of cyber criminals and future technology?

Finally cyber crime resulted in the emergence of an alternative approach to traditional law enforcement (that traditionally means that the law should be enforced by the State).[54] Co-operation and collaboration between the State and the private sector are necessary to effectively deal with the advent of cyber crime.[55] This necessitates that a criminal law for cyberspace should be developed with specific provisions that relate to cyber crime.[56]

[53] See Bernard P Zajac, Jr *Tomorrow's computer criminal* (1990-91) 1 The Computer Law and Security Report 40.

[54] According to Susan W Brenner *Toward a criminal law for cyberspace: a new model of law enforcement?* (2004) Rutgers Computer and Technology Law Journal Vol. 30 No. 1 1 *et seq.*

[55] Brenner (footnote 54 *supra*).

[56] Brenner (footnote 54 *supra)*.