E-CRIMES AND E-AUTHENTICATION – A LEGAL PERSPECTIVE

By

MZUKISI NJOTINI

Submitted in accordance with the requirements
for the degree of

DOCTOR OF LAWS

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: Prof I Kroeze

CO-SUPERVISOR: Prof E Kritzinger

SEPTEMBER 2016

STATEMENT

Student Number: 44661592

I, Mzukisi Njotini, do hereby declare that *E-crimes and E-authentication – a legal perspective* is my own work. I also affirm that the sources or references that I used and quoted herein have been indicated and acknowledged by means of complete references.

…….. …….

Mzukisi Njotini Date

ACKNOWLEDGEMENTS

This research would not have been successful without the support and guidance of certain people. Therefore, I wish to thank everyone who contributed directly or indirectly towards its preparation and completion. The following people need particular reference:

- I wish to thank my promoters Proff I Kroeze and E Kritzinger for believing in me. All your efforts and time were not in vain. I know that you had other commitments to fulfil and boxes to tick but you chose to dedicate your energy and time to this research.

- I wish to extend a word of thanks to Mr T Constable, the Personal Librarian of the School of Criminal Justice, Unisa. I know how much pressure I sometimes exerted upon you. Despite this you remained composed and directed all your energy to giving me proper assistance and outstanding service.

- I wish to thank my mother Mrs Francis N Njotini. You have been the pillar of my strength for many years. I am fortunate and grateful that God has kept you alive to bear witness to this milestone of an achievement. I dedicate this research to you.

- I thank my brothers and sister for having been patient and understanding. I know that I did not spend as much time as I would have liked with all of you.

- I would also like to extend a word of gratitude to all my friends and colleagues in the Department of Jurisprudence, College of Law, and University of South Africa.

The list of people whom I can thank is long. I have faith that those that I have omitted to mention by name will understand.

ABSTRACT

E-crimes continue to generate grave challenges to the ICT regulatory agenda. Because e-crimes involve a wrongful appropriation of information online, it is enquired whether information is property which is capable of being stolen. This then requires an investigation to be made of the law of property. The basis for this scrutiny is to establish if information is property for purposes of the law. Following a study of the Roman-Dutch law approach to property, it is argued that the emergence of an information society makes real rights in information possible. This is the position because information is one of the indispensable assets of an information society. Given the fact that information can be the object of property, its position in the law of theft is investigated. This study is followed by an examination of the conventional risks that ICTs generate. For example, a risk exists that ICTs may be used as the object of e-crimes. Furthermore, there is a risk that ICTs may become a tool in order to appropriate information unlawfully. Accordingly, the scale and impact of e-crimes is more than those of the offline crimes, for example theft or fraud.

The severe challenges that ICTs pose to an information society are likely to continue if clarity is not sought regarding: whether ICTs can be regulated or not, if ICTs can be regulated, how should an ICT regulatory framework be structured? A study of the law and regulation for regulatory purposes reveals that ICTs are spheres where regulations apply or should apply. However, *better regulations* are appropriate in dealing with the dynamics of these technologies. Smart-regulations, meta-regulations or reflexive regulations, self-regulations and co-regulations are concepts that support *better regulations*. *Better regulations* enjoin the regulatory industries, for example the state, businesses and computer users to be involved in establishing ICT regulations. These ICT regulations should specifically be in keeping with the existing e-authentication measures. Furthermore, the codes-based theory, the Danger or Artificial Immune Systems (the AIS) theory, the Systems theory and the Good Regulator Theorem ought to inform ICT regulations.

The basis for all this should be to establish a holistic approach to e-authentication. This approach must conform to the *Precautionary Approach to E-Authentication* or *PAEA*. PAEA accepts the importance of legal rules in the ICT regulatory agenda. However, it argues that flexible regulations could provide a suitable framework within which ICTs

and the ICT risks are controlled. In addition, PAEA submit that a state should not be the single role-player in ICT regulations. Social norms, the market and nature or architecture of the technology to be regulated are also fundamental to the ICT regulatory agenda.

KEY TERMS: Biometric characters, computer hacking, distributed denial of service (DDoS) attacks, e-authentication, *furtum*, ICT regulation, ICTs, ID fraud, ID theft, information or computer systems, larceny, man-in-the-middle attacks, PAEAN, phishing, precautionary principle and user characters.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

Information and communication technologies[1] have had a significant impact on society. These ICTs include technologies that facilitate the 'application of scientific knowledge, materials, techniques, systems,[2] methods of organisation and the use of electronic and mechanical devices'.[3] ICTs can particularly be used to 'manage and support the efficient gathering, processing, storing and dissemination of information (or data) as a strategic resource'.[4] Both the terms information and data have relevance to a particular resource, for example ICTs. Despite this, the meaning of the terms differs. Diverse connotations are ascribed to the term information. There are some who define information as any 'piece of news with a meaning for the recipient; its assimilation usually causes a change within the recipient'.[5] There are also those who describe it as a resource in terms of which a message or instruction is conveyed.[6] The word data is sometimes defined differently from the notion computer data. It refers to the electronic representation of information in any form.[7] However, the concept computer data

---

1 Hereinafter referred to as ICTs. Examples of the various forms of technologies that have an impact on society are the World-Wide-Web or the Web, the Internet, interactive and multimedia communications, video conferences, virtual realities, computer-aided design, the information superhighway, and technologies of electronic or e-surveillance and consumer profiling. See Woolger S (ed) *Virtual society? technology, cyberbole, reality* (Oxford University Press Oxford 2002) 1.

2 Systems are referred to as the entities that are composed of related parts (sub-systems) and are directed at a purposeful activity. They have inputs and outputs. See, Emery JC *Management information systems: the critical strategic resource* (Oxford University Press Oxford 1987) 240-243.

3 Bowling B, Marks A and Murphy CC "Crime control technologies – towards an analytical framework and research agenda" in Brownsword R and Yeung K (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart Publishing Oxford 2008) 51-78 51.

4 See, s 1 of the State Information Technology Agency Act 88 of 1998.

5 Sieber U "The emergence of information law - object and characteristics of a new legal order" in Lederman E and Shapira R (eds) *Law, information and information technology* (Kluwer Law International The Hague 2001) 1-30 10-11.

6 Kaken H *Information and self-organisation: a macroscopic approach to complex systems* 3rd ed (Springer Berlin 2006) 15.

7 S 1 of the Electronic Communications and Transactions Act 25 of 2002 (hereinafter referred to as the ECT Act). It is important to note that there is a proposed change in the definition of the term data. This change is contained in the Draft Cybercrime and Cybersecurity Bill of 2015 (hereinafter referred to as the CaC Bill). The CaC Bill defines

denotes 'any representation of facts, information or concepts in a form (which is) suitable for processing in a computer system, including a program (which is) suitable to cause a computer system to perform a function'.[8] Having examined these definitions, it would appear that the meaning of the word data is wider than that of the concept computer data.

ICTs have been depended upon and used to carry out functions that are foreign to their traditional intended purposes. For example, the Internet, originally known as the Advanced Research Projects Agency Network,[9] was designed subsequent to an assignment by the Advanced Research Project Agency.[10] ARPANET was a military venture which was established in order to facilitate and conceal communication between the Marines of the United States of America immediately after the Second World War.[11] Following its successes, the ARPANET Transmission Connection Protocols (TCPs) were rolled out to other organisations or institutions that were involved in information security, for example, the University of California.[12] Soon thereafter, the Internet emerged.[13] This emergence culminated in the Internet

---

the word data as any representation of facts, information, concepts, elements, or instructions in a form suitable for communications, interpretation, or processing in a computer device, a computer network, a database, an electronic communications network or their accessories or components or any part thereof and includes a computer program and traffic data. See s 1 of the CaC Bill.

8 Council of Europe's Convention on Cybercrime of 23 November 2001. In this research the difference between the terms information and data is acknowledged. However, the words are for purposes of this research used interchangeably. Thus, a reference to information shall, unless the context indicates otherwise, be construed as referring to data and *vice versa*.

9 Hereinafter referred to as ARPANET.

10 Castells M *The internet galaxy: reflections on the internet, business, and society* (Oxford University Press Oxford 2001) 10-11; Lloyd I *Legal aspects of the information society* (Butterworths London 2000) 26-28 and Wyatt S, Thomas G and Terranova T "They came, they surfed, they went back to the beach - conceptualising use and non-use of the Internet" in Woolgar S (ed) *Virtual society? technology, cyberbole, reality* (Oxford University Press Oxford 2002) 23-40 23).

11 Kidder DS and Oppenheim NO *The intellectual devotional: American history* (TID Volumes New York 2007) 354.

12 Larson M, Liu C and Allen R *Mastering the domain name system: DNS on windows server 2003* (O'Reilly Media Inc. Sebastopol 2004) 1-2.

13 Larson, Liu and Allen *Mastering* 3.

becoming a major part of the 'fabric of our (daily) lives'.[14] The abovementioned was particularly compelled by the Internet's nature as a network of computer[15] networks.[16]

The Internet is an interconnected system of networks that connects computers around the world using the Transmission Control Protocol Internet Protocol (TCP/IP).[17] It is comprised of a mixture of infrastructures.[18] These infrastructures are codes, architectures, hardware or software that facilitates communication by or between computer users.[19] These infrastructures assist or enable computers to locate other computers, to communicate with one another and to transmit and receive information online.[20] The examples of the aforementioned information are drawings, illustrations, sketches, models, formulae, engineering designs, specifications, manuals and other instructions.

Recent technologies, for example the Internet, have become more essential in doing business online. Furthermore, these technologies are indispensable in exchanging information by or between governments, businesses or individual computer users. Consequently, they compel or facilitate the development of a new society. This society is referred to as the information society[21] or knowledge society.[22] An information

---

14 Castells *Internet galaxy* 1.

15 The term computer is derived from the Latin word *compŭto*, that is, to reckon together, calculate or compute. See Simpson DP *Cassell's new Latin-English English-Latin Dictionary* (Cassell & Co London 1959) 125. With the emergence of new forms of technologies, the term computer has however been understood to mean an electronic or e-device that stores, retrieves and processes information. See Williams MR "A preview of things to come - some remarks on the first generation of computers" in Rojas R and Hashagen U (eds) *The first computers: history and architectures* (The MIT Press London 2002) 1-16 1-2. For further interesting reading of the description of a computer, see, s 1(1) of the Computer Evidence Act 57 of 1983.

16 See Okin JR *The internet revolution: the not-for-dummies guide to the history, technology, and use of the internet* (Ironbound Press Winter Harbor 2005) 19 and Reed C *Internet law: text and materials* 2nd ed (Cambridge University Press Cambridge 2004) 8.

17 S 1 of the ECT Act.

18 Okin *Internet revolution* 19.

19 Papadopoulos S "An introduction to cyberlaw" in Papadopoulos S and Snail S (eds) *Cyberlaw @SA III: The law of the internet in South Africa* (Van Schaik Publishers Hatfield 2012) 1-8 2-3, Lee O and Lee W "Mobile commerce and national IT infrastructure" in Pour MK (ed) *Information technology and organisations: trends, issues, challenges and solutions* (Idea Group Publishing Hershey 2003) 352-354 352 and Byrne http://edbyrne.me/what-is-internet-infrastructure/ (Date of use: 26 September 2012).

20 Okin *Internet revolution* 19.

21 Webster F *Theories of the information society* 3rd ed (Routledge Abington 2006) 8-25.

society is generally the equivalence of what is sometimes known as the 'virtual world'.[23] It may be described as follows:

> (It is) the society (which is) currently being put into place, where low-cost information and data storage and transmission technologies are in general use. This generalisation of information or data use is being accompanied by organisational, commercial, social and legal innovations that will profoundly change life both in the world of work and in society generally.[24]

Another definition is that an information society is where:

> A high level of information intensity (exists) in the everyday lives of most citizens, in most organisations and workplaces, by the use of common or compatible technology for a wide range of personal, social, educational or business activities, and by the ability to transmit, receive and exchange digital data rapidly between places irrespective of distance.[25]

Lastly, this society enjoys the benefits of cheaper and faster access to ICTs, the provision of digital content for worldwide networks and the acceleration of electronic or

---

22 See Mansell R and Wehn U *Information technology for sustainable development* (Oxford University Press Oxford 1998).

23 Ross RA, Mortinger S, Christ R, Scelsi C and Alemi F (eds) *Computer games and virtual worlds: a new frontier in intellectual property law* (ABA Publishing Illinois 2010) 3-4.

24 Soete L *Building the European information society for us all: final policy report of the high level expert group* (European Communities Brussels 1997) 11.

25 Durrani S *Information and liberation: writings on the politics of information and librarianship* (Library Juice Press Duluth 2008) 256 and Manning T *Radical strategy: How South African companies can win against global competition* (Zebra Press Sandton 1997) 134.

e-commerce.[26] The aforementioned enables information to be processed and exchanged *ad infinitum.*[27]

1.2 LEGAL CONTEXT

The advent of contemporary forms of technologies has created innumerable drawbacks or limitations in the legal field. These shortcomings are for purposes of this research referred to as the risks or threats. Risks are generally old phenomena. They are practically as old as the human race itself.[28] They draw their existence from the fact that human life is subject to a number of risks, one of which is death.[29] A reference to a risk is here used to denote the existence of a likelihood that damage or an upsetting consequence will or is about to occur.[30] A lack of trust or the desire to exercise caution (or precaution) often leads some to view risks in a negative way.[31]

Customarily, the duty to identify and control technological risks was bestowed on scientists, the technologically brilliant and engineers of these ICTs. This was the case because it was felt that uncovering the proficiency of these technologies 'requires long, tedious hours of solitary work in laboratories or in isolated rooms full of machines'.[32] However, the developments in ICTs necessitated that even those who formerly had nothing to do with the conceptualisation and commencement of ICTs, namely lawyers, become involved in the identification and control of the ICT risks. Consequently, it

---

26 See generally, Council of the European Union and Commission of the European Communities (2000) http://ec.europa.eu/information_society/eeurope/2002/action_plan/pdf/actionplan_en.pdf (Date of use: 16 June 2012) (hereinafter referred to as the E-Europe Action Plan).

27 Ross *et al Computer Games* 3-4.

28 Beck U "From industrial society to the risk society – questions of survival, social structure and ecological enlightenment" 1992 (9) *Theory, Culture and Society* 97-123 97.

29 Beck 1992 *Theory, Culture and Society* 97. (Journal)

30 World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) *The precautionary principle* (United Nations Educational, Scientific and Cultural Organisation Paris 2005) 28. See also Perez FX "Risk regulation, precaution and trade" in Wüger D and Cottier T (eds) *Genetic engineering and the world trade system: World Trade Forum* (Cambridge University Press Cambridge 2008) 246-284 247.

31 Lofstedt RE "The precautionary principle, risk, regulation and politics" 2003 (81) *Trans IChemE* 36-43 39. An elaborate study of risks or threats is made in Chapter 7 (The Precautionary Approach to E-Authentication) of this research.

32 Tiagha E "Technology management and technology transfer in Africa" in Waiguchu JM, Tiagha E and Mwaura M (eds) *Management of organisations in Africa: A handbook and reference* (Quorum Books Westport 1999) 243-263 243.

became necessary to extend the ambit of the common law in order to deal with activities that traditionally were viewed to be irrelevant to law.[33]

The risks that ICTs generate relate to the criminal exploitation of modern technologies to commit novel crimes or the use of ICTs to commit traditional crimes. The examples of the new crimes include computer cracking, distributed-denial-of-service (DDoS) attacks, man-in-the-middle attacks and phishing.[34] Conversely, the examples of the traditional crimes which are committed through the use of ICTs include theft or *furtum* (including theft of funds in bank accounts), trespassing, damage to or destruction of property, fraud and possession or distribution of child pornography.

Technological crimes are sometimes referred to as Internet-related crimes, electronic or e-crimes, cybercrimes, computer crimes or net crimes.[35] Although some illustrate the difference in the terminology used in these crimes,[36] this difference is insignificant for purposes of this research. The important point, within the context of this research, is that the aggregation of modern forms of technologies has resulted in the aforementioned crimes (in this case, e-crimes) becoming a 'constituent aspect of the wider political, social and economic restructuring'.[37] Because of this, it is no longer satisfactory to only involve the engineers of these technologies in the process to prevent and curb e-crimes. More specifically, it has also become meaningful to

---

33 See *S v Mashiyi* 2002 (2) SACR 387 (Tk) where it was held that a computer print-out does not constitute evidence in terms of s 34 of the Civil Proceedings Evidence Act 25 of 1965. The reason for the exclusion of computer print-out was that a computer is not a person. Consequently, a computer print-out does not amount to a statement that is a made by a person. See also *S v Van den Berg* 1991 (1) SACR 104 (T) where the common law principles of *crime iniuria* were applied to a case involving fraud committed online (cyber fraud or cyber smearing). See also *S v Ndiki* 2008 (2) SACR 252 (Ck), *Ndlovu v Minister of Correctional Services* 2006 (4) SA 165 (W) and *S v Harper* and another 1981 (1) SA 88 (D).

34 Chapter 4 below provides a study of these novel crimes.

35 Van der Merwe DP *Information and communication technology law* (LexisNexis Durban 2008) 61 and Van der Merwe D "Criminal law – your partner in preventing information loss" (Paper presented at the *Lex Informatica* Conference on 23 May 2008).

36 See Downing RW "Shoring up the weakest link – what lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime" in Carr I (ed) *Computer crime* (Ashgate Publishing Limited Surrey 2009) 4-72 9.

37 Savona EU and Mignone M "The fox and the hunters - how ICT technologies change the crime race" in Savona EU (ed) *Crime and technology: new frontiers for regulation, law enforcement and research* (Springer Dordrecht 2004) 7-28 8.

establish legal frameworks that assist in controlling or regulating the manner of processing information contained in these technologies.[38]

The definition of e-crimes has been subject to academic debate for a number of years. More often than not, the definitions provided have been imprecise and disappointing.[39] There are some who suggest that e-crimes are crimes involving computers.[40] In this sense, e-crimes are 'any violation of criminal law that involves knowledge of computer technology by the perpetrator, investigator or prosecutor'.[41] Therefore, it amounts to any form of dishonest conduct or act which is associated with the mechanical processing or transmission of information.[42] There are also those who argue that e-crimes 'generally include(s) any crime carried out primarily by means of a computer or the Internet'.[43] Watney supports the view that cybercrime may be committed on a computer or the Internet.[44] The latter states that the example of a case where cybercrime is carried out on a computer is where an employee deletes information from a computer without authorisation.[45] Furthermore, the example of a situation wherein it is committed on the Internet is the defacing of a website, that is, the so-called web graffiti.[46] With this in mind, it would appear that a computer or the Internet fulfil two functions at once. It becomes an object of e-crimes, in cases where hardware or

---

38 In South Africa, the processing of or the manner of processing information is dealt with in Chapter 3 of the Protection of Personal Information Act 4 of 2013.

39 Sometimes, some elect not to define the term cybercrime for fear that, given the absence of academic consensus regarding the true meaning of the term, any such attempt will fall short of properly providing a meaningful description. See Brown I, Edwards L and Marsden C "Information security and cyberspace" in Edwards L and Waelde C (eds) *Law and the internet* (Hart Publishing Oxford 2009) 671-684 672-676.

40 Franklin CJ *The investigator's guide to computer crime* (Charles C Thomas Publisher Ltd Illinois 2006) 7 and Snail S "Cyber crime in South Africa - Hacking, cracking, and other unlawful online activities" 2009 (1) *Journal of Information, Law & Technology* 1-13 1.

41 Bazelon E *et al* "Computer crimes" 2006 (43) *The American Criminal Law Review* 260-308 260.

42 Franklin *Investigator's Guide* 7-13.

43 Berg T "The changing face of cybercrime – New Internet threats create challenges to law enforcement" 2007 (86) *Michigan Bar Journal* 18-22 18.

44 Watney M "Cybercrime and the investigation of cybercrime" in Papadopoulos S and Snail S (eds) *Cyberlaw @SA III: The law of the internet in South Africa* (Van Schaik Publishers Hartfield 2012) 333-351 337.

45 Watney "Cybercrime" 337.

46 Watney "Cybercrime" 337.

software is appropriated illegally, and it becomes a tool used in order to appropriate information unlawfully.[47]

The above-mentioned does not appear to be accurately dealt with by Chapter XIII (Cybercrime) of the ECT Act. More specifically, this chapter does not necessarily define e-crimes. It merely prohibits the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and, despite this awareness, still continues to access that data.[48] Having ascertained the existence of this anomaly, the South African Department of Communications issued Notice 888 of 2012[49] proposing that a definition of e-crimes should be inserted in section 1 of the ECT Act. In terms of the proposed definition, e-crimes should mean the following:

> Any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them.[50]

It is argued that this definition confirms the point that ICTs can be used as an instrument to commit e-crimes. However, whether or not this description of e-crimes is enough is not clear. Furthermore, the proposed CaC Bill does not appear to be addressing this uncertainty. Instead, it encumbers regulators with more work by creating in its chapter 2 no less than fifty-nine e-crimes.

Despite the aforementioned, Chapter XIII of the ECT Act established a number of e-crimes. These e-crimes depend on whether the accessing of information is intentional and without authority.[51] In particular, section 87 of the ECT Act extends the ambit of Chapter XIII to also include 'attempt', 'aiding' and 'abetting' as elements of e-crimes. Accordingly, it is enough for purposes of Chapter XIII to establish if the act or conduct

---

47 Cassim F "Formulating specialised legislation to address the growing spectre of cybercrime – A comparative study" 2009 (12) *PER* 36-79 36.

48 S 85 of the ECT Act.

49 Hereinafter referred to as the Electronic Communications and Transactions Amendment Bill, 2012.

50 S 1 of the Electronic Communications and Transactions Amendment Bill, 2012.

51 See section 86(1)-(4) of the ECT Act.

amounts to an unauthorised accessing of, interception of or interference with data;[52] if the act or conduct is computer-related extortion, fraud and forgery;[53] or if the act or conduct relates to an attempt, and aiding and abetting an unauthorised accessing of, interception of or interference with data; or computer-related extortion, fraud and forgery.[54]

It is important to note that the methods or techniques that are used to commit e-crimes are generally different from those known to traditional societies.[55] For example, dangerous codes,[56] such as a virus,[57] worm[58] and Trojan horse,[59] may be used in order to appropriate information without the required authority.[60] Viewed in this manner, these codes transform the methods that are commonly used in order to commit conventional crimes.[61] Furthermore, information may be appropriated online in circumstances where the lawful possessor is not actually dispossessed of the original information. For legal purposes, this modification generates challenges in relation to the regulation[62] of the nefarious acts that are committed through the use of ICTs. This

---

52 S 86 of the ECT Act.

53 S 87 of the ECT Act.

54 S 88 of the ECT Act.

55 See UK Cabinet Office http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf (Date of use: 10 May 2012).

56 Snail 2009 *Journal of Information, Law and Technology* 4.

57 A virus is a 'piece of programming code (which is) usually disguised as something else that causes some unexpected, and for the victim (commonly a user of a computer) usually undesirable event and which is often designed so that it is automatically spread to other computer users'. See Henning JJ and Ebersöhn GJ "Insider trading, money laundering and computer crime" 2001 *Transactions of the Centre for Business Law* 105-152 111.

58 A worm is a particular type of virus that 'situates itself in a computer system in a place where it can do harm'. See Henning and Ebersöhn 2001 *Transactions of the Centre for Business Law* 112.

59 A Trojan horse is a 'destructive computer program disguised as a game, a utility, or an application'. It does something 'devious to the computer system while appearing to do something useful'. See Henning and Ebersöhn 2001 *Transactions of the Centre for Business Law* 112.

60 Chapter 4 below delves into the workings and effects these codes to an information system.

61 UK Cabinet Office http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf (Date of use: 10 May 2012).

62 It will be established from Chapter 5 of this research that no single description of the term regulation currently exists. Numerous descriptions of the term have been proposed over the years. See for example, Joskow PL and Rose NL "The effects of economic regulation" in Armstrong M and Porter RH (eds) *Handbook of industrial organisation* (Elsevier Amsterdam 1989) 1450-1506 and Mitnick BM *Planning regulation: a framework for the analysis of regulatory possibilities* (University of Pittsburgh Pittsburgh 1979) 3-5. However, none of the proposed descriptions seem to capture the essence of

regulatory difficulty is acknowledged by Burchell[63] and Cassim.[64] Burchell submits that the criminal justice system in South Africa is at the 'crossroads'.[65] This is the case because offline rules have been found to be inadequate in dealing with the challenges that exist online.[66] Given the aforesaid, it has become necessary to establish systems that assist in separating challenges or risks from opportunities or benefits.[67] This could be achieved by discarding a particular legislative practice called the 'blunderbuss option'. This is a term which Burchell has borrowed from Stuart.[68] The word relates to the fact that technologies evolve almost daily. When these changes occur, new forms of e-crimes emerge. Therefore, the creation of new offences and harsher punishments in order to control emerging e-crimes may not be the best regulatory measure. Cassim follows Burchell's reasoning by stating that the South African legal system is confronted with incalculable ICT regulatory challenges.[69] According to Cassim, the challenges are twofold. On the one hand, there is a lack of precision in defining e-crimes.[70] On the other hand, the challenges have something to do with the inadequate mechanisms employed in detecting cybercrime.[71] Therefore, Cassim contends that an answer to these problems rests in 'formulating specialised legislation to address the growing spectre of cybercrime'.[72]

Against the background of the challenges posed by ICTs to an information society, this research examines the effect that e-crimes have for purposes of technology regulation. This is the case because e-crimes are or generally use conventional methods in order

---

regulation. Therefore, in Chapter 5 of this research the term regulation is interpreted to mean a process or scheme that seeks to serve 'diverse, even contradictory, ends, some economic, some political, some cultural, (and some technological)'. See McCraw TK *Regulation in perspective: historical essays* (Harvard University Press Boston 1981) 196.

63 Burchell J "Criminal justice at the crossroads" 2002 (119) *South African Law Journal* 579-602.

64 Cassim 2009 *PER* 36-79.

65 Burchell 2002 *South African Law Journal* 579.

66 Burchell 2002 *South African Law Journal* 579.

67 Burchell 2002 *South African Law Journal* 579.

68 Stuart D "An entrenched bill of rights best protects against law and order expediency" 1998 (11) *South African Journal of Criminal Justice* 325-336 328.

69 Cassim 2009 *PER* 36.

70 Cassim 2009 *PER* 36-37.

71 Cassim 2009 *PER* 37-42.

72 Cassim 2009 *PER* 66-69.

to commit traditional crimes, for example theft. In this instance, recent technologies become a tool whereby e-crimes are commenced and dispatched. By so doing, they then become analogous to ordinary crimes, for example theft. In particular, they involve an interference with a particular type of property, that is, information.

Because e-crimes involve an interference with a person's information online, the principles of the law of property become relevant. The most important aspect in this research relates to those that have to do with the objects of property. Accordingly, it is inquired whether information can be the object of rights or not. This investigation is necessary because not all objects are property for purposes of the law of property.[73] Some things can be the objects of real rights and duties whereas others cannot. Furthermore, an inquiry regarding whether a property right to information exists or not is essential because this research uses as a point of departure the fact that e-crimes can sometimes be seen as the contemporary version of conventional crimes. E-crimes generally involve an interference with the property of another person. The example of *furtum* or theft best illustrates the aforementioned.[74] When a study of theft is made the elements of for example the unauthorised appropriation of a thing or property of another with fraudulent (*fraudulosa*) intent can be abstracted.[75] Similarly, when an examination of e-crimes, for example phishing is made elements such as online identity theft and online identity fraud are present.[76] Because of this, it is hypothesised that e-crimes, for example phishing, computer cracking, distributed denial of service (DDoS) attacks and man in the middle attacks,[77] are contemporary versions of the crime of theft. Following this, the crime of theft is first analysed in order to test this hypothesis. Thereafter, e-crimes are examined in more detail. Consequently, it is submitted that the complexity and extent of ICTs make e-crimes pervasive in an information society.[78]

---

73 Van der Vyver JD "The doctrine of private law rights" in Straus SA (ed) *Huldigingsbudel vir W.A. Joubert: aan hom aangebied by geleentheid van sy sewentigste verjaardag op 27 Oktober 1988* (Butterworths Durban 1988) 201-246 231.

74 A complete examination of the crime of *furtum* or theft is undertaken in Chapter 3 below.

75 See the Chapter 3 below.

76 See Chapter 4 below.

77 The meaning and pervasive nature of these e-crimes is discussed in Chapter 4 below.

78 Costa *Crime and technology* 2-5.

This is particularly so given the global and borderless nature of recent technologies and the ease with which information is shared online.[79]

Having studied the above-mentioned, it is argued that regulators are confronted with questions such as whether or not current technologies can be managed or regulated, and whether the challenges that are generated by contemporary technologies can be regulated or not. If so, how should such a technology management, controlling or regulatory framework be structured?

This, in turn, raises questions regarding the nature of law and legal regulation. For example, if it is found that ICTs can be regulated, the question is or may be asked whether or not the law is the appropriate mechanism for such regulation. Given law's geographical constraints, as well as the more general limitations on legal regulation, that might not be the most appropriate method. For this reason, this research examines the various regulatory frameworks that are modelled from ICTs. However, such scrutiny is still made in full recognition of the importance of legal rules or principles to the overall scheme of regulation. This analysis is made with due regard to the essential fabric of an information society, namely the availability, reliability,[80] confidentiality and security of information systems[81] or networks.

1.3 TOPICAL ISSUES

It is conceded that various regulatory measures may be used in order to discourage or forbid e-crimes. In one case, firewalls may be built or engraved into a system or network. Firewalls monitor data which enter a system or network.[82] They then block

---

79 Cassim 2009 *PER* 66.

80 The reliability of information may be linked to what Dutton and Shepherd refer to as cyber trust, namely a 'confidential expectation in the reliability and value of the Internet and related ICTs'. See Dutton and Shepherd http://www.bis.gov.uk/files/file15271.pdf (Date of use: 13 May 2013).

81 An information system within the context of the ECT Act is a system for generating, sending, receiving, storing, displaying or processing data messages and includes the Internet. See s 1 of the ECT Act. See also the definition of an information system in terms of section 1 of the State Information Technology Agency Act 88 of 1998.

82 Blöcher U "Network and system security" in Fumy W and Sauerbrey J (eds) *Enterprise security - IT solutions: concepts, practical experiences technologies* (Publicis Corporate Publishing Erlangen 2006) 44-56 46.

unwanted information before it infiltrates a system or network.[83] In other cases, programs (awareness programs) may be commenced that are aimed at teaching or alerting society about the risks of e-crimes. Notwithstanding these developments, it is hypothesised in this research that e-authentication measures may provide a possible solution to the question regarding the regulation of ICTs and their ensuing risks. This viewpoint is not aimed at rendering the other mechanisms of preventing e-crimes insignificant. It is intended to supplement or support them.

E-authentication measures build on existing legal jurisprudence regarding the identification of a person and the verification, that is, the authentication, of his or her information. Traditionally, its significance within the context of the law is to be found in the law of testate succession and the law of contract. Quite recently, authentication mechanisms were found to be essential in preventing money-laundering[84] and terrorism or terrorist-related activities.[85] Within the context of FICA, the measures are contained in section 21 which deals with the identification and verification of the identity of a person.

E-authentication can be defined in the following manner:

> (A) process by which a person or legal entity seeks to verify the validity or genuineness of a particular piece of information. Alternatively, it can mean the formal assertion of validity, such as the signing of a certificate: we authenticate what it certifies.[86]

Identifying information is therefore indispensable in undertaking the e-authentication process. In particular, this information ensures that the e-authentication process has credibility and validity. The information includes, inter alia, PIN, username and

---

83 Blöcher *Network* 46.

84 See the definition of money laundering in section 1 of Financial Intelligence Centre Act 38 of 2001 (hereinafter referred to as FICA).

85 See the definition of terrorism or terrorist-related activities in section 1 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004.

86 Mason S *Electronic signatures in law* 2nd ed (Tottel West Sussex 2007) 1.

password; credit card and bank ATM cards, bank statements, pre-approved credit offers or tax information.[87]

This research submits that the e-authentication process needs to be controlled and regulated in order to ensure that it is effective. However, the extent and degree of such regulation should depend on the type of organisation or institution which undertakes the process and the person in respect of whom the e-authentication process is undertaken, the so-called risk-sensitive approach.

1.4 SIGNIFICANCE OF THE STUDY

In recent times, technologies have adapted and continue to modify the manner in which society or people communicate and share information. Some of the methods that are used for this modification were traditionally only imagined in science fiction. For example, recent technologies may be used as a defence mechanism against crime; technologies may be used for surveillance purposes; technologies may be used to investigate crime; and technologies may assist a court in order to pass an appropriate sentence and punishment.[88] These developments have implications not only for criminal law, but also for private and constitutional law. For example, they might entail invasions of privacy and other freedoms. Globalisation and the pervasive nature of these technologies exacerbate these adjustments.

South Africa has so far taken measures to ensure its participation in the global village and information society. More specifically, South Africa is enthusiastically moving ahead to become the kind of information society where a free flow of information is the norm. Furthermore, South Africa acknowledges that ICTs have a significant role to play in issues related to trade, e-commerce and the prevention of e-crimes. However, it is argued that South Africa should recognise the dual shift which is generated by modern technologies. In particular, South Africa ought to be aware of the fact that the prevalence of and dependency on ICTs is likely to lead to an increase in e-crimes.

---

87 Jasper MC *Identity theft and how to protect yourself* 2nd ed (Oceana Oxford 2006) 2-3 and Granova P and Eloff JHP "A legal overview of phishing" 2005 *Computer Fraud and Security* 6-11 6.

88 Bowling, Marks and Murphy *Crime control* 59-70.

Given this increase, this research seeks to address the legal challenges that are created by the illegal use of innovative technologies. In particular, it participates in the current scholarly debate regarding the proper methods to be used in order to control these new forms of technologies or the risks that are generated by these technologies. It also seeks to determine whether legal regulation is appropriate and effective or not. It is accepted that the debate as evidenced above is also relevant to South Africa. Consequently, this research presumes that a strong e-authentication paradigm is appropriate for South Africa. Such a structure should aim to re-establish the confidence and restore the integrity of computer or information systems or networks.

1.5 SCOPE OF THE STUDY

This research has identified the crimes that are associated with ICTs as a particular legal problem. It focuses on e-crimes as specific crimes related to the traditional crime of *furtum* or theft. The first objective of this research is to determine whether or not this assumption is correct. It particularly recognises that *furtum* or theft encompasses, amongst others, an unauthorised movement of property or a thing from the lawful possessor to the thief, that is, appropriation. Therefore, it scrutinises the meaning and importance of property to the law of theft. Thereafter, it examines the historical roots and contemporary incarnation of theft to test this assumption. It is also assumed that legal regulation is generally the appropriate mechanism to deal with e-crimes. Although it seems self-evident that the law should deal with e-crimes, the nature and extent of e-crimes may sometimes make this problematic. This is particularly so given the fact that the law or legal rules operate within borders whereas e-crimes do not. The second objective is therefore to examine this hypothesis.

It has also already been stated as a hypothesis that e-authentication can be seen as one of the solutions to the problem of e-crimes. However, e-authentication must take place within a particular legal, regulatory framework. The latter subsequently leads to the posing of a question regarding what that framework should look like. This obviously has implications in terms of privacy concerns and the limits of legal regulation. Despite this, this research is limited only to the regulation of ICTs. It does not encompass a study of the principles related to privacy, the protection of data online (data protection principles) and the like. Neither does it examine the sufficiency or not of the rules of criminal law and the issues pertaining to the trans-border monitoring and detection of crime, for example e-crimes. Simply put, this research assumes that e-authentication is

particularly suited to this regulatory process. Although it accepts that different systems and subsystems are essential to e-authentication, it excludes a study of systems or subsystems. In other words, it is not aimed at establishing a particular systematic process, namely firewalls, that could prevent or seek to prevent user-to-user computer attacks.

It should be understood that this research must be conducted within the confines and ambit of what is technologically possible. Technological constraints determine or should determine what kinds of e-authentication are possible, reliable and effective. Related technological developments therefore also need to be studied.

1.6 RESEARCH METHODOLOGY

This research recognises that traditional legal research is almost always text-based. This implies that the study of authoritative sources, typically common law, legislation and case law, forms the backbone of such research. Distinct from the natural sciences, which emphasise empirical observation and experimentation, law is arguably not an empirical science.[89] Put differently, the existence or not, and the sufficiency or not of legal rules or principles are not a matter of empirical study. Furthermore, this research is undertaken against the background of the divergent approaches relating to the nature of legal research and the question of what kind of science law (really) is.[90] For example, academics like Ross, submit that legal research is the province of empirical social science.[91] Therefore, the principles of verification that are found in legal research originate, according to Ross, from social facts.[92] On the other, Van Hoecke and Samuel contend that law or legal research is not a social science.[93] The

---

89 See Van Hoecke M "Legal doctrine - which method(s) for what kind of discipline?" in *Methodologies of legal research: what kind of methods for what kind of discipline* (Hart Publishing Oxford 2011) 1-18 5-6.

90 See in general Ross A *On law and justice* (The Law Book Exchange Ltd New Jersey 2004), Samuel G "Is law really a social science? – a view from comparative law" 2008 (67) *The Cambridge Law Journal* 288-321 and Vick DW "Interdisciplinarity and the discipline of law" 2004 (31) *Journal of Law and Society* 163-193.

91 Ross *Law and justice* 40.

92 Ross *Law and justice* 40.

93 Van Hoecke *Legal doctrine* 5-6 and Samuel 2008 *The Cambridge Law Journal* 292-296.

abovementioned is gleaned from the fact that legal research scrutinises 'normative judgments' as opposed to 'human interaction and behaviour'.[94]

Given the discussion above, this research accepts that because legal research is text-based, it is definitely a hermeneutic and argumentative science. In particular, legal research generally entails the development of solid arguments and interpretation of relevant texts and documents.[95] Viewed broadly, legal research usually involves a historical component (because the basis of South African law is the common law) and a comparative component (in order to establish how other legal systems have dealt with the problem). Therefore, this research examines the development of the South African law of property and of theft. Such investigation is made in order to establish how the law of property and of theft has evolved when influenced by outside innovations, for example, agriculture and technology. Accordingly, this research identifies problems within the existing law in order to support the necessity for a regulatory framework.

In this research it is averred that a scrutiny of the related structures dealing with e-crimes has relevance to the study of the aforesaid regulatory framework. Therefore, the developments of the measures in various selected legal systems, for example, the United Kingdom, Canada and South Africa are investigated.

Because e-crimes have to do with the appropriation of incorporeal property, for example information, the developments of the principles of property law are examined. These principles relate to property as an object of rights. The study of the latter principles then requires that an investigation should be made of the impact that concepts such as property and theft have or will have in dealing with some non-traditional forms of property. These include computer or information programming tools, computer hardware or software, architectures, infrastructures, codes, data, metadata, flowcharts or tables.

1.7 SUMMARY OF CHAPTERS

---

94 Samuel 2008 *The Cambridge Law Journal* 292.

95 See Kroeze IJ "Legal research methodology and the dream of interdisciplinarity" 2013 (16) *PER* 36-65 41-50.

In Chapter 2 certain selected aspects of property law are discussed. These are based on the Roman-Dutch, English and South African law. The discussion continues from the premise that ICTs are both essential and detrimental to the information society. Therefore, an answer is sought to the question whether or not the principles of property law can be stretched or are stretchable so as to render or allow information to be the object of property rights.

In Chapter 3 the various developments in the law of *furtum* or theft are examined. The Roman-Dutch, English and South African law approaches to *furtum* or theft are investigated. The basis is to establish whether or not the principles of *furtum* or theft have reached such a stage of development where unlawful appropriation of incorporeal or intangible things, for example information, can be recognised as theft in South Africa.

In Chapter 4 a study of e-crimes is made. It focuses on computer cracking, distributed-denial of service (DDoS) attacks, man-in-the-middle attacks and phishing. Chapter 4 particularly accepts that e-crimes are an extension of traditional crimes, for example, *furtum* or theft. Furthermore, Chapter 4 recognises that e-crimes are also novel crimes. However, the practices or activities that are involved in carrying out e-crimes are old occurrences. *Dolus malus* and *crimen injuria* are discussed in order to demonstrate the aforementioned.

In Chapter 5 the nature and character of legal regulation is investigated. It is revealed that an approach that relies on the law as the only mechanism to model the regulation of e-crimes is doomed to fail. Put differently, Chapter 5 argues that regulations, as opposed to the law, can provide effective measures in order to control and prevent e-crimes. Such regulations should consequently abandon, it is argued, a culture that encourages the re-invention of the ICT regulatory wheel. Therefore, Chapter 5 examines the traditional theories or approaches to ICT regulation. The investigation of the theories or approaches leads to the discussion of the drawbacks or limitations of legal regulations in general.

In Chapter 6 a theoretical and practical approach to the study of the measures against e-crimes is examined. As a starting point, it is argued that the measures are vast.

Some deal with the criminalisation of e-crimes. Others focus on preventing e-crimes. The measures to prevent e-crimes are thus selected. Following this selection, these measures are investigated as part of a *System or Process of E-Authentication*. Consequently, this selection leads to the scrutiny of the United Kingdom, Canadian and South African approaches to e-authentication.

In Chapter 7 a system of e-authentication or an e-authentication framework is introduced. This system is referred to as the *Precautionary Approach to E-Authentication or PAEA*. It accepts that every scheme that aims to regulate technologies and to subsequently prevent e-crimes should be founded on a risk-sensitive based framework. This structure concedes that ICTs evolve almost on a daily basis, and with these evolutions come the risks (for example the suppression of the free-flow of information) to the information society. Therefore, the relevance which PAEA has to the general scheme or structure to regulate e-crimes is examined.

In Chapter 8 an ICT regulatory approach which is founded on PAEA is proposed. The structure is not aimed at replacing the existing e-authentication measures. However, it intends to supplement them. It is then discussed, keeping in mind the study of the ICT regulatory theories that are examined in Chapter 5 of this research. Thereafter, Chapter 8 proposes the way forward for South Africa in regulating ICTs and controlling the scale of e-crimes.

CHAPTER 2

INFORMATION – ASPECTS OF PROPERTY LAW

CHAPTER 2

INFORMATION – ASPECTS OF PROPERTY LAW

2.1 INTRODUCTION

In chapter 1 it was demonstrated that ICTs can be both beneficial and detrimental to society. In some cases, recent technologies are essential in doing business and exchanging information online. Accordingly, they compel the formation of a new society. This society is referred to as the information or knowledge society.[1] Van Klink argues that technologies, for example the Web and the Internet, are interwoven with this information society.[2] In other cases, ICTs are commonly used for nefarious purposes. E-crimes are particularly identified as a threat or risk to the information society. More specifically, it is revealed that information could be essential assets that are or can be used as a tool for these devious dealings.[3] Insofar as information is indispensable to the information society, the law of property and the impact of information on the law of property are examined. In particular, it is enquired whether or not a computer user has a legally recognised and valid claim to a certain piece of information which he or she keeps or stores in his or her computer or someone else's computer or database. Some of the important works undertaken by Erlank[4] and Jankowich[5] on virtual property helps in making the aforementioned investigation.

The revision of the related principles of property law is not meant to re-invent the wheel or to re-write property law. Simply, it seeks to investigate the concept of property against the background assumption that all objects of property must or should be

---

1 Webster F *Theories of the information society* 3rd ed (Routledge Abington 2006) 8-25.

2 Van Klink BMJ and Prins JEJ *Law and regulation: scenarios for the information age* (IOS Press Amsterdam 2002) 5.

3 For a study regarding the importance of information or data to the information society see Weinrib AS "Information and property" 1988 (38) *The University of Toronto Law Journal* 117-150 117-118.

4 Erlank W *Property in virtual worlds* (LLD Thesis Stellenbosch University 2012).

5 Jankowich AE "Property and democracy in virtual worlds" 2005 (11) *Boston University Journal of Science and Technology Law* http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume112/JankowichArticleWEB.pdf%3Fq%3Dproperty-and-democracy-in-virtual-worlds (Date of use: 04 December 201).

corporeal or tangible.[6] Therefore, the scope of this chapter is restricted merely to the discussion of property as a right or property as an object of rights. In other words, this chapter ascertains the meaning and nature of the legal entitlement which a person has over or in respect of his or her property. It also investigates whether this property must be corporeal or not. In discussing property as a right, the remarks by Tomkins and Jencken on the meaning of the term right provide a useful guide.[7] Tomkins and Jencken argue that rights, in the subjective sense, denote 'the power or dominion which a person is entitled to exercise over an object, in which exercise there is involved the freedom of the will'.[8]

In view of the above-mentioned, the fact that this right to property is sometimes historically considered to be either absolute or composite (double ownership) falls outside the domain of this research. Consequently, the distinction between different kinds of *dominium* or ownership is irrelevant for purposes of this research. The most important aspect to be explored in this research is whether property as an object of a right depends on the needs of a particular society or not. The Roman-Dutch, English and South African law approaches to property assist in demonstrating the aforementioned.

2.2 ROMAN LAW

2.2.1 Old Roman Law (250 BC)

In the main, old Roman law recognised the importance of the relationship between a person and a thing or property.[9] Following this, the law of things was dealt with as the progression from the law of persons. For example, Table IV.V of the Twelve Tables regarded property as that which could be acquired by Roman citizens. Accordingly,

---

6 *Consolidated News Agency (Pty) Ltd (In Liquidation) v Mobile Telephone Networks (Pty) Ltd* 2010 3 SA 382 (SCA) 29-32 and *Cornelissen NO v Universal Caravan Sales (Pty) Ltd* 1971 3 S 158 (A) 179D-E. See also *Millar v Taylor* (1769) 98 E.R. 201 232.

7 Tomkins FJ and Jencken HD *A compendium of the modern Roman law founded upon the treatises of Puchta, Von Vangerow, Arndts, Franz Moehler, and the Copus Juris Civilis* (Butterworths London 1870) 40.

8 Tomkins and Jencken *A compendium of the modern Roman law* 40.

9 See Maine HS *Ancient law: its connection with the early history of society and its relation to modern ideas* (Spottiswoode London 1897) 258-259.

Roman citizens had an action against those who intruded on their property. The most notable were the *actio in rem* and *actio in personam*.[10] The *actio in rem* was a protection that was afforded to a person in relation to the use and enjoyment of his corporeal and physical *res*.[11] The *actio in personam* was a claim which a person had that others should acknowledge that the property is subject to his use and enjoyment.[12]

The Twelve Tables did not particularly discriminate between things as such. All the Twelve Tables required was that a thing must be capable of being touched, that is, the so-called *quae tangi possunt*. Literally, this can be taken to refer to *res corporales* or corporeals. Van Warmelo supports this viewpoint.[13] He states that 'in an early and unsophisticated community, the interests of the person were centred on what he could see and touch and perceive with his senses'.[14] Therefore, if a person could hold or possess a thing it was consequently said that such a thing served the interests of such a person.[15] Van Warmelo then concludes that 'in the early Roman community possession of objects was the centre of all interests'.[16]

A reference to the term interest is of specific importance to an examination of property as an object of rights in old Roman law. This is the position because the Twelve Tables did not specifically refer to the notion of ownership. More specifically, the position in old Roman law regarding ownership can be summarised as follows:

> (The) technical word for ownership of things: it (ownership) was an element of the house-father's *manus*. In time, although it is impossible to say when, the word *dominium* came into use; but, so far as can be discovered, it did not occur in the Tables, and must have been of later introduction. In those days, when a man asserted

---

10 Nasmith D *Outline of Roman history from Romulus to Justinian (including translation of the Twelve Tables, the Institutes of Gaius, and the Institutes of Justinian), with special reference to the growth, development and decay of Roman jurisprudence* (The Lawbook Exchange New Jersey 2006) 327-328.

11 Mousourakis G *Fundamentals of Roman private law* (Springer Berlin 2012) 312.

12 Mousourakis *Roman private law* 312.

13 Van Warmelo P *An introduction to the principles of Roman civil law* (Juta Cape Town 1976) 63.

14 Van Warmelo *Roman civil law* 63.

15 Van Warmelo *Roman civil law* 63.

16 Johnson D *Roman law in context* (Cambridge University Press Cambridge 1999) 53.

> ownership of a thing, he was content to say, - 'It is mine,' or 'It is mine according to the law of Quirites'.[17]

Therefore, it may be submitted that *dominium* was but 'one manifestation of the comprehensive domestic powers which the *paterfamilias* wielded over certain persons (*patria potestas* over his children in power, *manus* over his wife) no less than over his property'.[18]

In summary, old Roman law recognised that rights in property were only vested in corporeal things. The justification for this is that the Roman society around 250 BC was unsophisticated and simple.[19] Thus, it was simply accepted that the objects of property rights were those objects that could be observed and touched.[20]

2.2.2 Pre-Classical Roman Law

Pre-classical Roman law marked a development of the law that was known and accepted in old Roman law. In this period, things were classified into things corporeal or *res corporales* and things incorporeal or *res incoporales*.[21] Corporeal things were those objects that were by nature tangible.[22] The examples of these were the land, a slave,[23] a garment, gold and silver. Incorporeal things were those things that were not

---

17 Muirhead J *Historical introduction to the private law of Rome* (Gaunt Inc. Florida 1998) 126. See also, Bouckaert B "What is property?" 1990 (13) *Harvard Journal of Law and Public Policy* 775-816 781.

18 Kaser M *Roman private law* (translated by Dannenbring R) (University of South Africa Pretoria 1980) 115-116. See also, Muirhead J *Historical introduction to the private law of Rome* 3rd ed (A & C Black Ltd London 1916) 120 and Bouckaert 1990 *Harvard Journal of Law and Public Policy* 781.

19 Van Warmelo *Roman civil law* 63.

20 Van Warmelo *Roman civil law* 63.

21 Cairns JW "The definition of slavery in eighteenth-century thinking" in Allain J (ed) *The legal understanding of slavery* (Oxford University Press Oxford 2012) 61-84 61-62.

22 Sohm R *The institutes: a text-book of the history and systems of Roman private law* 2nd ed (Gaunt Inc. Florida 1901) 320.

23 In relation to a slave being an object of property in pre-classical Roman law, Buckland states that a slave 'was the one human being who could be owned. There were men in many inferior positions which look almost like slavery: there were the *nexus*, the *auctoratus*, the *addictus* and others. But none of these was, like the slave, a *Res'.* See Buckland WW *The Roman law of slavery: the condition of the slave in private law from Augustus to Justinian* (Cambridge University Press Cambridge 2010) 10.

tangible, for example an inheritance, usufruct, obligation or servitude.[24] The last-mentioned things had the quality of being rights over property.[25]

The inclusion of slaves or slavery within the domain of *res corporales* is instructive. This is the position because pre-classical Romans accepted that, by virtue of the *ius gentium* or the laws common to all, certain human beings are free whereas others are not.[26] Slaves represented the category of humans that lacked freedom. Nicholas summarises the position of slaves and slavery in pre-Roman law by stating the following:

> Being endowed with reason…he (slave) was inevitably a peculiar thing and could, for example, acquire rights for his master. But he himself had no rights: he was merely an object of rights, like an animal.[27]

Given this, they (slaves) remained the property of the other person and were subject to the ownership of that other.[28] Understandably, the aforementioned was consistent with the needs of this society at that point in time.

In summary, pre-classical Roman law represented a departure from the old Roman law view in relation to property. In particular, this law accepted that rights in property vested not only in tangible things, for example land, garment, gold, silver and slaves, but also in intangible things. For this reason, things such as an inheritance, usufruct, obligation and servitude were regarded as the objects over which a person had an interest which deserved protection. This development of the objects of property reflected the particular needs of the pre-classical Roman law society.

2.2.3 Classical Roman Law

Classical Roman law represented an era which is essential to the history of the Roman law of property. Firstly, most of the ideas from this period continue to influence the modern understanding of property. Secondly, classical Roman law characterised a

---

24 Sohm *The institutes* 320.

25 De Zulueta F *The Institutes of Gaius: part ii commentary* (Oxford University Press London 1963) 62.

26 Cairns "The definition of slavery in eighteenth-century thinking" 61-62.

27 Nicholas B *Introduction to Roman law* (Oxford University Press Oxford 1987) 69.

28 Cairns "The definition of slavery in eighteenth-century thinking" 61.

period wherein the notion of *dominium* or ownership of property, as opposed to the word *belonging to*, was expressly conceived.[29] On the one hand, the owner of a thing was referred to as a *dominus*, *proprietarius*, or *dominus proprietatis*.[30] On the other hand, the notion of *esse alicuius* was used in order to demonstrate that a thing was owned by another person.[31] Given the aforesaid, ownership denoted a right which a person possessed to use, enjoy, destroy and transfer his property subject to certain limitations.[32] These restrictions could be established by 'rules of nuisance as well as the rules for the protection of slaves and the right to transfer limited rights to others….e.g. in the form of a user's rights or servitudes'.[33]

Furthermore, a broader approach was followed in relation to the meaning of the term property.[34] Property signified the totality of the objects that were of economic value to a person.[35] These things were regarded as *res in commercio*.[36] The examples included a

---

29 Schulz F *Classical Roman law* (Oxford University Press London 1961) 338-339.

30 Schulz *Classical Roman law* 338-339.

31 Schulz *Classical Roman law* 338-339. Roman law jurists differed as to the true nature of *dominium*. There are some who argue that ownership was the 'most comprehensive private right to a thing' which a private person could have. See Kaser M *Roman private law* (translated by Dannenbring R) 2nd ed (Butterworths Durban 1968) 92. See also Declareuil J *Rome the law-giver* (Greenwood Press Westport 1970) 158. It this sense, it amounted to a legal right over a thing which gave the holder the full power of enjoyment and use. See Sohm *Roman private law* 325. Accordingly, a Roman owner had unrestricted right of control over a thing, and could claim the thing he owned 'wherever it is and no matter who possesses it'. Jolowicz HF and Nichols B *Historical introduction to the study of Roman law* 3rd ed (Cambridge University Press London 1972) 140. However, there are also those who question the reality of the aforementioned viewpoint. This opposition rests on the premise that it is illogical as a 'proposition that the owner of a sword could do what he liked with it, including applying it to the neck of his neighbour's slave'. See Birks P "The Roman law concept of *dominium* and the idea of absolute ownership" 1985 *Acta Juridica* 1-37 1 and Scott H "Absolute ownership and legal pluralism in Roman law – two arguments" 2011 *Acta Juridica* 23-34 24. It is particularly submitted that the view on the absolute nature of *dominium* was inconsistent with the earlier attempts in the old and pre-classical Roman law of property in relation to the control, use and enjoyment of property. See Table VII of the Twelve Tables and Gaius 4 (limitations on the control of salves).

32 Garnsey P *Thinking about property: from Antiquity to the Age of Revolution* (Cambridge University Press Cambridge 2007) 177, Buckland WW *A manual of Roman private law* (Cambridge University Press Cambridge 1939) 111 and Buckland WW *The main institutions of Roman private law* (Cambridge University Press Cambridge 1931) 93.

33 Roby HJ *Roman private law in the times of Cicero and of the Antonines* (Cambridge University Press Cambridge 1902) 414.

34 Buckland *The main institutions* 91.

35 Kaser *Roman private law* 80.

36 Kaser *Roman private law* 80.

building, land, animals, slaves, gold or silver.[37] In addition, property denoted 'any legally guaranteed economic interest having monetary value, that a person could hold in respect thereof'.[38] In view of its monetary value, humans (Roman citizens) had an interest in property. This interest was protected by various laws, for example natural law or *iure naturali*, and civil law or *ius civile*.[39]

Lastly, classical Roman law differentiated between corporeal and incorporeal things, *res mobilis* (movable things) and *res immobilis* (immovable things), *res mancipi* and *res nec mancipi*.[40] Corporeals represented the original category of things that were recognised in classical Rome.[41] They were one of the classical groups of things that were regarded as *res in patrimonio*.[42] They included property that was perceptible through the senses.[43] Examples of corporeals were the land, house, horse, slave, garment, gold or silver.[44] Incorporeals, for example a right, servitude, inheritance, *hereditas*,[45] were traditionally not regarded as *res* in the true sense of the word. This was because the latter things were considered to be interests or rights which accrue over *res corporales*. Therefore, to regard them as *res* in the stricter sense of the word could be taken to mean that a right (being the *res incoporales*) could have a 'right (for example, ownership) to a right'.[46] Over a passage of time, the strict meaning ascribed to incorporeals was discarded. Following this, a convenient mode of expressing these things was adopted. It became common to accept that a person could also have interest in particular abstract and non-physical entities.[47] This interest did not

---

37 Kaser *Roman private law* 80.

38 Moussourakis *Roman private law* 119.

39 Mommsen T *The Digest of Justinian* (University of Pennsylvania Press Philadelphia 1985) 1.1.11.

40 This research does not examine the difference between *res mobilis* and *res immobilis*, *res mancipi* and *res nec mancipi*. It simply discusses the distinction between corporeals and incorporeals. Furthermore, it is acknowledged that other differences between properties or *res* were made. Examples of these included *res divini iuris* or things dedicated to the gods, *res publicae* or public properties, *res omnium communes* (air, water or the sea) and *res in commercio* (*res nullius* or ownerless things, consumable things and *res fungibiles* money, wine or grain and divisible things). See Sohm *The Institutes* 302-305.

41 Thomas JAC *The Institutes of Justinian: text, translation and commentary* (Juta Cape Town 1975) 73.

42 Van Warmelo *Roman civil law* 65-66.

43 Moussourakis *Roman private law* 121.

44 Moussourakis *Roman private law* 121.

45 Sohm *Roman private law* 225.

46 Van Warmelo *Roman civil law* 66.

47 Van Warmelo *Roman civil law* 66.

necessarily amount to ownership. Simply, it was equated to a *res quae tangi non possunt* or a right to intangible things.[48]

In summary, classical Roman law marked a development of the old and pre-classical Roman law ideas on the law of property. Firstly, this law recognised that rights in property vested in those things that were of economic value to a person. It then listed things, for example a building, land, slave, gold and silver as *res in commercio*. The understanding of property as that which bestowed on a person an economic interest marked a further development in the law of property. More specifically, it is unique to the classical Roman society in the sense that it was not known in old and pre-classical Roman law. Secondly, classical Roman law followed the pre-classical view on property by stating that the objects of rights were *res corporales* and *res incorporales*. The aforementioned classification of things was in keeping with the values and needs of the classical Roman society.

2.2.4 Post-Classical Roman Law

Two systems influenced the law of property in post-classical Roman law. These are the developments of the Roman vulgar law in the West and the Roman law under Justinian in the East.

(a) Roman Law in the West

Roman law in the West is the law which grew out of the practical consideration of old Roman law sources.[49] This law was 'averse to strict concepts and neither able nor inclined to live up to the standards of classical jurisprudence with regard to the artistic elaboration or logical construction'.[50] It took place in the period between 350 AD until 550 AD. It did not appear to distinguish between the terms ownership and possession, that is, the factual control of a thing. More often than not, the essence and clear

---

48 Van Warmelo *Roman civil law* 65.

49 Levy E *West Roman vulgar law: the law of property* (American Philosophical society Philadelphia 1951) 2.

50 Berman HJ *Law and revolution - the formation of the Western legal tradition* (Harvard University Press Cambridge 1983) 53.

meaning of the notion of ownership as found in classical Roman law systems was diluted. Consequently, the concept of *dominium*:

> '….once radiant with lucidity, appeared largely drained of substance and void of any precise meaning. Not only did it take in former *iura in re aliena* such as *emphyteusis* and *superficies*, *usufructus*, and perhaps *servitus*; it was even interchangeably used with *possessio*'.[51]

Concepts such as *possidere*, *possessio* and *possessor* were particularly applied as a replacement for the word ownership in order to illustrate the legal right to use and control a thing.[52] Accordingly, the right to possess which was referred to as the *inconcussum possessionis ius*, *ut dominus possidet* or *iure dominium possidere*, as opposed to a *dominium* over a thing gained prominence.[53] The above-mentioned reflected the needs of that society and had to do more with the protection of possession than for ownership.

(b) Roman Law in the East

The Roman law in the East was an additional development of pre-classical and classical Roman law. This law distinguished between things in general. There was property that was capable of being owned and that which could not be owned (*de iure personarum exposuimus*).[54] The property that was capable of being owned was also referred to as the *res nostro patrimonio*.[55] Furthermore, the things that were incapable of being owned were called *res extra nostrum partimonium*.[56] Other divisions of property were also made possible, for example those things that were common to all,[57] public things,[58] things belonging to the community[59] and those that belonged to no one.[60] In relation to *res nostro patrimonio*, it was stated that ownership in relation to these could be acquired either by natural law (law of nations) or civil law. Accordingly,

---

51 Levy *West Roman vulgar law* 61.
52 Levy *West Roman vulgar law* 26-27.
53 Levy *West Roman vulgar law* 27.
54 Institutes of Justinian 2.1.
55 I.2.1.
56 I.2.1.
57 For example the air, running water, rivers, the sea and seashores. See I.2.1.1.
58 The examples of these are the river banks, seashores, things lying under the sea, earth or sand. See I.2.1.4-5.
59 For example cities, theatres and *stadia*. See I.2.1.6.
60 I.2.1. Things belonging to no one were sacred things, religious things or those things that were placed under divine protection. See I.2.1.7.

animals,[61] slaves,[62] precious stones[63] and buildings[64] were categorised as things that were capable of being owned.

In addition, a distinction was made between corporeal and incorporeal property.[65] Corporeals were defined as those things that, by nature, could be observed and touched.[66] The list of examples included the land, a slave, garment, gold and silver.[67] Incorporeals were referred to as those things that were recognised by the law despite the fact that these things could not be observed and touched.[68] The examples were an inheritance, usufruct and obligation.[69]

In summary, the law of property in post-classical Rome was founded on two systems. There was the Roman law of property that was practiced in the West and the Roman law of property that was followed in the East. Roman law in the West was particularly an era wherein the Roman law of property as it was understood in the earlier periods lost meaning and relevance to society. It was then in the East that an attempt was made to recapture the ideas of property law of the old, pre-classical and classical periods. Specifically, it was accepted that rights in property vested in tangibles, for example land, slave, garment, gold or silver, and other rights, for example an inheritance, usufruct or obligation.

The above-mentioned demonstrates how societies and the needs of societies differ. For example, the Roman law in the West was more concerned with protecting the possession of a thing. However, the Roman law in the East sought to retain the meaning of property that was known in old, pre-classical and classical Roman societies.

2.3 GERMANIC LAW

---

61 I.2.1.12-16.
62 I.2.1.17.
63 I.2.1.18.
64 I.2.1.29-35.
65 I.2.2.
66 I.2.2.1.
67 I.2.2.1.
68 I.2.2.2.
69 I.2.2.2.

2.3.1 Old Germanic Law

In old Germanic law, property or *Sache*, being the 'impersonal corporeal pieces of the outer world',[70] was regarded as that which belonged to people collectively.[71] For example, people would seize the land and such land would consequently belong to all of them as a unit. Because of this, rights in property were conceived 'as belonging to families and kinship, not as absolute individual rights'.[72] The term belong is indispensable to the study of the old Germanic private law. Words like '*eigen*' or '*eigan*' and '*haben*', were frequently used in order to demonstrate who had ownership in each case.[73]

Ownership denoted the fullest right that could be possessed over things.[74] Hübner argues that this right was concentrated on the *dominion* in respect of property in its entirety.[75] However, it appears from Calisse that it was not always necessary in old Germanic private law that ownership should be in respect of the whole property. Calisse submits that it was particularly possible to have a situation where one person was the owner of a house and the other of the land on which a house was built.[76] With this in mind, the powers and rights to exercise ownership could be bestowed on a certain collective or 'landholding corporate group'.[77] This collective had to use these rights for the common benefit of all the members of the community. The manner of exercising this use depended on whether the property belonged to the tribe or to the family.[78]

However, developments in the law of property necessitated that ownership of property should also be extended to other personal things, for example carts, flocks, fruits, clothes and weapons. According to Murray, these changes in the law of property were

---

70 Hübner R *A history of Germanic private law* (Augustus M Kelly Publishers New York 1968) 160.

71 Murray AC *Germanic kinship structure: studies in law and society in Antiquity and the early Middle ages* (Pontifical Institute of Medieval Studies Toronto 1983) 18 and Calisse C *A history of Italian law* (Augustus M. Kelly Publishers New York 1969) 653.

72 Bouckaert 1990 *Harvard Journal of Law and Public Policy* 780.

73 Hübner *Germanic private law* 227.

74 Hübner *Germanic private law* 227.

75 Hübner *Germanic private law* 227.

76 Calisse *Italian law* 671.

77 Murray *Germanic kinship structure* 19.

78 See Calisse *Italian law* 657-664. See also, Vinogradoff P "The organisation of Kinship" in Krader L (ed) *Anthropology and early law* (Basic Books Inc. New York 1966) 57-74 57.

compelled by the confrontation of old Germanic law with Roman law.[79] Because of this, the nature of property was no longer only limited to that which a tribe or family could have *dominium* over. However, it also became conventional to refer to things as that which were or could be held or belonged to an individual (*allodium*).[80] Consequently, the rights in (individual) things or *Sachenrechte* were recognised.[81] These rights were separated into those attaching to corporeal and incorporeal things.[82] An important point about all this is that a certain category of slaves (*servi casati*) could have *dominium* over land cultivated by them.[83] Therefore, they could enjoy all the fruits of their labour.

In relation to corporeals (land, animal, gold, silver and certain precious stones), old Germanic private law followed the Roman law approach to property. It stated that ownership was vested in these things by virtue of them being capable of being touched (*res quae tangi possunt*). However, a slightly different approach was followed. In particular, it was argued that corporeals were not naturally property for legal purposes. They only became property in the legal sense as soon as legal rights were attached to them.[84] These rights were called *dengliche* or real rights. The aforesaid rights secured for the owner the direct control of a thing subject to certain legal limits.[85] Other rights (including rights in property), inheritance and usufruct were regarded as incorporeal things.

In summary, old Germanic law traditionally regarded property as that which belonged to a family or kinship. What this meant was that individual rights to property were impossible. However, the interaction between the old Germanic and Roman law of property resulted in the recognition of individual rights to property. Following this, it became common to recognise real rights in property. These rights were vested in

---

79 Murray *Germanic kinship structure* 179-180. Vinogradoff refers to this confrontation as rather startling, in the sense that 'it seemed at the outset as if there would not be much room for Roman doctrine in a country with a German-speaking population of Germanic stock'. See Vinogradoff P *Roman law in medieval Europe* 3rd ed (Oxford University Press Oxford 1929) 119.

80 Calisse *Italian law* 665.

81 Hübner *Germanic private law* 162.

82 Hübner *Germanic private law* 162.

83 Calisse *Italian law* 416.

84 Hübner *Germanic private law* 161.

85 Hübner *Germanic private law* 162.

corporeals and incorporeals. Despite the aforesaid, slaves were excluded from the category of corporeal property. In particular, it was acknowledged that a certain category of slaves could own property or could possess rights in property.

Therefore, the aforementioned demonstrates that the objects of rights are not always limited to those that a particular legal system recognises and protects at a particular point in time. Specifically, it reveals that as the society changes, so does its needs. Because of these changes, variations in the law of property become necessary.

2.3.2 Frankish Law

Frankish law consisted of the practices which were followed by the West German tribes across the Rhine. Although Roman law had a strong influence on these usages,[86] the law that was followed was far removed from its classical Roman law formulations.[87] The feudal system also provided a shift in the manner in which the relationship between a person and a thing (fief) could be understood.[88] This system had its roots in feudal law. It marked a regime of underdevelopment[89] and a system of exploitation.[90] It reflected the 'particular viewer's biases, values and orientations'.[91] The feudal system represented itself in situations where a weaker person, namely the peasants or vassal, would turn to a stronger man, that is the lord, in order to derive some forms of rights in property. In this sense, the vassal became a tenant over property held by the lord.[92] For purposes of studying the law of property, the lord (the king or the church) was at

---

86 Stein P *Roman law in European history* (Cambridge University Press Cambridge 1991) 41-42 and Wallace-Hadrill JM *The long-haired kings and other studies in Frankish history* (Methuen & Co Ltd London 1962) 1-2.

87 Van Caenegem RC *An historical introduction to private law* (Cambridge University Press Cambridge 1992) 21-24.

88 The word 'feudalism' can be traced to the later part of the eighteenth century. Its origin 'must be looked for in Frankish kingdom of the Merovingians, and more particularly in the heart of the kingdom between the Loire and the Rhine'. See Ganshof FL *Feudalism* (translated by Grierson P) (Medieval Academy of America New York 1996) 3. For further interesting reading, see Davies W and Fouracre P (eds) *Property and power in the early middle ages* (Cambridge University Press Cambridge 1995) 4-15.

89 Okey R *Eastern Europe 1740-1980* (Hutchinson Minneapolis 1982) 21.

90 Lyon BD *The Middle ages in recent historical thought: selected topics* (American Historical Association Washington DC 1965) 13.

91 Brown EAR "The Tyranny of a construct – feudalism and historians of mediaeval Europe" 1974 (79) *The American Historical Review* 1063-1088 1086.

92 Volokh A "Property rights and contract form in Medieval Europe" 2009 (VII) *American Law and Economics Review* 399-459 422.

the top of the property law chain while the peasants were at the bottom.[93] Accordingly, the right (*droit*)[94] to property did not bestow on the holder (peasant) ownership of the property.[95] It only amounted to that which a king or church could grant to a vassal.[96] Because of this, the vassal was prevented from transferring the rights that flowed from this property.[97]

It is indeed true that feudal law frustrated the proper development of the Roman law of property. It specifically treated the classical Roman law term *dominium* as denoting simply a beneficial right or *usufructus*.[98] Thus, a vassal only had *proprietas* or right of control. This *proprietas* was limited in that it did not necessarily mean that the property could be alienated or inherited.[99] It only meant that the vassal was a recipient or *bucellarius*.[100] Given this, his right to control the property depended on the continuation of the relationship between himself and the *dominus*, namely the king or the church.[101]

Besides all this confusion, a difference was created between corporeals or *fief corporel* and incorporeals or *fief incorporel*.[102] Land, office and animals were regarded as *fief corporel*. Household goods were excluded from the definition of *fief corporels*.[103] The reason for this was that these goods were perishable by nature.[104] *Fief incorporels* included rights, *usufructus*, inheritance and income.[105]

In summary, Frankish law was the law which was practiced by the West German tribes across the Rhine. This law did not necessarily embody the Roman law principles that were comparable to old, pre-classical and classical Rome. For purposes of studying

---

93 Pejovich S *The economics of property rights: towards a theory of comparative systems* (Kluwer Academic Publishers Dordrecht 1990) 8-9.

94 McSweeney TJ "Property before property – Romanising the English law of land" 2012 (60) *Buffalo Law Review* 1139-1199 1147.

95 Brissaud J *A History of French public law* (as translated by Garner JW) (Augustus M. Kelly Publishers New York 1969) 339-340.

96 Anderson P *Passages from antiquity to feudalism* (Verso London 1974) 147-148.

97 Anderson *Passages from antiquity to feudalism* 147-148.

98 Brissaud *French public law* 260 and Levy *West Roman vulgar law* 88.

99 Levy *West Roman vulgar law* 89-90.

100 Levy *West Roman vulgar law* 89-90.

101 Levy *West Roman vulgar law* 89-90.

102 Brissaud *French public law* 265.

103 Brissaud *French public law* 265.

104 Brissaud *French public law* 265.

105 Brissaud *French public law* 265.

the law of property, a distinction was made between a person and a fief. Rights to a fief were bestowed on the superior persons in society, that is, the lord. The weaker persons, that is, the peasants, only had a right to use and possess a fief. This right was limited in that it could not be transferred to another person. The feudal system therefore created a society that had different needs from that of the Roman society and this is reflected in the different objects of property.

2.4 MEDIEVAL LAW

2.4.1 The Romanists

The Glossators and Ultramontani are important to an investigation of Roman law during the Romanist period.

(a) The Glossators

The Glossators were the Roman law intellectuals who were located in Bologna, Italy between 1100 and 1250 AD.[106] Samuel summarises the position of the Glossators in the law by stating the following:

> The Glossators and the Post-Glossators had an unsurpassed knowledge of the Roman source materials and for them law as a concept and legal science (*scientia juris*) was equivalent to Roman law. However, the society in which they lived was anything but Roman.[107]

They commented on the phrases and texts that were contained in the *Corpus Iuris Civilis* by means of Glosses. However, the Glossators deviated from the old, pre-classical and classical Roman law of property in relation to the wording to be preferred when referring to the legal right which a person had to property. In particular, they spoke about the *ius in re* as opposed to an *actio in rem*.[108] In modern English, the tem *ius in re* is interpreted to mean a property right.[109] It was then argued that this right to

---

106 Garnsey *Thinking about property* 195.

107 Samuel G "The many dimensions of property" in McLean J (ed) *Property and the constitution* (Hart Publishing Oxford 1999) 40-63 43.

108 See Tuck R *Natural rights theories: their origin and development* (Cambridge University Press Cambridge 1979) 16.

109 It is accepted that Bartolus de Saxoferrato (1313-1357) mentioned a third form of dominium. This he referred to as *quasi dominium*. However, this form of ownership did

property, of which *dominium* was the most important, amounted to an *ius perfecte disponere*.[110] This *ius pefecte disponere* granted to the owner of an object the full or complete disposal over a corporeal thing.[111] They then described these rights as either those that 'belong as an individual possession to each person, assigned to him by law' or those over which a person had 'capacity and power assigned by law'.[112] In more abstract terms, *ius pefecte disponere* bestowed on the *dominus* the 'claim to total control against the entire world'.[113] Despite the above-mentioned, the Glossators did not concern themselves with providing a definition of the term rights. Because of this, a clear line could not be drawn between *ius in re* and *ius in personam* (that is, personal rights).[114]

Furthermore, the glossators recognised that the starting point to the study of property is the acceptance of the 'exclusive bond between a person and a thing'.[115] In so doing, they recognised the division between corporeals and incorporeals. Following this recognition, the rights in respect to corporeal and incorporeal things were referred to as the *ius reale*, that is, real rights.[116] These rights did not necessarily translate to ownership. They merely denoted that, by reason of the close association between a person and a thing, a person had an interest over such a property.[117]

In summary, the Glossators contributed much to the understanding of property as an object of right. Firstly, they recognised that property rights generally granted to a person the complete powers to use and dispose of the property. Secondly, they

---

not found favour. See Feenstra "*Dominium* and *ius in re aliena* - the origins of a civil law distinction" in Birks P (ed) *New perspectives in the Roman private law of property: essays for Barry Nicholas* (Clarendon Press Oxford 1989) 111-122 113.

110 Bartolus de Saxoferrato (1314-1357) spoke, for example of *quid ergo est dominium? Responde est ius de re corporali perfecte disponendi, nisi lege prohibeatur.* See Bartolus ad D 51.2.17.1.

111 Garnsey *Thinking about property* 198 and Visser DP "The 'absoluteness' of ownership – the South African common law perspective" 1985 *Acta Juridica* 39-52 43.

112 Garnsey *Thinking about property* 202.

113 Tuck *Natural rights theories* 15.

114 Feenstra "*Dominium* and *ius in re aliena* - the origins of a civil law distinction" 112.

115 Samuel "The many dimensions of property" 47.

116 Pottage A and Sherman B "On the prehistory of intellectual property" in Howe HR and Griffiths J (eds) *Concepts of property in intellectual property law* (Cambridge University Press Cambridge 2013) 11-28 22.

117 Pottage and Sherman "On the prehistory of intellectual property" 22.

introduced, for the first time in the history of the Roman law of property, the concept of *ius reale*. Having done all this, they argued that rights in property, corporeal or incorporeal, are to be referred to as the real rights.[118] This development of the rights in property reflected the attitudes of the Glossators to Roman law principles.

(b) The Ultramontani

The word Ultramontani was used in reference to the French Romanists who resided in the North of Italy 'across the mountains'.[119] These scholars were mostly French-speaking and belonged to the school of Orléans.[120] The Ultramontani followed the work of the Glossators of Bologna. Despite this, their thinking was greatly influenced by the domestic French and Canon laws which existed at the time. In relation to the law of property, the Ultramontani provided a much more refined approach to property.[121] The refinement of the Ultramontani's view on property is furthermore made explicit by Du Plessis.[122] Du Plessis states the 'scientific approach of the school of Orleans (ultramontani), which influenced legal science during the thirteenth century, was not exactly revolutionary, but their approach towards textual analysis and textual authority was novel'.[123]

The French Romanists accepted the separation between corporeals and incorporeals. Such acceptance can be extrapolated from one of the prominent French jurists by the name of Jacques de Revigny (1230-1296 AD). In his *Lectura supra Codice* Revigny spoke about certain tangibles such as agricultural land, cattle and house.[124] In relation to incorporeal objects, especially those that are attached to land, Revigny mentioned a hypothec as an example.[125] Furthermore, the Ultramontani accepted that usufructs, gains or profits from tangible property were the kinds of intangibles that should be

---

118 Pottage and Sherman "On the prehistory of intellectual property" 22.

119 Du Plessis JP *Barkowski's textbook on Roman law* 4th ed (Oxford University Press Oxford 2010) 376.

120 Knoll PW "*Nationes* and other bonding groups at late medieval central European universities" in van Deusen N and Koff LM (eds) *Mobs: an interdisciplinary inquiry* (Koninklijke Brill Leiden 2010) 79-94 85-86.

121 Van der Walt AJ *Die ontwikkeling van houerskap* (LLD Thesis Potchefstroom University 1985) 183.

122 See Du Plessis PJ "Towards the medieval law of hypothec" in Cairns JW and du Plessis PJ (eds) *The creation of the ius commune: from Casus to Regula* (Edinburgh University Press Edinburgh 2010) 159-175.

123 Du Plessis "Towards the medieval law of hypothec" 172.

124 De Revigny J *Lectura supra Codice* on C 4.65.5.

125 De Revigny *Lectura supra Codice.*

recognised and protected by the law of property.[126] This recognition and protection did not necessarily exist because dominium over these things was possible. It existed because a person had an interest in the aforementioned property.[127]

In summary, the Ultramontani had a sophisticated approach to property. On the one hand, these jurists followed the classical Roman law idea of the law of property. On the other hand, they acknowledged that property was no longer only limited to that which was known and accepted in classical Roman law.[128] Therefore, the objects of property rights, but not ownership, could be extended to those things that were not recognised in classical Roman law. Some of the examples of these included certain incorporeal objects, such as fruits or gains from tangibles. So, as this society became more sophisticated, the specific needs of this society changed.

2.4.2 Canon Law

Canon law (and later, Church law) is the whole body of legal rules which was developed in order to deal with matters that fell within the domain of the Roman Catholic Church.[129] This law also regulated the relationship between the Church and the secular sphere.[130] Canon law developed separately from Roman law. This progression took place following the prevalence of the rules of Canon law, that is, the *canones* in medieval Rome. Besides this separation, Canon law relied heavily on certain principles of Roman law for its sustenance. One example of such is the principle that regulated the property of the Church. Accordingly, it is conceivable that the Roman law of property was applied by the Church only insofar as this law was not in conflict with Canon law.[131]

---

126 Van der Merwe C and Verbeke AL (eds) *Time-limited interests in law* (Cambridge University Press Cambridge 2012) 25-26.

127 Van der Merwe and Verbeke *Time-limited interests in law* 25-26.

128 Du Plessis "Towards the medieval law of hypothec" 171-172.

129 Van Zyl DH *Geskiedenis van die Romeins-Hollandse Reg* (Butterworths Durban 1979) 160.

130 Van Zyl *Geskiedenis van die Romeins-Hollandse Reg* 160.

131 Tamm D *Roman law and European legal history* (Djøf Publishing Copenhagen 1997) 212.

The acceptance of the notion of individual rights to property by Canon law is difficult to establish with precision. For example, the Canonists differentiated between the *ius* of a heavenly origin and those that were granted by human or positive law. In relation to the first-mentioned, reference was made to common property. This common property was regarded as the property of God. Being so, it was accepted that God had ascribed this property to humans for their common nourishment. The aforementioned view was held because the earth belonged to the Lord.[132] Consequently, all earthly property was to be held in common in accordance with God's wishes.[133] As for the second-mentioned rights, the Canonists, for example Gratian, held that *dominium* over these objects rested or was ascribed to private individuals.[134] However, the manner in which this ownership was exercised or operated was determined by the creator of this *dominium* that is the emperor.[135]

A departure from the above-mentioned could be found in one of the most prominent jurists of Canon law, namely, Bonagratia of Bergamo.[136] Bonagratia made reference to the term *habere*. *Habere*, in the sense in which Bonagratio used the term, could mean three things.[137] Firstly, it could signify the actual *dominium* of the *dominus*.[138] Secondly, it could be interpreted to mean the *usus facti*, that is, the *usufructus* without a legal title to the property itself.[139] Thirdly, *habere* could denote the modern idea of possession.[140] Bonagratia's narration above seems to have been followed by William of Ockham. Ockham initially defined property as a competence (*facultas*) to claim a good.[141] He then referred to this good as the *ius*. The *ius* represented the unique power to deal with the good itself, that is, the *facultas utendi*.[142] Following this, rights in property were

---

132 D.8.C.I.

133 D.8.C.I.

134 Helmholz RH "Human rights in the Canon law" in Witte J and Alexander FS (eds) *Christianity and human rights: an introduction* (Cambridge University Press Cambridge 2010) 99-112 101.

135 Helmholz "Human rights in the Canon law" 101.

136 Shogimen T *Ockham and political discourse in the late Middle ages* (Cambridge University Press Cambridge 2007) 41-42.

137 Van der Walt *Die ontwikkeling van houerskap* 213.

138 Van der Walt *Die ontwikkeling van houerskap* 214.

139 Van der Walt *Die ontwikkeling van houerskap* 214.

140 Van der Walt *Die ontwikkeling van houerskap* 214.

141 Bouckaert 1990 *Harvard Journal of Law and Public Policy* 787.

142 Robinson JW *William of Ockham's early theory of property rights in context* (Koninkljke Brill Leiden 2008) 208.

deemed to have vested in the *dominium* of the human person[143] and the rights to the use of a thing belonging to another without prejudice to the substance of the thing itself.[144] The aforementioned rights were vested in both *res corporales* and *res incorporale*.[145]

In summary, Canon law recognised the fact that rights in property existed. In particular, there were some rights that originated from God, that is, the common rights and those that were derived from positive law, namely, the individual rights.[146] As regards to property, Canon law accepted that rights in property were vested in both corporeal and incorporeal things. Thus, a use of thing or *usus facti* or usufruct were categorised as examples of incorporeal objects.[147] So, the law around this time was changed in order to fit the needs of the church and thus making provision for the role of God.

2.5 SIXTEENTH CENTURY

2.5.1 *Mos Italicus*

Mos italicus signified the Italian law which was followed and applied during the sixteenth century. For its existence, this law relied massively on Bartolus' ideas on law.[148] Bartolus' influence on the *mos italicus* was by no mean accidental. It existed because Bartolus was the most famous jurist of the Middle Ages.[149] His ideas on law were particularly authoritative in Italy for a long period of time. Because of this importance, the phrase *nemo jurista nisi Bartolista* (no one is a jurist who is not a Bartolist) was commonly used.[150]

---

143 '*Dominium est postesta human principalis rem temporalem in iudico venticandi et omni modo, qui non est a iure naturali prohibitus, pertrectandi*'. See Van der Walt *Die ontwikkeling van houerskap* 215.

144 '*Usus est ius utendi rebus alienis, salva rerum substantia*'. See Van der Walt *Die ontwikkeling van houerskap* 215.

145 Van der Walt *Die ontwikkeling van houerskap* 215.

146 D.8.C.I.

147 Van der Walt *Die ontwikkeling van houerskap* 214.

148 Woollfson J *Padua and the Tudors: English students in Italy, 1485-1603* (James Clarke & Co Cambridge 1998) 45-46 and Van der Walt *Die ontwikkeling van houerskap* 233.

149 Tamm *Roman law* 206.

150 Tamm *Roman law* 206.

Jacobus Menochius held the view that property meant that which belonged to a person and is in turn the object of his own.[151] If this was established, Menochius argued that the latter could dispose freely of this property.[152] However, Gomezius spoke of *dominium* as the right to a corporeal thing in terms of which a person had *libere disponendi*. To this end he accepted that only one form of *dominium* existed in law. This acceptance is made evident by the following passage:

> *An sit autem duplex dominium directum et utile aut unum tantum sit, est controversum inter doctors et Batolum. Sed unicum tantum dominium esse in punto iuris posset defendi cum Duarenus. Alias dixi quod est detentatio, et illa nihil aliud est quam sole, nuda, et simplex insistetia rei quae consistit in facto, ex qua ne dominium nec possessio aliqua resultat propter qualitatem personae vel rei, vel ex ipsa natura actus: puta si traditur mihi aliqua res, vel ego eam accipio, et est actus per quem non potest causari possessio iuridica, certe tunc dico habere nudam detentationem: et illa dicitur nuda et simplex detentatio*.[153]

In the aforementioned passage, Gomezius acknowledged the challenges that were created by Bartolus' theory of *duplex dominium*. He stated that the premise upon which the law - presumably, Gomezius was referring to the classical Roman law – was founded was that there is only one *dominium*.[154] Having stated all this, Gomezius distinguished between *dominium* and what he referred to as *detentatio*, that is, discretion over the object of property as guaranteed and protected by law.[155]

In summary, the jurists of the *Mos italicus* followed Bartolus' idea of property as an object of right. More specifically, these jurists argued that property rights for purposes

---

151 Menochius' *Consilia*.492.12.

152 Van der Walt *Die ontwikkeling van houerskap* 234.

153 In English, the aforementioned passage can be translated to mean that 'whether there a two kinds of ownership or there is only one is a matter that the jurists of the Bartolum theory do not have agreement. *Detentatio* I said , which is the other, and that is nothing other than the sun, on the bare, and the task, which consists of a simple fact, for the sake of the quality of the results from any person or is not to be the dominion nor the possession of the thing or by reason of the nature of the act: for example, if it is handed down to me, a real thing, or I receive it, I will, by means of which it cannot be caused, and it is an act of the inheritance of the law, indeed, we shall, I say to have a bare *detentationem*: naked and simple, and it is said *detentatio*'. (Own translation).

154 Grossi P *A history of European law* (Blackwell Publishing West Sussex 2010) 16.

155 Grossi *European law* 16.

of the law existed in respect of only one type of property, that is, corporeal property. So, the interpretation of Roman law in the context of this society meant that rules were interpreted differently.

2.5.2 *Mos Gallicus*

Mos gallicus was the humanist method of reasoning that was developed in Italy but had France as its centre.[156] The contribution of this humanist model to law can be summarised as follows:

> The humanists wanted new source versions, *ad fonts* (back to the sources) was one of the catchphrases of the time. They read Greek - *graeca leguntur* - in contrast to the medieval jurists. Thus, they had a new independent access to the texts that did not require the use of a gloss as an authority. The actual teaching of law was also changed as the humanists emphasised the *Institutiones* as the introduction to the study of Roman law….the humanists were dissatisfied with the system of the digest and sought to resystematise it in new ways.[157]

Jacques Cuiacius (1522-1590) was the most prominent jurist of this time. In relation to property, Cuiacius was confronted with the challenges of defining the ambit of the rights to property belonging to a vassal and those of a superior. His solution to this was simply that: 'the nature of the vassal's right to property was a usufruct with undivided *dominium* vesting in the superior'.[158] By this, he sought to align his theory of property, especially ownership, with that of the classical Romans and with feudal law.

In summary, the jurists of *Mos gallicus* were not satisfied with how the law of property had evolved in the periods before them. They then developed an independent idea of property. This was modelled from the classical Roman law approach to property. Specifically, they discarded the view that rights in property were only vested in

---

156 Goddu A *Copernicus and the Aristotelian tradition: education, reading, and philosophy in Copernicus's path to Heliocentrism* (Koninklijke Brill Leiden 2010) 178.

157 Tamm *Roman law* 222.

158 Cairns JW "Craig, Cujas and the definition of *feudum*" in Birks P (ed) *New Perspectives in the Roman law of property: essays for Barry Nicholas* (Claredon Press Oxford 1989) 75-84 81.

corporeal things. To them, the object of rights and not ownership were corporeals and incorporeals.[159] Consequently, the amalgamation of Roman law with the needs of a feudal society created a different view of objects of rights.

2.5.3 Moral Philosophers

One of the most essential philosophers of this time is Aquinas. In his *Summa Theologica*, Aquinas differentiated between things by stating the following:

> We can consider a material object in two ways. One is with regard to its nature, and that does not lie within human power, but only divine power, to which all things are obedient. The other is with regard to its use. And here man does have natural *dominium* over material things, for through his reason and will he can use material objects for his own benefit.[160]

He then referred to the first-mentioned property as those things that God gave to mankind in common.[161] Consequently, the rights which flowed from this property were ascribed to the natural law.[162]

In relation to the second-mentioned property, Aquinas submitted that God (the creator of all property) retained the absolute *dominium* over property. This meant that a person simply had an usufruct over property. Accordingly, a person merely had 'the power and privilege of making a purposive use of things'.[163] This power to use property had to be exercised within the limits as set out by natural law.[164]

---

159 Cairns "Craig, Cujas and the definition of *feudum*" 81.

160 Aquinas *Summa theologica* 2a 2ae. 66. 1.

161 Aquinas *Summa theologica* 2.2, 66, 1.

162 Aquinas *Summa theologica* 2.2, 66, 1. In relation to *ius naturale*, Aquinas stated that 'something can be said to according to *ius* natural in two ways. One, if nature inclines us to it: such as not to harm another human being. The other, if nature does not prescribe the opposite: so that we can say a man is naked under the *ius* natural, since he received no clothes from nature but invented them himself. In all this way the common possession of all things, and the equal liberty of all is said to be according to the *ius* natural: for distinctions between possessions and slavery were not the product of nature, but were made by human reason for the advantage of human life'. See Aquinas *Suma theologica* 2ae, 94.5.

163 O'Rahilly A "S. Thomas's theory of property" 1920 (9) *Studies: An Irish Quarterly Review* 337-354 339.

164 Ignatieff M and Hont I (eds) *Wealth and virtue: the shaping of political economy in the Scottish enlightenment* (Cambridge University Press Cambridge 1983) 27.

Furthermore, Aquinas inquired whether 'the possession of exterior things is natural to man' or not.[165] He also investigated whether or not 'it is lawful that anyone should possess anything as his own'.[166] In response to this, Aquinas argued that man had a natural *dominion* over private property. This ownership arose from human agreement which is the domain of positive law.[167] More specifically, the private *dominion* simply amounted to a 'super-addition or *adinventio* that is devised by human reason'.[168]

In summary, the moral philosophers, for example Aquinas recognised the existence of a person's right to property. They argued that this right is in respect of material objects. Things, such as slaves, were thus categorised as the material objects over which a person had property rights. However, these philosophers accepted that God retained the absolute ownership over property. Because of this, the principles of natural law dictated the manner in which property rights were to be dealt with.

2.6 THE PANDECTISTS

The Pandectists' theory of law was based on a method of reasoning which was referred to as *Private Law Dogma*. This method was drawn from an idea which Georg Friedrich Puchta (1798-1846) developed called the *Genealogy der Begriffe*, that is, the genealogy of legal concepts.[169] From this, a philosophical or systematic way of interpreting texts or documents was established. Accordingly, the law which was conventionally used was a product of rigorous scientific deductions and was thus more refined.[170] In relation to ownership, Puchta referred to a thing as denoting the 'exclusive authority to use and dispose of a thing'.[171] Following this, he talked of an easement in the sense of 'a property's right to another property'. According to Puchta, rights either

---

165 Aquinas *Summa theologica* 2.2, 66, 1-2.

166 Aquinas *Summa theologica* 2.2, 66, 1-2.

167 Aquinas *Summa theologica* 2.2, 66, 1.

168 Chroust AH and Affeldt RJ "The problem of private property according to St. Thomas Aquinas" 1950-1951 (34) *Marquette Law Review* 151-182 151. See also Hirschfeld M "How a Thomistic model framework can take social causality seriously" in Finn DK (ed) *Distant markets, distant harms: economic complicity and Christian ethics* (Oxford University Press Oxford 2014) 146-172 152.

169 Siltala R *Law, truth, and reason: a treatise on legal argumentation* (Springer Dordrecht 2011) 188.

170 Van der Walt *Die ontwikkeling van houerskap* 332.

171 Gordley J *The Jurists: a critical history* (Oxford University Press Oxford 2013) 225.

belonged to an individual or a family.[172] He then referred to these rights as the private rights. The latter rights were in Puchta's view private in nature and were separated from public rights and ecclesiastical rights.[173] Despite this, private rights were recognised as the most important of the rights.[174] Heinrich Dernburg (1829-1907) referred to this as *die wichtigste ist das Eigentumsrecht*.[175]

Furthermore, the Pandectists seemed to have a more grounded view of the notion of *dominium*. On the one hand, Thibaut developed an approach to ownership which was more aligned to that of the classical Roman law. He rejected the medieval idea of property as generating dual ownership.[176] He stated that the separation between *dominium directus* and *dominium utile* had no place in the law of property.[177] This rejection resulted in the acceptance of only one form of *dominium* over property, namely, direct ownership. Van der Walt finds justification for this viewpoint by saying that property rights insofar as they were understood during this time were seen to be part of the external sphere of the individual.[178]

On the other hand, Bernhard Windscheid (1817-1892) provided a useful guide illuminating the rejection of *duplex dominium*.[179] Firstly, Windscheid spoke of ownership as an exclusive or individualistic right.[180] Secondly, he talked of ownership as an absolute right.[181] He referred to ownership as an abstract right, in the sense that an owner possessed certain powers by virtue of having ownership of property.[182]

Having examined the above-mentioned, it would appear that the Pandectists recognised that the objects of rights are corporeal and incorporeal things.[183] These

---

172 Korkunov NM and Hastings WG *General theory of law* (The Boston Book Company Washington 1909) 244.

173 Korkunov and Hastings *General theory of law* 244.

174 Van der Walt *Die ontwikkeling van houerskap* 338.

175 As quoted in Van der Walt *Die ontwikkeling van houerskap* 338.

176 Whitman JQ *The legacy of Roman law in the German Romantic era: historical vision and legal change* (Princeton University Press New Jersey 1990) 180.

177 As quoted in Whitman *Roman law in the German Romantic era* 180.

178 Van der Walt *Die ontwikkeling van houerskap* 333-334.

179 See Windscheid B *Lehrbuch des Pandektenrechts* 7th ed (Buddesus Düsseldorf 1863) 490-493.

180 Windscheid *Lehrbuch des Pandektenrechts* 490-493.

181 Windscheid *Lehrbuch des Pandektenrechts* 490-493.

182 Windscheid *Lehrbuch des Pandektenrechts* 490-493.

183 Raff M *Private property and environmental responsibility: a comparative study of German real property law* (Kluwer Law International The Hague 2003) 136.

rights do not necessarily translate to ownership. Accordingly, an interest in property was enough to justify the aforesaid rights to exist.[184]

In summary, one of the most essential developments in this period was the acceptance of private rights. Property rights were regarded as the fundamental component of these private rights. In relation to the objects of rights, the Pandectists were of the view that corporeals and incorporeals were, insofar as they satisfy the needs and ambitions of a person, the objects of private rights but not necessarily ownership.[185] This is an important period as it is where the idea of individual personal rights really came to the fore. The political or economic needs of that society therefore determined this development.

2.7 DUTCH DEVELOPMENTS

Some of the prominent jurists of the Dutch law of property were Hugo de Groot (1583-1645)[186] and Johannes Voet. Grotius dealt with private property in *De Jure Belli ac Pacis*.[187] In this seminal work, Grotius spoke of property that God conferred on all humans.[188] In relation to this property, he contended that humans had a general right, as opposed to a private right, to the use and control of this property. This general right related only to the right to use the property.[189] For that reason, a human 'could at once take whatever he wished for his own needs, and could consume whatever was capable of being consumed'.[190] Lastly, Grotius retained the mediaeval Roman law approach to property. He equated property with *gerechtigheid*, that is, a right.[191] Rights, in this sense, meant subjective rights. These rights came into being through a steady process

---

184 Van der Walt *Die ontwikkeling van houerskap* 333-334.
185 Raff *Private property* 136.
186 Hereinafter referred to as Grotius.
187 See Grotius H *De Jure Belli ac Pacis* (Clarendon Press London 1625) II.II.II.1.
188 Grotius *De Jure Belli ac Pacis* II.II.II.1.
189 De Araujo M "Hugo Grotius, contractualism, and the concept of private property – an institutionalist interpretation" 2009 (26) *History of Philosophy Quarterly* 353-371 356.
190 Grotius *De Jure Belli ac Pacis* II.II.II.1.
191 See Wilson E *Savage Republic: De Indis of Hugo Grotius, republicanism, and Dutch hegemony within the early modern world-system* (Martinus Nijhoff Publishers Leiden 2008) 235.

of individuals dealing with each other.[192] The exercise of these rights had to be made in a manner which considered the property rights of 'that which is another's'.[193]

On the other hand, Voet stated that there were certain things over which private ownership was impossible.[194] He then followed the Roman law approach to property by calling these objects the *res nullius* and *res derelictae*.[195] The examples of these things included wild animals, birds, fish, shells, the sea, rain-water and abandoned property.[196] He also stated that some things can be owned. In this respect, they can be the object of rights.[197] He gave as an example corporeal and incorporeal property. In relation to incorporeals, Voet argued that these things did not possess a tangible existence.[198] However, they were still property for purposes of the law.[199] This recognition existed because incorporeals had an inherent value to the person who had an interest in them.[200] This value was attributable to ownership and was not only equated to monetary value.

In summary, the works of Grotius and Voet are fundamental to the study of the Dutch approach to property. In relation to property as an object of rights, Grotius introduced, amongst others, the concept of subjective rights. This right, Grotius argued, arose through human dealings with each other. However, Voet stated that things generally become the object of rights if they are capable of being owned. In other words, the objects must be of some value to a person. Accordingly, he submitted that *res corporeal* and *res incorporeal* were the objects of rights. The aforementioned demonstrates the link between individualism or capitalism and ownership. This was done in order to fit in with the commercial goals of Holland, especially overseas.

2.8 ENGLISH LAW

---

192 De Araujo 2009 *History of Philosophy Quarterly* 356.
193 Grotius *De Jure Belli ac Pacis* I.I. and VIII.2.
194 Voet 45.1.6.
195 Voet 41.1.16.
196 Van der Merwe CG and Pope A "Property" in Du Bois F (ed) *Wille's principles of South African Law* 9th ed (Juta Cape Town 2007) 405-731 416.
197 Voet 1.8.11.
198 Voet 1.8.11.
199 Voet 1.8.11.
200 Voet 1.8.11.

English law illustrates a strong separation between the study of property law and that of the law of persons.[201] Within the context of the English law of property, the term 'ownership' denotes a 'particular relationship which exists between a person and certain rights which are vested in him'.[202] It is classified as the 'greatest right or collection of rights – the ultimate right – which a person can have over a thing'.[203] Accordingly, it can be acquired either by original or derivative means.[204]

Property in England encompasses those objects that are considered to be inanimate.[205] Inanimate has to do with the inorganic objects that are permanent.[206] The requirement of permanency is satisfied in cases where the property can be sensed or observed over a period of time.[207] Therefore, a property attachment or its physical component assists in determining the permanency of the object.[208] Most importantly, the English law of property distinguishes between real and personal property (things real and things personal).[209]

2.8.1 Real Property

Blackstone argues that the equivalent term for real property is corporeal hereditaments.[210] By this Blackstone means such things 'as may be seen and handled by the body'.[211] Real properties are permanent, stationary and immovable objects.[212] It

---

201 Austin J *Lectures on jurisprudence or the philosophy of positive law* (Spottiswoode London 1879) 802.

202 Smith K and Keenan DJ *English law* 2nd ed (Sir Isaac Pitman London 1966) 210.

203 Smith and Keenan *Law* 210.

204 Nasmith *English private* 315.

205 Austin *Philosophy* 803.

206 Austin *Philosophy* 802.

207 Paton GW and Derham DP (eds) *A textbook of jurisprudence* 4th ed (Claredon Press Oxford 1972) 506.

208 Paton and Derham *Jurisprudence* 506.

209 Blackstone W *Commentaries on the laws of England: in four books, with an analysis of the Work by Sir William Blackstone, KNT, one of the Justices of the Court of Common Please* 18th ed (Sweet and Maxwell London 1829) 16.

210 Blackstone W *Commentaries on the laws of England: a facsimile of the first edition of 1765-1769* (The University of Chicago Press London 1972) 17.

211 Blackstone *Commentaries* 17.

212 Pound R and Plucknett T *Readings on the history and systems of the common law* 3rd ed (WM.W. Gaunt Florida 1993) 643.

is necessary that this property be such that it cannot be carried or moved from one place to the other.[213] Examples of things real are the land and a dwelling.[214]

The inclusion of the land as one of the examples of things real is very interesting. This interest is drawn from the fact that the term land in English law denotes the 'works of nature and of humans within a particular space on the earth'.[215] It also consists of 'any definite portion of the planet's surface with the natural resources on or under the surface'.[216] Consequently, all other things, for example, plants, woods, moors, water and seeds are regarded as part of the land.[217]

2.8.2 Things Personal

Personal property refers to movable objects.[218] Examples of these are money excluding its value, goods, and other movables, for example, animals, plants and seeds. Things personal are subdivided into choses in possession and choses in actions.[219] The term chose is a French word which literally means a thing.[220] This word was borrowed by Blackstone in order to discuss the various types of property which he deemed personal.

Choses in possession denote tangible or corporeal things.[221] Jewellery and furniture are examples of choses in possession.[222] Accordingly, a possession in respect of these things is physical.[223] However, chooses in action are classes of intangible or incorporeal objects that are incapable of physical possession.[224] Examples of choses in action are debts, patents, copyrights, trademarks, shares and negotiable instruments.[225] Therefore, it is required of a property owner to bring an action (*actio in*

---

213 Pound and Plucknett *Readings* 643, Smith and Keenan *Law* 17.
214 Pound and Plucknett *Readings* 643, Smith and Keenan *Law* 17.
215 Lawson FH and Rudden B *The law of property* 3rd ed (Oxford University Press Oxford 2002) 22.
216 Lawson and Rudden *Property* 22.
217 Lawson and Rudden *Property* 22. See also, Blackstone *Commentaries* 17.
218 Blackstone *Laws of England* 16.
219 Keenan D *Smith and Keenan's English law* 8th ed (Pitman Publishing Ltd London 1986) 412 and Smith and Keenan *Law* 186.
220 Garner BA *Garner's dictionary of legal usage* 3rd ed (Oxford University Press Oxford 2011) 155.
221 Keenan Smith *and Keenan's English law* 412.
222 Keenan Smith *and Keenan's English law* 412.
223 Keenan Smith *and Keenan's English law* 412.
224 Lawson and Rudden *Law of property* 29.
225 Keenan *Smith and Keenan's English law* 412.

personam) if the latter wishes to enforce his or her right over choses in action.[226] The incorporeal hereditaments of Blackstone are equivalent to the form of property referred to as the choses in action.[227] He argues that incorporeal hereditaments include the rights that accrue out of things real.[228] They are annexed to and exercisable within corporeal hereditaments.[229] Their examples include contributions, commons, offices, dignities, franchises, pensions, annuities and rents.[230]

The term possession in English law is sometimes used interchangeably with the word ownership.[231] The word possession is derived from the concepts of *corpus* (actual physical detention) and *animus* (mental state to possess).[232] It means a physical control of property with the intention to exclude all others in society.[233] Furthermore, it presupposes the existence of *dominium* over a particular property.[234] This *dominium* amounts to the assumption of control of or over property.

In summary, English law deviates markedly from the property law viewpoints that are found in Roman-Dutch law. Instead of dealing with corporeal and incorporeal things, it states that the objects of property rights vest in corporeal hereditaments and incorporeal hereditaments. Corporeal hereditaments are real property. The equivalent term which is used for corporeal hereditaments is choses in possession. These objects are permanent, stationary and physical. The examples include land, house, jewellery and furniture. Incorporeal hereditaments refer to the intangible things. These things have no physical presence and are not capable of physical possession. The examples of these objects include debts, patents, copyrights, shares, contributions, pensions, annuities and rents. Consequently, the law of property in England differs from the Roman-Dutch law and is geared towards meeting the requirements or needs of the English society.

---

226 Keenan *Smith and Keenan's English law* 412.
227 Blackstone *Commentaries* 20.
228 Blackstone *Commentaries* 20.
229 Pound and Plucknett *Readings* 645.
230 Blackstone *Commentaries* 21.
231 *McAdams v Fiander's Trustee & Bell* NO 1919 AD 207 232.
232 Keenan *Smith and Keenan's English law* 412.
233 Smith and Keenan *Law* 211.
234 Nasmith *English private law* 310.

2.9 SOUTH AFRICAN LAW

2.9.1 Background

The law of property in South Africa regulates the relationship between legal subjects (humans) and legal objects.[235] In this relationship, four kinds of rights are distinguished. The rights in property are referred to as the real rights. The other rights are personality rights, immaterial property rights and personal rights or claims. Debates relating to the need to classify rights have a long history in the South African law of property.[236] However, the prevailing view is that the above-mentioned distinction is essential because rights are generally 'exercised, protected and acquired differently' in law.[237]

Real rights are absolute.[238] This implies that a holder of a real right possesses wide powers in relation to or over a thing. Thus, he or she has what is referred to as *ius in rem suam* and can within the confines of the law do with the thing as he or she pleases.[239] In addition, real rights establish a legal relationship between a person and a thing, may be enforced against anyone else in the society,[240] and are 'maintainable against the whole world'.[241] Consequently, where the object of right is a thing (*res*) it is presumed that real rights accrue to the property.[242] Ownership, servitude, mortgage and pledge are examples of real rights. Personality rights refer to the rights which a person has to his or her physical or psychological wellbeing. In most cases these rights

---

235 Legal objects refer to those things that a person 'requires for the satisfaction of his (or her) juridical needs'. See Van der Vyver JD "The doctrine of private law rights" in Strauss SA (ed) *Huldigingsbundel vir W.A. Joubert: aan hom aangebied by geleentheid van sy sewentigste verjaardag op 27 Oktober 1988* (Butterworths Durban 1988) 201-246 231.

236 *Ex parte Geldenhuys* 1926 OPD 155, *Lorentz v Melle* 1978 3 SA 1044 (T)*, Pearly Beach Trust v Registrar of Deeds* 1990 4 SA 614 (C), *Cape Explosive Works Ltd and Another v Denel (Pty) and others* 2001 3 SA 569 (SCA) and *Investgold CC v Uys & Another* (686/2013) [2014] ZASCA 166 (1 October 2014) fully illustrate this debates.

237 Van der Walt AJ "The enforceability of tenant's rights" 2012 (1) *TSAR* 35-52 38.

238 Van der Merwe CG and de Waal MJ *The law of things and servitudes* (Butterworths Durban 1993) 7.

239 Van der Walt AJ and Kleyn DG "Duplex dominium – the theory and significance of the concept of divided ownership" in Visser DP (ed) *Essays on the history of law* (Juta Cape Town 1989) 213 at 213 and Hosten WJ and Schoeman J "Private law – law of things" in Hosten et al (eds) *Introduction to South African law and legal theory* (Butterworths Durban 1997) 622-659 624.

240 Badenhorst PJ, Pienaar JM and Mostert H *Silberberg and Schoeman's the law of property* 5th ed (LexisNexis Durban 2006) 43.

241 *Cape Explosive Works Ltd and Another v Denel (Pty) and Others* 20.

242 Hahlo HR and Kahn E *The Union of South Africa: the development of its laws and constitution* (Juta London 1960) 571.

are claimed in delict where damage or harm was caused to a person. Immaterial property rights relate to the rights in respect of certain intangibles.[243] These include those which are a creation of a person's mind, for example an invention or symbol.[244] The object of right in the case of personal rights is a claim for specific performance.[245] These rights are referred to as patrimonial rights.[246]

In South Africa, the notion of rights or property rights is essential to the overall study of the law of property. A right in property means a legally justified entitlement or interest.[247] It gives a person (legal person) a valid claim to or over property (a legal object) as against other persons.[248] Most importantly, it refers to the 'classical triad of liberal entitlements' that usually has connection with property.[249] These are possession, use and disposal of property.[250] Rights are generally subjective or objective in nature. Subjective rights relates to the relationship between the bearer of rights (legal subject) and other legal subjects.[251] Objective rights have to do with the relationship between a legal subject and the object of the right, that is, the legal object.[252] Accordingly, although all material objects qualify as property in an informal sense,[253] not all objects can be regarded as the objects of private property rights. The examples of the latter objects are the sun or a grain of sand.[254] Consequently, in order for an object to be

---

243 Badenhorst, Pienaar and Mostert *Law of property* 5th ed 23.

244 Van der Walt AJ and Pienaar GJ *Introduction to the law of property* 6th ed (Juta & Co Claremont 2009) 307-312.

245 Hosten WJ et al *Introduction to South African law and legal theory* 2nd ed (Butterworths Publishers Durban 1997) 625.

246 *Isaacman v Miller* 1922 TPD 56 61. See also *Odendaalsrus Gold, General Investments and Extensions Ltd v Registrar of Deeds* 1953 1 SA 600 (O), *Lozentz v Melle* 1978 3 SA 1044 (T) and *Erlax Properties (Pty) Ltd v Registrar of Deeds* 1992 1 SA 879 (A).

247 Van der Walt and Pienaar *Law of property* 6th ed 8 and Van der Walt and Pienaar *Property* 2nd ed 13.

248 Badenhorst, Pienaar and Mostert *Law of property* 5th ed 9.

249 Van der Walt AJ "Towards a theory of rights in property - exploratory observations on the paradigm of post-apartheid property law" 1995 (10) *SA Public Law* 298-345 306.

250 Van der Walt 1995 *SA Public Law* 306.

251 Kruger H and Skelton A (eds) *The law of persons* (Oxford University Press Southern Africa Cape Town 2010) 2.

252 Kruger and Skelton (eds) *The law of persons* 12 and Mostert H *The constitutional protection and regulation of property and its influence on the reform of private law and landownership in South Africa and Germany: a comparative analysis* (Springer Berlin 2002) 11-12.

253 Van der Walt and Pienaar *Law of property* 6th ed 8-9.

254 Hosten and Schoeman *Private law* 623.

regarded as property for juridical purposes they must result in the establishment of a legal relationship between persons.[255] The objects must be such that a person will be able to 'acquire and hold a (subjective) right'.[256]

The association of property with a right is sometimes also described as a *truncated right*.[257] It is not property *per se*. It is rather a guarantee that the entitlement to property will not be tampered with otherwise than in accordance with the law.[258] Different tests or requirements are commonly applied in order to determine whether or not an object is indeed a thing for purposes of the law. These tests are that the object must be capable of human control, it must be of some value or valuable to a person, and it must be the object of rights and duties.[259] The attribution of value to the concept of property needs additional clarification. More specifically, a reference to value does not only or necessarily imply an economic or market value. Objects that are of value to a person, for example, a family photograph, are also regarded as object of property rights in South Africa. Therefore, it does not matter whether the value is sentimental or not.

It is necessary at this stage to describe some of the concepts which have relations to the law of property in South Africa. These are things, ownership and possession. A single approach regarding the true meaning of the concept of property cannot be found in South African law. Maasdorp provides that this concept amounts to anything which can be the object of a right.[260] In other words, property establishes a relationship whereby one person is entitled to a right and another person is subject to a duty.[261] Maasdorp's view is followed by Schoeman.[262] Schoeman argues that property implies a legal relationship between a person and an object.[263] From this relationship it may be inferred that such a person is the owner or lawful possessor of property.[264] This determines whether a person has exclusive control of or over an object which he or she

---

255 Oosthuizen AJ *The law of property* (Juta Cape Town 1981) 3.

256 Van der Walt AJ and Pienaar GJ *Introduction to the law of property* 2nd ed (Juta Kenwyn 1997) 11.

257 Roux T "Property" in Cheadle MH, Davis DM and Hayson NRL (eds) *South African constitutional law: the Bill of Rights* (Butterworths Durban 2002) 429-472 440.

258 Van der Walt AJ *Constitutional property law* (Juta Cape Town 2005) 63.

259 Van der Merwe and de Waal *Things and servitudes* 12.

260 Maasdorp AFS *The Institutes of Cape Town: being a compendium of the common law, decided cases and statute law of the colony of the Cape of Good Hope* (Juta Cape Town 1923) 1.

261 Maasdorp *Institutes of Cape Town* 1.

262 See generally Badenhorst, Pienaar and Mostert *The law of property*.

263 Badenhorst, Pienaar and Mostert *The law of property* 1.

264 Badenhorst, Pienaar and Mostert *The law of property* 1.

can enforce against anyone in society.[265] However, other authors (for example Hahlo and Kahn) oppose the aforementioned description.[266] They contend that property amounts to everything which has a monetary value.[267] The description of property can be summarised by providing that the notion amounts to 'everything which can form part of a person's estate'.[268]

For a study of the word ownership, it is necessary to examine the term by looking at what it means in general terms and for legal purposes. This investigation also helps in the discussion regarding the position of information below. In laymen's terms the word ownership applies to everything that belongs to a person or a person's estate. Therefore, it does not matter whether the object is corporeal or incorporeal. However, in a legal sense ownership is the 'sum-total of all the real rights which a person can possibly have to and over a….thing, subject to the legal maxim: *Sic utere tuo ut alienum non laedas* (So use your own that you do not do injury to that which is another)'.[269] It includes the 'power (or right) to use, alter, destroy or alienate the thing concerned and to enjoy the fruits thereof, to prevent others from using it and to transfer rights to the thing'.[270] Possession or to possess has to do with the physical (that is, to physically hold) and mental (that is, the desire to actually hold) situations of a person towards property.[271] It is simply a restricted right to property to use and possess property. This right does not amount to ownership.

2.9.2 Property as a Right

Insofar as the meaning of the term property vary in South Africa, it is inevitable that the definitions of the laws that regulate this institution will also diverge. For example, one viewpoint regards the law of property as a body of legal rules and principles that

---

265 Kleyn, Boraine and Du Plessis *Silberberg and Schoeman's* 162.

266 See generally Hahlo and Kahn *Laws and constitution*.

267 Hahlo and Kahn *Laws and constitution* 571.

268 Mostert *The constitutional protection and regulation of property* 253.

269 Maasdorp AFS *The Institutes of South African law being a compendium of the common Law, decided cases, and statutes law of the Union of South Africa* 5th ed (Juta Cape Town 1938) 17.

270 Schoeman *The law of property*.

271 Maasdorp AFS *Institutes of South African law* 10th ed (Juta Cape Town 1976) 12-13. See also Maasdorp *Institutes of South African law* 16.

regulate the use and control of commercial resources.[272] In view of that, the law of property aims to safeguard the foundation for the 'acquisition, enjoyment and disposal of wealth'.[273] Another perspective maintains that the law of property is that fragment of private law which governs 'the nature, content, acquisition, protection, transfer or loss and other implications of the different real relationships that may exist between a legal subject and a thing and the rights, entitlements, obligations and remedies that may accompany it'.[274]

As regards things that can be owned, South Africa follows more of the classical Roman law approach to property. In particular, property is classified according to its relation to people and according to its nature.[275] In relation to its relationship with people, a difference is made between *res in commercium* and *res extra commercium*.[276] *Res in commercium* refer to the objects that can be owned or can be the object of rights.[277] Conversely, *res extra commercium* are the objects that cannot be owned or can never be the object of a right.[278] Examples of *res extra commercium* are *res communes* (property common to all people) and *res publicae* (property held by the state). With regard to its nature, a difference is made between corporeal and incorporeal, movable and immovable, divisible and indivisible, consumable and inconsumable, fungible and non-fungible, and single and complex properties.[279] For purposes of this research a revision of corporeal and incorporeal property is made.

(a) Corporeal property

Corporeal property refers to physical objects. These are objects that are part of a tangible reality.[280] A tangible reality can be interpreted to mean an object which is perceptible through sight and touch.[281] The object must occupy some space. It must

---

272 Oosthuizen *Law of property* 1.
273 Oosthuizen *Law of property* 1.
274 Kleyn, Boraine and Du Plessis *Silberberg and Schoeman's* 16-31.
275 Oosthuizen *The Law of Property* 8.
276 Badenhorst, Pienaar and Mostert *The law of property* 21-29.
277 Oosthuizen *The Law of Property* 8 and Badenhorst, Pienaar and Mostert *The law of property* 21.
278 Oosthuizen *The law of property* 8 and Badenhorst, Pienaar and Mostert *The law of property* 21.
279 Badenhorst, Pienaar and Mostert *The law of property* 29-42.
280 Van der Walt and Pienaar *Law of property* 3rd ed 14.
281 Maasdorp *The Institutes* 1.

also be capable of being sensed by means of any of the five traditional senses.[282] These may be movables, for example horses, furniture, motor bikes, a cylinder with oxygen or ships, or immovables, for example landed property, fruits that still hang on the tree, etc.[283]

There are some who criticises the present-day description of corporeal property.[284] They argue that a reliance on the tangibility of an object as one of the criteria for determining its corporeality can generate challenges.[285] In particular, such reliance can lead to objects, for example, various gases, that naturally are excluded in the description of corporeal property being recognised as such.[286] For example, gasses can, despite the fact that they cannot be touched, be perceived by some of the external factors.[287] The other criticism is levelled against the exclusion of natural forces and energies, for example gravity, heat, sound and electricity, as property. It is averred that such exclusion relies on an ancient description of property.[288] Heat, sound and electricity are so analogous to traditional corporeal property that they should be regarded as having corporeal existence.[289] This can be illustrated by examining the example of electricity. Electricity can be touched, although this may result to injury or death. As a result, it may be said that electricity meets the requirement of tangibility. This position seems to have been followed in *BonQuelle (Edms) Bpk v Munisipalitet van Otavi*,[290] *Froman v Herbmore Timber and Hardware (Pty) Ltd* [291] and *Naidoo v Moodley*.[292]

Tindall AJP argued in the case of *Liebenberg v Koster Village Council* that it does not seem possible to adapt the language which is used in describing corporeal things in a

---

282 Van der Walt and Pienaar *Law of property* 3rd ed 14.
283 Van der Walt and Pienaar *Law of property* 3rd ed 14.
284 Badenhorst, Pienaar and Mostert *The law of property* 30.
285 Badenhorst, Pienaar and Mostert *The law of property* 30.
286 Kleyn, Boraine and Du Plessis *Silberberg and Schoeman's* 30.
287 Badenhorst, Pienaar and Mostert *The law of property* 30.
288 Van der Merwe CG *The Law of Things* (Butterworths Durban 1987) 13.
289 Van der Merwe CG *Sakereg* 2nd ed (Butterworths Durban 1987) 25. See also, *Froman v Herbmore Timber and Hardware (Pty) Ltd* 1984 3 SA 609 (W).
290 *Froman v Herbmore Timber and Hardware (Pty) Ltd* 1984 3 SA 609 (W) para 515C-E.
291 *Froman v Herbmore Timber and Hardware (Pty) Ltd* 1984 3 SA 609 (W) para 610I.
292 *Naidoo v Moodley* 1982 4 SA 82 (TPD).

way that also incorporates objects such as natural gases, electricity or sound.[293] This view seems to be supported by some English authors, for example Glanville.[294] Glanville states in relation to electricity that it is not 'scientifically regarded as a physical thing…..but is (only) a form of energy.[295]

(b) Incorporeal property

Traditionally, scepticism existed as to whether or not ownership should also exist in respect of incorporeal things. *Ex parte Eloff*[296] is an example of a case where this doubt was illustrated. This was the case because it was deemed to be legally illogical to define property as the object of a right and then submit that a right is also the object of a right. However, it was soon realised that ownership should generally not be limited to tangible and physical objects. The cases of *Cooper v Boyes No and Another*[297] and *S v Kotze*[298] can be mentioned as examples where this was made. In the first-mentioned case the court concluded that although incorporeal property (a share) cannot be compared to corporeal property, however, they sometimes generate interest or value to an owner.[299] This interest thus gives an owner a reasonable expectation that this interest or value will be recognised as property by the law.[300] Furthermore, in *S v Kotze* the court conceded that a bank retains ownership of the funds or credits which are kept in an account holder's bank account.[301]

Incorporeal things are the artificial or fictitious objects.[302] Traditionally, these were objects that were neither visible nor tangible.[303] They were considered to be incapable of being owned.[304] Accordingly, it was argued that a possession of these things in the sense of a factual or physical control or *corpus* or an intention to possess or *animus*

---

293 *Liebenberg v Koster Village Council* 1935 TPD 413 417-418.
294 See, Glanville W *Textbook of criminal law* 2nd ed (Stevens & Sons London 1983).
295 Glanville *Criminal law* 736.
296 See *Ex parte Eloff* 1953 1 SA 617 (T).
297 See *Cooper v Boyes No and Another* 1994 4 SA 521 (CPD).
298 See S v Kotze 1961 1 SA 118 (SCA).
299 *Cooper v Boyes No and Another* 1994 4 SA 521 (CPD) para 535B-C.
300 *Cooper v Boyes No and Another* 1994 4 SA 521 (CPD) para 535F.
301 *S v Kotze* 1961 1 SA 118 (SCA).
302 Maasdorp *Institutes of South Africa* 1.
303 Maasdorp *Institutes of South Africa* 1. See, the discussion of natural energies, gravity and heat above.
304 Nathan M *The common law of South Africa: a treatise based on Voet's commentaries on the pandects, with reference to the leading Roman-Dutch authorities, South African decisions, and statutory enactments in South Africa* (Africa Book Company London 1904) 310-311.

possidendi was impossible.[305] The most obvious examples of incorporeal property were a right and duty.[306] Incorporeal property in the form of rights and duties operates exactly like objects of limited real rights.[307]

In addition, South Africa has enacted statutes and the courts have been pivotal in supporting the ideal of developing the realm of incorporeal property. The aforementioned improvements have resulted in the vesting of ownership over things where the object of rights is not a corporeal thing but another subjective right. These are real rights, personality rights, intellectual property rights and personal rights. The aforementioned is associated with the phenomenon of *dephysicalisation of property*.[308] More specifically, it is compelled by the fact that 'complex social, economic and legal processes by which incorporeal or intangible property are becoming increasingly important for personal wealth and security and for social welfare, while the importance of traditional tangible property such as land declines'.[309]

Having studied everything as evidenced above, it is important to note that the distinction between corporeal and incorporeal property is central to the study to determine the position of information in the law of property. It particularly helps in establishing whether or not the principles of property law are so flexible that information can be the object of rights. In other words, an inquiry is undertaken regarding whether ownership could be vested in information or not.

The distinction between corporeals and incorporeals has to be examined against the background of section 25 of the Constitution (the property clause).[310] The property clause has far-reaching provisions in relation to the protection of property. It deals with

---

305 Van der Merwe CG "Law of property" in Van der Merwe CG, Du Plessis JE and Zimmermann R (eds) *Introduction to the law of South Africa* (Kluwer Law International The Hague 2004) 201-242 203-204.

306 *Chauvier v Pelican Pools (Pty) Ltd* 1992 (2) SA 39 (T) 41G.

307 See the criticism regarding the corporeality of such things in Oosthuizen *Law of property* 4.

308 Vandevelde KJ "The new property of the nineteenth century – the development of the modern concept of property" 1980 (29) *Buffalo Law Review* 325-367 333.

309 Van der Walt *Constitutional property law* 66.

310 The Constitution of the Republic of South Africa, 1996 (hereinafter referred to as the Constitution).

the protection of property against arbitrary deprivation and expropriation of property.[311] Furthermore, it covers such wide-ranging factors as the right to property and property as a constitutional right.[312] The concept of property within the framework of section 25 refers to both private and public property.[313] The effect of this discussion in the overall approach to property – more specifically, with regard to corporeals and incorporeals – is that it requires a balancing act to be commenced which examines the interests of an individual owner and those of the general public.[314] Public interests includes: 'the nation's commitment to land reform, and to reforms to bring about equitable access to all South Africa's natural resources'.[315] Consequently, the private-law views on property as the solitary object under the *dominium* of an individual owner should be reconciled with what the public views as property.[316]

In summary, different rights are recognised in South Africa. These are referred to as the real, personal, personality and immaterial property rights. The rights in property are referred to as the real rights. These rights establish a legal relationship between a person and a thing. A distinction is made between corporeals and incorporeals. Corporeals are tangible objects that occupy some space and are capable of being sensed. The examples include a house, furniture, motorbike, cylinder with oxygen and fruits that hangs in a tree. Incorporeals are the intangible things. Generally, a factual or physical control over incorporeals is impossible. Furthermore, South Africa has adopted an approach for the dephysicalisation of property. In this respect, rights in property have become vested in things that were traditionally not recognised as property for legal purposes.

The above-mentioned developments reflect the needs of the South African society. They found their basis from classical Roman law and the expansions and changes which occurred in the Dutch law of property. The most significant of these are those relating to property as an object of real rights. According to this, a thing becomes a property if it can be shown that a person has a legal interest in the thing. The aforesaid

---

311 S 25(1)-(3) of the property clause.

312 Van der Walt *The constitutional property clause: a comparative analysis of section 25 of the South African Constitution of 1996* (Juta Kenwyn 1997) 64-66.

313 Van der Walt *The constitutional property clause* 53.

314 Van der Walt *The constitutional property clause* 53.

315 S 25 (4)(a) of the property clause.

316 Van der Walt *The constitutional property clause* 53.

interest does not necessarily have to translate to the actual dominium over the thing itself.

2.10 SUMMARY

Property is generally a vibrant idea. It evolves with the times and is adaptable to societal developments and challenges. For example, old Roman law only knew of property as denoting that which served a person's interest.[317] This property was corporeal in nature and amounted to that which was referred to as *quae tangi possunt*. During this time, there was no specific mention of the term *dominium*. *Dominium* was simply inferred from the interest which a person had to property. Furthermore, old Roman law spoke of actions, that is, *actio in rem* and *actio in personam*, as opposed to rights in property. The idea of property as a right is only conceivable when a study is made of the classical Roman law of property. In classical times, the person who had an interest (economic or pecuniary), that is, *dominium*, in property was referred to as a *dominus, proprietaries* or *domonus proprietatis*. It was then argued that this *dominium* bestowed to the *dominus* a legal right to a thing in relation to its control, use and enjoyment. In addition, *dominium* did not vest only in corporeal things, for example buildings, land, animals, slaves, gold or silver. It was also possible that a *dominus* could have an interest or a right over those things which were not necessarily *quae tangi possunt*. These were referred to as incorporeal things, for example rights, servitudes, inheritance and *hereditas*.[318]

These classical developments were essential in shaping the approaches to the law of property that succeeded it. In particular, the period between 350 AD until 550 AD (Vulgar law in the West of Rome) was an era where the meaning attached to the notion of *dominium* lost its classical radiance and lucidity.[319] More specifically, *dominium* was replaced with concepts such as *possidere* and *possessio*. The effect of this was to render the *dominus* a mere possessor with the rights similar to those of a *usufructus*.[320] However, *duplex dominium* does not appear in the English and South African property

---

317 Van Warmello *Roman civil law* 63.
318 Sohm *The Institutes* 225.
319 Levy *West Roman vulgar law* 61.
320 Levy *West Roman vulgar law* 61.

law approaches. More specifically, South Africa follows more or less the Pandectists' idea of property and rights in property. The latter view is to the effect that an object is property for legal purposes if certain rights can be abstracted from the object itself. Real, personality, immaterial and personal rights are distinguished. These rights may be subjective (between a legal subject and another legal subject) or objective (between a legal subject and legal object).

Having ascertained that the understanding and meaning of rights in property depend on the structure of a particular society, the section below discusses the position of information in the law of property. This argument is made having in mind the fact that information is nowadays kept and stored online. Therefore, a challenge may exist in accepting and recognising this information as property for purposes of the law. More specifically, it may be cumbersome to establish property rights to information kept and stored in computer systems. However, the fact that the principles of property law vary according to the needs of a particular society may assist in shaping the discussion on the position of information in the law of property. One may be tempted to deduce that a computer which stores information is analogous to a container which stores the gas. By reason of the aforesaid, if property rights do not only vest in the container but also to the gas, then it should also be possible for a person to have real rights over information kept in a computer. These rights do not essentially translate to the ownership of information. Simply, they signify that a person has an interest in information stored or kept online.

2.11 POSITION OF INFORMATION

2.11.1 Background

The law of property is clear in relation to the objects of real rights. Property rights, but not ownership, vest in corporeal and incorporeal objects. The position in relation to information does not appear to be properly examined. Although *Cooper v Boyes No and Another* recognises that the law of property should be developed so as to regard shares as property for legal purposes, it does not indicate, expressly or implicitly, that the information contained in those shares is also property in South Africa.[321] By way of illustration, a document can be owned in terms of the principles of the law of property.

---

[321] See *Cooper v Boyes No and Another* 1994 4 SA 521 (CPD) para 535B-C.

However, the information which is contained in such document is not property for legal purposes. In other words, a person may, in law, have a real right over information stored or kept in his computer. But, this right does not mean that such a person owns the information. Consequently, the view that every object of property rights must have corporeal subsistence seems to prevail.[322] The fact that South Africa refers to principal, accessory or auxiliary property is immaterial in the aforementioned regard. The question is or should be whether or not information can be the object of ownership. In order to examine this question, the developments of the principles of property law in South Africa, insofar as they relate to corporeal and incorporeal property, are paramount.

In the recent past, attempts have been made to study the legal significance of property in online environments, that is, virtual property. This examination has occurred both in South Africa and abroad. Erlank[323] and Jankowich[324] generally lead the scrutiny regarding whether information could be the object of ownership. On the one hand, Erlank examines virtual property as represented by animated characters (avatars)[325] and virtual worlds. He relies for his study on Lastowka and Hunter.[326] Lastowka and Hunter argue that virtual worlds replicate real, physical worlds.[327] More specifically, the social interactions that occur in these worlds marks a new development which legal subjects (namely, computer users) consider as being important.[328] Given the aforementioned, Erlank states that virtual property is scarce and some form of economic connotation can be attached to it. Because of its scarcity and commercial success rate, there is 'justification' for virtual property to be recognised as property that

---

322 *Consolidated News Agency (Pty) Ltd (In Liquidation) v Mobile Telephone Networks (Pty) Ltd* 2010 3 SA 382 (SCA) 29-32; *Cornelissen NO v Universal Caravan Sales (Pty) Ltd* 1971 3 SA 158 (A) 179D-E.

323 Erlank *Property in virtual worlds* 141-80.

324 Jankowich 2005 *Boston University Journal of Science and Technology Law* http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume112/JankowichArticleWEB.pdf%3Fq%3Dproperty-and-democracy-in-virtual-worlds.

325 Lastowka G *Virtual justice: the new laws of online worlds* (Yale University Press New Haven 2010) 9 and Moringiello JM "What virtual worlds can do for property law" 2010 *Widener University School of Law* 1-50 1.

326 See, Lastowka FG and Hunter D "The laws of the virtual worlds" 2004 (92) *California Law Review* 1-75.

327 Lastowka 2004 *California Law Review* 56-66.

328 Griemmelmann JTL "Virtual worlds as comparative law" 2004 (49) *New York Law School Law Review* 147-184.

is capable of being owned.[329] On the other hand, Jankowich submits that there is indeed something called 'property in virtual worlds'.[330] However, this property does not appear to meet the traditional legal description of property. In other words, it does not fit the requirement of corporeality which is required by the law of property. Jankowich uses the science-fiction movie 'The Matrix' in order to demonstrate the aforesaid view.[331] In that movie, computer-generated simulations or characters are used, in a fictitious manner, as a form of communication in a computer-generated setting.[332] It is demonstrated in that movie that this method of communication is of interest to the users of this computer-generated world. This is the case because this method is deemed to be effective. Similarly, virtual property, Jankowich argues, is of interest to the users in virtual worlds.[333] Therefore, it is worthy of protection and recognition by the law.[334] However, Jankowich concedes that, perhaps, it may be challenging to find a description of virtual property which suitably conforms to the one that is found in the law. [335]

In this section the approaches by Erlank and Jankowich are followed. However, the discussion diverges, albeit slightly, from those of the aforementioned authors in that it deals with the position of information (as opposed to games or avatars) in the law of property. The cases discussed here highlight the fact that ancient measures are usually not well suited to address modern, or even post-modern, occurrences. With regard to the law of property, it may be necessary to modify the traditional maxims or practices

---

329 Erlank *Property in virtual worlds* 141-80. See also, Erlank W "Acquisition of ownership inside virtual worlds" 2013 *De Jure* 770-782 776-782.

330 Jankowich 2005 *Boston University Journal of Science and Technology Law* http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume112/JankowichArticleWEB.pdf%3Fq%3Dproperty-and-democracy-in-virtual-worlds.

331 Jankowich 2005 *Boston University Journal of Science and Technology Law* http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume112/JankowichArticleWEB.pdf%3Fq%3Dproperty-and-democracy-in-virtual-worlds. See also Lederman L "Stranger than fiction – Taxing virtual worlds" 2007 (82) *New York University Law Review* 1620-1672 1621-1627.

332 Jankowich 2005 *Boston University Journal of Science and Technology Law* http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume112/JankowichArticleWEB.pdf%3Fq%3Dproperty-and-democracy-in-virtual-worlds.

333 Jankowich 2005 *Boston University Journal of Science and Technology Law* http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume112/JankowichArticleWEB.pdf%3Fq%3Dproperty-and-democracy-in-virtual-worlds.

334 Jankowich 2005 *Boston University Journal of Science and Technology Law* http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume112/JankowichArticleWEB.pdf%3Fq%3Dproperty-and-democracy-in-virtual-worlds.

335 Jankowich 2005 *Boston University Journal of Science and Technology Law* http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume112/JankowichArticleWEB.pdf%3Fq%3Dproperty-and-democracy-in-virtual-worlds.

relating to its principles.[336] This could be the case because property is generally not an immutable concept and does not always remain the same.[337] As Macpherson puts it:

> When the theory of property is examined, (whether) historically and logically, it turns out to be more flexible than the classical liberals or their twentieth-century followers have allowed for. The concept of property has changed more than once, and in more than one way, in the past few centuries. It changed in discernible ways with the rise of modern capitalism, and it is again now with the maturation of capitalism.[338]

As a result of this, it may be necessary to establish a framework which recognises that the concept property evolves and can be adapted to accommodate developments that take place external to it.[339]

2.11.2 Information

Information or data is an essential asset of an information society. Westbrook,[340] Horowitz,[341] Vacca,[342] and Koster[343] illustrate this significance.[344] On the one hand, Horowitz and Vacca agree that information has characteristic traits that mirror or mimic real property.[345] Accordingly, holders of information are or should be entitled to

---

336 Gray K "Property in thin air" 1991 (50) *Cambridge Law Journal* 252-307 253-254.

337 Lafargue P *The evolution of property from savagery to civilisation* (New Parks London 1975) 3.

338 Macpherson CB *Democratic theory* (Claredon Press Oxford 1973) 122.

339 Lafargue *The evolution of property* 3.

340 See Westbrook TJ "Owned – finding a place for virtual world property rights" 2006 (779) *Michigan State Law Review* 779-812.

341 See Horowitz SJ "Competing Lockean claims to virtual property" 2007 (20) *Harvard Journal of Law and Technology* 443-458.

342 Vacca RG "Viewing virtual property ownership through the lens of innovation" in *Virtual property* (Papers delivered at the 2008 Cornell Law Student Inter-University Graduate Student Conference Paper 3 June 2008 Cornell University) 1-28.

343 Koster R "Declaring the rights of players" in Balkin JM and Noveck BS (eds) *The State of Play: Law, Games, and Virtual Worlds* (2006) 55-67 55.

344 Virtual property is described as an entitlement to a right in a virtual product or good. See Westbrook 2006 *Michigan State Law Review* 782, Horowitz 2007 *Harvard Journal of Law and Technology* 444 and Vacca "Virtual property" 5-6.

345 Westbrook 2006 *Michigan State Law Review* 782 and Horowitz 2007 *Harvard Journal of Law and Technology* 444-448.

protection.[346] If this protection is granted it should then lead to information being granted legal recognition as the object over which ownership exists.[347] On the other hand, Koster relies on two theories of (property) rights in order to establish whether or not property rights in information are possible.[348] The one theory argues that rights are granted to people by virtue of them being part of a particular populace.[349] The other theory submits that rights are inherent to people. [350] Thus, they are not bestowed to people following them becoming a member of a particular community. Having examined all this, Koster then states the following:

> That avatars are the manifestation of actual people in an online medium, and that their utterances, actions, thoughts, and emotions should be considered to be as valid as the utterances, actions, thoughts, and emotions of people in any other forum, venue, location, or space…. That by the act of affirming membership in the community within the virtual space, the avatars form a social contract with the community, forming a populace which may and must self-affirm and self-impose rights and concomitant restrictions upon their behaviour.[351]

The emergence of an information society has resulted in information becoming a public good.[352] Institutions, governments, businesses and individuals expend time, effort and money in gathering information.[353] Following these efforts, they then (reasonably) expect that they have real rights in or over this information.[354] Furthermore, information or other data has become essential in discouraging other crimes, for example, money

---

346 Westbrook 2006 *Michigan State Law Review* 782 and Horowitz 2007 *Harvard Journal of Law and Technology* 444-448.

347 Westbrook 2006 *Michigan State Law Review* 782 and Horowitz 2007 *Harvard Journal of Law and Technology* 444-448.

348 Koster "Declaring the rights of players" 55 55-56.

349 Koster "Declaring the rights of players" 55.

350 Koster "Declaring the rights of players" 55-56.

351 Koster "Declaring the rights of players" 56.

352 Elkin-Koren N and Salzberger EM *Law, economics and cyberspace: the effects of cyberspace on the economic analysis of law* (Edward Elgar Cheltenham 2004) 49-50.

353 *Regina v Stewart* (1983) 149 D.L.R. (3d) 583 595 (hereinafter referred to as Stewart case) and Weinrib 1988 *The University of Toronto Law Journal* 117.

354 *Regina v Stewart* 598. See also *Thomas Marshall (Exports) Ltd. v Guinle* [1978] 3 All E.R. 193 209-210 and Samuelson P "Is information property?" 1991 (34) *Communications of the ACM* 15-18 15.

laundering and terrorism or terrorist financing.[355] This is normally done by encouraging or compelling certain information to be furnished or disclosed.[356] This revelation generally enables and assists institution (Accountable Institutions)[357] in order to establish whether or not a person or funds are or can be linked to a crime.[358]

It is acknowledged that developments have occurred in South Africa wherein the ambit of the law of property had been expanded to also give legal recognition and protection to certain intangibles, such as electricity.[359] For example, in *Froman v Herbmore Timber and Hardware (Pty) Ltd* the issue to be decided by the court was whether electricity is *res incorporales* or not. The court acknowledged that incorporeals, in this case, electricity, deserves protection.[360] This protection does not *per se* arise by virtue of the incorporeals being seen as analogous with corporeals. However, it exists because there is merit or legal justification to recognise the rights but not ownership that flow from these properties.[361] These expansions of the law of property thus demonstrate that the law of property is not founded on inflexible principles. More specifically, the principles may be developed in order to respond to emerging societal challenges.

Notwithstanding the above-mentioned, the question regarding whether real rights in information exist or not in South Africa is not specifically dealt with. South African courts do not appear to have pronounced on the aforementioned. Given this uncertainty, a revision of certain English and Canadian cases is made. These cases reveal that information may in certain circumstances be protected and granted legal

---

355 See for example, the Financial Intelligence Centre Act 38 of 2001 (hereinafter referred to as FICA), the Proceeds of Crime Act 76 of 1996, and the Drugs and Drugs Trafficking Act 120 of 1992.

356 See in general, s 21 of FICA.

357 These institutions are listed in Schedule 1 of FICA.

358 S 21 of FICA.

359 See *BonQuelle (Edms) bpk v Munisipalitet van Otavi* 1988 1 SA 508 (A), *Froman v Herbmore Timber and Hardware (Pty) Ltd* 1984 3 SA 609 (WLD), *Naidoo v Moodley* and *Boyers v Stansfield Ratcliffe & Co Ltd* 1951 3 SA 307 (TPD).

360 *Froman v Herbmore Timber and Hardware (Pty) Ltd* 1984 3 SA 609 (WLD) 610H-I.

361 *Froman v Herbmore Timber and Hardware (Pty) Ltd* 1984 3 SA 609 (WLD) 610I.

recognition in private law. The most important of these are the *Exchange Telegraph Co Ltd v Gregory & Co*,[362] *Oxford v Mos*s,[363] *Stewart* case and *R v Offley*.[364]

(a) Moss Case

In this case, the defendant (namely, Moss) was a student in the Faculty of Engineering at the University of London. It was alleged that the defendant dishonestly took possession of certain confidential information. The information was contained in examination question papers (questions) for a Civil Engineering examination.[365] It was contended and not disputed that the defendant did not intend to deprive the university or the senate permanently of the exam paper.[366] The defendant simply wished to memorise the questions in order to prepare for the exams. The court, per Smith J, conceded that the defendant's conduct amounted to cheating.[367] Given this dishonesty, society condemns or should condemn such conduct.[368] Despite this, the court concluded however that information, and not the exam question paper, was not property in terms of the existing principles of property law.[369] In other words, there was no ownership which was vested in this information. Consequently, the defendant did not assume ownership of the information following the taking of the exam question paper.[370]

(b) Offley Case

In the Offley case, the court followed the wording in the Moss case.[371] In this case, Offley had a security firm. Part of his duties was to do security checks for employers of job applicants. On one reported occasion, Offley needed detailed information belonging to various persons. The information was stored at the Canadian Police Information Centre (C.P.I.C.).[372] It was contained in a 'pool of computer stored information'. Offley then requested the Chief of the Edmonton City Police Department (Edmonton City

---

362 *Exchange Telegraph Co Ltd v Gregory & Co* C.A. [1896] 1 Q.B. 147 (hereinafter referred to as Gregory case).
363 *Oxford v Mos*s (1979) 68 Cr. APP. R. 183 (hereinafter referred to as Moss case).
364 *R v Offley* (1986) 45 Alta. L.R. (2d) 23 (hereinafter referred to as Offley case).
365 Moss case 184-185.
366 Moss case 185.
367 Moss case 184-185.
368 Moss case 184-185.
369 Moss case 184-185.
370 Moss case 184-185.
371 Offley case 29.
372 Offley case 24.

Police) to check those details for him. However, he was advised that the information was only available to law enforcement agencies. Out of desperation, Offley promised to pay a Constable (Brown) of the Edmonton City Police a sum of $2 in relation to each piece of information supplied.[373] Brown reported the promise to his superiors who then devised a plan (set-up) to catch Offley. Offley was subsequently captured and criminal charges were commenced against him.[374] During the hearing, the court had to determine whether or not the information can be the object of rights. In its attempt to answer this question, the court stated that the intrinsic nature of a thing (not its quality) is essential in determining whether such a thing is property in the legal sense or not.[375] Accordingly, the court concluded that the inherent nature of information is such that it, whether confidential or not, is incapable in law of being the object of property rights.[376]

(c) Gregory Case

This case represented a departure from the view that was held in both the Moss and Offley cases. This case dealt with an action to prevent the defendant (Gregory) from publishing certain information.[377] The information was contained in various tapes that the defendant had earlier obtained.[378] The court examined the tapes and consequently concluded that the information in those tapes was valuable to the plaintiff. This importance, the court stated, was demonstrated by the fact that the plaintiff incurred time and money to collect such information.[379] Furthermore, although the defendant was allowed to furnish the information to its subscribers these subscribers were entitled to pay the plaintiff for the information. In view of the aforesaid, the court held the view that this information is property. Consequently, its dishonest taking and obtaining should entitle the plaintiff to enforce its rights in terms of the principles of the law of property.[380]

(d) Stewart Case

---

373 Offley case 24.
374 Offley case 24.
375 Offley case 27.
376 *R v Offley* 27-28.
377 Gregory case 147-151.
378 Gregory case 147-151.
379 Gregory case 151.
380 Gregory case 155-156. See also the argument by Rigby L.J. in Gregory case 156-158.

The court in the Stewart case was divided in relation to the question regarding whether or not information is property within the purview of the law of property. The minority view, as per Lacourcière J.A., was that information cannot be regarded as property.[381] Accordingly, property rights to information, it was concluded, are not possible in terms of the law of property.[382]

However, the majority, as per Houlden J.A. and Cory J.A., held that contemporary societal developments require that information should be the object of property rights.[383] In particular, Cory J.A. emphasised the importance of information by saying that 'information and its collection, collation and interpretation are vital to most modern commercial enterprises. Compilations of information are often of such importance to the business community that they are securely kept to ensure their confidentiality'.[384] Information of the nature as aforesaid above attracts or should attract all the protection which the law attaches to property.[385]

2.11.3 Summary

It is illustrated in the sections above that information is central to the information society. Because of this, it has become a 'public good'.[386] It can be used as a tool to establish and develop a business.[387] Furthermore, it can be utilised in order to control certain economic crimes.[388] Consequently, users of information have an interest in it and they regard this interest to be important enough to warrant protection and recognition by the law. From *Cooper v Boyes No and Another*[389] it is established that an interest or value indicates whether or not property status should be granted to an object. This value or interest does not necessarily imply an economic or market value

---

381 Stewart case 594.
382 Stewart case 594.
383 Stewart case 598-604.
384 Stewart case 599.
385 Stewart case 600-604. See also *Boardman v Phipps* [1967] 2 A.C. 46 107.
386 Elkin-Koren and Salzberger *Effects of Cyberspace* 49-50.
387 *Regina v Stewart* 598, *Thomas Marshall (Exports) Ltd v Guinle* 209-210 and Samuelson 1991 *Communications of the ACM* 15.
388 FICA, the Proceeds of Crime Act 76 of 1996, and the Drugs and Drugs Trafficking Act 140 of 1992.
389 *Cooper v Boyes No and Another* 1994 4 SA 521 (CPD).

or interest. It is only important that the object could form part of a person's estate.[390] It should be useful and valuable objects and those that are regarded as *in commercio*.[391]

The fact that courts differ on the question regarding whether or not information is property is problematic. On the one hand, there is a view which encourages an examination of information according to its intrinsic nature. It concludes that because information cannot be physically or actually possessed or owned, then, it fails to be property that could be owned. On the other hand, there are some who attack the latter view and says that that it is out-dated and out of touch with the current realities of information flows or overflows.[392] The basis for this is that information is of value to humans and that there is a general expectation that it should be the object of property rights.[393]

2.12 CONCLUSION

The law of property is dynamic and flexible. Its meaning and essence varies depending on the needs of a particular society. This flexibility is also inimical to the discussion of property as a right or an object of rights. For example, the object rights theory is found in old Roman law of the 250 BC. More specifically, the Romans of this time only spoke of actions (*actio in rem* and *actio in personam*) as means of protecting the interest which a person had over property. Exactly when these actions became rights cannot be ascertained with precision. Suffice to say that *dominium* was viewed as the most comprehensive of the rights to property. This completeness varied from society to society. Accordingly, its meaning was usually derived from the circumstances that were relevant to a specific society.

It is conceivable that the approach by the Pandectists had an influence on South Africa's understanding of property as a right. South Africa creates a clear distinction between objects in the conventional and legal senses. To be regarded as property in

---

390 Van der Walt and Pienaar *Law of property* 3rd ed 8.

391 Kleyn, Boraine and Du Plessis *Silberberg and Schoeman's law of property* 19. See also Nigri DF "Theft of information and the concept of property in the information age" in Harris JW (ed) *Property problems: from genes to pension funds* (Kluwer Law International London 1997) 48-60 48-50.

392 Nigri *Property problems* 48-50.

393 Gregory case 155-156 and Stewart case 600-604.

the legal sense, an object must generate legal relationships.[394] It must be capable of human control, be of some value to humans and be the object of rights and duties.[395] Four categories of rights are differentiated for purposes of the law of property. These are real rights, personality rights, immaterial property rights and personal rights.[396] Furthermore, ownership is characterised according to its nature and the relations it has with people. With regard to the former, a distinction is made between *res in commercium* and *res extra commercium*. In relation to the latter, it is differentiated between corporeal and incorporeal, movable and immovable, divisible and indivisible, consumable and inconsumable, fungible and non-fungible and single and complex properties.[397] Corporeal property refers to physical objects. These objects must occupy some space, and be capable of being seen and touched.[398] Incorporeal property is 'artificial or fictitious' objects.[399]

From the developments in the law of property above, the position of information is not entirely clear. It is not clear whether information is or can be regarded as property for purposes of law. Despite this, it is evident that as people migrate into the virtual world; a need arises to recognise property in online settings. In this chapter, this argument for virtual property in virtual worlds is taken into account. This is the case because a person may have an interest or right to information. Although this interest may not necessarily translate to dominium, however, it may be such that it requires protection and recognition in terms of the law. In view of this, it is argued that a more balanced argument for the recognition of information as an object of rights should be placed on the fact that the principles of property law are not rigid and inflexible. Therefore, the principles could be developed in a manner that considers the progressions of recent technologies. More specifically, it is essential to accept that a society is not necessarily a stationed or offline society. The term society also refers to an information society. An information society evolves and cannot be sensed using the traditional sensing techniques or methods. Accordingly, the property rights that are derived from this society are vested in non-physical objects, namely information. The character of these rights usually differs with those that are found in offline societies. However, the

---

394 Oosthuizen *Law of property* 3.
395 Oosthuizen *Law of property* 3.
396 See also constitutional property rights.
397 Kleyn, Boraine and Du Plessis *Silberberg and Schoeman's* 29-42.
398 Maasdorp *Institutes of South Africa* 1.
399 Maasdorp *Institutes of South Africa* 1.

importance of these rights to the *dominus* does not depend on whether the society is offline or online.

Therefore, because information is an object over which property rights or interests are possible, it now becomes essential to investigate whether or not this property can be the object of theft. In other words, is information property that is capable of being stolen? The scrutiny of this question is made in chapter 3 below. The discussion leads to the study of the various e-crimes in chapter 4 below. It is important to note that chapter 3 is limited only to the Roman-Dutch, English and South African law approaches to theft.

CHAPTER 3

THE LAW OF THEFT – HISTORICAL DEVELOPMENTS

CHAPTER 3

THE LAW OF THEFT – HISTORICAL DEVELOPMENTS

3.1 INTRODUCTION

In chapter 2 property as a right or as an object of rights was discussed. Particular periods in the jurisprudence of property law were examined. It was revealed that the rights in property are called real rights. These rights bestow on the *dominus* wide powers in relation to or over property. In general, the objects of rights are corporeal and incorporeal things. Following the above-mentioned, it was then argued in chapter 2 that recent developments in ICTs necessitate that information should be regarded as an object of real rights. This is the case because information has nowadays become valuable to modern society, namely an information society. Governments, organisations and computer users collect, gather and process information on a daily basis. Furthermore, information is essential in concluding transactions and preventing e-crime.

This chapter builds from the discussion in chapter 2. Specifically, it examines whether or not the law of theft has reached a stage of development where other forms of intangibles or incorporeal things, for example information, could be regarded as capable of being stolen. It may be stated from the outset that a similar question was discussed by the South African Law Commission[1] in the late 1990s.[2] In seeking to answer this question, the SALC relied on two propositions. Firstly, it recognised the benefits and detriments that modern technologies generate for the information society. More specifically, the SALC commented that current technologies encourage and can be used as instruments or tools to commit e-crimes.[3] Secondly, it stated that e-crimes are usually carried out through the accessing of information or computer systems or networks.[4] Thereafter, it concluded that an endeavour to develop the principles of theft

---

1 Hereinafter referred to as the SALC.

2 See The SALC, Discussion Paper 99, Project 108 of 2 July 2001 (hereinafter referred to as SALC Project 108. To be accessed at http://www.justice.gov.za/salrc/dpapers/dp99_prj108_comp_2001jul.pdf.

3 SALC Project 108.

4 SALC Project 108.

in order to deal with the developments in ICTs would be pointless.[5] To the SALC, it was sufficient to simply criminalise the unauthorised accessing of, interception of or interference with particular information. The aforesaid criminalisation can be deduced from Chapter XIII of the ECT Act.

Despite the arguments or conclusions by the SALC, it is submitted that the principles of theft are not founded on stationary or inflexible systems of rules. In particular, the principles on which the law of theft is built change and are able to respond to emerging societal developments. This move or adaptability was witnessed in the past when external factors, for example, agriculture and industrialisation, necessitated the transformation of the principles with the aim of addressing new challenges.[6] The Roman-Dutch, English and South African law approaches to theft reveal these modifications. More specifically, it is acknowledged that what amounted to theft or the objects of theft in a certain period of time is bound to change in another. This change is sometimes attributed to the fact that the principles of theft are part of an evolving legal system.

3.2 ROMAN LAW

3.2.1 Old Roman Law

The idea of theft or *furtum* was captured in Table VIII of the Twelve Tables. This Table provided:

> A thief taken in the act, if a freeman, shall be scourged and made over by *addictio* to the person robbed; if a slave, shall be scourged and thrown from the Tarpeian rock; but those under the age of puberty shall, at the discretion of the magistrate, be scourged and condemned to repair the damage.[7]

---

5 SALC Project 108.

6 Hall J *Theft, law and society* 2nd ed (Bobbs-Merrill Indianapolis 1952) 14-33. See also Fletcher GP *Rethinking criminal law* (Little Brown Boston 1978) 59-60 and Fletcher GP "The metamorphosis of larceny" 1976 (89) *Harvard Law Review* 469-530 469-471.

7 See Ortolan J *The history of Roman law from the text of Ortolan's histoire de la legislation Romaine et généralisation du droit* (Butterworths London 1871)116. The Tarpeian rock was an execution site or place for criminals in the early Roman Republic.

However, it does not appear from Table VIII that the meaning and nature of *furtum* was specifically provided for in the Twelve Tables. It is only evident that all Table VIII of the Twelve Tables did was to demonstrate that particular forms of theft were manifest (*furtum manifestum*) whereas others were non-manifest (*furtum nec manifestum*).[8] Moyle concedes that this classification of theft in early Roman law originated from Greece.[9] In Greece, the term 'δεδέσθαι άν τις άλώ ποιώ' denoted theft that was detected in the place where the theft was committed.[10] Sometimes, the term 'έπ αύτοφώρώ' (or *ep'autophoro*) was used in order to demonstrate cases of manifest theft.[11] This word literally meant 'in self-detection' or 'during the undeniable act'.[12] It presupposed a situation where a thief was 'caught in highly incriminating circumstances'.[13] In other words, the thief must have been caught in possession of the physical thing or *corpus delicti*.[14]

Furtum manifestum was dealt with in table VIII.15 of the Twelve Tables. It amounted to theft where the stolen property was discovered in the possession of a thief.[15] As regards non-manifest theft the position was not quite clear. More specifically, the Twelve Tables did not particularly define *furtum nec manifestum*. Despite this, a holistic reading of the Table VIII of the Twelve Tables suggests that non-manifest theft could have included the theft of a physical thing where the requirements of manifest theft were not present.

In summary, old Roman law did not specifically describe the term theft. All this law did was to recognise that certain forms of theft were manifest, whereas others were non-manifest. Thus, a theft could be committed in situations where a thief was found in

---

See Smith M "Capital punishment and burial in the Roman empire" in Ellens J H (ed) *Bethsaida in archaeology, history and ancient culture: a festschrift in honour of J.T Greene* (Cambridge Scholars Publishing Newcastle 2014) 395 436 402.

8 Watson A *The spirit of Roman law* (The University of Georgia Press Athens 1995) 30.

9 Moyle JB *The Institutes of Justinian* 5th ed (Clarendon Press Oxford 1913) 159. See also Cohen D *Münchener Beiträge zur Papyrusforschung Heft 74: Theft in Athenian Law* (C.H. Beck'sche Verlagsbuchhandlung München 1983) 52-54.

10 Cohen D *Theft in Athenian law* (C.H. Beck'sche Verlagsbuchhandlung Müchen 1983) 58-593.

11 Bryant BH and Krause MS *John* (College Press Publishing Missouri 1998) 196.

12 Bryant and Krause *John* 196.

13 Harris EM *The rule of law in action in democratic Athens* (Oxford University Press Oxford 2013) 167.

14 Harris *The rule of law* 167.

15 See Table VIII. 15 of the Twelve Tables.

possession of the physical thing or in cases where the requirements of manifest theft were not present.

3.2.2 Pre-Classical Roman Law

In pre-classical Roman law, *furtum* was theoretically understood to have originated from the Latin expression *furvus*.[16] In English the phrase *furvus* denotes dusky, swarthy, dark or darkness.[17] From this, a suggestion was made that *furtum* could be understood by examining the method or methods that were used to perpetrate theft. A further scrutiny of the concept of *furtum* illustrates that this notion shared particular resemblance with the Greek concept of 'φέρω'. The term 'φέρω' literally meant to move or propel by bearing; move or, to be conveyed or borne, with the suggestion of force or speed.[18]

Given the above-mentioned, *furtum* was referred to as the crime of 'swindling' or *stellionatus*.[19] It involved the surreptitious carrying away or *auferre* of a thing with fraudulent intention.[20] The required *auferre* had to be physical or tangible. Particularly, it had to translate to the tangible removal of a thing.[21] However, gain was not necessarily a prerequisite for the carrying away of property. Because rights in property over slaves existed during this period, it was possible for the slaves to be the object of theft. Watson argues that 'to take away another's female slave to gratify one's lust' was in pre-classical Roman law regarded as theft.[22]

A question existed regarding whether or not the required *auferre* had to be in respect of a part or whole of the thing. Specifically, did a person commit theft of the heap of grain in situations where he or she only carried out the *auferre* in relation to 'a small quantity

---

16 Colquhoun PMC *A summary of the Roman civil law, illustrated by commentaries on and parallels for the Mosaic, Canon, Mohammedan, English and Foreign Law* (William Benning London 1860) 206.

17 Valpy FEJ *An etymological dictionary of the Latin language* (Baldwin London 1828) 169.

18 Luschnig CAE *An introduction to ancient Greek: a literary approach* 2nd ed (Hackett Publishing Indianapolis 2007) 22.

19 Von Bar L *A history of continental criminal law* (Augustus M. Kelley Publishers New York 1968) 40.

20 Du Plessis P *Borkowski's textbook on Roman law* 5th ed (Oxford University Press Oxford 2015) 338.

21 Du Plessis *Roman law* 338.

22 Watson *Roman law* 101.

from the heap of grain'?[23] Although this question was acknowledged in pre-classical Roman law, it was however left open for determination by the jurists in the later Roman law periods.[24]

In summary, an attempt was made in pre-classical Roman law to define theft. It was submitted that theft has to do with the unlawful and fraudulent carrying away of a corporeal thing. It was not necessary that the *auferre* should be made with the aim of making a profit out of the thing. Thus, theft could arise in situations where a person carried away property of another to the point where the lawful owner could not find it. However, pre-classical Roman law omitted to examine whether or not the *auferre* should be in respect of the whole or part of the property.

3.2.3 Classical Roman Law

Classical Roman law regarded *furtum* as a private wrong or delict.[25] Accordingly, theft was one of the four (4) pillars of delicts that formed the basis of the Roman law of obligations.[26] The other categories of wrongs were *iniuria*, for example *convicium, adtemptata puditia* and *ne quid infamandi causa fiat*; damage to property (excluding violence), and *rapina* or violent damage to property.[27] Collectively, the delicts were referred to as the *crimen*.[28]

Classical Roman law jurists developed the pre-classical Roman law idea of theft or *furtum*. They argued that *furtum* was the *contrectatio rei fraudulosa lucri faciendi gratia vel ipsius rei vel usus eius possessionisve quod lege naturali prohibitum est admittere.*[29] In English this may be translated to mean the 'dishonest handling of a thing (or property) in order to make a gain either out of the thing (or property) itself or

---

23 See Watson A *Roman law and comparative law* (The University of Georgia Press Athens 1991) 69.
24 Watson *Roman law and comparative law* 69.
25 Institutes of Gaius III.182.
26 Watson A *The evolution of western private law* (Johns Hopkins University Press Baltimore 2001) 124.
27 Watson *The evolution of western private law* 124.
28 Smith W and Anthon C (eds) *A dictionary of Greek and Roman antiquities* (American Book New York 1843) 463.
29 D XLVII.2.3.

else out of the use or possession thereof. From such conduct natural law commands us to abstain'.[30]

Having examined the definition of *furtum* above, certain elements of this wrong could be deduced. These are *contrectatio*, *rei fraudulosa* or fraud, *lucri faciendi gratia* and *ipsius rei vel usus eius possessionisve*. The aforementioned elements are discussed in the sections below.

(a) Contrectatio

Contrectatio was sometimes referred to as *adtrectatio.*[31] It meant a 'touching, handling, fondling, pawing or interfering with' the object of property.[32] Some academics challenge the suggestion that *contrectatio* connotes the touching or handling of property.[33] They submit that *contrectatio* encompassed a definite meddling with the property.[34] Meddling in the former sense translates to any dishonest taking and carrying away of property.[35] However, other Roman law jurists denounce the introduction of meddling to the study of *contrectatio*. Watson particularly argues that the view regarding the meddling with the property is not founded on and does not represent the traditional Roman law description of *furtum*.[36]

Classical Roman law jurists disagreed in relation to the scale and extent of the handling or touching. Paulus argued that liability should ensue as if the *contrectatio* was in respect of the whole property.[37] In this instance, a touching or handling of a part or portion of property could be equated to the touching or handling of the entire property.[38] However, Ulpian provided that *contrectatio* should only be limited to the part

---

30 Jolowicz HF *Digest XLVII.2 de furtis* (Cambridge University Press Cambridge 1940) 1-2.
31 See Aulus Gellius, *Noctes atticae* 11.18.20.22.23.
32 Zimmerman R *The law of obligations: Roman foundations of the civilian tradition* (Juta Cape Town 1990) 924-925.
33 Buckland WW *A textbook of Roman law: from Augustus to Justinian* 3rd ed (Cambridge University Press Cambridge 1963) 557.
34 Buckland *Roman law* 557.
35 Buckland *Roman law* 557.
36 Watson *Studies* 269.
37 D. 47. 2. 21.
38 D. 47. 2. 21.

of the property that was touched or handled.[39] Accordingly, a partial *contrectatio* was necessary in order to establish whether or not a touching or handling of property existed in each case.[40]

(b) *Rei Fraudulosa*

Scott provides an explanation of the classical Roman law approach to fraud.[41] He does this by referring to Paulus' Book I.VIII.I.[42] According to Scott, fraud took place 'when one (thing) was done, and another (thing) was presented'.[43] It was required that there should be an unacceptable or dishonest act or conduct which accompanied the touching or handling. This inappropriate and fraudulent conduct must have amounted to an 'unlawful or fraudulent' touching or handling of the property.[44] Consequently, the *contrectatio* must have been *invito domino.* Wicked intention or *dolus malus* was required to be alleged and proved.[45] This *dolus malus* related to an intention to commit *furtum*.[46] In other words, *contrectatio* should have been committed with the necessary fraudulent intention.[47] Consent to the touching or handling of the property thus excluded the fraudulent intention.[48]

To classical Romans, *furtum* did not arise in cases where a person broke into a house with the intention to injure the owner of a house, and thereafter another person entered the house, while still broken into, with the intention to touch or handle property belonging to the owner.[49] Furthermore, the fact that a person changed his (or her) mind

---

39 D. 47. 2. 21, Honoré T *Justinian's Digest: character and compilation* (Oxford University Press Oxford 2010) 138 and Duff PW "*Furtum* and Larceny" 1954 (12) *The Cambridge Law Journal* 86-88 87.

40 D. 47. 2. 21, Honoré *Justinian's Digest* 138 and Duff 1954 *The Cambridge Law Journal* 87.

41 See Scott SP *The civil law including the Twelve Tables, the Institutes of Gaius, the Rules of Ulpian, the Opinions of Paulus, the Enactments of Justinian, and the Constitutions of Leo* Vol 1 (AMS Press New York 1973).

42 Scott *Civil law* 262.

43 Scott *Civil law* 262.

44 Burdick WL *The principles of Roman law and their relation to modern law* (The Lawbook Exchange New Jersey 2004) 487.

45 Jolowicz *De furtis* lv and Burdick *Principles* 487.

46 Burdick *Principles* 487.

47 Gaius III.197.

48 Frazel TD "'Furtum' and the description of stolen objects in Cicero 'In Verrem'" 2005 (126) *The American Journal of Philosophy* 363-376 366-367.

49 D XLVII.2.54.

and decided to restore the property to the owner did not release or exonerate him (or her) from liability.[50] Lastly, *furtum* was deemed to arise in circumstances where a person recognised that what he or she committed was theft.[51] It was essential that 'some object on which the guilty mind can operate'[52] must be or have been present. This intention must have led such a person to touch or handle the property in cases where he or she knew that consent would not be granted or given.[53] In this instance, an intention to touch or handle the property in order to deprive the other of ownership did not suffice.[54]

(c) Lucri Faciendi Gratia

Lucri faciendi gratia primarily appeared in the work that was prepared by Gellius called the *Noctes Atticae*.[55] It was from the *Noctes Atticae*, it is argued, that a passage which resembled *lucri faciendi gratia* was borrowed. The passage read as follows: *Qui alienum iacens lucri faciendi causa sustulit, furti obstringitur....*[56] In English this meant that: a person who 'silently carries off another's property for the sake of gain is guilty of theft'.[57] Subsequent to this development, the Digest followed more or less the particular wording of the passage which was contained in the *Noctes Atticae*. More specifically, the Digest affirmed that: *Qui alienum quid iacens lucri faciendi causa sustulit furti obstringitur, sive scit cuius sit sive ignoravit; nihil enim ad furtum minuendum facit quod cuius sit ignoret*.[58] This meant that a touching or handling of property which belongs to another person, that is, the owner, with intent to make a gain amounts to *furtum*.[59] The aforementioned theft occurs even in situations where a person found the property lying about.[60]

---

50 D XLVII.2.66.
51 Rolfe JC *The attic nights of Aulus Gellius* (Harvard University Press Cambridge 1927) 349.
52 Jolowicz *De Furtis* lvii.
53 Burdick *Principles* 487-488.
54 Burdick *Principles* 488.
55 Watson *Studies* 271.
56 *Noctes atticae* XI.XVIII.XXI.
57 Rolfe *Attic nights* 349.
58 D XLVII.2.54.4.
59 D XLVII.2.54.4.
60 D XLVII.2.54.4.

In classical Rome, *lucri faciendi gratia* referred to any benefit, increase or satisfaction.[61] This benefit, increase or satisfaction was not restricted or translated to mean a financial or pecuniary profit.[62] In other words, a benefit, increase or satisfaction, for purposes of *furtum*, was not circumscribed or measured by the presence or not of a financial or monetary loss or reward.[63] Important for the law of theft is that this interpretation of *lucri faciendi gratia* made it possible to differentiate between *furtum* and cases involving *damnum iniuria datum*.[64]

(d) *Ipsius Rei Vel Usus Eius Possessionisve*

The *ipsius* element revealed three (3) separate categories of *furtum*. These groupings were *furtum rei, furtum usus* and *furtum possessionis.*[65] To begin with, *furtum rei* denoted the actual stealing of property (*furtum rei ipsius)*. In this instance, a physical touching and handling of property was necessary*.* Secondly, *furtum usus* basically meant the 'theft of use'.[66] It occurred in cases where the property was used unlawfully or improperly, or the property was obtained without the consent of the owner, or the property was obtained from an owner for an unambiguous purpose and the use of it was beyond the limits that were imposed by an owner.[67] Consequently, it follows from the above that *et si quis utendam rem acceperit eamque in alium usum transtulerit, furti obligatur.*[68] This meant that a person who received property to be used from the other and converted it to another use was guilty of *furtum usus.*[69]

Thirdly, *furtum possessionis* signified 'theft of possession'.[70] It was in line with the principle that *furtum* can be committed against a person who had an interest in the

---

61 Burdick *Principles* 487.
62 Jolowicz *De furtis* lix and Watson *Studies* 271.
63 Jolowicz *De furtis* lix and Watson *Studies* 271.
64 Watson *Studies* 271.
65 Watson regards this classification as un-classical. See, Watson A "The Definition of Furtum and the Trichotomy" 1960 (28) *Tijdschrift voor Rechtsgeschiedenis* 197-210 202-203.
66 Adeley G *et al World dictionary of foreign expressions: a resource for readers and writers* (Bolchazy-Carducci Publishers Wauconda 1999) 152.
67 *R v Olivier and Others* 1921 TPD 120 1921-1922 (hereinafter referred to as *R v Olivier and* Others) and Zimmermann *The law of obligations* 196.
68 Gai III.196.
69 Ardy JT and Walker B *The commentaries of Gaius and rules of Ulpian* 3rd ed (The Law Book Exchange New Jersey 2005) 259.
70 Burchell J and Milton J *Principles of criminal law* 2nd ed (Juta Kenwyn 1997) 548.

property.[71] These persons were *bona fide* or legitimate possessors of property.[72] Aggrieved persons could re-claim the property in terms of the Roman law *actio furti*.[73] *Actio furti* was instituted in cases where there had been a theft of possession from a lawful possessor.

In summary, classical Roman law expanded the pre-classical Roman law idea of theft. This law categorised theft as a private wrong. It consisted of at least four elements. These included *contrectatio*, *rei fraudulosa* or fraud, *lucri faciendi gratia* and *ipsius rei vel usus eius possessionisve*. Firstly, *contrectatio* did not necessarily mean the carrying away of the physical property. It only denoted the touching, handling, fondling or interfering with the property. However, there was disagreement in relation to the degree of the required *contrectatio*. Some jurists were of the view that a touching or handling of the part of the property was enough,[74] whereas others argued that *contrectatio* should be in respect of the whole property.[75] Secondly, *rei fraudulosa* related to the fact that the *contrectatio* must be or had been fraudulent. Thus, *dolus malus* was indicative of the *rei fraudulosa*. Thirdly, *lucri faciendi gratia* had to do with the fact that the fraudulent touching or handling of property should be made for the sake of gain. This profit did not necessarily mean a pecuniary gain. Fourthly, *ipsius rei vel usus eius possessionisve* evidenced about three separate categories. These were the *furtum rei* or the actual theft of property, *furtum usus* or the theft of use and *furtum possessionis* or the theft of possession.

3.2.4 Post-Classical Roman Law

The Institutes of Justinian are central to the discussion of theft in post-classical Rome. In terms of the Institutes, *furtum* was the *contrectatio rei fraudulosa vel ipsius rei vel etiam usus eius possessionisve: quod lege naturali prohibitum est admittere.*[76] In this respect, theft meant a fraudulent and deceitful appropriation of property in its entirety, for purposes of either making use of property or of attaining possession over

---

71 Buckland *Roman law* 557.
72 Jolowicz *De furtis* 1-2.
73 Jolowicz *De furtis* 1-2.
74 D. 47. 2. 21, Honoré *Justinian's Digest* 138 and Duff 1954 *The Cambridge Law Journal* 87.
75 D. 47. 2. 21.
76 I IV.1.1.

property.[77] It is submitted that the fact that the *contrectatio* must be or have been in respect of the entire property is fundamental. In particular, the inclusion of the notion 'in its entirety' remedied the uncertainty or confusion that existed in classical Roman law regarding whether or not the *contrectatio* should be in respect of the part or whole of the property.[78]

Furthermore, the definition that was contained in the Institutes of Justinian required that a wrong must exist or have existed. In other words, the touching or handling must have been against the law (that is, fraudulent) and intentional.[79] Mackenzie particularly favours this post-classical description of *furtum*.[80] Mackenzie describes *furtum* as the 'felonious taking or carrying away of property of another' in order to make a profit.[81] Mackenzie also argues that the taking or carrying away must be made or have been made with the intention to steal property.[82] Therefore, *furtum* was deemed to have been committed in circumstances where a person handled or removed property without the lawful and required consent of the lawful possessor of the property.[83] In addition, a person or borrower committed theft if he (or she) had put another's property to the use other than that for which it was lent.[84]

Another departure from the classical Roman law formulation of *furtum* could be found in two separate situations. The first related to the omission of *lucri faciendi gratia*. The second had to do with the revision of the element of *ipsius rei vel etiam usus eius possessionisve*. In relation to *lucri faciendi gratia*, there are some scholars who supported its exclusion.[85] They submitted that there was no basis in law for including

---

77 Sohm R *The Institutes: a textbook of the history and system of Roman private law* 3rd ed (Clarendon Press Oxford 1907) 417 and Burdick *Principles* 487.

78 For a study of the uncertainties in classical Roman law regarding whether or not *contrectatio* should be in respect of the part or whole of the property, see the debate between Paulus and Ulpian above.

79 Howes RB and Davis RPB *The elements of Roman law: being selections from the Institutes of Justinian, with explanatory notes, for the use of students* (Juta Cape Town 1923) 216 and Descheemaeker E *The division of wrongs: a historical comparative study* (Oxford University Press Oxford 2009) 3.

80 MacKenzie L *Studies in Roman law with comparative views of laws of France, England and Scotland* (Gaunt Holmes Beach 1991) 230.

81 MacKenzie *Comparative views* 230.

82 MacKenzie *Comparative views* 230.

83 I IV.1.6.

84 I IV.1.6.

85 Howes and Davis *Elements* 216.

lucri faciendi gratia in the definition of *furtum*.[86] However, there are those academics who condemned such exclusion.[87] They argued that the definition contained in the Institutes of Justinian relied on a non-classical formulation of the meaning of *furtum.*[88] With regard to *ipsius rei vel etiam usus eius possessionisve*, it is argued that this revision is *prima facie* outlandish.[89] In particular, it is strange and bizarre insofar as it suggested or demonstrated that a 'touching or handling of the use or possession' of property was impossible*.*[90]

In summary, the meaning of theft as it was known and accepted in classical Roman law was altered in post-classical Roman law. Firstly, it was stated that only a fraudulent touching or handling of the entire property was required. Secondly, the element of *lucri faciendi gratia* was omitted from the definition of theft. The foundation for this was that there was no basis in including the element of gain or profit as the pre-condition for theft. Thirdly, post-classical Roman law revised the element of *ipsius rei vel etiam usus eius possessionisve*. The effect of this revision was to render a theft of use and possession impossible in post classical Roman law.

3.3 GERMANIC LAW

In Germanic law, the principles of theft or *diefstal* were contained in specific legal records. These records were called the *leges barbarorum*. *Leges barbarorum* is a Latin term which is translated to mean the laws of the barbarians[91] or barbaric laws.[92] The laws of the barbarians were generally the unwritten customary laws of the various Germanic tribes.[93] These laws were a combination of Roman and old German law.[94] Barbaric laws were embodied in different codes. The codes were referred to as the *Lex*

---

86 Howes and Davis *Elements* 216.
87 Watson *Studies* 269.
88 Watson *Studies* 269.
89 Watson *Studies* 272.
90 Watson *Studies* 272.
91 Treviño AJ *The sociology of law: classical and contemporary perspectives* (Transaction Publishers New Brunswick 1996) 139.
92 Shaffern RW *Law and justice form antiquity to enlightenment* (Rowman & Littlefield Publishers Lanham 2009) 103.
93 Green DH *Language and history in the early Germanic world* (Cambridge University Press New York 1998) 31.
94 Shaffern *Law and justice* 103. For a study regarding the mixture of Roman and Germanic law, see Drew KF *The laws of the Salian Franks* (University of Pennsylvania Press Philadelphia 1991).

Salica or laws of the Salian Franks[95] and the *Lex Ripuaria* or law of the Ripuarian Franks.[96]

The laws which were included in these codes did not specifically regard theft as a public wrong or wrong against society or social order.[97] Simply, theft was deemed to be one of the private wrongs.[98] The other private wrongs included 'homicide, personal injuries short of death, rape, adultery and seduction'.[99] Theft was a private wrong because it was considered to have been directed against a person, that is, the owner of private property.[100] Given the above-mentioned, it was equated with the *hlafordsearu* or deceitfulness against the king.[101]

Theft took place in situations where a person held in his possession a thing or property which belonged to someone else or which a person knew was not his without lawful or justifiable reasons.[102] Holmes argues that this possession of property was an essential ingredient for theft.[103] The above-mentioned was the position because 'only he who was in possession could say that he had lost the property against his will'.[104] Zimmermann is of the view that before a person could have gained possession of property wrongfully he must have actually removed the property from the custody of another person.[105]

In summary, Germanic law regarded theft as a private wrong. Theft took place in cases where a person had physical possession of property which belonged to someone else.

---

95 Drew *Salian Franks* 1-11.

96 Dixon R *Karl Marx, Frederick Engels: collected works* (International Publishers New York 1975) 653.

97 Burchell J and Milton J *Principles of criminal law* 3rd ed (Juta & Co Lansdowne 2005) 23.

98 Burchell and Milton *Principles of criminal law* 3rd ed 23.

99 Diamond AS *Primitive law, past and present* (Routledge London 1971) 61.

100 Burchell and Milton *Principles of criminal law* 23.

101 Pratt D *The political thought of King Alfred the great* (Cambridge University Press Cambridge 2007) 234.

102 Hüebner R *A history of Germanic private law* (The Lawbook Exchange New Jersey 2000) 412-414.

103 Holmes OW *The common law* (The Lawbook Exchange New Jersey 2005) 166.

104 Holmes *Common law* 166.

105 Zimmermann *The law of obligations* 946.

This possession must have arisen in situations where a person had physically removed the property from the custody of the lawful owner.[106]

3.4 MEDIEVAL LAW

The Romanists had a slightly different approach to theft. On the one hand, they used the definition of theft that was contained in the Digest. The latter is to the effect that *furtum est contrectatio re fraudulosa lucrifaciendi gratia vel ipsius rei vel etium usus eius possessionisve*.[107] On the other hand, they modified this description of *furtum* by saying that theft occurred in cases where a person to whom the property belonged was unlawfully deprived of the full possession of such property.[108] Raymund of Peȟafort (1175-1275 AD) provided justification for this view. In one of his seminal works titled *Summa de poenitentia et matrimonio cum glossis loannis de Friburge*, Raymund submitted that *furtum est contrectatio re aliena, mobilis, corporalis, fraudulosa, invito domino, lucrifaciendi gratia, vel ipsius rei, vel etiam usus eius, possesseonisve.*[109] In English, this means that theft is:

> The fraudulent seizure of a thing that belongs to another, movable and corporeal, against the will of the *dominus*, for the sake of making profit, either of the thing itself, or of its use or its possession.[110]

It is deduced from the aforementioned paragraph that only the theft of movables or corporeals was regarded as legally possible.[111] This theft had to be effected for purposes of making gain out of the property or the use or possession of the property.[112] The aforementioned view seemed to be the most welcomed by the glossators and the post-glossators. Specifically, Angelus Carletus de Clavasio (1411-1495 AD) affirmed

---

106 Zimmermann *The law of obligations* 946.
107 See D 47.2.1.3.
108 Brett AS *Liberty, right and nature: individual rights in later scholastic thought* (Cambridge University Press Cambridge 1997) 27.
109 Raymund of Peȟafort 2.6.219
110 Brett *Liberty, right and nature* 26.
111 Raymund of Peȟafort 2.6.219
112 Raymund of Peȟafort 2.6.219

the understanding that there could never be a theft of immovables and incorporeals for legal purposes.[113]

In summary, the jurists of the medieval period accepted the classical Roman law approach to theft. However, they argued that theft presupposed a situation wherein the owner of property was fraudulently disposed of the full rights to his property. They submitted that only movables and corporeals were or could be the objects of theft in law. Furthermore, theft was not only limited to property. It was also extended to the use and possession of the thing.

3.5 CANON LAW

Canonists distinguished between two forms of theft. These were called the sacrilegious theft and theft in a general sense. The first-mentioned theft related to the appropriation of ecclesiastical property or property of the church.[114] This property referred to those things that were reserved for the 'furtherance of the Christian religion'.[115] A theft of these things was considered to be an atrocious wrong. The aforementioned was attributed to the fact that church property belonged to God as the father of the church. Therefore, a theft of church property amounted to stealing from God.[116] To this end, Proverbs 28: 24 (those who steal from their father and mother, and say, 'it's not a crime', are friends of vandals) was invoked in order to condemn this form of theft. The second-mentioned theft was in regard to the stealing of any other property not belonging to the church.[117]

A more acceptable definition of theft, either of church or private property, by the canonists appeared in Gratian's *Decretum.*[118] Gratian stated that theft had similar connotations as the term *raptus* or rape.[119] Therefore, theft was, in the same way as *raptus* was corruption through illicit intercourse, a corruption through the appropriation

---

113 Angelus Carletus de Clavasio *Summa angelica* (1488) 115v.
114 Austin G *Shaping church law around the year 1000: the Decretum of Burchard of Worms* (Ashgate Publishing Surrey 2009) 189.
115 Hull E *The institution and abuse of ecclesiastical property* (T. Cadell Strand London 1831) 196.
116 Austin *Shaping church law* 188.
117 See Romans 2: 22 and Austin *Shaping church law* 188.
118 Gratian *Decretum magistri Gratiani* 2.37.2.
119 Gratian *Decretum* 2.37.2.

or seizure of property.[120] The association between theft and rape was also followed by other jurists of canon law, for example Bernardus Papiensis (1150-1213 AD). Papiensis created a separation between theft of persons and things by stating that r*aptor dicitur duobus modis; dicitur enim raptor rerum et raptor hominum, et praecipue foeminarum; dicitur autem proprie rapina rerum, et raptus mulierum*.[121] This means that a person could be a thief in two separate ways. He could be a thief of property or a thief of other persons, for example women.[122] This theft had to be effected for purposes of making gain out of the property or the use or possession of the property.[123]

In summary, canonists differentiated between theft of church property and theft in general. They defined theft as a corrupt act which led to the unlawful appropriation of property. Accordingly, theft of property and theft of the use and possession of the property were recognised. This idea of theft was then accepted and developed by the moral philosophers during the sixteenth century.

3.6 MORAL PHILOSOPHERS

These philosophers adopted the moralistic viewpoint on theft. This view was based on the understanding that the notion of private property or private ownership was generally the result of sin.[124] For example, Singer quotes one of the moral philosophers, Rufinus (1160 AD), as saying that immediately after the fall of Adam a state of lawlessness ensued in society.[125] Particularly, humans conducted themselves like 'brute beasts'.[126] This, according to Tierney, resulted in the acceptance of private property and private rights.[127]

---

120 Gratian *Decretum* 2.37.48 and Todeschini G "The origin of medieval anti-Jewish stereotype – the Jews as the receivers of stolen goods (twelfth to thirteenth centuries)" in Adams J and Hanska J (eds) *The Jewish-Christian encounter in medieval preaching* (Routledge New York 2015) 240-252 249.

121 Bernardus P *Summa Decretalium* 5.14.1.

122 Saunders CJ *Rape and ravishment in the Literature of medieval England* (Boydell & Brewer Ltd Cambridge 2001) 79.

123 Saunders *Rape and ravishment* 80.

124 See Aquinas *Summa theologiae* 66.9.1.

125 Singer H (ed) *Die summa decretorum des Magister Rufinus* (Ferdinand Schöningh Paderborn 1902) 6-7.

126 Tierney B "Permissive natural law and property – Gratian to Kant" 2001 (62) *Journal of the History of Ideas* 381-399 384-385.

127 Tierney 2001 *Journal of the History of Ideas* 384-385.

To the moral philosophers, God vested all the rights in property to all the people for their common nourishment. Given this, any appropriation of property outside this common enjoyment was against the law of nature as dictated by God.[128] This view seemed to have been followed by Aquinas. Aquinas relied on the precept *peccatum non dimititur, nisi restituatur ablatum*.[129] Accordingly, he stated that theft was a moral sin.[130] Being so, it was more perverse than other crimes, for example robbery. It was deemed to arise in situations where there was a fraudulent taking away of property which belonged to someone else.[131] The Corpus Iuris Canonici used the phrase *furti enim nomine bene intelligitur omnis illicita usurpatio rei alienae* in order to demonstrate this fraud.[132] This phrase means that the taking away or appropriation of property for gain had to be against the wishes of the lawful owner of property.[133] However, the appropriation did not have to be in respect of the whole thing. It was satisfactory if the thief was simply in possession or had dispossessed the owner of the rights of ownership in relation to the property.[134]

In summary, the moral philosophers accepted the moralistic view to the idea of theft that was developed by the canonist. They regarded theft as a moral sin. It arose in situations where property was fraudulently taken away from the owner. This taking away did not necessarily have to be in respect of the whole thing. It was enough if the taking away had subsequently resulted in the owner being dispossessed of the rights of ownership which he had to the property. This moralistic idea of theft was also adopted and followed in the Dutch law of theft.

3.7 DUTCH DEVELOPMENTS

---

128 Tierney 2001 *Journal of the History of Ideas* 384-385.

129 Aquinas *Summa theologiae* 66.9.1-3. This precept meant that there could be 'no forgiveness of a sin unless restitution' was effected.

130 *Liber Sextus Decretalium* 5.13.4 and Stump E *Aquinas* (Routledge London 2003) 322.

131 Pope RTP *Roman Misquotation or certain Passages from the fathers adduced in a work entitled "The Faith of Catholics,"* (William Curry & Co. London 1840) 200.

132 C.14.

133 Decock W *Theologians and Contract Law: The Moral Transformation of the Ius Commune (ca. 1500-1650)* (Koninklijke Brill Leiden 2013) 546.

134 Decock *Theologians and Contract Law* 546.

In Dutch law, theft was regarded as a wrong which impinged upon or was against natural and divine law.[135] Against this background, it was placed in the same category as homicide and was referred to as a 'moral wrong'.[136] Theft was a wrong because it was carried out in secret and with a fraudulent intent. In committing theft, a thief physically deprived the other person of his property. This deprivation was against the will of the person, in the sense that a thief had fraudulently retained the property and taken it away from the lawful possessor.[137] Following this deprivation, the thief derived some benefit or gain from the thing.[138] This gain did not necessarily translate to a monetary advantage.[139] Therefore, it was comparable to the *lucri faciendi gratia* that formed the basis of the classical Roman law approach to theft.[140]

Furthermore, two points are significant in the discussion of theft in Dutch legal jurisprudence. The first point has to do with the fact that theft was treated as a continuous moral wrong.[141] This meant that a thing remained stolen for as long as it was still in possession of the thief.[142] Accordingly, the fact that a thief relocated to another state or country with the stolen thing did not exonerate him from legal liability. The second point related to the fact that the Dutch law of theft recognised the so-called *furtum usus* or theft of use.[143] In this instance, the thief did not necessarily have to permanently deprive a person of the property. Instead, it was enough or adequate if the fraudulent retention and the subsequent taking away of property of another was made for a particular purpose, that is, the use of the property.[144]

In summary, the Dutch law of theft followed the moralistic idea of theft that originated from the moral philosophers. Specifically, this law regarded theft as a wrong which

---

135 Guillaume HM and Posthumus M *Hugo Grotius: meletius, sive de IIS quae inter Christianos conveniunt epistola* (E.J. Brill Leiden 1988) 126.

136 Neff SC (ed) *Hugo Grotius on the law of war and peace: student edition* (Cambridge University Press Cambridge 2012) 30.

137 Voet J *De furti* 19. See also Hebbert C *The introduction to Dutch jurisprudence of Hugo Grotius* (John van Voorst London 1945) 449-450.

138 Voet J *Commentarius ad Pandectas* (1698) 47.2.1

139 Voet 47.2.1

140 Voet 47.2.1

141 Van Leeuwen S *Commentaries on Roman-Dutch law* (Stevens and Haynes London 1886) 314.

142 Van Leeuwen *Roman-Dutch law* 314.

143 Van Leeuwen *Roman-Dutch law* 314.

144 Zimmermann *The law of obligations* 196.

impinged upon natural and divine law.[145] Despite the aforesaid, the formulation of the Dutch law of theft is similar to that which is traceable from classical Roman law. In particular, this law recognised the cases where a *contrectatio* was in respect of the whole property and those where it was only partial. The latter category of *contrectatio* was referred to as the theft of use.[146] Therefore, it was conceded that theft could arise in instances where the property was simply touched and handled with a view to achieve a particular result. In this instance, a temporary deprivation of property as opposed to a permanent deprivation of property was also possible.[147]

3.8 ENGLISH LAW

3.8.1 Background

The English law of theft has undergone a number of changes and modifications over the years. For example, early English law merely recognised violent and forceful appropriations[148] and dispossessions of property.[149] However, it was later felt that a more relaxed and less forceful description of theft was necessary. Consequently, the capacity of the English criminal law was developed to also encompass non-violent and non-forceful appropriations or dispossessions of property.[150] Following this, a distinction was made between robbery and theft. On the one hand, robbery was

---

145 Guillaume and Posthumus *Hugo Grotius: meletius, sive de IIS quae inter Christianos conveniunt epistola* 126.

146 Van Leeuwen *Roman-Dutch law* 314.

147 Zimmermann *The law of obligations* 196.

148 The term 'appropriates' has had particular significance to the English-law of theft. For example, the notion was regarded as having similar meaning with the concept of 'conversion'. See Griew E *The theft acts* 7th ed (Sweet Maxwell London 1995) 42. However, due to its vague and misleading meaning, the concept 'conversion' fell into disuse and was later abandoned. Thus, it is nowadays accepted that the term 'appropriate' means any assumption by a person of the rights of an owner (that is, a person having possession or control of or over property or anything capable of being stolen). See s 1(2)(iii) of the Larceny Act of 1916 (hereinafter referred to as the Larceny Act). Therefore, it does not matter whether or not such person keeps or deals with the property as an owner. See s 3(1) of the Theft Act of 1968 (hereinafter referred to as the Theft Act).

149 Property, for purposes of theft, excluded land, roofs and particular portions of buildings. In some cases, title deeds were regarded as incapable of being stolen. See Kiralfy AKR *Potters historical introduction to English law and its institutions* 4th ed (Sweet Maxwell London 1962) 368.

150 Dressler J *Understanding criminal law* 3rd ed (Lexis Publications New York 2001) 545.

defined as an aggravated theft as it involved violence.[151] It was treated as an open and less dishonourable offence than theft.[152] On the other hand, theft encompassed a surreptitious (or stealthy)[153] and dishonourable appropriation of another person's personal property.[154] Dishonesty was deemed to exist if the possession of property was obtained by trick, intimidation or it was known that an owner did not consent or could not have consented to the appropriation.[155] Also included in the definition of theft was a 'fraudulent meddling' with another's private property.[156]

There are two periods that influenced the manner in which the notion of property within the context of the law of theft was understood in early England. On the one hand, there is a period before 1968. On the other hand, there is one after 1968. The Larceny Act represents the era before 1968 and the Theft Act characterises the period after 1968. Before 1968, property included real and personal property, money (for example coins), debts, legacies, deeds and instruments relating to the title or right to property.[157] Accordingly, incorporeal or intangible property was not expressly mentioned before 1968. However, it is conceded that section 46(1) of the Larceny Act was capable of being interpreted broadly.[158] Such interpretation led or could lead to that section being read to mean that property also encompassed incorporeal things.[159] After 1968, property also referred to intangibles.[160] These intangibles were a debt, a right under a trust, an obligation which was created by the law and property capable of enforcement, for example, credit or benefit.[161]

---

151 Pollock F and Maitland FW *The history of English law Before the Time of Edward I* 2nd ed (The Lawbook Exchange New Jersey 2008) 493-495.

152 McLynn F *Crime and punishment in the eighteenth-century England* (Routledge London New York 1989) 90.

153 McLynn *Crime and punishment* 90.

154 Pollock and Maitland *History of English law* 493-494. See also s 1(5) of the Theft Act.

155 S 2(1)(a)-(c) of the Larceny Act.

156 Bentham J *Of the limits of the penal branch of jurisprudence* (Clarendon Press Oxford 2010) 127-128.

157 S 46(1) of the Larceny Act.

158 Loubser MM *The theft of money in South African law: with a comparison of other legal systems* (LLD Thesis University of Stellenbosch 1978) 58.

159 Loubser *Theft of money* 58.

160 S 4(1) of the Theft Act.

161 Plucknett TFT *A concise history of the common law* 5th ed (The Law Book Exchange New Jersey 2001) 446 and Brickey KF "The jurisprudence of larceny – an historical inquiry and interest analysis" 1980 (33) *Vanderbilt Law Review* 1101-1142 1102.

In addition, two wrongs constitute theft in England. These are larceny[162] and receiving stolen property.[163] In this chapter the principles of larceny are discussed. These principles are distinguished from those that are related to the crime of receiving stolen properties.[164] This is the case because larceny has everything to do with the actual stealing of property.[165] Receiving stolen property relates to the incidents that follow the fact of stealing. In this instance, a person must knowingly receive possession and control of property.[166] This receiving and control should subsequently be intended to permanently deprive the other of such property.[167]

3.8.2 Larceny

There is no single and concise description of larceny in English law. There are some who define larceny as the *contrectatio rei alienae fraudulenta, cum animo furandi, invito illo domino, cujus rei illa fuerit*.[168] In this instance, it is submitted that a physical and actual removal of property is essential.[169] This removal is or should be made with the intention to permanently deprive the other person of his or her property.[170] Others describe larceny in the following manner:

> The dealing, from any motive whatever (or whatsoever), unlawfully and without claim of right with anything capable of being stolen, in any of the ways in which theft can be committed, with the intention of

---

162 The English common law crime of larceny encompassed the crime of embezzlement and larceny by false pretences. Embezzlement is particularly a 'statutory refinement of the common-law crime of larceny'. See Fletcher *Rethinking* 4. It includes a deceitful appropriation of property which is under the custody and control of a person. See, s 17-19 of the Larceny Act. Whereas, larceny by false pretences amounts to the dishonest obtaining of possession of property. See Stephen JF *A digest of the criminal law (crimes and punishments)* 5th ed (MacMillan & Co New York 1894) 259.

163 Scheb JM *Criminal law and procedure* 4th ed (Wadsworth Thomson Belmont 2002) 168.

164 Turner JWC *Russell on crime* 12th ed (Stevens London 1964) 884.

165 S 1(1) of the Theft Act.

166 S 33(1) of the Theft Act.

167 S 33(1) of the Theft Act.

168 Bracton H *On the laws and customs of England* (Harvard University Press Cambridge 1968) 428. See also Reeves J *History of English law, from the times of Saxons, to the end of the reign of Philip and Mary* 2nd ed (Temple-Bar London 1787) 41 and Pollock and Maitland *History of English law* 496.

169 Kiralfy *Potters* 368.

170 Kiralfy *Potters* 368.

> permanently converting that thing to the use of any person other than the general or special owner thereof.[171]

Lastly, there are those who argue that larceny is a 'felonious intent' which excludes any claim of right. This view initially appeared in an early English case of *R v Holloway.*[172] It continues from the basis that in order for larceny to arise there must be or have been a taking and carrying away of property; the taking or carrying away of property must be or have been trespassory in nature, that is, it must amount to a meddling; the meddling must be against the will of the other person (owner), and the meddling must be or have been made with a felonious intent.[173]

This last-mentioned viewpoint on larceny seems to be the most welcomed in England. Given this, its meaning within the context of the English law of theft is investigated in the sections below.

(a) Trespassory Taking and Carrying Away of Property

The trespassory taking of property is also referred to as the 'caption' and the trespassory carrying away of property is known as the 'asportation'.[174] Caption is the actual or physical capturing of property. It entails a substantial taking or severance of property from the possession of an owner or a lawful possessor. Furthermore, it represents the existence of control over property. Asportation implies the physical carrying away of property.[175] The carrying away of property does not need to be distant.[176] In other words, asportation is presumed to have ensued in cases where:

> (Every part) of it (the property) is moved from that specific portion of space which it occupied before it was moved.....and when it is severed

---

171 Stephen *Digest* 254.

172 See *R v Holloway*, 1 Den. C.C. 370.

173 *R v Ashwell*, 16 Q. B. D. 190 and *R v Lawrence* [1970] 3 All ER 933 935.

174 Kiralfy *Potters* 368 and Dressler *Understanding* 546.

175 Hall DE *Criminal law and procedure* 6th ed (Delmar Cengage Learning New York 2012) 138-139.

176 Singer RG and La Fond JQ *Criminal law* 5th ed (Wolters Kluwer Austin Boston 2010) 273-274.

> from any person or thing to which it was attached in such a manner that the taker has, for however short a time, complete control of it.[177]

Consequently, it is submitted that even a carrying away of property to a distance of 'hair's breadth' is satisfactory.[178] By way of illustration, asportation is required to follow the taking of property. For example, larceny does not arise and is not deemed to arise in circumstances where a thief is found guilty of caption but not asportation.[179] By reason of the aforementioned, both the caption and asportation must be alleged and proved independently.[180]

The trespassory nature of the caption and asportation is deduced from the (wrongful or unlawful) manner in which a property is acquired.[181] The fact that the caption and asportation have the effect of depriving a possessor of possession demonstrates the existence or not of the trespassory taking and carrying away.[182] This view is particularly followed by Pollock and Maitland.[183] They state that larceny involves 'a violation of possession; it is an offence against a possessor and therefore can never be committed by a possessor'.[184] Given the aforementioned, an objective or purposeful inquisition is undertaken. This investigation assists in determining whether or not there is a caption and asportation; the caption and asportation deprives the owner of ownership of the property; and the caption and asportation is contrary to the wishes of an owner.[185]

(b) Absence of Consent or *Invito Domino*

Originally, uncertainty existed regarding the relevance of *invito domino* to the English law of larceny. However, it appears that the study of *invito domino* in Roman law might have motivated its adoption in England. It can be deduced from the works of Bracton

---

177 Stephen *Digest* 246.
178 Hall *Law and procedure* 259.
179 Scurlock J "The element of trespass in larceny at Common Law" 1948 (22) *Temple Law Quarterly* 12-45 12.
180 Scurlock 1948 *Temple Law Quarterly* 12.
181 Scheb *Criminal Law* 169.
182 Brody DC and Acker JR *Criminal law* 2nd ed (Aspen Publishers Gaithersburg 2001) 305. For further interesting reading on the study regarding the deprivation of the possessor of possession of the property see in general *R v Hudson* [1943] 1 K. B. 458.
183 Pollock and Maitland *History of English law* 497.
184 Pollock and Maitland *History of English law* 497.
185 Fletcher *Rethinking* 5-6.

that *invito domino* is essential to the English law of larceny.[186] In particular, Bracton mentions and discusses the concept of *invito illo domino* to his definition of larceny.[187] Therefore, it is argued that Bracton's insistence on *invito domino* influenced the addition of this notion as one of the elements of larceny.

However, the position relating to *invito domino* seems to have changed after 1968. More specifically, section 1 of the Theft Act excludes the fact that the caption and asportation must be without the consent of the owner. This omission is particularly welcomed by some English courts.[188] In particular, the exclusion of *invito domino* in section 1 of the Theft Act is said to be deliberate rather than inadvertent.[189] Accordingly, it is commented that the presence or absence of consent is simply relevant to the question regarding whether or not there was a dishonest appropriation of property.[190] The requisite dishonesty cannot be inferred or implied from the existence of consent to the caption and asportation.[191]

Invito domino relates to the mental state of mind or *mens rea* of a thief at the time that larceny is committed.[192] It requires that both the caption and asportation must be such that the owner or lawful possessor could not have consented or could not be expected to have consented to the taking or carrying away.[193]

(c) *Animus Furandi*

English law jurists differ in relation to the significance or not of *animus furandi* to the study of larceny. Plucknett argues that the early English law of larceny did not rely on intention.[194] As a result of this, the presence or absence of *animus* was insignificant.[195] Fletcher and Blackstone state that *animus furandi* is fundamental to the English law of

---

186 Bracton *Laws and customs* 424.
187 Bracton *Laws and customs* 424.
188 See *R v Lawrence* [1970] 3 All ER 933 and *Lawrence v Commissioner of the Police for the Metropolis* [1971] 2 All ER 1253.
189 *R v Lawrence* 935-936.
190 *R v Lawrence* 936 and *Lawrence v Commissioner of the Police for the Metropolis* 1255-1256.
191 *R v Lawrence* 935.
192 Turner 1942 *The University of Toronto Law Journal* 913.
193 Turner 1942 *The University of Toronto Law Journal 913*.
194 Plucknett *Common law* 447.
195 Plucknett *Common law* 447.

larceny.[196] They disagree however as to the nature and content of the required *animus furandi*. Blackstone submits that *animus furandi* serves or can serve as the replacement of the Roman law principle of *lucri causa faciendi* (for the sake of profit or gain).[197] In particular, the acquiring of property 'for the sake of gain' is, according to Blackstone, tantamount to the obtaining of property feloniously.[198] However, Fletcher opposes the idea that *animus furandi* could be equated with *lucri causa faciendi.*[199] He particularly advocates the idea that the intention to appropriate property is sufficient in order to attract liability for larceny.[200] This appropriation must be accompanied by an intention to steal[201] or, as sometimes declared elsewhere, 'an intent to deprive the owner permanently of his or her property'.[202] Furthermore, it ought to be present at the time that the property is taken or carried away.[203] Consequently, a person (thief) who takes or carries away the property must 'know when he (or she) takes (and carries away) it (property) that it is the property of another person, and he (or she) must take (or carry away) deliberately, not by mistake, and with an intention to deprive the person from whom it taken of the property in it'.[204]

It is established from the discussion above that the English law of larceny emphasises a permanent deprivation as opposed to a temporary deprivation of property.[205] Therefore, permanent deprivation does not apply to things that cannot be physically captured and asported, for example, information.[206] Similarly, permanent deprivation is not extended to property which cannot be or is incapable of being owned, for example, the sky or the water in the seas.

---

196 Fletcher *Rethinking* 6 and Blackstone W *Commentaries on the laws of England* 18th ed (Sweet Maxwell London 1836) 237-232.

197 Blackstone *Commentaries* 237-232. See also, Rapalje S "Larceny distinguished from other offences" 1892 (14) *The Criminal Law Magazine and Reporter* 706 and Turner 1942 *The University of Toronto Law Journal* 297-298.

198 Blackstone *Commentaries* 237-232.

199 Fletcher *Rethinking* 7.

200 Fletcher *Rethinking* 7.

201 S 1(1) of the Larceny Act and s (1) of the Theft Act.

202 S 1(1) of the Larceny Act read with s 1(1) of the Theft Act.

203 Griew *Theft* 11.

204 Turner JWC and Armitage A *Cases on criminal law* 3rd ed (Cambridge University Press London 1964) 452.

205 Brickey 1980 *Vanderbilt Law Review* 1109.

206 *Oxford v Moss* (1979) 68 Cr. App. R. 183 184-186.

In summary, a number of occurrences have had an impact or effect on the development of the English principles of theft. Violent and forceful appropriations and dispossessions of property are examples of such phenomena. However, it is argued that flexible modes of appropriating property of others were introduced in order to respond to the developments that were unique to an English society.[207] These methods came about because of the need to respond to cases where violence or force was not present. This culminated in the establishment of the law of theft. Theft has to do with the dishonest meddling with the property of another.[208] A proper understanding of property that is capable of being stolen creates a split in English literature. More specifically, the difference between the description of theft before and after 1968 is central to this chapter. In both these periods, theft could be carried out in respect of certain incorporeals, for example a debt, legacy, deed, right under a trust or an obligation. However, it is accepted that information that is contained in a document is not property for legal purposes.[209] The basis for this viewpoint is that a physical or actual taking and carrying away of information is impossible.[210] Lastly, English law differentiates between larceny and receiving stolen property. Larceny is the dishonest taking and carrying away of property.[211] It really is not clear whether the taking and carrying away should be accompanied by the desire to derive some gain or benefit from the property. However, it is evident that an intention to meddle with the property could be viewed as an indication that the property was appropriated feloniously or with fraudulent intent.

From the above, it appears that the English law of larceny deals with the fraudulent meddling with corporeal and incorporeal property. It specifically defines the kinds of incorporeals that could form the basis of theft. With a view to accommodate novel developments, the definition of property that is capable of being stolen as contained in the Larceny Act was modified. This then compelled a move towards the inclusion of things, for example a right or obligation in the definition of property. However, other incorporeal things, such as, information, are excluded from this definition. Therefore,

---

207 Dressler *Understanding* 545.
208 Bentham *Limits* 127-128.
209 *Oxford v Moss* 184-186.
210 *Oxford v Moss* 184-186.
211 S 1(1) of the Theft Act.

the position seems to suggest that information is intangible property and that a physical taking and carrying away is consequently not possible.

3.9 SOUTH AFRICAN LAW

3.9.1 Background

The law of theft in South Africa is founded on or originates from a mixed or hybrid legal system.[212] The principles upon which this system is based are a combination of the Roman-Dutch and English legal principles. The Roman-Dutch and English legal systems were transplanted to the Cape of Good Hope during 1652 and 1795 respectively.[213] Following the latter-mentioned, an examination of the principles of theft in South Africa is generally partly Roman-Dutch and partly English.[214] These principles have evolved over the years and were adapted in a number of ways to accommodate new forms of challenges.

In this section the developments of the principles of theft in South Africa are investigated. In undertaking such a study, different nomenclatures that represent the developing of these principles are distinguished. These are, for the purpose of this research, referred to as the traditional and adapted formulations of the principles of theft.

3.9.2 Traditional Description of Theft

---

212 A hybrid legal system is also referred to as the 'mixed legal system'. See MacQueen HL "Two toms and the ideology for Scots Law – TB Smith and Lord Cooper of Culross" in Reid E and Miller DLC (eds) *A mixed legal system in transition: TB Smith and the process of Scots Law* (Edinburgh University Press Edinburgh 2005) 44-72 55. It has primary features of more than one system of law. See Sinatambou E "The approach of mixed legal systems – the case of Mauritius" in Bowman M and Bole A (eds) *Environmental damages in international and comparative law: problems of definition and valuation* (Oxford University Press Oxford 2002) 271-280 271 and Kim K "Mixed systems in legal origins analysis" 2010 (83) *Southern California Law Review* 693-730 696-709.

213 Burchell J "Criminal law" in van der Merwe CG and du Plessis JE (eds) *Introduction to the law of South Africa* (Aspen Publishers The Hague 2004) 447-492 447.

214 Burchell *Criminal law* 447.

The traditional view is that theft is the unauthorised *contrectatio* with the intention to steal property which is capable of being stolen.[215] An intention to steal, that is, *animus furandi*, demonstrates whether or not the *contrectatio* is unlawful or wrongful.[216] Consequently, the *animus* must evidence an 'evil intent' or 'kwaad voornemen' on the part of a thief.[217] In relation to property that is capable of being stolen, a distinction is made between property that is absolutely and those that are relatively incapable of being stolen.[218] The examples of the former category are immovable properties, incorporeal properties (an idea or design) and properties that are common to all (air, water of the sea and public streams).[219] The examples of property which are relatively incapable of being stolen are things that are not owned but can be owned (*res nullius*),[220] one's own property (*res sua*) and wild animals.[221]

The traditional formulation of theft was followed in the case of *R v Larforte.*[222] This case was heard by the then Cape Provincial Division of the High Court. The facts were briefly that the accused broke into another person's (Dr. Abdurahman) garage and took the latter's motor car. The accused drove the car around Cape Town. While still driving, the accused bumped the car into a lamp post and caused damage to it. Thereafter, the accused abandoned the car a couple of streets away from Dr. Abdurahman's garage. In finding the accused guilty of theft, the court concluded that theft encompasses an intention to terminate the owner's enjoyment of his or her right to ownership.[223] In this respect, the court stated that an intention to suspend the owner's enjoyment of his or her right to ownership is inadequate.[224]

---

215 Burchell and Milton *Law* 479. See also Anders PC and Ellson SE *The Criminal Law of South Africa* (Hortor Johannesburg 1917) 264-265 and Maré MC "Public law – criminal law" in Hosten WJ, Edwards AB, Bosman F and Church J *Introduction to South African law and legal theory* 2nd ed (Butterworths Durban 1995) 1082-1125 1125.

216 Gardiner FG *Gardiner and Lansdown: South African criminal law and procedure* 6th ed (Juta Cape Town 1957) 1661.

217 *R v Sibiya* [1955] 4 All SA 312 (A) 418 (hereinafter referred to as *R v Sibiya*).

218 Burchell and Milton *Law* 480.

219 Burchell and Milton *Law* 480.

220 For an exception to the rule that *res nullius* are property that is incapable of being stolen, see the Game Theft Act 105 of 1991.

221 Burchell and Milton *Law* 480 and Gardiner *Criminal law and procedure* 1655-1658.

222 *R v Larforte* 1922 CPD 487 (hereinafter referred to as *R v Laforte*).

223 *R v Laforte* 497.

224 *R v Laforte* 497.

In this chapter, it is argued that the traditional description of theft is problematic. Firstly, the fact that the requisite *contrectatio* must be in respect of corporeal and tangible property is illogical.[225] In particular, it demonstrates a total disregard of the fact that other objects, for example, information, are naturally incapable of being physically touched or handled.[226] Consequently, it fails to recognise that a *contrectatio* in respect of these objects can be achieved even in circumstances where the actual or physical touching or handling is absent.[227] Secondly, the traditional description of theft fails to regulate or deal with cases where the appropriation is temporal. One such a case is *R v Dier.*[228] The aforesaid case dealt with an appeal from a decision of the Magistrate's Court. In this case, Dier wished to cross a particular river (Kowie River). In order to carry out his objective, Dier needed to board a boat. While still deciding on the next step to take, Dier saw that there were ferryboats that were tied to the edge of the river. He untied one of those boats and duly crossed Kowie River.[229] One of the ferryboats was subsequently found damaged the following morning. The question was whether or not the taking of the ferryboat, although it was not permanent, could be prosecuted under the crime of theft.[230] The court answered this question in the affirmative. In particular, Smith J held that:

> I do not intend by anything ..... to lay down that - if a man takes away anything belonging to another and applies it to his own purposes, and then abandons it with a reckless disregard as to whether it is destroyed or not, and it is (so) destroyed – such an act is not criminal. On the contrary, I am of the opinion that a man so acting can clearly be found guilty of theft. [231]

---

225 Burchell and Milton *Law* 543.
226 Burchell and Milton *Law* 543.
227 Burchell and Milton *Law 543*.
228 *R v Dier* (1883-1884) 3 EDC 436 (hereinafter referred to as *R v Dier*).
229 *R v Dier* 437.
230 *R v Dier* 437.
231 *R v Dier* 439 and *R v Fortuin* (1880-1884) 1 Buch AC 290 299 (hereinafter referred to as *R v Fortuin*).

It is imperative to take note that the passage above omits the fact that theft should be committed with the necessary intention to derive a benefit or gain.[232] In particular, Smith J argues that only a fraudulent taking is necessary in order for the law of theft to ensue in South Africa.[233] The fraudulent taking is commonly equated with the notion of *contrectatio fraudulosa.*[234] Therefore, only *contrectatio fraudulosa* leads to theft in South Africa.[235] An enquiry regarding the presence of *contrectatio fraudulosa* requires that one establishes whether or not the requisite intention to deprive an owner of the property exists.[236] If the latter exists, *contrectatio fraudulosa* is inferred from the manner in which the property is dealt with after the taking.[237] Consequently, a person who fraudulently appropriates property and deprives the owner of property is generally liable for theft.[238]

The case of *R v Olivier and Others* also exposed the fallacies that are associated with the traditional description.[239] In this case, the accused (Olivier and others) took property (being a motor vehicle) belonging to another person. They used this property for their purposes and thereafter carelessly abandoned it. The court per Wessels JP stated that it would be an injustice to the innocent party, that is, the owner or lawful possessor:

> (If) our law were otherwise for then it would be no offence for a person who is a stranger to me to take my motor car out of the garage and drive it to Cape Town, leave it at a garage there with as much petrol as it contained, and then write to me that he is off to America and that he only

---

232 *R v Dier* 439. The description of theft by Smith J partially resembles that which is advanced by Gardiner. They provide that 'theft is committed when a person, fraudulently and without a claim of right made in good faith, takes or converts to his use anything capable of being stolen, with intent to deprive the owner thereof of his ownership or any person having any special property or interest therein of such property or interest'. See Gardiner *Criminal law and procedure* 1652.

233 *R v Dier* 439.

234 *R v Murphy and Another* (1990) 20 EDC 62 63 (hereinafter referred to as *R v Murphy*).

235 *R v Lessing* (1907) 21 EDC 220 222 (hereinafter referred to as *R v Lessing*), *R v Makogo* (1915) TPD 516 518 and *R v Murphy and Another* 63.

236 *R v Lessing* 222.

237 *R v Lessing* 222.

238 *R v Fortuin* 299.

239 See *R v Olivier and Others* 1921 TPD 120 125.

> took my car for the temporary purpose of getting to Table Bay in order to catch the boat.[240]

Consequently, the court developed the elements related to 'fraud'. It particularly argued that *contrectatio fraudulosa* depends, or at least should depend, on the existence of an intention to deprive.[241] The requisite intention is deduced from the act itself, that is, the fraudulent appropriation and the subsequent reckless dealing with the property.[242] This is the case because not only is the thing required to be taken without the consent of the owner, but also that 'the taker should have intended to terminate the owner's enjoyment of his (or her) rights'.[243] Intention is generally inferred from various factors, especially those that are related to the reckless dealing with the property.[244]

From the above, it is established that courts in South Africa have accommodated a move away from the traditional approach to theft. In particular, these courts have recognised the need to expand the principles that regulate this crime. This growth has enabled courts to examine some of the external effects that motivate the perpetration of theft.[245] In so doing, courts have denounced the idea of being 'hypnotised by the concrete mechanics by means of which the crime is committed'.[246] However, they adopt a cautious approach when developing these principles.[247] More specifically, they accept that a court's duty is not to create a new crime of theft, or to extend the definition of theft so as to establish novel ways to prevent modern confrontations.[248] The above-mentioned obligation is the responsibility of or is assumed by the legislature. Accordingly, it is simply expected of courts that they adapt the principles of

---

240 *R v Olivier and Others* 125.
241 *R v Olivier and Others* 126.
242 *R v Olivier and Others* 126.
243 *R v Mtshali* [1960] 4 All SA 156 (N) 158 (hereinafter referred to *R v Mtshali*).
244 *R v Mtshali* 158.
245 *R v Sibiya* 325.
246 *R v Sibiya* 325.
247 *R v Sibiya* 321.
248 *R v Sibiya* 321.

theft so that these principles are able to respond to recent societal developments.[249] However, such adaptation should still retain the fundamental components of theft.[250]

3.9.3 Adapted Description of Theft

In recent times, the principles of theft have been expanded. This expansion resulted in the traditional *contrectatio* being discarded in favour of an English law concept of appropriation.[251] Snyman provides justification for the move from *contrectatio* to appropriation in South Africa.[252] He states the following:

> *Contrectatio* might have been a satisfactory criterion centuries ago when the economy was relatively primitive and primarily based on agriculture. In today's world with its much more complicated economic structure, it is far better to use the more abstract concept of appropriation to describe the act of theft than the term *contrectatio*, unless one discards the original meaning of the latter term and uses it merely as a technical *erudite-sounding* word to describe the act of theft.[253]

Appropriation means the intention to 'deprive the owner permanently of the benefits of ownership'.[254] Simply put, it is the assumption of control of or over property of another person.[255] However, control does not translate or extend to a touching or handling of property. It is equated with the gaining of control or possession of property.[256] Furthermore, appropriation must be illegal or wrongful.

This meaning of appropriation has been read by South African courts to also mean that an appropriation in respect of other intangible or incorporeal objects is possible. An example is the case of *S v Graham*.[257] In this case, company (A) was on the verge of being liquidated. During this period, A received a cheque amounting to thirty-seven

---

249 *Phame (Pty) Ltd v Paizes* [1973] 3 All SA 501 (A) 514 (hereinafter referred to as *Phame (Pty) Ltd v Paizes*).
250 *Phame (Pty) Ltd v Paizes* 514.
251 Burchell and Milton *Law* 479.
252 See the definition of theft in Snyman CR *Criminal law* 5th ed (LexisNexis Durban 2008) 483.
253 Snyman *Criminal law* 487.
254 Burchell and Milton *Law* 479.
255 Burchell and Milton *Law* 479.
256 Snyman *Criminal law* 487.
257 *S v Graham* [1975] 3 All SA 572 (A) (hereinafter referred to as *S v Graham*).

thousand one hundred and fifty three rand eighty eight cents (R 7 153.88). It was later established that the cheque was erroneously sent to A. The Managing Director of A (Graham) was aware of such a mistake. However, Graham paid or caused the cheque to be paid to the overdrawn bank account of A. Graham thought that A would recover from its debts and thereafter be in a position to repay the money. However, A was finally wound-up. At the time of its winding-up only a portion of the money was repaid. Graham was charged in his personal capacity with the theft of the cheque and the sum of money paid to A.[258] The question was whether the paying of the cheque into A's account amounted to theft or not.[259] The court conceded that traditionally theft amounts to a physical and actual appropriation of property. In this respect, tangible and corporeal objects, save where these are expressly or impliedly excluded, constitute the aforesaid property. However, the court stated that the principles of theft are founded on a 'living system'. This system is flexible and adaptable. In addition, this flexibility enables the system to be in touch with current realities and to be able to respond to existing societal conditions.[260] Consequently, the court concluded that money is capable of being stolen even in cases where it is represented by entries in books of accounts, for example, credits.[261]

Another development in the law of theft is that which pertains to the appropriation of intangible property, for example electricity and cash represented by a credit entry in books of accounts. These are fully captured in the cases of *S v Kotze*,[262] *S v Mintoor*,[263] *Nissan South Africa (Pty) Limited v Marnitz No and Others (stand 1 at 6 Aeroport (Pty) Limited intervening)*[264] and *S v Ndebele and Others*.[265] These cases acknowledge the impact that recent advances have on the principles of theft. More specifically, the *Nissan South Africa* case followed the reasoning of the court in the

---

258 *S v Graham* 572-575.
259 *S v Graham* 572-575.
260 *S v Graham* 578.
261 See *R v Herholdt and Others* [1957] 3 All SA 105 (A). See also *R v Stanbridge* [1959] 3 All SA 218 (C).
262 *S v Kotze* (1961) 1 SA 118 (SCA) (hereinafter referred to as *S v Kotze*).
263 *S v Mintoor* (1996) 1 SASV 514 (K) (hereinafter referred to as the Mintoor case).
264 *Nissan South Africa (Pty) Limited v Marnitz No and Others (stand 186 Aeroport (Pty) Limited intervening)* (2005) 1 SA 441 (SCA) (hereinafter referred to as the *Nissan South Africa* case).
265 *S v Ndebele and Others* (2002) 1 SACR 245 (GSJ) (hereinafter referred to as the *Ndebele* case).

case of *S v Graham* that the Roman-Dutch law principles of theft are a living system that is 'adaptable to modern conditions'.[266] Therefore, it is no longer possible to apply the traditional Roman-Dutch law principle of *contrectatio* in order to establish if theft has arisen in each case.[267] Appropriation in the sense of an assumption of control over property that belongs to another person is adequate.[268]

The *Ndebele* case is also important in demonstrating the move from the traditional view on theft. In this case, the decision of the court in the *Mintoor* case was criticised.[269] In the *Mintoor* case the court had to decide whether electricity can be an object of theft or not. In responding to this question the court followed the view that things which do not have corporeal existence are incapable of being stolen.[270] Consequently, it was stated that electricity is energy and that energy is incapable of being stolen.[271] Following this reasoning the court in the *Ndebele* case held that *Mintoor* disregarded existing authority and failed to consider the existing developments in the law of theft.[272] The facts in the *Ndebele* case were briefly that: the accused (Ndebele and others) faced a number of charges regarding the theft of vending machines and electricity belonging to Eskom. The position regarding the theft of the machines was easy to determine. These were tangible objects or property and a *contrectatio* or appropriation in relation to them was established. The most difficulty question was whether or not electricity is capable of being stolen. In other words, is *contrectatio* of or over electricity possible? Following the decision in the *Mintoor* case, it was submitted on behalf of the accused that electricity 'could not be stolen'.[273] Before it could comment on this, the court referred to a number of previous court decisions (for example, *S v Kotze*, the *Mintoor* case, the *Nissan South Africa* case and *S v Harper and another*[274]) and surmised:

> It appeared to me that there was a more than slight possibility (which would be more conveniently decided at the end of the case) that

---

266 *Nissan South Africa* case 14.
267 *Nissan South Africa* case 14.
268 *Nissan South Africa* case 14.
269 *Ndebele* case 255.
270 Williams G *Textbook of criminal law* 2nd ed (Stevens & Sons London 1983) 736.
271 *Mintoor* case 515.
272 *Ndebele* case 255.
273 *Mintoor* case 248.
274 *S v Harper and another* (1981) 2 SA 638 (D).

> electricity is in fact capable of theft and that the law had already been advanced by judgements relating, in particular, to theft of incorporeals.[275]

As a result, the court examined the meaning and importance of *contrectatio* for purposes of the law of theft in South Africa. It acknowledged that according to Roman-Dutch law only corporeal or movable things are capable of being stolen.[276] Therefore, property stolen must be ''n selfstandige deel van die stoflike natuur'.[277] However, it applied *S v Harper and another* (where it was said that an incorporeal is capable of being stolen)[278] and held that *contrectatio* is or should not only be constituted by the physical touching or handling of property. It is or should also be constituted by an appropriation of a 'characteristic which attaches to a thing and by depriving the owner of that characteristic'.[279] This is the case because of the following:

> (If) electricity is incapable of being stolen, then anyone would be entitled without permission of the owner to attach a load to his batteries and deplete the energy within them, thereby rendering the batteries useless. Yet nothing will have been stolen. Nothing physically has been taken from the battery; however, its characteristics have changed.[280]

In view of the aforementioned, the court concluded that electricity can, notwithstanding the fact that it only amounts to energy and is incorporeal property, be the object of theft.[281]

In summary, the law of theft in South Africa is a combination of the Roman-Dutch and English legal systems.[282] In examining theft in South Africa, it is distinguished between the traditional and adapted description. The traditional description rests on the premise

---

275 *Ndebele* case 248.
276 Milton JRL *South African criminal law and procedure* 3rd ed (Juta Cape Town 1996) 600.
277 See in general Snyman CR *Strafreg* (LexisNexis Durban 2012).
278 *S v Harper and another* 664.
279 *Ndebele* case 254-255.
280 *Ndebele* case 256.
281 *Ndebele* case 254-255.
282 Burchell *Criminal law* 447.

that theft is a wrongful *contrectatio* with the intention to permanently deprive the owner of the benefits of ownership.[283] In this respect, a *contrectatio* which is made in order to temporarily suspend the benefits of the owner over the property does not amount to theft.[284] The adapted description requires a move from the rigid *contrectatio* to a more flexible appropriation. It is compelled by the idea that a dependence on *contrectatio* disregards the fact that an appropriation of other intangibles, for example information, has nowadays become a reality. This appropriation does not necessarily deprive the owner of information of the benefits of ownership. Simply, a thief could have a copy of the information without actually depriving the owner of the original information. In this respect, a thief possesses the information belonging to the owner.[285] The effect of all this is to deny the owner the exclusive use and enjoyment of the information. The adapted description of theft assists in making a case to the effect that a theft of information is necessary in South Africa. This theft deprives the owner of the full benefits of ownership. These benefits are the control, use and enjoyment of information. In view of this, regard is had to *S v Graham* where it was stated that the principles of theft are generally founded on a living system of rules.[286] This system is flexible and can be altered in order to conform to contemporary societal developments or challenges.[287] However, this adaptation has to minimal,[288] in the sense that it should not be so severe and relentless that these principles lose their meaning and importance in criminal law.[289]

3.10 CONCLUSION

The law of theft is generally a dynamic and flexible field. It is particularly adaptable to change and it is receptive to modifications. This flexibility was observed in the discussion of *furtum* in Roman-Dutch law. On the one hand, the Roman law of theft followed the viewpoint that *furtum* related to the dishonest *contrectatio* of or over property. Given this, only things that were capable of being physically touched or

---

283 Burchell and Milton *Law* 479. See also Anders and Ellson *Criminal law* 264-265 and Maré *Law* 1125.
284 *R v Laforte* 497.
285 Snyman *Criminal Law* 487.
286 *S v Graham* 578.
287 *S v Graham* 578.
288 *R v Sibiya* 321.
289 *Phame (Pty) Ltd v Paizes* 514.

handled were regarded as property for this purpose. Because information could not be touched, it was excluded from the categories of things that were capable of being stolen.[290] Accordingly, a *contrectatio* over information held by another person was deemed to be impossible. The latter view is supported by the notion that *furtum* constituted an *autem fit non solum cum quis intercipiendi causa rem alienam amouet, sed generaliter cum quis rem alienam invito domino contrectat*.[291] This can be translated to mean that a touching or handling of property, on its own, is satisfactory for *furtum* to arise.[292] On the other hand, the Dutch law recognised that *furtum* did not always amount to a permanent deprivation of property. Consequently, theft could also be committed in cases where there was a temporal deprivation of property. The significance of this is that e-crimes result in a temporal or partial deprivation of information belonging to a person. Therefore, a person does not necessarily have to be deprived of the original information in order for e-crimes to be carried out completely. The manner in which the aforementioned happens or is carried out is explained in chapter 4 below.

The adaptability of the law of theft is also acknowledged in England and South Africa. In England, matters external to larceny, for example, agriculture and industrialisation necessitated that the principles that govern theft should be re-arranged. These modifications were necessitated by the inability of the traditional principles to regulate these external factors. In South Africa courts have also commenced an investigation into the essence and principles of theft. They consequently found that these principles originated from a 'living' and elastic system of law. This elasticity means that the principles can be adapted or modified with a view to make them compatible with current social realities and challenges.[293] However, the courts have cautioned that a process to alter and develop the principles of theft should be negligible.[294] More specifically, this process ought not to be so stringent and unremitting that it renders the elements of theft meaningless and insignificant to the discussion of criminal law.[295]

---

290 Burchell and Milton oppose and condemn this view. See Burchell and Milton *Law* 543.
291 G III.195.
292 Jolowicz *De furtis xvii*.
293 *S v Graham* 578.
294 *R v Sibiya* 321.
295 *Phame (Pty) Ltd v Paizes* 514.

Based on the above-mentioned, it is submitted that the principles of theft should be adapted and developed so as to deal with the appropriation of other intangibles, such as information. More specifically, this research follows the suggestion by Snyman that there is currently a need to move away from the rigid *contrectatio*.[296] This is specifically the case because e-crimes have emerged that resemble theft or *furtum*. Although these e-crimes mimic these traditional crimes, they are perverse and their reach is far more elongated than offline crimes. The National Research Council puts it bluntly and states that 'the modern thief can steal more with a computer than with a gun'.[297] Furthermore, e-crimes do not necessarily lead to the actual taking and carrying away of information. Simply, they result in the wrongful interference or meddling with the information of another. This meddling does not always pertain to the entire information. It can arise in situations where a person is only dispossessed of the part or copy of the information without the latter's consent. With this in mind, it becomes necessary to develop the law of theft in a manner that accelerates a response to the challenges that are posed by e-crimes to the information society. In particular, it has to be recognised that e-crimes and the techniques that are normally used in e-crimes constitute the modern risks to the information society.

Because of this, e-crimes are discussed in chapter 4 below. In discussing e-crimes, it is accepted that crimes are vast. They particularly differ in form and content. Thus, it is conceded that an examination of all the crimes that are carried out online will be impossible to achieve in this research. This is the position because the emergence of new forms of technologies brings about a change in the nature of e-crimes and the methods of attacks criminals follow. Therefore, the most common of e-crimes, for example computer cracking, denial of service (DDOS) attacks, man-in-the-middle attacks and phishing, are investigated. This selection supports the view that a theft of online information is possible.

---

296 Snyman *Criminal law* 487.

297 National Research Council *Computers at risk: safe computing in the information age* (National Academy Press Washington DC 1991) 7.

CHAPTER 4

THE STUDY OF E-CRIMES

CHAPTER 4

THE STUDY OF E-CRIMES

4.1 INTRODUCTION

In chapter 3 the stages of development of the principles of theft were investigated. These are the Roman-Dutch, English and South African law approaches to theft. It was submitted that the principles of theft generally form part of a living system of laws. This system is flexible and can be modified in a way that accommodates other societal developments. Given this elasticity, *contrectatio* as an element of *furtum* may no longer have the same significance it traditionally had in Roman-Dutch law. Accordingly, it may be necessary to improve the aforesaid element in a manner that also considers a fraudulent appropriation of information as theft. Furthermore, it was argued in chapter 3 that appropriation as opposed to *contrectatio* can be appropriate in studying theft and the challenges that are posed or generated by ICTs. Costa discusses the 'emerging challenges' of recent technologies.[1] He states that the 'presence of ICT in societies is pervasive, which makes crimes, especially ICT-related crimes, a constituent aspect of the wider political, social and economic restructuring currently affecting countries worldwide'.[2]

In this chapter it is submitted that ICTs present opportunities for criminals to commit crime. In the main, criminals rely on recent technologies to refine and purify their *modus operandi*.[3] In addition, criminals use modern forms of technologies as a vehicle to transform the manner of committing the traditional crimes, for example, *furtum* or theft.[4] Downing lists three distinct circumstances in which these technologies may be

---

1 Costa AM "Emerging challenges" in Savona EU (ed) *Crime and technology: new frontiers for regulation, law enforcement and research* (Springer Dordrecht 2001) 1-6 1.

2 Costa *Crime and technology* 4.

3 Savona EU and Mignone M "The fox and the hunters - how ICT technologies change the crime race" in Savona EU (ed) *Crime and technology: new frontiers for regulation, law enforcement and research* (Springer Dordrecht 2004) 7-28 8.

4 Sussmann MA "The critical challenges from international high-tech and computer-related crime at the millennium" in Carr I (ed) *Computer crime* (Ashgate Publishing Limited Surrey 2009) 379-418 379-381.

used as a tool to commit crime.[5] He submits that ICTs may be used as an instrument to perpetrate offences, as a target for criminals to attack and carry out attacks or as storage machinery which is exploited in order to preserve information related to crime.[6]

The dependence on current technologies in order to commit conventional crimes leads to the emergence of e-crimes. E-crimes are a 'migration of real-world crime (or crimes) into cyberspace'.[7] The examples of e-crimes are vast. These include cyber-terrorism, cyber-extortion, harassment, cyber-bullying, online predators and cyber-stalking. In this research, computer cracking, distributed denial of service (DDoS) attacks, man-in-the-middle attacks and phishing are examined. This selection is made because the aforementioned e-crimes demonstrate the manner in which criminals devise methods of stealing information online.

4.2 COMPUTER CRACKING

4.2.1 Background

In earlier times, 'computer hackers' were an assemblage of computer experts and what Raymond refers to as 'Real Programmers'.[8] In particular, they were formerly harmless people who were associated with Open-Source development.[9] In this instance, hackers would continuously test and evaluate the security of computer or information systems or networks.[10] In order to do this, they launched attacks against a system or network.

---

5 Downing RW "Shoring up the weakest link – what lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime" in Carr I (ed) *Computer crime* (Ashgate Publishing Limited Surrey 2009) 4-72 9.

6 Downing *Weakest link* 9.

7 Brenner SW "History of computer crime" in de Leeuw K and Bergstra J (eds) *The history of information security: a comprehensive handbook"* (Elsevier Amsterdam 2007) 705-721 706.

8 Raymond ES *The cathedral and the bazaar: musings on linux and open source by an accidental revolutionary* (O'Reilly and Associates Beijing 2001) 3-4.

9 For a definition of the term 'open source' see Perens B "The open source definition" in DiBona C, Ockman S and Stone M (eds) *Open sources: voices from the open source revolution* (O'Reilly and Associates Beijing 1999)171-188 176-180. Open Source is the opposite or precursor to 'Free Software'. See Raymond ES "The revenge of the hackers" in DiBona C, Ockman S and Stone M (eds) *Open sources: voices from the open source revolution* (O'Reilly and Associates Beijing 1999) 207-219 212.

10 A description of computer or information systems or networks does not refer only to computer hardware (physical technology that houses and executes the software, stores and transport data). It also refers to a set of software (applications, operating systems and assorted command utilities), data, computer users and procedures to carry out certain tasks. See Whitman ME and Mattord HJ *Principles of information security* 4th ed (Cengage Learning Australia 2012) 16.

These attacks included acts that take advantage of vulnerability in controlled or regulated systems or networks.[11] The goal was not to destroy the systems or networks. Instead, the attacks were aimed at exposing and identifying limitations or vulnerabilities in existing computer security protocols.[12] In cases where vulnerability was detected, computer hackers would re-design the system or network.

However, we have in the recent past come to know of computer hacking (originally, computer cracking)[13] as an activity whereby information belonging to a computer user (victim)[14] is altered or retrieved dishonestly.[15] This change in the meaning of computer hacking represents a stage wherein 'serious cracking episodes were first covered in the mainstream press – and journalists began to misapply the term hacker to refer to computer vandal'.[16] Given these developments, the term 'computer cracking' or 'computer cracker' is preferred in this research.

4.2.2 Method of Attack

In computer cracking schemes, the security (or lack thereof) of information systems or networks is exposed or sought to be exposed. In order to do this, a computer cracker infiltrates and infects a victim's computer with computer viruses[17] or worms.[18] Most of

---

11 Whitman and Mattord *Principles of information security* 63.

12 Gupta MS *Cyber crimes* (Centrum Press New Delhi 2013) 2 and Bossler AM and Burruss GW "The general theory of crime and computer hacking - low self-control hackers?" in Holt TJ and Schell BH (eds) *Corporate hacking and technology-driven crime: social dynamics and implications* (Information Science Reference Hershey 2011) 38-67 40.

13 Simply put, the difference between hackers and crackers is that hackers built information systems or networks and crackers break these. See Raymond *Cathedral and the bazaar* 196-197.

14 For purposes of this research, the term 'victim' refers to governments, companies (private or public), financial or payment services providers and computer users that are targets of e-crimes.

15 Summers D (ed) *Longman dictionary of contemporary English* 3rd ed (Longman Harlow Essex 1995). See also Fraud Advisory Panel Cybercrime Working Group "Recent attack trends" in Reuvid J (ed) *The secure online business handbook: a practical guide to risk management and business continuity* 4th ed (Kogan Page Limited London 2006) 5-10 6. See also s 86(1) and (2) of the ECT Act.

16 See Raymond *Cathedral and the bazaar* 3-4.

17 Computer viruses consist of a number of codes. These codes carry out illegal actions on computer systems or networks. They operate more like the viral pathogens that attacks humans, animals and plants. See Whitman and Mattord *Principles of information security* 44 and Gordon BJ "Internet criminal law" in Buys (ed) *Cyberlaw @ SA: the law of the Internet in South Africa* (Van Schaik Publishers Pretoria 2000) 426.

these viruses or worms are created and transported cheaply and effortlessly. Accordingly, they can be sent over local systems or networks or be carried out on a removable medium, for example a CD, DVD or USB modem.[19] As soon as a system or network is infiltrated with viruses or worms, a computer cracker then takes control of victims' computer systems or networks.[20] Thereafter, they deliberately and maliciously appropriate victims' personal or sensitive particulars. This theft occurs in circumstances where a victim is not even aware that his or her computer is being accessed unlawfully.[21]

Figure 4.1 below demonstrates how victims' computer or information systems or networks are normally cracked.[22]

---

18 Computer worms are a set of malicious programmes. They generate other programmes within information systems or networks. See Whitman and Mattord *Principles of information security* 45-46 and Forst ML *Cybercrime: Appellate court interpretations* (Montclair Enterprises San Francisco 1999) 133.

19 CIFAS http://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/Digital_Thieves_October2010.pdf (Date of use: 20 August 2012).

20 Sciglimpaglia RJ "Computer hacking - a global offense" 1991 (3) *Pace International Law Review* 199-266 200-201.

21 LIoyd I *Legal aspects of the information society* (Butterworths London 2000) 100 and Singh N "Digital economy" in Bidgoli H (ed) *Handbook of information security: threats, vulnerabilities, prevention, detection, and management* (John Wiley New Jersey 2006) 15-36 31. See also Commission of the European Communities "Proposal for a Council framework decision on attacks against information systems" 19 April 2002 (hereinafter referred to as COM (2002) 173). To be accessed at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52002PC0173&from=EN.

22 Fig 4.1 is inspired by the discussion of computer cracking which is made by Bossler and Burruss. See Bossler and Burruss "The general theory of crime and computer hacking - low self-control hackers?" 40-41.

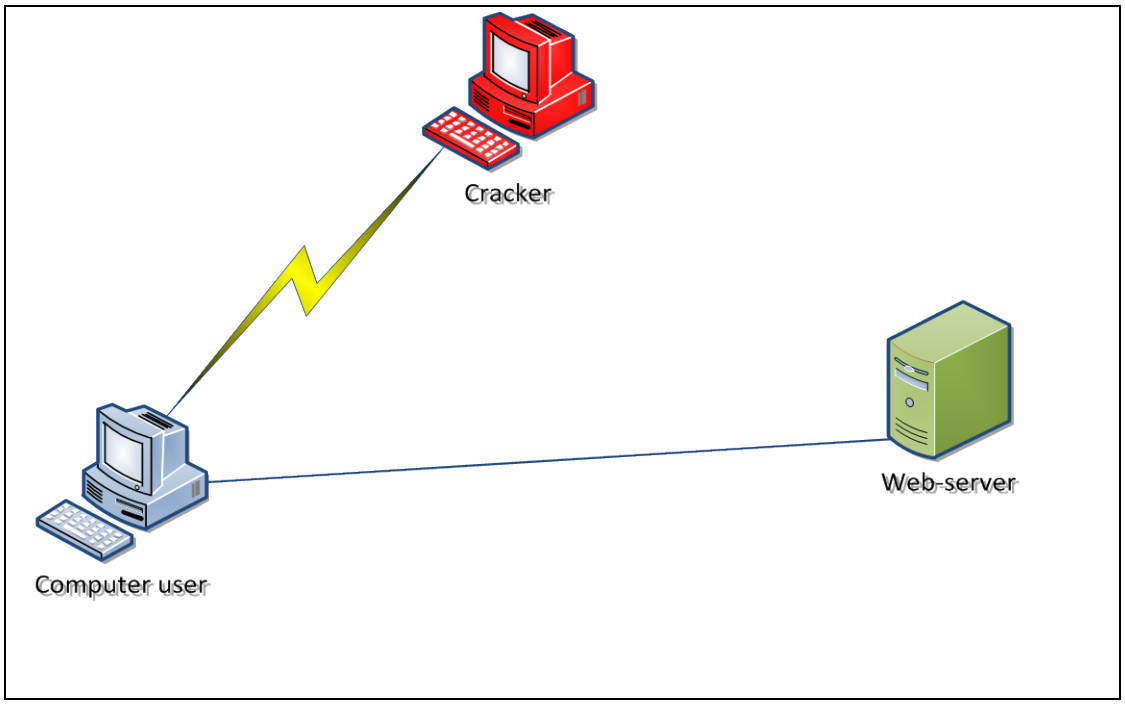

Figure 4.1: A typical computer cracking procedure

In figure 4.1 above the original connection between a computer user (victim) and Web-server is shown. This is the connection which usually facilitates the communication between a victim and the outside world. In addition, it enables a transfer of information from the Web-server to a victim. In figure 4.1 above a typical computer cracker monitors the communication. It then attacks the victim's computer system or network with a view to access and to intercept information.[23] It is noteworthy that the victim is not necessarily dispossessed of the original contents of the information. Furthermore, it is commonly difficult and sometimes impossible to establish whether or not particular information has moved from the victim to the cracker, that is, an unlawful appropriation has taken place.

4.3 DDOS ATTACKS

4.3.1 Background

[23] Bossler and Burruss "The general theory of crime and computer hacking - low self-control hackers?" 40-41.

DDoS attacks are sometimes described as the 'mischievous attacks'.[24] This mischief is attributed to the fact that these attacks make or renders the targeted systems or networks 'unusable or inaccessible'.[25] Furthermore, the harm is associated with the fact that the attacks cause 'catastrophic errors' that interrupt the proper functioning of a system or network.[26] Immediately after the aforementioned occurs, computer crackers gain entry into the system and steal information.[27]

Furthermore, DDoS attacks are generally pervasive. Their scope and effect extends beyond borders. In other words, they can be started or commenced in one or different locations and their adverse impact can be felt by victims in other localities.[28] Also, the affected or targeted systems or networks do not have to be situated in a single jurisdiction. They can be located or situated in diverse jurisdictions as well.[29]

4.3.2 Method of Attack

In carrying out DDoS attacks, a computer cracker generally sends a number of connections or information requests to victims. These can be requests for information, or requests that victims enter their sensitive or secret credentials to certain allocated spaces. A promise is often made to victims that such entering will entitle them to a specific benefit, normally money.[30] Most DDoS attacks overloads or burdens the targeted systems or networks with a number of requests.[31] As a result, they interrupt the appropriate functioning of a system or network and afterwards deny victims the lawful or legitimate accessing of information or documents stored in a computer.[32] Thereafter, computer crackers access the system without the consent of the victim and steal information. Figure 4.2 below illustrate the manner and form of DDoS attacks.

---

24 Schwabach A *Internet and the law: technology, society and compromises* (ABC-CLIO California 2006) 83.

25 Kessler GC and Levine DE "Denial-of-service attacks" in Bosworth S, Kabay ME and Whyne E (eds) *Computer security handbook* 5th ed (John Wiley and Sons New Jersey 2009) 18.1-18.28 18.1. See also s 86(5) of the ECT Act.

26 Kessler and Levine *Attacks* 18.1.

27 Kessler and Levine *Attacks* 18.1.

28 Schwabach *Internet and the law* 83.

29 Schwabach *Internet and the law* 83.

30 Whitman and Mattord *Principles of information security* 67-68.

31 Schwabach *Internet and the law* 83.

32 Schwabach *Internet and the law* 83.

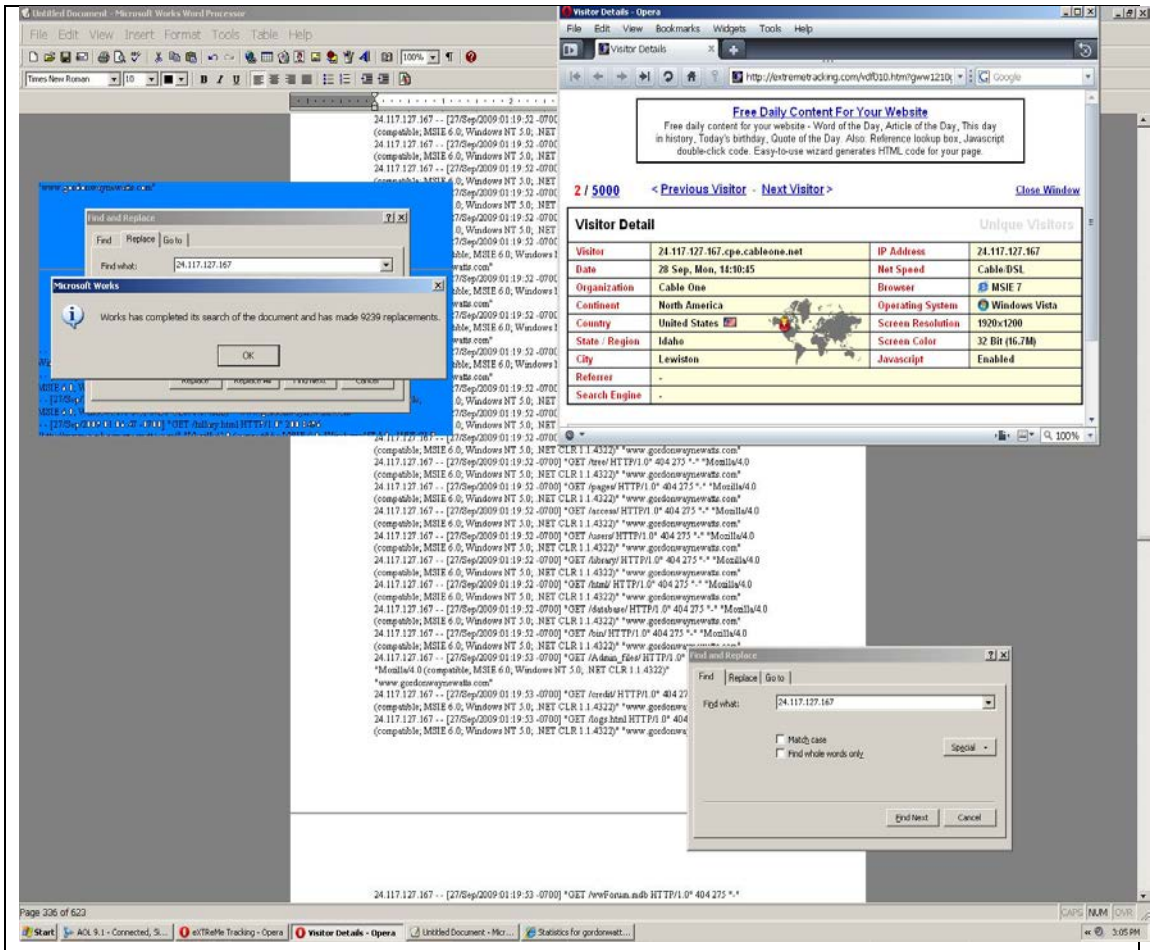

Figure 4.2: DDoS attack appears in what seems to be Webpage.

In figure 4.2 above a page, file or document which resembles that which victims ordinarily works on is shown. The number of messages that appear on top of the page, file or document are also demonstrated. The messages masquerade as genuine software[33] applications that are relevant to the security of victims' computer systems or networks. They sometimes resemble those that a computer user normally receives from his or her Web administrator. In these messages victims are informed about a particular software that is necessary for the security of their computer systems or networks. Victims are also assured that the presence of this software is indispensable as it assists in the installation or downloading of conventional information security

[33] This may be component of the information system and has applications, operating systems and assorted command utilities. See Whitman and Mattord *Principles of information security* 16.

facilities. In addition, the messages request victims to enter or punch-in their sensitive information or particulars from certain allocated spaces. The victim is consequently denied access to work on a document or file until the requested information is entered.

4.4 MAN-IN-THE-MIDDLE ATTACKS

4.4.1 Background

Man-in-the-middle attacks are sometimes referred to as the transport control protocol or (TCP) hijacking attacks.[34] These attacks take place in situations where a computer cracker takes control of an information system or network.[35] This is made by forcing a system or network to operate in a manner intended to by a computer cracker. In carrying out these attacks, a computer cracker operates between computers.[36] These can be computers that are used by computer users in one location or those that are operated by computer users in different jurisdictions.

Furthermore, man-in-the-middle attacks generally attack and compromise a computer or the Internet or other local area networks (LANs) or Web-server.[37] As soon as these networks are compromised, computer crackers eavesdrop and monitor the communication, information which passes through from the Web-server to the victims. This monitoring enables computer crackers to illegally appropriate sensitive or useful information that belongs to the victims.

4.4.2 Method of Attack

In man-in-the-middle attacks, a computer cracker would turn a victim's computer into a 'zombie'. Once this happens, a computer cracker then controls and takes charge of a computer. Consequently, the cracker can change, delete, reroute, add, forge or divert information which is stored in a victims' computer system or network. Furthermore, it can access, control and divert information to use other than that intended for by victims.

---

34 Whitman and Mattord *Principles of information security* 66-67.

35 S 86(4) of the ECT Act.

36 Strebe M *Network security jumpstart: computer and network security basics* (SYBEX Inc. Alameda 2002) 41.

37 Strebe *Network security* 41. See also COM (2002) 173.

Figure 4.3 below illustrates the manner in which man-in-the-middle attacks are commonly carried out.[38]

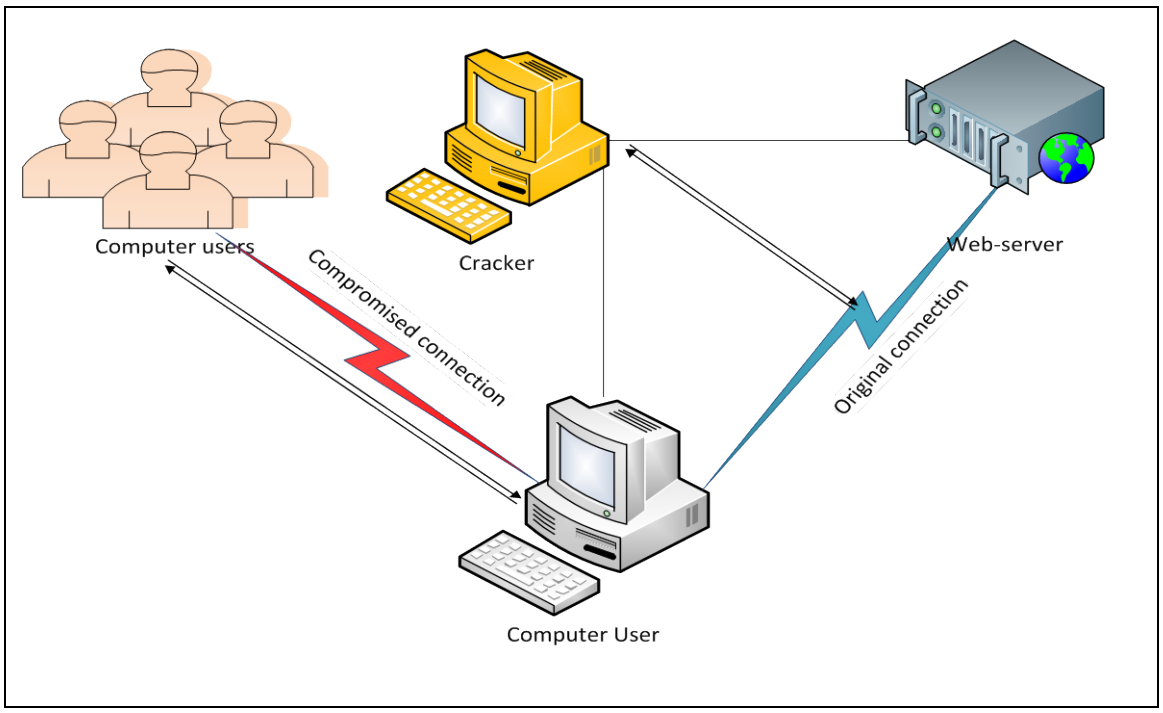

Figure 4.3: Caption

In figure 4.3 above a computer cracker is situated between the Web-server and the computer which is used by victims. In one case, it monitors the information which passes through from the Web-server to a victim's computer. In other cases, it interrupts the connection between a victim and the Web-server and intercepts information belonging to a victim. The compromised or cracked connection does not only affect a victim. It also has an impact on other computer users that have relations with or are connected to victims' computers.

4.5 PHISHING

4.5.1 Background

---

[38] Exhibits 18.1 and 18.4 in the handbook by Kessler and Levine had an influence in the structure of figure 4.3. See Kessler and Levine *Attacks* 18.8. See also, Ornaghi http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-ornaghi-valleri.pdf (Date of use: 13 August 2013).

It is often said that phishing is a completely recent occurrence.[39] In particular, the criminal attacks on the American Online Network systems, that is, the AOL attacks, are identified as the first phishing attacks ever witnessed worldwide.[40] Consequently, it is stated that phishing gained worldwide recognition or prominence immediately after the AOL attacks.[41] The AOL attacks included scams whereby information or particulars, for example usernames and passwords, belonging to various computer users were intercepted.[42]

Despite the perceived novelty of phishing, it appears however that the trends that are used for phishing are old.[43] More specifically, comparable phishing activities can be traced back to ancient Rome.[44] In one case, a scrutiny of *dolus malus* illustrates the ancient nature of the trends.[45] Literally, *dolus malus* denotes fraud or dishonesty where treachery is precipitated.[46] Fraud or *fraus* in the sense in which the word was applied in Roman law denoted an intelligent trick, deception or machination.[47] The trick, deception or machination had to be made in order to induce another to do something which is different to that which was primarily professed.[48] *Dolus malus* is also applied by South African courts in certain circumstances. For example, cases dealing with

---

39 Sullins LL "'Phishing' for a solution – domestic and international approaches to decreasing online identity theft" in Carr I (ed) *Computer crime* (Ashgate Publishing Limited Surerey 2009) 73-109 77-78 and Myers S "Introduction to phishing" in Jakobsson M and Myers S (eds) *Phishing and counter-measures: understanding the increasing problem of online identity theft* (John Wiley New Jersey 2007) 1-30 2-3.

40 Sullins *Computer crime* 77-78.

41 Whitman and Mattord *Principles of information security* 72.

42 Dunham K (ed) *Mobile malware attacks and defence* (Syngress Publishing Inc. Burlington 2009) 127.

43 The story of Jacob in the Bible is one of the classical examples wherein an identity of a person may be stolen. See Genesis 27:1-40. In the aforementioned case, Jacob, who was motivated by greed and envy, misrepresented his blind father (Isaac) into believing that he (Jacob) was his brother (Esau). The aim was to steal away the blessings that were meant for Esau. See Genesis 27:19-29.

44 See in general Smith W and Anthon C (eds) *A dictionary of Greek and Roman antiquities* 3rd ed (Harper New York 1870) and Fantham E "With malice aforethought – the ethic of *militia* on stage and law" in Sluiter I and Rosen RM (eds) *Kakos: badness and anti-value in classical antiquity* (Brill Leiden 2008) 319-334.

45 In its entirety, the concept of *dolus malus* is referred to as *dolus malus est omnis callidity fallacia, machination ad circumveniendum, fallendum, decipiendum alterum adhibita.*

46 Fantham *Malice aforethought* 331. The accepted Roman law term is *totus ex fraude et mendaciis studio et artificio quodam malitiae condivisset*.

47 Frier BW and McGinn TAJ *A casebook on Roman family law* (Oxford University Press Oxford 2004) 483. See also *Kazazis v Georghiades* (1979) 3 TPD 886 892 (hereafter referred to as *Kazazis v Georghiades*).

48 Smith and Anthon *Greek and Roman* 164.

misrepresentation,[49] undue influence[50] and breach of contract[51] demonstrate such application. In South Africa, *dolus malus* amounts to anything which the law does not sanction. This extends to everything which is unwarranted and is carried out with the comprehension that one is acting contrary to the 'law or good faith'.[52]

In other cases, the principles of *crimen injuria* are applied to occurrences that are comparable to phishing. *Crimen injuria* is an act or conduct which impairs a person's *dignitas*.[53] *Dignitas* is one of the interests of personality which is protected under the *actio inuriarum*. The other interests of personality are *corpus* and *fama*. *Dignitas* is a wider notion than *corpus* and *fama*. It particularly encapsulates *corpus* and *fama.*[54] The famous South African case of *R v Umfaan*[55] provides meaning to the notion of *dignitas*. In *R v Umfaan* the following was stated about *dignitas*:

> (Every) person has an inborn right to the tranquil enjoyment of his (or her) peace of mind, secure against aggression upon his (or her) person, against the impairment of that character for moral and social worth to which he (or she) may rightly lay claim, and of that respect and esteem of his (or her) fellow-men (or women) of which he (or she) is deserving, and against the degrading and humiliating treatment; and there is a corresponding obligation incumbent on all others to refrain from assailing that to which he (or she) has such right.[56]

The necessity to safeguard the 'tranquil enjoyment of a person's peace of mind' was also acknowledged in another South African case of *S v A*.[57] The parties in *S v A* were Mr Swartzberg (the Complainant), the wife of Mr Swartzberg (the First Appellant) and

---

49 See in general *Macduff & Co Ltd (in liquidation) v Johannesburg Consolidated Investment Co Ltd* 1924 AD 573 (hereinafter referred to as *Macduff & Co Ltd (in liquidation) v Johannesburg Consolidated Investment Co Ltd*).

50 See *Preller v Jordaan* 1956 1 AD 483.

51 See *Kazazis v Georghiades* 892-893.

52 *Macduff & Co Ltd (in liquidation) v Johannesburg Consolidated Investment Co Ltd* 610 and *Jajbhay v Cassim* 1939 AD 537 551.

53 Burchell J and Milton J *Principles of criminal law* 3rd ed (Juta Lansdowne 2005) 748.

54 *O'Keeffe v Argus Printing and Publication Co Ltd* 1954 3 SA 244 (C) and Neethling J, Potgieter JM and Visser PJ *Law of delict* 2nd ed (Butterworths Durban 1994) 13-17.

55 See in general *R v Umfaan* 1908 TS 62 (hereinafter referred to as *R v Umfaan*).

56 *R v Umfaan* 67.

57 See *S v A* (1971) 2 TPD 293 (hereinafter referred to as *S v A*).

Tel Peda Investigation Bureau (the Second Appellant). The Complainant and the First Appellant were married to each other. However, they had, due to other factors, separated from each other. The Complainant was thus living alone in a block of apartment flats. The First Appellant was, at all reasonable times, suspicious of the Complainant's activities. In particular, she suspected that the Complainant had extra-marital affairs. By reason of this suspicion, the First Appellant instructed another person (Kenneth Mills) to manufacture a spying device (the device). As soon as it was produced, the device was to be installed or fitted inside the complainant's apartment flat. The aim was to enable the First Appellant and Kenneth Mills to listen to various conversations of the Complainant, and possibly those of his mistresses. Kenneth Mills followed and carried out the First Appellant's instructions and handed the device to the Second Appellant. The Second Appellant thereafter caused the device to be hidden underneath a 'vanity drawer' in the Complainant's apartment flats.[58] The Complainant discovered the device when he was opening the drawer. From the Complainant's viewpoint, the device appeared to be a 'transmitting bugging device'.[59] On apprehending the intended purpose of the device, the Complainant alleged that he felt 'terribly indignant and hurt' because his privacy had been compromised.[60] In view of this, the Complainant opened a case against the First and Second Appellants for *crimen injuria.* The court stated that the prevailing *boni mores* in accordance with public opinions were essential. The requisite *boni mores* particularly demonstrated, the court held, whether or not the conduct or action in question impairs a person's *dignitas*. In view of the aforementioned, the court concluded that the actions of the First and Second Appellants were of such a nature as to amount to an impairment of the Complainant's *dignitas.*[61] The First and Second Appellants' actions were of such a reprehensive nature that they deserved punishment.[62]

From the above-mentioned we can extrapolate that although the notion of phishing is new practices always existed however that were comparable to phishing. They varied depending on the time or place and the object to be exploited. For example, in the biblical story of Jacob the object of theft was the blessings that were intended for Esau and in the case of *S v A* the reason was to intercept and listen to the victim's

---

58 *S v A* 295.
59 *S v A* 295.
60 *S v A* 295.
61 *S v A* 297-299.
62 *S v A* 299.

conversations. However, in recent times ICTs have extended the scope of application of these practices. They particularly augment the methods that were traditionally used for phishing. As a result, computer crackers possess innovative ways that ease the burden of cracking or breaking systems or networks. Consequently, they are able to 'communicate, to organise themselves better, to widen the spectrum of their businesses, to update their *modus operandi* and techniques, and to avoid law enforcement'.

Having identified the complexities that are created by contemporary technologies, it is now essential to explicitly describe the boundaries within which phishing operates. By doing this, it is contemplated that such a description will assist in distinguishing phishing from the other e-crimes. However, such a description acknowledges that computer crackers usually conduct themselves in ways comparable to those of people who are in business. Their concerns are to decrease their expenditure and maximise the proceeds which originate from phishing.[63]

4.5.2 Conception of Phishing

Academics disagree as to the foundation of the concept of 'phishing'. Some are of the opinion that the notion of phishing was formulated following the phone cracking scams called 'phreaking'.[64] Phreaking, it is argued, has particular resemblance with computer cracking.[65] Phreaking is an unauthorised accessing[66] of a telephone system.[67] The accessing enables the cracker to direct a telephone system to make lengthy and free telephone-calls; to alter the appropriate operation of a telephone service; to steal

---

63 Sullivan D *The definitive guide to controlling malware, spyware, phishing, and spam* (Realtime publishers.com San Francisco 2006) 32.

64 Schwabach *Internet and law* 235.

65 Moore R *Cybercrime: investigating high-technology computer crime* 2nd ed (Anderson Publishing Oxford 2011) 42-43.

66 'Unauthorised access' refers to the accessing, interception or misusing of a system, resource, file, or database without the requisite lawful authority. See Kapoor N *Computerised banking system in India* (Sublime Jaipur 2008) 16 and Gattiker UE *The information security dictionary: defining the terms that define security for e-business, internet, information and wireless technology* (Kluwer Academic Publishers New York 2004) 3.

67 Schwabach *Internet and law* 235.

specialised telephone services, and to cause disruptions to a telephone service.[68] There are also those who hold the viewpoint that the term 'fishing' has particular influence on the notion of 'phishing'.[69] Minnaar is specifically the follower of this proposal.[70] According to Minnaar, the expression 'phishing' is 'derived from 'fishing' i.e. baiting the hook (the temptation and the believable convincing solicitation (approach) and throwing in your fishing line (e-mailing the tempting offer) and go fishing and see what you can catch (a gullible victim's identity details)'.[71]

The opinion by Minnaar above seems to stem from the understanding that the trends or methods that are used in phishing are comparable to those of a fisherman.[72] In fishing activities, for example a fisherman entices a fish by concealing the menacing nature of the emblematic methods that are used.[73] These emblematic techniques are commonly referred to as the 'lure', the 'hook' and the 'catch'.[74] Figure 4.4 demonstrates how the aforesaid methods operate in phishing schemes.[75] They are demonstrated by reference to certain phases (phases 1, 2 and 3) that are considered to be fundamental in completing the crime of phishing.

---

68 Stewart JM, Chapple M and Gibson D *Cissp: certified information systems security professional study guide* (John Wiley San Francisco 2005).

69 Gorge M and Brudenall P "Phishing, pharming and the requirement for strong user authentication" in Reuvid J (ed) *The secure online business handbook: a practical guide to risk management and business continuity* 4th ed (Kogan Page London 2006) 91-94 91.

70 Minnaar A "You've received a greeting e-card from.... – the changing face of cybercrime email spam scams" 2008 (2) *Acta Criminologica* 92-116 99.

71 Minnaar 2008 *Acta Criminologica* 99.

72 Brown BC *How to stop e-mail spam, spyware, malware, computer viruses and hackers from running your computer or network: the complete guide for your home and work* (Atlantic Publishing Group Florida 2011) 32.

73 Wehmeier S et al *Oxford advanced learner's dictionary of current English* 7th ed (Oxford University Press Oxford 2005) 581.

74 Myers *Counter-measures* 5-6.

75 Garber L "Denial-of-service attacks rip the Internet" 2000 *Technology news* 1-17 15.

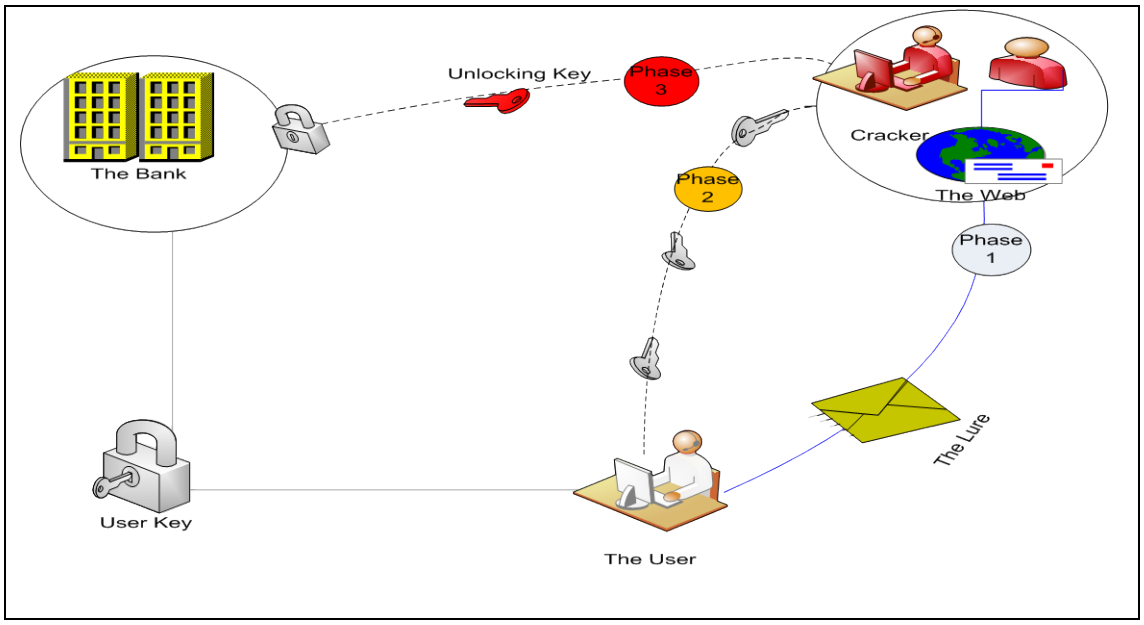

Figure 4.4: Phishing scheme

Phase 1 in figure 4.4 above represents the lure. The bank is used as an example in order to represent the ultimate object of phishing, that is, where money is. The user key signifies the login details or identifying information or particulars, for example pins or passwords. In this instance, a computer cracker monitors the online activities or sessions of a user. It can do this by either situating itself in the Web (Website) or by breaking the connection which a victim has with other users and the bank. Once this happens, it may hijack these activities or sessions (session hijacking) and masquerade as a genuine computer user. This is normally done by infiltrating the Web with malicious messages (malware) or requests. Sometimes a computer cracker will send message requests to a user that impersonates those of genuine institutions. The example of these messages is illustrated in figure 4.5 below.

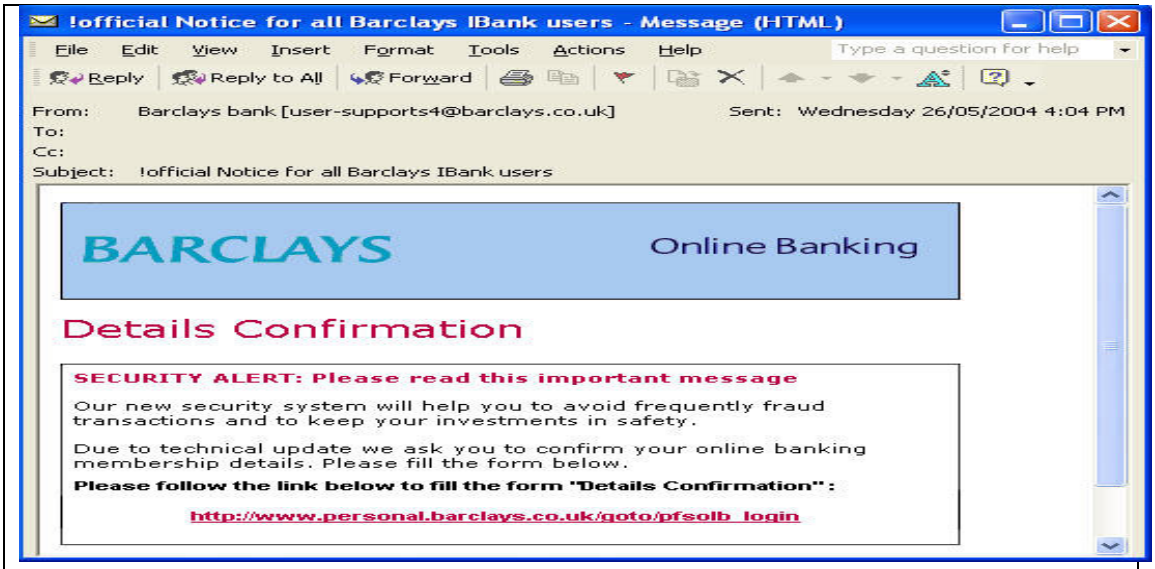

Figure 4.5: The lure

The message in Figure 4.5 has a malware. The malware prompts or requests victims to follow a particular URL hyperlink in order to provide or disclose certain information or particulars.[76] This information or particulars may provide a key as enunciated in figure 4.4 above. Thereafter, the key may be used in order to unlock the message and this unlocking enables a computer cracker to view the contents of the message. After doing all this, a computer cracker could masquerade as a victim and use the key in order to access networks, for example online banking facilities that should be available to or are designed for use by a victim.

The second phase or phase 2 symbolises the hook. In this instance, a victim has responded to the message or request and entered or punched-in the key as requested in phase 1. A computer cracker will thus receive this key and stores it on its database. The storage of the key is made in anticipation of phase 3. The third phase is referred to as the catch. In this case, a computer cracker uses the key to unlock the security mechanisms that are designed to protect a victim from outside phishing attacks. Consequently, a computer cracker is able to gain entry into a victim's computer system or network and retrieve sensitive information that is related to, for example e-banking facilities.[77]

---

[76] Myers *Counter-measures* 5-6.

[77] Myers *Counter-Measures* 5-6.

4.5.3 What is Phishing?

Scholars and computer specialists alike have had difficulty in defining the term 'phishing'. The aforesaid trouble is frequently attributed to the continuous progressions of the technologies that are used to commit phishing.[78] Despite this challenge, there is agreement that phishing is a pernicious transgression. Therefore, attempts to appropriately delineate and criminalise this wrong should be made. The Organisation for Economic Co-operation and Development (the OECD)[79] describes phishing as an amalgamated manifestation that encompasses both the communal and technological factors.[80] This approach originates from the fact that phishing is one of the types of e-crimes. Emails and Web addresses that impersonate original or genuine sources, for example, a government, a business or an institution are commonly created or designed.[81] The OECD's viewpoint on the description of phishing is followed by Myers.[82] Myers submits that phishing involves social and technical attacks.[83] In this instance, computer crackers trick or swindle victims, that is, to defraud, in order that they (victims) may disclose or surrender their personal information.[84] Consequently, it becomes 'an example of social engineering techniques (that are) used in order to take advantage of human ignorance'.[85] In technological terms, social engineering is the malicious act or conduct of manipulating victims, by deception, into giving information,

---

78 James L *Phishing exposed* (Syngress Publishing Rockland 2005) 10.

79 The OECD is an international institution which provides a forum in terms of which national governments can work together to share experiences and seek solutions to certain or common problems. The OECD work with national governments to understand what drives economic, social and environmental change. The OECD analyses and compares data to predict future trends. See OECD http://www.oecd.org/about/ (Date of use: 13 September 2012). The OECD currently has 34 member countries and 6 key partners including South Africa. See OECD http://www.oecd.org/about/membersandpartners/ (Date of use: 13 September 2012).

80 The OECD Directorate for Science, Technology and Industry Committee on Consumer Policy Committee for Information, Computer and Communications Policy http://www.oecd.org/dataoecd/63/28/36494147.pdf (Date of use: 13 May 2012).

81 Graham J, Howard R and Olson R (eds) *Cyber security essentials* (Auerbach Publishers Florida 2011) 87-88. See also Gorge and Brudenall *Secure online* 91-93.

82 Myers *Counter-measures* 1-2.

83 Myers *Counter-measures* 1-2.

84 Sullins *Computer crime* 78-80.

85 Reid http://www.allspammedup.com/2009/02/history-of-e-crimes/ (Date of use: 22 April 2010).

or performing an action.[86] In this activity, computer crackers 'exploit the weaknesses in web security technologies' and sometimes the lack of awareness on the part of victims.[87]

The viewpoint that phishing is a process which seeks to weaken existing IT security mechanisms is followed in section 87 of the ECT Act (Computer-related extortion, fraud and forgery). It may be deduced from this section that phishing is a process that includes the following:

> The ability or threat to, amongst others, access data without authority, interfere with data, unlawfully produce, sell, offer to sell, procures for use, design, adapt for use, distribute or possess any device (computer program or a component) which is designed primarily to overcome security measures with the intention of gaining an unlawful proprietary advantage (i.e. theft) by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic.[88]

Accordingly, phishing is 'social engineering' and 'technical subterfuge' attacks that exploits a blemish in existing computer security mechanisms.[89] In addition, it incorporates online identity (ID) theft and online ID fraud.[90]

(a) Online ID Theft

There is no comprehensible difference which currently exists between situations involving online ID theft and those related to online ID fraud. Online ID theft is sometimes referred to as 'online impersonation fraud'.[91] The association of theft with fraud is acknowledged in chapter 3 of this research. For example, chapter 3 describes theft as a fraudulent appropriation or *contrectatio fraudulosa* of another's property. In

---

86 Mann I *Hacking the human: social engineering techniques and security countermeasures* (Gower Publishing Hampshire 2008) 11.

87 Singh *Information security* 31.

88 See s 87(1) an (2) of the ECT Act.

89 Anti-Phishing Working Group (APWG) http://www.antiphishing.org/reports/apwg_trends_report_q1_2012.pdf (Date of use: 22 July 2012).

90 Myers *phishing* 2-3.

91 CIFAS https://www.cifas.org.uk/secure/contentPORT/uploads/documents/reports/Confidential-%20Fraudscape%202011.pdf (Date of use: 13 July 2012).

this instance, a physical touching or handling of property is necessary. The latter has to be carried out with the necessary fraud.

Because of the difficulty in differentiating theft from fraud it sometimes happens in practice that the meaning of online ID theft is mistakenly correlated to that of online ID fraud.[92] This inaccuracy can be found, for example, in Hoffman and McGinley, where online ID theft is described as the fraudulent or dishonest seizure of another's identity.[93] The fraudulent seizure exists in cases where a person's good name (*fama*) and reputation or communal status (*corpus*) is taken away or tampered with.[94]

ID theft is generally an old phenomenon. The American case of *TRW v Andrews* is an example of a case which involves and deals with ID theft.[95] The facts in *TRW v Andrews* were briefly that: Adelaide Andrews (Adelaide) visited the offices of a particular doctor (a radiologist). She was requested by a receptionist (Andrea Andrews) at the doctor's offices to fill in a consultation form (form). The form required her to disclose information or particulars such as her names, date of birth and Social Security Number. After completing the form, Adelaide handed in the form to Andrea. Andrea copied the information or particulars belonging to Adelaide, immediately resigned her position as the receptionist and moved to another state.[96] In that state Andrea made several attempts to seek and open credit accounts using Adelaide's last name, address and Social Security Number. On all occasions credit reports related to Adelaide were requested by the companies from which Andrea sought credit from TRW Inc.[97] In each case, TRW Inc's computers would register a match of Adelaide's last name, address

---

92 Finch E "The problem of stolen identity and the Internet" in Jewkes Y (ed) *Crime online* (Willan Devon 2007) 29-43 29-31.

93 Hoffman SK and McGinley TG *Identity theft* (Greenwood Publishing Group 2010) 2 and Vacca JR *Identity theft* (Pearson Education New Jersey 2003) 4. See also the European Union (EU) Fraud Prevention Expert Group (FEPG) http://ec.europa.eu/internal_market/fpeg/identity-theft_en.htm (Date of use: 20 July 2012).

94 Biegelman MT *Identity theft handbook: detection, prevention, and security* (John Wiley New Jersey 2009) 2-6.

95 See *TRW v Andrews*, 534 U.S. 19 (2001).

96 *TRW v Andrews* 23-24.

97 TRW Inc. is a global manufacturing and service company which has its headquarters in Cleveland, Ohio. TRW Inc. was founded in 1901 and focuses on providing products and services with a high technology or engineering content to the automotive, space and defence markets. See Military Analysis Network "TRW" http://www.fas.org/man/company/trw.htm (Date of use: 13 June 2012).

and Social Security Number. As soon as a match could be established, credit reports would consequently be furnished to the companies. The companies would thereafter, upon receipt of the aforementioned reports, grant credit to Andrea on the basis of the information or particulars contained on those reports.[98] Sometime later, Adelaide sought a loan for the re-financing of her home mortgage. Adelaide discovered the fraudulent activities when she was furnished with a credit report by TRW Inc. The report contained all the attempts and loans that were made and granted to Andrea in Adelaide's last name. Therefore, Adelaide sought an order from court averring that the disclosure of her information or particulars by TRW Inc were improper.[99] Adelaide submitted also that TRW Inc did not follow appropriate verification procedures. In other words, TRW Inc failed to ascertain whether or not the information or particulars belonged to a person who was seeking the credits (Andrea).[100] As a result of the omission by TRW Inc, the disclosure was, according to Adelaide, made in contravention of § 1681e(a) of the Fair Credit Reporting Act.[101] Conversely, TRW Inc failed, Adelaide argued, to maintain 'reasonable procedures' in order to prevent an improper disclosure of her credit information or particulars.[102]

The emergence of contemporary technologies and the desire to do business and transact online, has compelled a move from ID theft to online ID theft.[103] Online ID theft is an extension of ID theft. Online ID theft is one of the forms of fraud.[104] This theft is carried out in order to appropriate another person's information and to make gain.[105] E-

---

98 *TRW v Andrews* 24.

99 *TRW v Andrews* 24.

100 § 1681e(b) of the Fair Credit Reporting Act, 1996 (hereinafter referred to as the FCRA).

101 *TRW v Andrews* 25.

102 § 1681e(a) of FCRA. The aforementioned section stipulates that 'every consumer reporting agency shall maintain reasonable procedures (that are) designed to avoid violations of § 1681c of this title and to limit the furnishing of consumer reports to the purposes (that are) listed under § 1681b of this title. The procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. Every consumer reporting agency shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing such user a consumer report. No consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a purpose listed in § 1681b of this title'.

103 Hoffman and McGinley *Theft* 13-14.

104 Leary MS *Quantifying the discoverability of identity attributes in internet-based public records: impact on identity theft and knowledge-based authentication* (Ph.D thesis Capella University Minneapolis 2008) 13 and Watney M "Identity theft - the mirror reflects another face" 2004 (3) *TSAR* 511-519 511.

105 Watney 2004 *TSAR* 511.

crimes, for example computer cracking, DDoS or man-in-the-middle attacks may be used for this purpose.

The existence of 'gain' in cases involving online ID theft has caused considerable uncertainty. It is argued by some that 'gain', for purposes of online ID theft, amounts to a financial gain.[106] However, it appears from Vacca[107] and various others[108] that 'gain' also extends, or at least should extend, to factors beyond a financial gain.[109] More specifically, 'gain' should be present in cases where information or particulars are or were used in order to masquerade as another person or business.[110] Given this, online ID theft may also be aimed at achieving certain nefarious ends. These may include espionage, terrorism, revenge, illegal immigration or assuming a new identity in order to avoid a criminal charge.

(b) ***Online ID Fraud***

Online ID fraud is frequently described as the result of online ID theft, that is, the theft of information in order to commit an offence.[111] Viewed in the aforementioned sense, online ID fraud appears to be a forerunner of online ID theft.[112] For example, online ID fraud amounts to the use of stolen identities (IDs) in order to accomplish or achieve unlawful pecuniary and economic gains.[113] It is the actual theft of information for financial gain and 'occurs when criminals take (possession of) illegally obtained personal information and make fraudulent purchases or withdrawals, create false accounts or modify existing ones, and/or attempt to obtain services such as employment or health care'.[114]

---

106 Hoffman and McGinley *Theft* 6.

107 Vacca *Identity* 4-5.

108 Solove DT, Rotenberg M and Schwartz PM *Privacy, information, and technology* (Aspen Publishers New York 2006) 251-253.

109 Vacca *Identity* 4-5.

110 Vacca *Identity* 4-5.

111 Collins JM *Preventing identity theft in your business* (John Wiley New Jersey 2005) 8-13.

112 Collins *Identity theft* 8-13.

113 Finch *Crime online* 34-36.

114 The Javelin Strategy and Research https://www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveyConsumer.pdf (Date of use: 13 May 2012).

In addition, online ID fraud involves the unlawful appropriation or interception of information which is essential for the identification of a person.[115] This information includes the identifying information of victims, for example a pin, username, password, credit card, bank ATM card, bank statement, pre-approved credit offer and tax information.[116] The interception is often made in respect of e-transactions belonging to unsuspecting or credulous victims.[117] It is also made in order to commit crime, for example online theft.[118]

4.5.4 Method of Attack

Computer crackers generally do not always have to possess sophisticated technological skills or experience in order to carry out phishing attacks. Sometimes, minimal technical skills may be enough to break into computer systems or networks. For example, codes or devices that spy on victims and monitor their daily activities are easily available on the Internet. Examples of the codes or devises include keystrokes logger or keystrokes decoder and malicious software (malware).[119] Some of them can be easily accessed and downloaded from the Internet.

The manner in which codes or devices spy on victims is discussed below. This discussion is technically inclined. However, an attempt is made to simplify the study so that it becomes clear to an ordinary reader. The first section revises the use of sniffing devices, for example keystrokes loggers or keystrokes decoders in phishing. The second examines how malware works.

(a) Sniffing Devices

Sniffing devises are mostly microscopic devices. They are or may be attached to a computer keyboard.[120] Once there, they observe and record every keystroke which a

---

115 Best RB *Identity theft: a legal research guide* (Buffalo New York 2004) 2-3.

116 Jasper MC *Identity theft and how to protect yourself* 2nd ed (Oceana Oxford 2006) 2-3 and Granova P and Eloff JHP "A legal overview of phishing" 2005 *Computer Fraud and Security* 6-11 6.

117 Jasper *Identity* 1.

118 Whitson JR "Identity theft and the challenge of caring for your virtual self" 2000 (51) *British Journal of Sociology* 605-622 605-607.

119 BusinessWeek http://www.businessweek.com/magazine/content/06_15/b3979068.htm (Date of use: 14 January 2010).

120 Rasdale M "Denial of service attacks - legislating for robots and zombies" 2006 (22) *Computer Law and Security Report* 222.

victim types or enters.[121] Computer crackers use keystroke loggers or decoders in order to intercept the online activities of a victim. As soon as this happens, computer crackers steal the sensitive information of victims.

Two incidents can be mentioned that demonstrate the influence which keystrokes loggers or decoders have in illegally recording and stealing information. In one occurrence, a student compromised his school's computer system.[122] He hooked up a keystrokes logger in one of his teachers' computers. This was made with a view to access and intercept the teacher's confidential information, and to steal tests. The student carried out his deceitful dealings for several months without the school or the affected teacher being suspicious.[123] Consequently, information and documents relating to test questions and answers were retrieved and some were sold to other students. In another case, a computer and technologically intelligent learner cracked the computer systems of his school.[124] The student used his technological brilliance in order to steal his teachers' personal information, for example, usernames, IDs and passwords. When in possession of the information, he gained entry into or accessed the school's computer system, changed his friends' marks and credited himself for classes that he had failed to attend.[125]

(b) Malware

Malware is a section or portion of malicious software.[126] It comprises segments of cracking codes. They may be sets of numerical or phrases, codes or digits. These

---

121 Janczewski LJ and Colarik AM *Cyber warfare and cyber terrorism* (Information Science Reference London 2008) 310 and Di Pietro R and Verde NV "Digital forensic techniques and tools" in Jahankhani H, Watson DL, Me G and Leonhardt F (eds) *Handbook of electronic security and digital forensics* (World Scientific Publishing New Jersey 2010) 321-356 330.

122 Estes and Jan http://www.boston.com/news/local/articles/2006/04/29/boston_latin_teen_is_accused_of_hacking/ (Date of use: 14 January 2010).

123 Estes and Jan http://www.boston.com/news/local/articles/2006/04/29/boston_latin_teen_is_accused_of_hacking/ (Date of use: 14 January 2010).

124 Click2Houston.com http://www.click2houston.com/rducation/4152951/detail.html (Date of use: 14 January 2010).

125 Click2Houston.com http://www.click2houston.com/rducation/4152951/detail.html (Date of use: 14 January 2010).

126 Brown *E-mail spam* 23.

codes generate instructions on a computer and compel a computer system or network to function according to the wishes of a computer cracker.[127] In carrying out phishing attacks, computer crackers attach malware into computer systems or networks.[128] The malware generally causes harm to those systems or networks and subvert them to use other than that intended by a victim.[129]

Malware can take a number of forms. It can be a collection of computer viruses or worms.[130] The examples of these viruses or worms include rootkits,[131] trojan horses,[132] backdoors, botnets or spyware.[133] Like any other cracking attack, viruses or worms exploit a flaw or blemish in a computer system or network. They use a 'refined stealth technique'[134] in order to spread into the entire computer system or network and without the knowledge of a victim.[135] After they had spread, the viruses or worms hide and masquerade as genuine computer programmes and sometimes, other anti-virus software. Thereafter, victims may be directed to a particular Website or Webpage. A request will consequently follow to the effect that a computer user should click a

---

127 Skoudis ED and Zeltser L *Malware: fighting malicious code* (Pearson Education New Jersey 2004) 3.

128 OECD Directorate for Science, Technology and Industry Committee on Consumer Policy Committee for Information, Computer and Communications Policy http://www.oecd.org/dataoecd/63/28/36494147.pdf (Date of use: 13 May 2012).

129 CIFAS http://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/Digital_Thieves_October2010.pdf (Date of use: 20 August 2012).

130 OECD Directorate for Science, Technology and Industry Committee on Consumer Policy Committee for Information, Computer and Communications Policy http://www.oecd.org/dataoecd/63/28/36494147.pdf (Date of use: 13 May 2012).

131 A rootkit consist of spyware and other malicious programmes. These programmes monitor traffic and keystrokes in a computer keyboard; create a backdoor in the system for the hackers use; alter log files; attack other machines on the network, alter existing system tools to escape detection. See Graham, Howard and Olson *Essentials* 219.

132 Trojan horses are hidden and deceitful programmes that disguise themselves as other computer programmes. See Knittel J and Soto M *Everything you need to know about the dangers of hacking* (The Rosen Publishing Group New York 2003) 17.

133 Spyware is a particular type of malware. It secretly gathers information data belonging to a computer user without the latter being aware or suspecting such collection or the existence of the spyware. See CIFAS http://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/The_Anonymous_Attacker_CIFAS_Special_Report_Oct_2009.pdf (Date of use: 13 June 2012).

134 A refined stealth technique is a mechanism that is developed to enable viruses or worms to spread all over a computer or computer programme without detection. See Securelist http://www.securelist.com/en/analysis/204791996/Changing_threats_changing_solutions_A_history_of_viruses_and_antivirus (Date of use: 5 July 2010).

135 BusinessWeek http://www.businessweek.com/magazine/content/06_15/b3979068.htm (Date of use: 14 January 2010).

hyperlink which appears on such a Webpage.[136] As soon as it has been clicked, the malware becomes active and begins to phish for sensitive information.

Computer viruses or worms also download and invite other computer viruses or worms. This then frustrates or impedes the proper functioning of a victim's computer. The computer then becomes a safe sanctuary (zombies or bots) for other viruses and worms.[137] As soon as this happens, computer crackers commence and disperse viruses or worms to other victims from there.[138]

Figure 4.6 below illustrates the methods that are often used in turning a victim's computer into a zombie.[139]

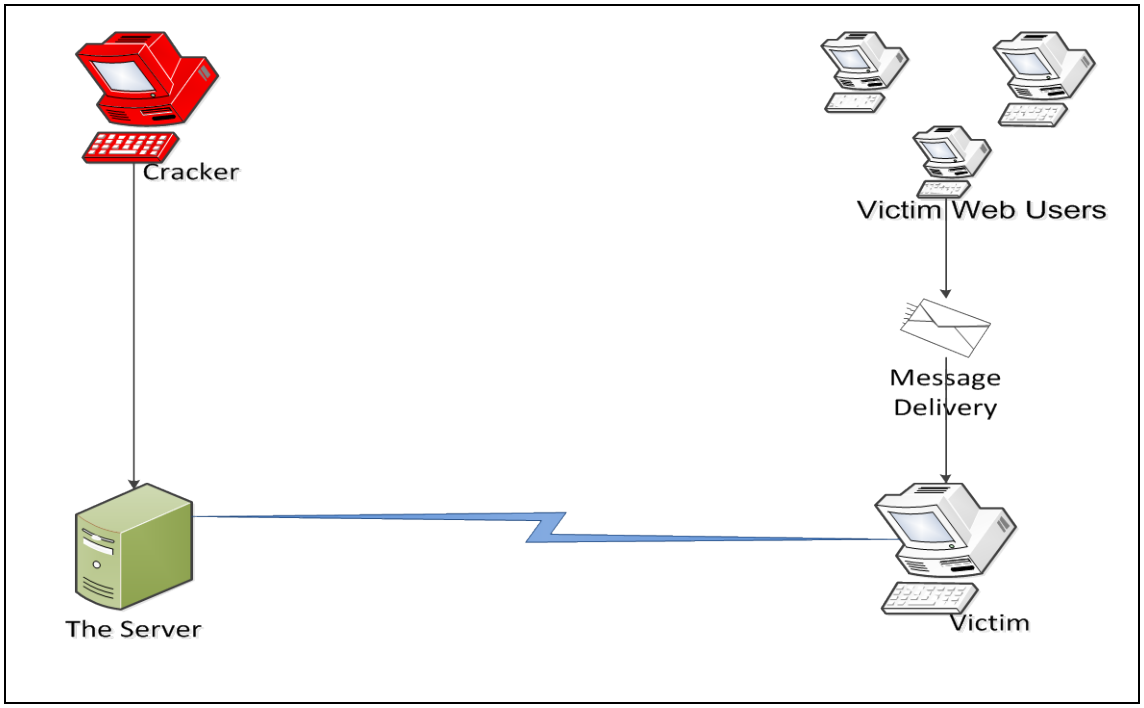

Figure 4.6: Compromise or attack of Web-servers.

136 OECD Directorate for Science, Technology and Industry Committee on Consumer Policy Committee for Information, Computer and Communications Policy http://www.oecd.org/dataoecd/63/28/36494147.pdf (Date of use: 13 May 2012).

137 OECD Directorate for Science, Technology and Industry Committee on Consumer Policy Committee for Information, Computer and Communications Policy http://www.oecd.org/dataoecd/63/28/36494147.pdf (Date of use: 13 May 2012).

138 Sullivan *Definitive guide* 32.

139 Garber 2000 *Technology news* 14-15.

In figure 4.6 the connection between a victim's computer and the Web-server is demonstrated. A cracker appears at the zombie computer at the top of figure 4.6. It (zombie) noticeably compromises and attacks the Web-server. It generates and installs Web-Sites and emails (mass-phishing emails) from this zombie computer. The latter lures and catches unsuspecting victims. Thereafter, it uses a victim's computer to send malware-infected Websites and emails to other computer users. For tracing purposes, the URL which is registered under a victim's name will appear from those Websites and emails.

4.5.5 Summary

ICTs present opportunities for criminals to commit theft of information online, that is, e-crimes. Three scenarios are stated where these ICTs can be used for the aforementioned purpose. They can be an 'instrument' to perpetrate offences, a 'target' for criminals to attack and carry out crime or 'storage machinery' which is exploited in order to preserve information related to crimes.[140] E-crimes mark a development of the established offences, for example theft or *furtum*. More specifically, they represent a migration of offline crimes in online settings. The different forms of e-crimes that are discussed in this chapter include computer cracking, DDoS attacks, man-in-the-middle attacks and phishing. Computer crackers exploit a blemish which is found in computer or information systems or networks. DDoS attacks deny and prevent victims from the lawfully accessing of computer or information systems or networks. Man-in-the-middle attacks operate effectively when a computer cracker is situated between the Web-server and a victim's computer. The expression 'phishing' was coined recently. In particular, the concept was formulated following contemporary criminal incidents. The AOL and phreaking attacks are but the few incidents that contributed to how the notion is currently understood. However, it is illustrated that criminals always found ways to commit phishing. A study of the crimes of *dolus malus* and *crimen injuria* reveals that behaviours comparable to phishing had long existed. These crimes were recognised in classical Rome and, to some extent, by South African courts. However, modern forms of technologies have transformed the manner of understanding phishing. They have also complicated the process to properly understand phishing. This has led some to

---

[140] Downing *Computer crime* 9.

regard it as a communal and technological crime and others to conclude that it is a form of a social engineering and technical subterfuge attack.[141]

Advanced computer skills are not necessary in order to carry out these forms of theft. Mostly, minimal expertise is sufficient to defraud victims of their sensitive information. Keystrokes loggers or decoders and malware serve as techniques that are frequently used for phishing. They generally moderate the efforts that are used for phishing. For example, they exclude the physical or actual removal of stolen information. In addition, there is no actual dispossession of information required in order for phishing to ensue. Lastly, there is no necessity to identify victims before the attacks are generated and sent. Computer crackers generate attacks online and indiscriminately send them to a number (or 'sea') victims.

4.6 SCALE OF E-CRIMES

4.6.1 Background

Estimating the degree and magnitude of e-crimes is generally a cumbersome activity. Two factors can be mentioned that influence this difficulty. Firstly, e-crimes are commonly carried out in underground financial systems or markets.[142] Such marketplaces do not publicise their accomplishments.[143]

Secondly, victims of e-crimes or computer cracking attacks are usually hesitant to report those attacks.[144] The fear of degradation, pecuniary losses and, sometimes, legal liabilities are but some of the issues that are associated with the abovementioned scepticisms.[145] Despite these limitations, it is accepted that e-crimes continue to be the fast-growing internet crimes.

4.6.2 Reported Data

---

141 APWG http://www.antie-crimes.org/reports/apwg_trends_report_q1_2012.pdf (Date of use: 22 July 2012).

142 Stavroulakis P and Stamp M (eds) *Handbook of information and communication security* (Springer Heidelberg 2010) 435.

143 Myers *Counter-measures* 4.

144 Myers *Counter-measures* 4.

145 Myers *Counter-measures* 4.

Various institutions assist in detailing the advances and declines in e-crimes. In this chapter the reports by the Anti-Phishing Working Group (APWG)[146] and MarkMonitor[147] are discussed. APWG detected a total number of 83 083 malware-infected Web Sites that targeted specific organisations or institutions during 2011.[148] It reported an increase in this number during 2012. More than half (56 859) of these Web Sites that were reported during 2011 were established and used during the month of February 2012. The number marked an 'all-time high' in the history of the APWG's reporting framework. About 70.86 per cent of these sites were hosted in the US. China was the most malware infected country (57.13 per cent during the second half of 2011 and 54.10 per cent in the first quarter of 2012). Furthermore, APWG reported that the HTTP port 80[149] had been the most used port in committing e-crimes (standing at 99.324 per cent as compared to other ports).[150]

MarkMonitor reports that typosquatting is mostly used in order to commit e-crimes.[151] Typosquatting is a particular form of cybersquatting.[152] In one case, computer crackers register a domain name which resembles an existing trade or mark.[153] The aim is to licence or sell the domain name to an owner of a mark or other victims.[154] In others, computer crackers register misspellings of popular websites.[155] For example,

---

146 The APWG is a non-profit global, pan-industrial and law enforcement association. It focuses on eliminating fraud, crime and identity theft that result from e-crimes, pharming, malware and email spoofing. See APWG http://www.antiphishing.org/ (Date of use: 13 September 2012).

147 MarkMonitor is an international institution which offers comprehensive online solutions that enable organisations around the globe to establish and defend themselves against multiple online risks. See MarkMonitor https://www.markmonitor.com/company/overview.php (Date of use: 13 September 2012).

148 APWG http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2011.pdf (Date of use: 22 July 2012).

149 HTTP port 80 is a specific port that a web server listens to for requests from web users. See Anson S *et al Mastering windows networks forensics and investigation* (John Wiley Indianapolis 2012) 140. See also, Dubrawsky I *How to cheat at securing your network* (Syngress Publishing Burlington 2007) 175.

150 APWG http://www.antiphishing.org/reports/apwg_trends_report_q1_2012.pdf (Date of use: 22 July 2012).

151 MarkMonitor https://www.markmonitor.com/mmblog/typosquatting-continues-to-pose-dangers-to-enterprises-consumers/ (Date of use: 20 August 2012).

152 Howells M "Beware cybersquatters and typosquatters" 2002 (20) *Ancestry Magazine* 55-58 56.

153 Schwabach *Internet and law* 67-68.

154 Howells 2002 *Ancestry Magazine* 56.

155 Moore T and Edelman B "Measuring the perpetrators and funders of typosquatting" in Sion R (ed) *Financial cryptography and data security* (Springer Berlin Heidelberg 2010) 175-191 175. See also Howell 2002 *Ancestry Magazine* 56.

http://mailyahoo.com may be entered instead of http://mail.yahoo.com, http://mailgmail.com as opposed to http://mail.gmail.com. This registration is made in anticipation that some victims will mistype a particular domain name or URL.[156] When such misspellings are entered victims will be directed to a fictitious Web Site where e-crimes are carried out.[157]

E-crimes also pose a financial burden to governments, commercial institutions and consumers. In the US, it is reported that it accounted for approximately 483 million US dollars during 2009.[158] The extent of the attacks resulted in about 545 000 US consumers being forced to replace their computers. The number of the attacks increased during 2010. For example, it is reported that the damage caused to consumers and their computers amounted to 650 million US dollars during 2010. As a result thereof, about 617 000 US consumers changed their affected or malware-infected computers.[159] The financial burden which is attributed to e-crimes is not limited only to the US. The UK government, institutions and consumers have also expended time and financial resources in an effort to prevent e-crimes. In particular, an amount that is estimated to be around 27 billion UK pounds was used during 2009 for the aforementioned purpose.[160] The latter amount is divided into the following: 2.2 billion pounds was used by the UK government; 21 billion pounds by the UK businesses responsible for securing sensitive information, and 3.1 billion pounds by individual consumers.[161]

---

156 Moore and Edelman *Typosquatting* 56.

157 In particular, it is reported that 15 per cent of the victims who visit hacked web sites disclose their personal or sensitive information or data. See Oghenerukeybe EA "Customers perception of security indicators in online banking sites in Nigeria" 2009 (14) *Journal of Internet Banking and Commerce* 1-15 2.

158 Consumer Report Magazine http://www.consumerreports.org/cro/magazine-archive/june-2009/electronics-computers/state-of-the-net/state-of-the-net-2009/state-of-the-net-2009.htm (Date of use: 24 July 2012).

159 Consumer Report http://www.consumerreports.org/cro/magazine-archive/2010/june/electronics-computers/social-insecurity/state-of-the-net-2010/index.htm (Date of use: 24 July 2012).

160 UK Cabinet Office http://www.cabinetoffice.gov.uk/news/making-travel-safer-cyberspace (Date of use: 18 July 2012).

161 UK Cabinet Office http://www.cabinetoffice.gov.uk/news/making-travel-safer-cyberspace (Date of use: 18 July 2012).

In South Africa, the economic impact of e-crimes equals to 0.14 per cent of the national GDP.[162] It is estimated to be around 5.8 billion rand each year.[163] It is then argued that this amount is likely to escalate in the event that e-crimes are insufficiently regulated.[164] These costs take various forms. They include costs of replacing the malware infected software and hardware, financial losses due to the theft of information, security costs and regulatory or costs that are necessary for the control of e-crimes.

4.6.3 Summary

Predicting the scale of e-crimes is commonly challenging. Secrecy of the activities involved in carrying out e-crimes, fear of victimisation and financial losses are some of the factors that contribute to this complexity. However, it is argued that incidents of e-crimes continue to grow. This progression is mostly related to the evolution of modern technologies.

Given this growth, a need exists to measure the scale of e-crimes. In doing so, the surveys and charts by APWG and MarkMonitor are studied. They demonstrate that countries continue to expend time and effort to curb e-crimes. In addition, these surveys reveal that computer crackers use typosquatting techniques for purposes of disguising the chain of e-crimes. In the latter instance, computer crackers establish and register Internet domain names that impersonate or masquerade as that of existing trades or marks. Examples are 'http://mailyahoo.com', 'http://mailgmail.com'.

4.7 CONCLUSION

E-crimes can be seen as the contemporary version of the traditional crimes. More specifically, they have the elements that are similar to those found in conventional crimes. For example, phishing amounts to an unauthorised or fraudulent appropriation of a person's information or particulars with the intention to of making gain out of the information. In this respect, e-crimes have some of the qualities of theft that are found in Roman-Dutch, English and South African law. However, e-crimes differ from

---

162 Fripp http://htxt.co.za/2014/11/11/cybercrime-costs-south-africa-about-r5-8-billion-a-year/ (Date of use: 13 April 2016).

163 Center for Strategic and International Studies http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf (Date of use: 13 April 2016).

164 Center for Strategic and International Studies http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf (Date of use: 13 April 2016).

traditional crimes in a number of respects. Firstly, they have to do with the appropriation of a particular kind of property, namely information. This appropriation does not necessarily amount to the tangible touching or handling of this property. Simply, a computer cracker attacks the security systems of a computer and accesses information that belongs to the victim. In this instance, a computer cracker does not actually dispossess the victim of physical possession of the information. In other words, the information does not physically move from the possession of the victim to the possession of computer cracker. Secondly, the scope of e-crimes is not limited by borders. In other words, e-crimes exploit the interconnectedness of computers in order to reach the vast number of victims in various locations. Accordingly, computer crackers do not essentially have to be in one particular jurisdiction in order to carry out malicious attacks. They may commence malware attacks in one location; disperse the attacks in another locality and the effect could be felt by victims in a number of jurisdictions.

Figure 4.7 below provides a summary of the main similarities and differences between e-crimes. It reveals the scale and severity of e-crimes to the victims.

E-Crimes	**Meaning**	**Attack methods**	**Severity**	**Counter-measures**
Computer Cracking	- Formally harmless attacks - Associated with Open-Source development - Aimed at identifying system insecurity / setbacks - Redesign security in order to correct identified system insecurities	- Expose system insecurity - System / session interruption - Disperse viruses / worms - Create a 'zombie' computer - Appropriate information wrongfully	- These attacks are not limited by borders - Computer crackers hides their identities and locations	The measures to prevent computer cracking form part of a study of what is referred to in this research as the of 'ICT regulatory agenda'. See Chapters 5, 6, 7 and 8.
DDoS Attacks	- Mischievous attacks - Render systems un-usable /inaccessible - Cause 'catastrophic' system errors - Interrupt system proper operation	- Create system errors - Overload system with malicious requests - Block proper functioning of systems - Render systems inaccessible	- DDoS attacks are pervasive - They are borderless (they know no borders) - Systems could be located in diverse - Effect felt by victims in diverse localities	The measures to curb DDoS Attacks are studied in Chapters 5, 6, 7 and 8.
Man-in-the-Middle Attacks	- Also referred to as transport protocol / TCP attacks - Computer cracker takes control of a system - Divert system / information	- Computer cracker operates between computers - Hijack the computers - Attack LAN / Web server - Delete / re-route information - Turn victim's	- Borderless attacks - Corroboration with local computer crackers is sometimes necessary - Attacks to international victims using remote	The measures to discourage man-in-the-middle attacks are studied in Chapters 5, 6, 7 and 8.

		computers into zombies - Eavesdrop on victim's computers - Divert information	locations	
Phishing	- Has close resemblances with 'phreaking' - Emblematic techniques are the lure, hook and catch. - Social and technical attacks - Trick or defraud victims - Manipulate victims by sending deceptive messages - Involves online ID theft and fraud - Computer crackers send malicious codes in order appropriate victims' information fraudulent - The motivation is to gain (financial, espionage, terrorism, revenge, illegal immigration / assuming a new identity	- Exploit weaknesses in systems - Impersonate genuine users - Sends sniffing / microscopic devices and malware - In one case, computers or computer keystroke loggers are targeted - The victims keystrokes in a computer keyboard are then monitored - Victims' information is then appropriated - In other cases, malware is dispersed in victims' system - Malware downloads other malicious codes - Victims' computer then becomes a safe sanctuary for other viruses / codes	- No sophisticated computer skills are necessary to carry out phishing - Messages that represents the lure, hook and catch are sent to diverse victims in different locations - Viruses / worms are attached to these messages - The refined stealth technique is usually used in order to hide the viruses / worms - Some of these viruses / worms are available on the Internet for free - The viruses / words are then spread into a victim's computer & those connected to a victim	The measures to prevent and deter phishing form part of a study of what is referred to in this research as the of 'ICT regulatory agenda'. See Chapters 5, 6, 7 and 8.

Figure 4.7: summative assessment of the e-crimes

Having examined the aforementioned disparities, it is argued that e-crimes generate grave challenges to the ICT regulatory agenda. On the one hand, the problem relates to the fact that law or legal rules operate within borders. This means that a state enforces its laws and legal rules in situations where a contravention of the rules occurred within its territory.[165] On the other hand, a challenge arises in relation to the control of ICTs and consequently, e-crimes. Therefore, it becomes necessary to investigate questions regarding whether it is possible to regulate ICTs or not, and whether the law is or legal rules are sufficient to adequately address ICTs and the challenges that are generated by these contemporary technologies or not. These questions are more relevant because modern forms of technologies continuously develop whereas law relies on inflexible legal rules.

Given the above-mentioned regulatory setbacks, chapter 5 below examines the structure of ICT regulations. It investigates an ICT regulatory framework which is founded on the law and that which is abstracted outside of the legal rules. Thus, a case is made that certain theories for regulation could assist in establishing an opposite ICT regulatory agenda. These theories are generally technology neutral and they assist in

165 Boczek BA *International law: a dictionary* (Scarecrow Press Maryland 2005) 77.

providing a regulatory framework that is appropriate in order to prevent and control e-crimes.

CHAPTER 5

THE STRUCTURE OF ICT REGULATIONS

CHAPTER 5

THE STRUCTURE OF ICT REGULATIONS

5.1 INTRODUCTION

The position of information in the law property was discussed in chapter 2 above. Specifically, it was investigated whether information is or should be property for legal purposes. Thus, it was revealed that information is a significant asset of an information society. Governments, institutions, businesses and individual computer users expend time, effort and money in order to gather information. Following this, there is legal interest in information. Because of this interest, these governments, institutions, businesses and individual computer users reasonably expect that this information should be legally recognised as an object of property rights. Because information is property for purposes of the law, an inquiry is made in chapter 3 regarding whether or not it is property that can be stolen. In that chapter, it was demonstrated that the law of theft is dynamic and flexible. It can be adapted according to the needs of a particular society. Given this flexibility, it is possible to regard information as property that is capable of being stolen.

In chapter 4 the manner in which information that is kept online may be stolen was revealed. This theft does not necessarily result in the physical taking and carrying away of information. It simply results in the wrongful interference with the information of the victim. In addition, an illegal appropriation of online information does not have to be in respect of the whole information as such. It can also arise in situations where a person is unlawfully dispossessed of the part or copy of the information. Because of this, it is argued in chapter 4 that ICTs generate challenges to the information society. Particularly, ICTs have become more pervasive in the information society.[1] This increase then leads to crimes especially the theft of information online, that is, e-crimes becoming widespread. Despite the fact that e-crimes are similar to the traditional forms of crimes, it is accepted that their impact and scope far exceeds those of its offline equivalents. The following example demonstrates in what way this occurs: a theft of a

---

[1] Costa AM "Emerging challenges" in Savona EU (ed) *Crime and technology: new frontiers for regulation, law enforcement and research* (Springer Dordrecht 2001) 1-6 1.

bicycle connotes a tangible or actual loss of that bicycle.[2] However, an appropriation of information, in cases when a copy is illegally made, does not amount to the actual loss of that information.[3] In this case, only the power to possess and deal with the information is lost.[4] Furthermore, the degree and scope of e-crimes is not limited by, for example geographical borders. E-crimes can be started in one place and completed in another.

Having examined the above-mentioned, it is submitted that ICTs or the challenges that are associated with ICTs generate difficulties for law. In view of these challenges, an effort is made in order to respond to and interrogate the questions that were mentioned in chapter 1. These questions are whether or not contemporary technologies can be managed, controlled or regulated by law, and whether the challenges that are generated by modern technologies can be managed and regulated by law or not. In addition, if ICTs and their associated challenges can be managed, controlled or regulated then how should such a technology management or regulatory framework be structured in law?

With a view to scrutinise and respond to the aforementioned questions this chapter is divided into three sections. Section 1 discusses the differences between the law and regulations. It is contended that the law does not regulate in the same way as regulations do. Section 2 deals with ICT regulation. Selected theories are investigated that assist in providing for or establishing appropriate ICT regulatory structures. These theories help in modelling or shaping a regulatory framework which is suitable for ICT. Furthermore, this discussion is intended to discover and establish an innovative approach to ICT regulation.[5] Section 3 is the conclusion. It examines the strengths and limitations of the theories in regulating ICTs. More specifically, it is illustrated that a discriminatory or selective way of studying the regulatory theories will undoubtedly not yield positive results to the overall study of ICT regulations. Therefore, it may be necessary to examine the principles upon which these theories are founded as a whole.

---

2 Von Klink BMJ and Prins JEJ *Law and regulation: scenarios for the information age* (IOS Press Amsterdam 2002) 11.

3 Von Klink and Prins *Law and regulation* 11.

4 Von Klink and Prins *Law and regulation* 11.

5 See Chapter 7 below.

5.2 THE LAW AND REGULATIONS

5.2.1 The Law

The traditional view regarding a process of regulating is that the law or legal rules regulate.[6] The state or government plays an essential role in this regulation.[7] The state specifically regulates in terms of 'tools or toolkits'.[8] The examples are the tools of detection and effecting. Detection enables the state to gather information about the society.[9] Effecting is one of the instruments which a government uses in order to have an impact on and to influence the behaviour of society.[10] This can be illustrated by means of an example: in cases where an allegation is made that a crime, for example *furtum* or theft is committed, the state investigates (tool of detection) the crime. This is aimed at ensuring that all the elements of the crime are present. Thereafter, the state imposes and enforces (tool of effecting) a penalty on a guilty person. The idea behind the aforesaid tools is to shape or assist in shaping the behaviour of society.[11] Consequently, one of the ideas of the positivist legal theory, wherein regulations assume a form of 'command and control', is adopted.[12] In this manner, the law becomes a support structure for a state whereby legal rules are used in order to channel and control the behaviour of society and (legal) sanctions being imposed against transgressors.[13] In other words, the law becomes a political tool wherein the most powerful in society imposes legal rules in order to regulate the conduct of those who are less powerful. This is the case because it 'claims to be authoritative, the rules

---

6 Black J *Critical reflections on regulation* (Centre for Analysis of Risk and Regulation London 2002) 2 and Ding J "Internet regulation" in Campbell D, Bán C, Bán S and Szabo S (eds) *Legal issues in the global information society* (Oceana Publications New York 2005) 279-351 281-282.

7 Torfing J *Politics, regulation and modern welfare state* (MacMillan Press Ltd Hampshire 1998) 142.

8 Hood CC and Margetts HZ *The tools of government in the digital age* (Palgrave MacMillan New York 2007) 2.

9 Hood and Margetts *Tools of government* 3.

10 Hood and Margetts *Tools of government* 3.

11 Hood and Margetts *Tools of government* 2.

12 Baldwin R and Cave M *Understanding regulation: theory, strategy, and practice* (Oxford University Press Oxford 1999) 1-2 and Coglianese C and Mendelson E "Meta-regulation and self-regulation" in Baldwin R, Cave M and Lodge M (eds) *The Oxford handbook of regulation* (Oxford University Press Oxford 2010) 146-168 146.

13 Black *Critical reflections* 2.

are part of a system, the system claims jurisdiction in a wide range of matters, the rules elicit obedience, and the rules are or derive from a sovereign's command'.[14]

A regulatory process which is founded on the law is generally stagnant and cumbersome.[15] It fails to evolve with the time and demands a strict adherence to established sets of rules. The latter can be demonstrated by examining the process of law-making in South Africa. This law-making process is contained in the South African Constitution.[16] For example, the legislative process commences with a discussion document which is referred to as a Green Paper. The Green Paper is followed by a second document which is known as a White Paper. This White Paper generally sets out the policy or programme of the current or existing government. After that, a Bill that embodies a draft version of the legislation or statute is prepared.[17] The Bill is introduced or tabled in the National Assembly or the National Council of Provinces for consideration by the members. It is then referred to the related committee and published in the Government Gazette for the public to comment on it. The committee where the bill was referred will debate the bill and make certain amendments, if necessary. Accordingly, the last stage of the law-making process is to have the Bill assented to and signed into law by the president.[18]

The ECT Act is currently one of the legal mechanisms to regulate ICTs. Chapter XIII of the ECT Act particularly sets out the ways of controlling the behaviours of computer users. It states that a user is or shall be guilty of an offence if the latter accesses or interferes with data without the requisite authority.[19] Before this Chapter of the ECT Act was passed into law, it had to be subjected to the long and cumbersome process that is enunciated in Chapter 4 of the Constitution. It is submitted that this process poses a

---

14 Watson A *The nature of law* (Edinburgh University Press Edinburgh 1977) 35.

15 Barlow JP https://projects.eff.org/~barlow/EconomyOfIdeas.html (Date of use: 24 October 2012).

16 Chapter 4 of the Constitution.

17 Various types of Bills are therefore distinguished, namely: Ordinary Bills (the Section 75 Bills), Ordinary Bills that affect provinces (the Section 76 Bills), Money Bill (the Section 77 Bills) and Constitutional Amendments (the Section 74 Bills). See Parliamentary Monitoring Group (PMG) http://www.pmg.org.za/parlinfo/sectionb3 (Date of use: 2 November 2012).

18 Ss 74(9), 75(1)(d) and 76(1)-(3) of the Constitution. It is important to note that the provision of assenting to and signing of Money Bills by the president is not expressly set out in the Constitution. See s 77 of the Constitution.

19 See s 86 and 87 of the ECT Act.

challenge for ICT regulation. This is the case because ICTs change and develop almost on a daily basis. With these developments criminals explore innovative ways to circumvent the existing security measures of a system. Consequently, by the time all the steps that are listed in Chapter 4 of the Constitution are exhausted new e-crimes would have emerged which would not have been anticipated at the time of drafting the legislation.

The challenges as set out above are even more apparent after studying Chapter XIII of the ECT Act. This Chapter deals with the interference with and destruction of data. It commences by discussing the unauthorised accessing of data. It will be recalled from chapter 1 of this research that the term data means the 'electronic representations of information in any form'.[20] This then indicates that computers or other electronic devices, for example mobile cellular phones are essential to the representation of information online. Taken further, this means that an unauthorised accessing of data is only possible in situations where computers or these devices have an Internet connection. Therefore, if a computer cracker only uses a computer or other means other than the Internet in phishing for information, then the e-crimes that are listed in sections 86 and 87 of the ECT Act cannot be expected to ensue.

The above-mentioned may not be a misjudgement. This is specifically so if recent developments in e-crimes are to be taken into account. Nowadays, e-crimes do not only result in the destruction of or interfering with data. They also result in the unauthorised use of data. This use of data does not necessarily render the actual or original data meaningless to the victims of e-crimes. Furthermore, it does not mean that the data loses or will lose its shape and content given the fact that it is also available to a computer cracker. Following this reasoning, it is argued that it may have been fair and reasonable for Chapter XIII of the ECT Act to have been drafted the way it did at some stage before its commencement. Furthermore, the Chapter may have covered the kinds of e-crimes that existed at the time of its conceptualisation. However, its limitation as a regulatory tool rests on the premise that it does not cover current, emerging or future e-crimes. Because of this, it lacks foresight in the sense that it does not forecast the developments in ICTs and thus regulate the risks that are likely to arise

---

[20] See s 1 of the ECT Act.

as a result thereof. Consequently, the shortcomings of the ECT Act result or can result in a situation where it may be necessary to unceasingly modify and improve the ECT Act or provide legal rules that seek to address the challenges in Chapter XIII of the ECT Act. The example of this is the Draft Cybercrime and Cybersecurity Bill of 2015[21] which encumbers the ICT regulatory agenda in South Africa by creating a long list of e-crimes.

5.2.2 Regulations

Recent developments in regulatory frameworks have supported a move away from state regulations. It is argued that regulations or regulatory structures are disciplines separate from the law.[22] Given this uniqueness, they should be allowed to develop as such.[23] Accordingly, the law is not the only technique of social control.[24] It becomes one of the four regulatory constraints or tools[25] that are essential to the control of societal behaviour.[26] The other constraints or tools are social norms,[27] market[28] and nature or 'architecture'.[29] These tools promote a shift or departure from a regulatory or controlling framework of state sanctions to a structure of regulation whereby other actors in regulatory paradigms, for example regulated industries, also play a role. They also illustrate a progression or development towards a 'balancing act (in terms of) which just the right amount of support and restriction of private sector innovation is

---

21 Hereinafter referred to as the CaC Bill.

22 Morgan B and Yeung K *An introduction to law and regulation: text and materials* (Cambridge University Press Cambridge 2007) 1.

23 Morgan and Yeung *Law and regulation* 1.

24 Lessig L "The laws of cyberspace" in Spinello RA and Tavani HT (eds) *Readings in cyberethics* (Jones Bartlett Sudbury 2004) 134-144 134 and Kesan JP and Shah JC "Deconstructing code" 2003 (6) *Yale Journal of Law and Technology* 277-389 279.

25 Raab CD and De Hert P "Tools for technology regulation – seeking analytical approaches beyond Lessig and Hood" in Brownsword R and Yeung K (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart Publishing Portland 2008) 263-285 263-264.

26 Lessig *Cyberspace* 134. See also Greenleaf G "An endnote on regulating cyberspace – architecture vs law" 1998 (21) *UNSW Law Journal* 593-622 602-605.

27 Social norms are the normative measures which distinguish between acceptable and unacceptable conducts. See Lessig L "The New Chicago School" 1998 (27) *The Journal of Legal Studies* 661-691 663.

28 The market constrains by means of the "devise price". See Lessig 1998 *The Journal of Legal Studies* 663.

29 Lessig *Cyberspace* 134. By architecture is meant the 'physical world as we find it'. See Lessig "The law of the horse – what cyberlaw might teach" 1999 (113) *Harvard Law Review* 501-549 507.

required for optimal results'.[30] The term innovation needs additional clarity. It signifies 'a process and it results ....in a new functionality or a new way of using an existing functionality'.[31] This functionality is relevant both in both the private and the public sectors.[32]

Regulations are (or appear to be) more flexible than the law or legal rules.[33] The ordinary law-making process is not applicable in regulations. Thus, they are introduced to the public (or society) whenever a country's state sees a need for their introduction and provided that they are empowered to do so. The intensity of this process is also not as rigorous as that demanded for law-making purposes.[34] In addition, regulations provide for an amorphous and adaptable controlling framework which is or can be applied to 'any widely derived source of control or direction'.[35] Given the flexibility of regulations, it is accepted that regulations should be seen as a field that is distinct from the law. However, this separation does not imply that the law does not or ceases to have a role to play in regulation. Conversely, the law continues to play a facilitative function in the sense of channelling the shape of regulations.

Notwithstanding the agreement regarding the necessity for a move towards regulatory instruments, it is argued that a holistic or all-inclusive view regarding the meaning and structure of regulations is currently lacking. Brownsword submits that regulations remain an 'unwieldy concept' whereby an absence of confidence regarding who regulates and what is being regulated subsists.[36] There are some who regard

---

30 Gregersen B "The public sector as a pacer in national systems of innovation" in Lundvall BÅ (ed) *National systems of innovation: toward a theory of innovation and interactive learning* (Anthem Press London 2010) 133-150 134-135.

31 Heldeweg MA "Legal design of smart rules and regimes – regulating innovation" in Heldeweg MA and Kica E (eds) *Regulating technological innovation: a multidisciplinary approach* (Palgrave Macmillan Hampshire 2011) 52-76 53.

32 Heldeweg *Legal design* 53.

33 Stenning PC *et al* "Controlling interests – two conceptions of order in regulating a financial market" in Friedland ML (ed) *Securing compliance: seven case studies* (University of Toronto Press Toronto 1990) 88-119 102.

34 Barlow JP https://projects.eff.org/~barlow/EconomyOfIdeas.html (Date of use: 24 October 2012).

35 Murray AD "Conceptualising the post-regulatory (cyber) state" in Brownsword R and Yeung K (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart Publishing Portland 2008) 287-315 288.

36 Brownsword R "Code, control, and choice – why East is East and West is West" 2005 (25) *Journal for Legal Studies* 1-21 4.

regulations or regulatory processes as instruments by a state (in order) to influence the behaviour of society by introducing legal rules.[37] To this end, a form of principal-agent or regulator-regulated relationship comes into existence. In this relationship, it is inferred that a state occupies a superior position in society or community. Given this supremacy, regulations become a tool for a state to inhibit and constrain the manner in which the agents of regulations, that is, a society, conducts or wishes to conduct themselves.[38] The regulator-regulated relationship is favoured by Koops,[39] Brownsword[40] and Canguilhem.[41] For Koops, every regulatory process is naturally a controlling exercise.[42] In this exercise, the behaviour of humans or society is directed towards a particular angle by means of rules or limitations.[43] To achieve this end, a state can use whatever means possible, sometimes including the imposing of sanctions.[44] Canguilhem states that a regulatory process is the 'adjustment in accordance with certain rules or norms of a plurality of movements or acts, and their effects or results, which (they) because of their diversity or succession are rendered alien to each other'.[45]

However, some academics criticise the rule-based examination of regulations.[46] They argue that rules are never neutral and objective.[47] In particular, they are human

---

37 Koops BJ "Should ICT regulation be technology neutral?" in Koop BJ, Lips M, Prins C and Schellekens M (eds) *Starting points for ICT regulation: deconstructing prevalent policy one-liners"* (Asser Press The Hague 2006) 77-108 80-71. See also Canguilhem G "Regulation" 1985 (XV) *Encyclopedia Universalis* 797-799 797. Morgan and Yeung regard this rule-based view of regulations as the narrow formulation of the concept of regulation. See Morgan and Yeung *Law and regulation* 3.

38 Mitnick BM *Planning regulation: a framework for the analysis of regulatory possibilities* (University of Pittsburg Pittsburg 1979) 4 and Mitnick BM *Regulation and the theory of agency: incentives, control, and reform in regulation* (University of Pittsburgh Pittsburgh 1979) 8.

39 Koops *Technology* 80-81.

40 Brownsword 2005 *Journal for Legal Studies* 4.

41 Canguilhem 1985 *Encyclopedia Universalis* 797.

42 Koops *Technology* 80-81.

43 Koops *Technology* 80-81.

44 Brownsword 2005 *Journal for Legal Studies* 4.

45 Canguilhem 1985 *Encyclopedia Universalis* 797.

46 Gunningham N "Enforcement and compliance strategies" in Baldwin R, Cave M and Lodge M (eds) *The Oxford handbook of regulation* (Oxford University Press Oxford 2010) 120-145 and Yeung K "Towards an understanding of regulation by design" in Bownsword R and Yeung K (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* ((Hart Publishing Portland 2008) 79-107.

47 Yeung *Regulation by design* 91-93.

inventions that 'rely on interpretation, enforcement and sanction' through human dealings.[48] To assist in moving away from this rule-based approach to regulation, a decentring analysis is proposed. The decentring analysis recognises that the use of different role-players, for example a state, individual firms or regulated industries and society or community in regulatory paradigms, produce or can produce *better regulation*.[49] *Better regulation* is opposed to or promotes a shift from *less regulation*.[50] It is sometimes equated with *Good Regulations*.[51] *Good Regulations* rely on whether regulations meet the necessary benchmarks for their evaluations or not.[52] These are whether a regulatory framework is supported by legislative authority; there is an appropriate scheme of accountability; the regulatory procedures are fair, accessible, and open; the regulator has the requisite expertise, and the framework for regulation is efficient or not.[53] They also improve regulations and the tools that are commonly used in regulatory frameworks.[54] The aforementioned is done by ensuring that regulations are both effective and efficient.[55] Because *better regulations* are not a product of the single state actor, the role-players in regulations, that is, the state and the regulated industries decide on proper regulatory benchmarks that are to be adopted and applied by them.

A number of concepts assist in ensuring that *better regulations* are attained. These concepts are referred to as smart-regulations, meta-regulations or reflexive regulations, self-regulations and co-regulations.[56] These concepts are important to this chapter. In particular, they help in understanding the ICT regulatory theories that are examined in section 5.3 below.

---

48 Yeung *Regulation by design* 93.

49 Gunningham *Enforcement* 131.

50 Kirkpatrick C and Parker D "Regulatory impact assessment – an overview" in *Regulatory Impact Assessment: Towards Better Regulation* (Edward Elgar Publishing Cheltenham 2007) 1-16 1-2. For further interesting reading see European Commission http://ec.europa.eu/governance/better_regulation/documents/brochure/br_brochure_en.pdf (Date of use: 13 November 2012)

51 Baldwin and Cave *Understanding regulation* 76.

52 Baldwin and Cave *Understanding regulation* 76.

53 Baldwin and Cave *Understanding regulation* 76.

54 Baldwin R "Better regulation in troubled times" 2006 (1) *Health Economics, Policy and Law* 203-207 204-205. See also Boyer R "The regulation approach as a theory of capitalism – a new derivation" in Labrousse A and Weisz JD (eds) *Institutional economics in France and Germany* (Springer Berlin 2001) 49-92 50.

55 Kirkpatrick and Parker *Regulatory impact assessment* 2.

56 See Baldwin 2006 *Health Economics, Policy and Law* 204-205.

(a) Smart Regulations

Smart regulations are the opposite of 'dumb regulations'. Dumb regulations present themselves in a number of ways. Firstly, they put 'pointless burdens on businesses'.[57] Secondly, they fail to 'reflect changing technology'.[58] Thirdly, they are 'overly protective of the turf' in the sense that they 'leave investors as sheep to be sheared'.[59] However, smart regulations emphasise a progression beyond state control and government rules.[60] They provide that legal rules are insufficient to control social behaviour.[61] Accordingly, they entail a study of legal rules and the normative frameworks within which the rules operate.[62] Therefore, rules do not become stationary or inflexible objects.[63] They evolve and allow for the establishment of regulatory structures that holistically mixes or matches all the role-players that are or should be involved in regulatory structures.[64]

In Europe, a move has been witnessed towards smart regulations. Specifically, this shift is motivated by the realisation that legal rules are the supporters of dumb regulations. This acceptance appears in fields such as consumer protection. For example, the European Consumer Organisation (The Consumer Voice in Europe) articulates the need for smart regulations.[65] It states that this form of regulating is

---

57 Flemming https://www.sec.gov/news/speech/importance-of-smart-regulation.html (Date of use: 13 March 2016).

58 Flemming https://www.sec.gov/news/speech/importance-of-smart-regulation.html (Date of use: 13 March 2016).

59 Flemming https://www.sec.gov/news/speech/importance-of-smart-regulation.html (Date of use: 13 March 2016).

60 House of Commons Regulatory Reform Committee *Getting results: the better regulation executive and the impact of the regulatory reform agenda* (The Stationery Office Limited London 2008) 181-184 and Gunningham N "Regulating biotechnology – lessons from environmental policy" in Somsen H (ed) *The regulatory challenge of biotechnology: human genetics, food and patents* (Edward Elgar Publishing Ltd Cheltenham 2007) 3-18 6.

61 House of Commons Regulatory Reform Committee *Getting results* 181-184.

62 European Commission "Smart regulation in the European Union" 8 October 2010 2-3 http://ec.europa.eu/smart-regulation/ (Date of use: 13 May 2015).

63 Gunningham *Enforcement* 132 and Brownsword 2005 *Journal for Legal Studies* 1.

64 Brownsword 2005 *Journal for Legal Studies* 6-8.

65 European Consumer Organisation http://ec.europa.eu/smart-regulation/consultation_2012/docs/registered_organisations/beuc_en.pdf (Date of use: 13 March 2016).

indispensable because it places the welfare of consumers at the forefront of the regulatory process.[66]

(b) Meta-Regulations

Meta-regulations are also referred to as reflexive regulations. Reflexive regulations entail a structure of regulation that controls and manages other associated regulatory structures.[67] In addition, they discourage the understanding that the state is the only primary role-player in regulation.[68] More specifically, they acknowledge that the 'capacity of the regulatory state to deal with increasingly complex social issues has declined dramatically'.[69]

Morgan submits that the notion of meta-regulation 'captures a desire to think reflexively about regulation, such that rather than regulating social and individual action directly, the process of regulation itself becomes regulated'.[70] Thus, a regulatory process, within the context of meta-regulations, is regarded as the progression within which affected industries establish their own systems of domestic or internal control and management.[71] In this instance, a state regulates at a distance,[72] and can sometimes be an agency within which regulations apply.[73] Ford supports the importance of meta-regulations.[74] He states the following:

---

66 European Consumer Organisation http://ec.europa.eu/smart-regulation/consultation_2012/docs/registered_organisations/beuc_en.pdf (Date of use: 13 March 2016).

67 Levi-Faur D "Regulation and regulatory governance" in *Handbook on the politics of regulation* (Edward Elgar Publishing Ltd Cheltenham 2011) 3-21 11.

68 Lee S "In the prison of the mind – punishment, social order, self-regulation" in Saral A, Douglas L and Umphrey MM (eds) *Law as punishment or law as regulation* (Stanford University Press California 2011) 124-154 127.

69 Gunningham *Enforcement Challenge* 8.

70 Morgan B "The economisation of politics – meta-regulation as a form of nonjudicial legality" 2003 (12) *Journal of Social and Legal Studies* 489-523 490.

71 Coglianese and Mendelson *Meta-regulation* 147.

72 Braithwaite J "The new regulatory state and the transformation of criminology" 2000 (40) *British Journal of Criminology* 222-238 225.

73 McHarg A "Devolution and the regulatory state – constraints and opportunities" in Oliver D, Prosser T and Rawlings R (eds) *The regulatory state: constitutional implications* (Oxford University Press Oxford 2010) 67-91 80.

74 See Ford CL "New governance, compliance, and principles-based securities regulation" 2008 (45) *American Business Law Journal* 1-60 39.

> ….open-ended, learning systems are preferable . . . where the regulator "knows the result it is trying to achieve but does not know the means for achieving it, when circumstances are likely to change in ways that the [regulator] cannot predict, or when the regulator does not even know the precise result that she desires."[75]

Meta-Regulations have been found by some to be more suited in environmental studies. Specifically, it is established that this particular form of regulating has worked very well in mitigating the risks caused by pollution.[76] This success is attributed to the fact that the regulatory role-players adopt specific regulatory measures and, thereafter, self-assess their performance in meeting these regulations.[77] In South Africa, this form of regulating seems to be preferred by, for example the Health Professions Council of South Africa.[78] The HPCSA works in conjunction and co-ordinates with its other 12 Professional Boards[79] in guiding and regulating the health professions in South Africa.[80]

(c) Self-Regulation

Self-regulation connotes self-control and self-correction.[81] Regulatory industries control and modify their behaviours and activities in order for those behaviours and activities to conform to particular desired ends.[82] It also presupposes an independent method or

---

75 Ford 2008 *American Business Law Journal* 39.

76 Gilad S "It runs in the family – meta-regulation and its sibling" 2010 (4) *Regulation and Governance* 485-506 491.

77 Gilad 2010 *Regulation and Governance* 491-492.

78 Hereinafter referred to as the HPCSA. The HPCSA is a statutory body which is established in terms of the Health Professions Act 56 of 1974. See preamble to the Health Professions Act 56 of 1974.

79 These Professional boards are the Dental Therapy and Oral Hygiene; Dietetics and Nutrition; Emergency Care; Environmental health; Medical and Dental; Medical Technology; Occupational Therapy, Medical Orthotics, Prosthetics and Arts Therapy; Optometry and Dispensing Opticians; Physiotherapy, Podiatry and Biokinetics; Psychology; Radiography and Clinical Technology and Speech Language and Hearing Professions.

80 HPCSA http://www.hpcsa.co.za/About/VisionMission (Date of use: 13 April 2016).

81 Carver CS and Scheier MF "Self-regulation of action and affect" in Vohs KD and Baumeister RF (eds) *Handbook of self-regulation, second edition: research, theory, and applications* (The Guilford Press New York 2011) 3-21 3-4.

82 Hrabok M and Kerns KA "The development of self-regulation – a neuropsychological perspective" in Solok BW, Müller U, Carpendale JIM, Young AR and Iarocci G (eds) *Self and social regulation: social interaction and the development of social*

structure of regulating.[83] For example, the regulatory industries interact with each other in order to establish a set of regulatory standards for their compliance.[84]

Schraw, Crippen and Hartley argue that self-regulations have been pivotal in science education.[85] From the forgoing, regulators are required to identify the desired regulatory objectives and remove certain impediments to the achievement of those targets.[86] In order to do this, it is necessary to 'select strategies that help us achieve these goals, implement those strategies, and monitor our progress towards our goals'.[87]

(d) Co-Regulation

Co-regulation is generally a combination of government and self-regulations.[88] In this instance, the government and self-regulatory industries collaborate in order to establish a particular regulatory paradigm.[89] On the one hand, the state recommends a particular regulatory framework.[90] On the other hand, the self-regulatory industries generate rules, methods and ways of administering the rules.[91]

One of the examples where co-regulations have been found to be productive is the area of food safety.[92] In this field, it was established that this form of regulating is the most transparent and trustworthy of the regulatory concepts.[93]

---

understanding and executive functions (Oxford University Press Oxford 2010) 129-154 129.

83 Bonnici JPM *Self-regulation in cyberspace* (TMC Asser Press The Hague 2008) 10.

84 Coglianese and Mendelson *Meta-regulation* 147.

85 See in general Schraw G, Crippen KJ and Hartley K "Promoting self-regulation in science education - metacognition as part of a broader perspective on learning" 2006 (36) *Research in Science Education* 111-139.

86 Schraw, Crippen and Hartley 2006 *Research in Science Education* 111. See also Leventhal H, Brissette I and Leventhal EA "The common-sense model of self-regulation of health and illness" in Cameron LD and Leventhal H (eds) *The self-regulation of health and illness behaviour* (Routledge London 2003) 42-65 43.

87 Schraw, Crippen and Hartley 2006 *Research in Science Education* 111.

88 Bonnici *Cyberspace* 15.

89 Bonnici *Cyberspace* 15.

90 Bonnici *Cyberspace* 15.

91 Bonnici *Cyberspace* 15.

92 Martinez MG, Fearne A, Caswell JA and Henson S "Co-regulation as a possible model for food safety governance - opportunities for public–private partnerships" 2007 (32) *Food Policy* 299-314 301.

5.2.3 Summary

Regulatory frameworks will almost always differ depending on the regulatory processes that are selected or used. For example, laborious sets of rules are required to be followed in order to commence the law-making process. When it has been passed, the law regulates in terms of particular tools or toolkits. These tools necessitate that a regulator-regulated relationship should commence. In this relationship, the state channels the behaviour or activities of society towards a particular angle.[94] In cases where society becomes disobedient of the rules, the state enforces the rules by imposing sanctions.

However, regulations as compared to law are flexible[95] and easier to establish.[96] For their commencement, a convenient and adaptable process is necessary. Despite this flexibility and convenience, differences exist regarding the proper meaning and structure of regulations. One viewpoint argues that regulations are a form of 'command and control' mechanism.[97] To this end, the state regulates in terms of legal rules.[98] However, others recommend a decentring analysis to regulation. This recognises the importance of other role-players, for example, society and regulated firms, to a regulatory structure.[99] It also leads to what is referred to as *better regulation*.[100] *Better regulation* is generally opposed to a rule-based framework of regulating. It acknowledges that rules are human inventions to control human relations.[101] Consequently, partial or subjective conjectures regarding the behaviours that are sanctioned or punished by the imposition of legal rules are likely to ensue. Concepts, for example smart-regulations, meta-regulations or reflexive regulations, self-regulations and co-regulations, are distinguished that supplement and, sometimes, contradict *better regulation*.

---

93 Martinez, Fearne, Caswell and Henson 2007 *Food Policy* 303-304.
94 Koops *Technology* 80-81.
95 Murray *Conceptualising* 288.
96 Barlow https://projects.eff.org/~barlow/EconomyOfIdeas.html (Date of use: 24 October 2012).
97 Black *Critical reflections* 2 and Coglianese and Mendelson *Meta-regulation* 146.
98 Koops *Technology* 80-81.
99 Gunningham *Enforcement challenge* 131.
100 Gunningham *Enforcement challenge* 131.
101 Yeung *Regulation by design* 93.

The move towards establishing *better regulations* does not necessarily mean that the state becomes insignificant to the ICT regulatory agenda. This essentially illustrates that ICT regulatory measures should generally not be a product of a single state actor. Rather, the state becomes or should become one of the role-players in ICT regulations.

5.3 ICT REGULATION

5.3.1 Background

There is no easy answer which currently exist regarding the question whether it is possible to regulate (or govern)[102] recent technologies or not. There is a viewpoint that a technology has or creates its own space.[103] This space is referred to as the 'cyberspace'.[104] Cyberspace, it is argued, is a space where no one is in charge. It is principally a space in which people are free from state control.[105] Furthermore, cyberspace is, as Biegel puts it, a 'mysterious conglomeration of virtual communities'[106] and a 'lawless frontier where anarchy and vigilantism are alive and well'.[107] In this space, regulations 'adapt by continuous increments and at pace second to geology in its stateliness. Technology advances in.....lunging jerks like punctuation of biological evolution grotesquely accelerated.....this Mismatch is permanent'.[108] Therefore, technology and regulations are opponents. Technology connotes marketplaces, new

---

102 Weber RH *Shaping internet governance: regulatory challenges* (Springer Heidelberg 2009) 203.

103 Johnson DR and Post D "Law and borders – the rise of law in cyberspace" 1996 (48) *Stanford Law Review* 1366-1402 1379.

104 Murray *Conceptualising* 300.

105 Lessig *Cyberspace* 135.

106 These communities are referred to as the 'persistent, interactive, simulated social places where (computer) users employ avatars'. See Castronova E *Synthetic worlds: the business and culture of online games* (University of Chicago Press Chicago 2005) 287.

107 Biegel S *Beyond our control?: confronting the limits of our legal systems in the age of cyberspace* (The MIT Press Cambridge 2003) 1-2.

108 Barlow http://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/idea_economy_article.html (Date of 13 October 2012).

ventures and development.[109] Regulations symbolise supervision, bureaucracy and affront to development.[110]

However, there are those who contest this alleged total exclusivity of cyberspace.[111] They state that cyberspace or the development of cyberspace is partially linked to the physical space.[112] More specifically, the activities that are carried out through the use of current technologies have relevance for the computer users or other entities relying on computers.[113] The aforementioned can be illustrated by means of an example: Suppose that M is a customer of B Bank. M wishes to access B Bank's Internet banking (e-banking) facilities in order to transfer money to C. In terms of B Bank's e-banking facilities, all its customers must enter their identifying particulars before they are or can be logged on to B Bank's e-banking facilities. In this regard M will have to comply with the laws and regulations of the country where he resides, of the country where the computers belonging to B Bank are located and of the country where B Bank is situated. These laws and regulations can include those that relate to privacy and the protection of national borders. Once logged on to B Bank's e-banking facilities, M has to obey the laws that are created for and by cyberspace. These include the laws that govern the manner of processing and sharing data or information, encryption or e-authentication. Given the aforementioned association, it is argued that technology regulation is not a phenomenon or process completely disconnected from real or physical space. An activity undertaken through the use of ICTs will, as shown in the example above, have an impact on other activities occurring in non-virtual spaces. Therefore, technology is a space or sphere where regulations apply or should apply. This consequently brings us to the next question, namely, how should these modern technologies be regulated, controlled and managed?

In this chapter, a selected number of theories for regulating ICTs and their associated challenges are discussed. The theories include the codes-based theory or regulation

---

109 Wiener JB "The regulation of technology, and the technology of regulation" 2004 (26) *Journal of Technology in Society* 483-500 483.

110 Wiener 2004 *Journal of Technology in Society* 483. See also Raymond ES *The cathedral and the bazaar: musings on linux and open source by an accidental revolution* (O'Reilly Beijing 1999) 55-61.

111 Weber *Internet governance* 3-4 and Bonnici *Cyberspace* 1.

112 Weber *Internet governance* 3-4.

113 Bonnici *Cyberspace* 1.

by codes, the Danger or Artificial Immune Systems (the AIS) theory, the Systems theory and the Good Regulator Theorem. These theories are not regulations as such. They merely assist in establishing better ICT regulations. The latter simply means that the different role-players in ICT regulation assume the role of a regulator. They also help in creating a method of regulating which is best suited to the technologies to be regulated and the challenges that are connected to ICTs. Furthermore, they support the hypothesis that *better regulations* can only be achieved in situations where the role-players in technology regulation and the interaction of the role-players during technology regulation is allowed to flourish. Lastly, the theories propagate the significance of developing technology-neutral or technology-independent[114] regulatory regimes.[115] The latter accepts that legal rules still have a facilitative role to play in ICT regulations.

The term 'theory' has to be understood according to what this concept particularly means for purposes of technology regulation. It shall therefore be understood to denote a 'set of propositions or hypothesis about why regulations or regulatory processes emerge, which actors contribute to that emergence and typical patterns of integration between regulatory actors'.[116]

5.3.2 The Codes-Based Theory

The theory of regulation by codes generally found its significance during the 1990s. Some of the founders of this theory are Reidenberg[117] and Lessig.[118] It is sometimes compared with 'techno-regulation'.[119] Techno-regulations accept that both the codes

---

114 See in general the Dutch Policy Memorandum Legislation for the Electronic Highways of 1998 http://www.burojansen.nl/crypto/english/5.html (Date of use: 13 April 2016).

115 The term 'regime' is vastly defined in academic literature. However, for purposes of technology regulation 'regime' means 'a system of ….rules, which in conjunction includes not only norms, but also the mechanisms of decision making and the network of involved actors'. See Heldeweg *Legal design* 59.

116 Morgan and Yeung *Law and regulation* 16.

117 Reidenberg JR "*Lex Informatica* – the formulation of information policy rules through technology" 1998 (76) *Texas Law Review* 553-584.

118 See generally Lessig L *Code and other laws of cyberspace* (Basic Books New York 1999), Lessig 1999 *Harvard Law Review* 546 and Lessig L "The path of cyberlaw" 1995 (104) *The Yale Law Journal* 17-46.

119 Brownsword 2005 *Journal of Legal Studies* 3.

and the design of the codes are indispensable to the 'regulatory repertoire'.[120] In the narrow sense, codes denote 'computer codes'.[121] The examples include a password, pin and username. In the broad sense, codes are referred to as the 'architecture'[122] and sometimes, the technical architecture of the Internet.[123] This relates to all the hardware and software that function as normative rules.[124] It comprises the layers that together make an ICT infrastructure. These layers are the content layer (the symbols and images), the application layer (the underlying infrastructure that the Internet or Web programmes operate on), the transport (TCP) layer, the Internet protocol (IP) layer (the infrastructure that handles the flow of data), the link layer (this is the interface between physical layer and the network layer) and the physical layer (the copper, wire and links).[125]

A study of the codes-based theory is divided into two (2) sub-sections. Sub-section (a) investigates the theory of *Lex Informatica*. Sub-section (b) examines the codes-based approach.

(a) *Lex Informatica*

Lex Informatica draws inspiration from the Law Merchant (*Lex Mercatoria*) of the Middle Ages.[126] Law Merchant included the laws of different nation states.[127] These laws were enshrined in the practices and customs of those nation states.[128] It developed as a result of the necessity to regulate and control expansions in cross-

---

120 Yeung *Regulation by design* 81.

121 Koops BJ "Criteria for normative technology – the acceptability of 'Code as Law' in light of democratic and constitutional values" in Brownsword R and Yeung K (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart Publishing Portland 2008) 157-174 158.

122 Lessig *Cyberspace* 134.

123 Bonnici *Cyberspace* 115.

124 Kesan and Shah 2003 *Yale Journal of Law and Technology* 281.

125 Chung M and Solum LB "The layers principle – internet architecture and the law" 2004 (79) *Notre Dame Law Review* 815-948.

126 Johnson and Post 1996 *Stanford Law Review* 1389.

127 Pollock F and Maitland FW *The history of English law before the time of Edward I* 2nd (Cambridge University Cambridge 1968) 467 and Trakman LE "From the medieval Law Merchant to E-Merchant Law" 2003 (53) *University of Toronto Law Journal* 265-304 265.

128 Trakman 2003 *University of Toronto Law Journal* 265.

border trading.[129] Consequently, it was necessary to establish a set of rules that were separate from those national laws. These rules were designed to control merchant activities. Furthermore, the merchant rules were to be applied by special Merchant courts. It is argued that the aforesaid rules grew rapidly and became so dynamic and resilient that they progressed with market improvements.[130]

Having monitored the successes of the merchant rules, *Lex Informatica* was developed. It studies the differences between legal rules and the technical architecture of the Internet. It accepts that legal rules and technological rules differ. For instance, the elementary structure for legal regulation is the law.[131] However, the basic structure or framework for *Lex Informatica* is the architectural standard of the Internet, for example, the HTTP and the defaults.[132] In addition, it concedes that the foundation of default rules for a law-making process is the state.[133] However, the foundation of default rules for *Lex Informatica* is the 'technology developer and the social process' in terms of which the use of technology develops.[134]

According to *Lex Informatica,* the technology itself or its applications impose regulations on computer users.[135] The nature of or the choices in the design of the technology generally establish the existence of these rules. Therefore, technologies can be regulated through or by relying on their design choices or architecture.[136] This is the position because the design or architecture of the technology determines who should access a particular technology and who should not.[137] This accessing depends on who holds the required authentication key, for example, username or password.

---

129 Benson BL "It takes two invisible hands to make a market – *Lex Mercatoria* (Law Merchant) always emerges to facilitate emerging market activity" 2010 (3) *Studies in Emerging Order* 100-128 101 and Kerr C "The origin and development of the Law Merchant" 1929 (15) *Virginia Law Review* 350-364.

130 Mefford A "*Lex Informatica* – foundations of law on the Internet" 1997 (5) *Indiana Journal of Global Legal Studies* 211-237 223-224.

131 Reidenberg 1998 *Texas Law Review* 566-567.

132 Reidenberg 1998 *Texas Law Review* 566-567.

133 Reidenberg 1998 *Texas Law Review* 566-567.

134 Reidenberg 1998 *Texas Law Review* 566-567.

135 Murray AD *The regulation of the internet: control in the online environment* (Routledge-Cavendish Abington 2007) 8 and Paré DJ *Internet governance in transition: who is the master of this domain?* (Rowman Littlefield Publishers Maryland 2003) 54.

136 Ong RYC *Mobile communication and the protection of children* (Leiden University Press Leiden 2010).

137 Paré *Internet governance* 54.

Regulations in accordance with *Lex Informatica* do not imply the direct regulation or management of cyberspace.[138] They signify a balancing exercise which influences a modification or change to a technological architecture.[139]

(b) The Codes-Based Approach

The codes-based approach is an additional development of *Lex Informatica*. It acknowledges the existing differences between the real or physical space and cyberspace, and the activities that take place in these respective spaces. The notion of 'dual presence' is introduced in order to illustrate these differences. It implies that computer users occupy two spaces at once. They are both offline or are in real physical world and online or in virtual spaces. It also accepts that the manner in which computer users communicate and transact whilst online is opposed to that which applies when they are in physical spaces.[140] In real spaces, legal rules regulate and constrain their activities or behaviours. In cyberspace, codes or architecture develop particular regulatory frameworks within which their activities should be controlled.[141] The examples of these codes include the software that provides for internet filtering or blocking. Internet filtering technologies prevent or limit the accessing or distribution of particular information.[142]

Having examined how codes regulate or operate, it is stated that a suitable method of controlling modern technologies is one which recognises the following:

> People meet, and talk (communicate), and live in cyberspace in ways not possible in real space. They build and define themselves in cyberspace in ways not possible in real space. And before they get cut

---

138 Paré *Internet governance* 54.

139 Paré *Internet governance* 54.

140 Lessig 1995 *The Yale Law Journal* 17-46

141 Lessig *Code* 88. See also, Grimmelmann J "Regulation by software" 2005 (114) *The Yale Law Journal* 1719-1758 1721.

142 McIntyre TJ and Scott C "Internet filtering – rhetoric, legitimacy, accountability and responsibility" in Brownsword R and Yeung K (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart Publishing Oxford 2008) 109-124 109.

> apart by regulation, we (regulators) should know something about their form, and more about their potential.[143]

Furthermore, the regulatory structures that are based on codes should comprehend the disparities between real physical spaces and automated or cyberspace communications.[144] This includes an understanding of how codes regulate as opposed to how legal rules govern.[145]

In summary, it is revealed that *Lex Informatica* and the codes-based approach belong to the same codes-based theory. The former follows the successes of *Lex Mercatoria.* It particularly draws a clear distinction between the foundation of legal rules and default rules. Consequently, the design or architecture of a technology determines the manner of controlling that technology. The latter accepts that regulating online behaviours will always be different as compared to the control of the activities that occur offline. For example, codes (and not the law) are relevant when regulating online activities. Therefore, it is essential for regulators to understand these disparities. This should compel them to model their regulatory frameworks using the aforesaid dissimilarities.

5.3.3 The Danger or AIS Theory

The danger or AIS theory is a biologically-inspired regulatory approach. It draws inspiration from the biological immune system (BIS).[146] The BIS consists of various kinds of cells or molecules or lymphocytes, macrophages, dendritic cells, natural killer cells, mast cells, interleukins and interferons.[147] It is generally a defence organism or mechanism for the human or organic body.[148] It also serves as a protection mechanism

---

143 Lessig 1995 *The Yale Law Journal* 17-46

144 Lessig 1995 *The Yale Law Journal* 17-46

145 Brownsword 2005 *Journal of Legal Studies* 3.

146 Lee H, Kim W and Hong M "Biological inspired computer virus detection system" in Ijspeert AJ, Murata M and Wakamiya M (eds) *Biologically inspired approaches to advanced information technology* (Springer Berlin 2004) 153-165 155.

147 Hofmeyr SA and Forrest S "Immunity by design - an artificial immune system" in *Genetic and evolutionary computation* (Papers presented at the Genetic and Evolutionary Computation Conference (GECCO-99) Orlando Florida 1999) 1289-1296 1290.

148 Rowe GW *Theoretical models in biology: the origin of life, the immune system and the brain* (Oxford University Press Oxford 1994) 121.

against external attacks (pathogens).[149] The examples of these attacks include bacteria and viruses.[150] The BIS distinguishes and discriminates between self and non-self attacks.[151] Self-attacks relate to those that are known to a system or human body. Non-self attacks include those that arise in the future as a result of a system being exposed to danger. For these attacks to be recognised by a system, alarm signals (Pattern Recognition Receptors) from injured tissues are reported.[152] Thereafter, the immune system reacts by breaking down these attacks. The aim of all this is to maintain or restore a balance in a body.[153] In cases where a balance cannot be maintained, it then becomes necessary to inject a body (process of immunisation) with security boosting or enhancement measures.

Having observed the workings of the BIS, the AIS theory was introduced. Its popularity can be attributed to the fact that a biological body is also understood in terms of 'codes, dispersals or networks'.[154] A biological body is armed with biological immune systems that are 'robust, adaptable and autonomous'.[155] Given the aforementioned, it is argued that computer systems or networks also possess characteristics that are analogous to that of a human body.[156] They are dynamic in that programmes and software are installed and erased whenever there is need, new computer users emerge almost every day and configurations always change.[157]

For purposes of technology regulation, the AIS theory supports a creation of a self-protective framework (immune system). The immune system should be able to respond to external non-self attacks or dangers. The dangers should be measured by 'damage to cells indicated by distress signals that are sent out when cells die an unnatural death

---

149 Rowe *Theoretical models* 121.

150 Rowe *Theoretical models* 121.

151 Matzinger P "The danger model – a renewed sense of self" 2002 (296) *Science* 301-305 301. For an interesting study of self-non-self attacks see Bretscher P and Cohn M "A theory of self-non-self discrimination" 1970 (169) *Science* 1042-1049 1042-1046.

152 Matzinger 2002 *Science* 301.

153 Matzinger 2002 Science 301.

154 Birke L *Feminism and the biological body* (Edinburgh University Press Edinburgh 1999) 142 and Dasgupta D, Yu S and Nino F "Recent advances in artificial immune systems – models and applications 2011 (1) *Applied Soft Computing* 1574-1587 1574-1575.

155 Hofmeyr SA and Forrest S "Architecture for an artificial immune system" 1999 (7) *Evolutionary Computation* 45-68 45.

156 Hofmeyr and Forrest 1999 *Evolutionary Computation* 46.

157 Hofmeyr and Forrest 1999 *Evolutionary Computation* 46.

(cell stress or lytic cell death, as opposed to programmed cell death or *apoptosis*)'.[158] In addition, it should facilitate the building of different sets of detectors (intrusion detection systems), for example anomaly and misuse detections. These detectors should correspond with conventional antigens.[159] These antigens must be empowered with sniffing capabilities. They ought to be able to sense external anomalies, for example the illegal use, exploitation and abuse (intrusions) of computer systems.[160] The anomalies should then be matched with known or probed intrusions. If there is a match, or should the anomalies go beyond a particular threshold, the detectors should be automatically activated.[161] This activation ought to consequently be reported to an operator who must then assess and evaluate the anomalies.[162]

5.3.4 The Systems Theory

The systems theory was first introduced by Von Bertalanffy during the 1930s. He acknowledges that a study of systems has been a province of academic scrutiny for many years. However, Von Bertalanffy observes that academics have failed to examine the dynamics of systems. Having spotted this loophole, he then introduced the idea of a 'general system theory'.[163] The general system theory holds the view that 'every living organism is an open system, characterised by a continuous import and export of substances or subsystems.[164] It also describes systems as elements or parts that are connected or attached to an operated organism, like a computer.[165] These systems can include a 'set of social, biological, technological or material partners' that

---

158 Aickelin U and Cayzer S "The danger theory and its application to artificial immune systems" (Papers delivered at the 1st Intentional Conference on ARtificial Immune Systems (ICARIS-2002), 2002 Canterbury) 141-148 141.

159 Aickelin et al "Danger theory - the link between AIS and IDS?" in Timmis J, Bentley P and Hart E (eds) *Artificial immune systems* (Springer Berlin 2003) 147-155 147-148.

160 Aickelin et al *Danger theory* 148.

161 Aickelin et al *Danger theory* 148-149.

162 Aickelin et al *Danger theory* 150.

163 See Von Bertalanffy L *General system theory: foundations, development, applications* (George Braziller Inc. New York 1968) and Von Bertalanffy L *Perspectives on general system theory: scientific-philosophical studies* (George Braziller Inc. New York 1975).

164 Von Bertalanffy *Perspectives* 38.

165 Von Bertalanffy *Perspectives* 159.

collaborate on a common purpose.[166] Von Bertalanffy calls this organism the 'whole or wholeness' of a system.[167]

The idea that computers operate in a similar fashion to other organisms, for example humans, animals or plants needs to be substantiated. It does not necessarily suggest that computers have a life of their own or that their operation can be linked to Plato's two world theory, namely the sensible and intelligible worlds.[168] Computers particularly carry out the functions as directed by humans. Sometimes, these functions are beyond the scope of what is normally anticipated in real physical spaces or offline. Simon appears to also support this viewpoint.[169] From his reasoning, it is inferred that computers fall within the category of things or objects that he refers to as the 'artificial' or 'man-made' things or objects.[170] These he calls objects that are a product of or generated by art rather than nature.[171] They are not authentic or natural and do not have relations with the essence of the matter, for example the force of gravity.[172]

The general systems theory acknowledges that various systems produce their own existence within a living organism.[173] They cultivate their own languages. These languages are appropriately understood by those who habitually or consistently work with those living organism, that is, technicians or computer programmers.[174] Von Bertalanffy cautions technicians and computer programmers against the danger of becoming a computer 'moron, button-pusher or learned idiot'.[175] These he describes as people who do not contribute to computer innovation or solve existing technology

---

166 See Hjørland and Nicolaisen http://www.iva.dk/jni/lifeboat-_old/Positions/Systems%20theory.htm (Date of use: 10 December 2012). See also, Febbrajo A "The rules of the game in the welfare state" in Teubner G (ed) *Dilemmas of Law in the Welfare State* (De Gruyte Berlin 1986) 129.

167 Von Bertalanffy *Foundations* 5 and Von Bertalanffy *Perspectives* 157.

168 Huard RL *Plato's political philosophy: the cave* (Algora Publishing New York 2007) 35-37. See also Solomon RC and Higgins KM *The big questions: a short introduction to philosophy* 8th ed (Cengage Learning Wadsworth 2010) 121-123.

169 Simon HA *The sciences of the artificial* 3rd ed (The MIT Press Cambridge 1996) 3-5.

170 Simon *Artificial* 3-5.

171 Simon *Artificial* 4.

172 Simon *Artificial* 4.

173 Samuelson P "Five challenges for regulating the global information society" in Marsden CT (ed) *Regulating the global information society* (Routledge London 2000) 317-319.

174 Von Bertalanffy *Foundations* 10.

175 Von Bertalanffy *Foundations* 10.

regulatory challenges.[176] He then requires that a technology regulatory framework should examine the 'whole or wholeness' of all the systems that make-up the living organism.[177]

The works of Morgan and Yeung in relation to the systems theory of regulation are also worth noting. They group the systems theory under the label 'institutionalist'.[178] This grouping is made following the criticism of the systems theory that it fails to recognise the important role played by institutions in regulatory settings.[179] Morgan and Yeung acknowledge that institutional dynamics have 'a life of their own in regulatory regimes'.[180] Also, they concede that regulatory theories must accept that rule-based spheres, for example regulatory organisation, corporations or states are essential in 'explaining why or how regulation emerges'.[181] In particular, they must accept that regulations are a product of an organisational structure.[182] Therefore, processes, for example rules, norms and routines, serve as a guide for such a structure.[183] The meaning of 'rules', norms and routines in this instance is not attributed to legal rules, norms and routines. However, they connote for purposes of the systems theory of regulating 'rules, norms or routines of technology' or 'technological rules, norms or routines'.[184]

An approach to an ICT regulation which is abstracted from the institutionalist label is one which recognises and is modelled from society or societal developments. In particular, it accentuates the idea that systems are closed and self-referential spaces.[185] In addition, systems generate or re-generate their own constituent parts

---

176 Von Bertalanffy *Foundations* 10.

177 Von Bertalanffy *Perspectives* 157.

178 Morgan and Yeung *Law and regulation* 53. Other theories that are grouped under the institutionalist label are the 'Tripartism' and 'regulatory space' theories.

179 Hjørland and Nicolaisen http://www.iva.dk/jni/lifeboat-_old/Positions/Systems%20theory.htm (Date of use: 10 December 2012).

180 Morgan and Yeung *Law and regulation* 53.

181 Morgan and Yeung *Law and regulation* 53.

182 Scott http://icos.groups.si.umich.edu/Institutional%20Theory%20Oxford04.pdf (Date of use: 13 May 2011).

183 Scott http://icos.groups.si.umich.edu/Institutional%20Theory%20Oxford04.pdf (Date of use: 13 May 2011).

184 Brownsword R and Yeung K "Regulating technologies – tools, targets and thematic" in *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing Oxford 2008) 3-22 5.

185 Morgan and Yeung *Law and regulation* 69.

through interaction with their various constituent parts.[186] Accordingly, legal rules do not shape the activities or behaviours of systems. Simply, legal rules are peripheral nuisances to the workings and operations of systems.[187]

5.3.5 The Good Regulator Theorem

Conant and Ashby are the champions of the Good Regulator Theorem.[188] The theorem claims that every good regulator of any arrangement must be a model or reproduction of that specific arrangement.[189] For our purposes, this means that a framework to regulate ICTs must be a representation of the software or networks that form the basis of the technology to be regulated.[190] From this, it is deduced the theory that 'every good key must be a model of a lock it opens'.[191] Simply put, it means something like the following:

> (The) *pursuit* of a goal by some dynamic agent (Regulator) in the face of a source of obstacles (System) places at least one particular and unavoidable *demand* on that agent, which is that the agent's behaviours *must* be executed in such reliable and predictable way that they can serve as a *representation* (Model) of that source of obstacles.[192]

Having observed the argument by Scholten, it is argued that ICTs are a conglomeration of systems or networks many of which have sub-systems or sub-networks. They share similar characteristics. These characteristics have similar structures or shapes and others do not. Therefore, regulators are required to develop regulatory models that

---

186 Morgan and Yeung *Law and regulation* 70.

187 Morgan and Yeung *Law and regulation* 69.

188 See in general Conant RC and Ashby WR "Every good regulator of a system must be a model of that system" 1970 (1) *International Journal of Systems Science*. See also Scholten DL http://www.goodregulatorproject.org/images/A_Primer_For_Conant_And_Ashby_s_Good-Regulator_Theorem.pdf (Date of use: 18 December 2012).

189 Conant and Ashby 1970 *International Journal of Systems Science* 89.

190 Murray *Conceptualising* 290.

191 Scholten DL http://www.goodregulatorproject.org/images/Every_Good_Key_Must_Be_A_Model_Of_The_Lock_It_Opens.pdf (Date of use: 18 December 2012).

192 Scholten DL http://www.goodregulatorproject.org/images/Every_Good_Key_Must_Be_A_Model_Of_The_Lock_It_Opens.pdf (Date of use: 18 December 2012).

appreciate the functioning or non-functioning of the systems or networks. The basis must be to establish a framework to control existing hindrances and to also provide solutions to potential disputes.[193] This framework should discourage regulators from habitually and invariably re-inventing the technology 'regulatory wheel'.[194] In other words, regulators should anticipate the dynamics of systems or networks (system or network dynamics), and the various challenges that those systems are likely to generate.[195] This should enable them to create ICT regulatory paradigms that are bound to the technology and are evolving with it.[196] Lastly, it requires regulators to establish and identify areas where ICT challenges are likely to ensue and thereafter to map, design and re-design measures or processes that respond to the looming challenges.

Better regulations for purposes of the Good Regulator Theorem would be those that are conceptualised and adopted by the people who are involved in a particular industry. For example, regulations for ICT industry would require that expert or skilled people in that industry be involved. The basis for all this is to ensure that ICT regulations are modelled from the technology itself and the dynamics of the systems or networks that form the basis of the ICT.

5.3.6 Summary

The question regarding whether or not ICTs can properly be regulated is no longer only a question of fact. It has nowadays become a question which the legislators also grapple with. However, a proper scrutiny of this question has been hampered by the existing disagreements regarding whether or not recent forms of technologies can be regulated or controlled. For example, there are some who argue that ICTs and regulations are distinctive and, sometimes, opposing spheres. Technologies connote innovation, growth and development. However, regulations imply administration,

---

193 Susskind RE *The future of law: facing the challenges of information technology* (Clarendon New York 1996) 2-43.

194 Brownsword R "So what does the world need now? - reflections on regulating technologies" in Brownsword R and Yeung K (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart Publishing Oxford 2008) 23-48 30.

195 Forrester JW "Industrial dynamics - a major breakthrough for decision makers" 1958 (36) *Harvard Business Review* 37-66 37.

196 Brownsword *So what?* 27.

bureaucracy and an affront to innovation, growth and development. Given these differences, it is argued that one domain cannot or should not be used to control and manage the other. There are also others who contend that technologies or the activities that take place through the use of technologies are connected to real physical spaces. Consequently, technologies are spheres where regulations apply or should apply.

In this research, the view that ICTs can be regulated is preferred. Following this preference, it is then asked how such a technology controlling or regulatory framework should be structured? An attempt is made in this chapter to answer this question by examining the certain selected theories related to technology regulation. These are the codes-based theory, the AIS theory, the systems theory and the Good Regulator Theorem. The theories are not necessarily ICT regulations. They only assist in creating a regulatory structure which is able to respond to ICTs and the ease with which these technologies develop.

An examination of the codes-based theory is divided into two sections. There is *Lex Informatica* and the codes-based approach. *Lex Informatica* avers that the law is the structure of legal regulation. However, the Internet architecture or design structure is an indispensable framework for *lex Informatica.* The Internet architecture and the design of the technology regulate or impose regulations. The codes-based approach builds from *lex Informatica.* It accepts that codes are essential for technology regulation. These codes determine who should access the technology and who should not. An example of this is the technology related to Internet filtering. The AIS theory is an immunological regulatory approach which is inspired by biology. It is modelled on how a human body defends itself from the outside or non-self attacks, for example, germs and viruses. It submits that ICTs have characteristics that are similar to those found in a human body. Therefore, defence mechanisms that are analogous to those that are found in humans should be built. The defence measures are referred to as a set of detectors (immune system). They help in segregating between different attacks. They also assist in sniffing out non-self anomalies in computer systems or networks. The systems theory is influenced by the works of a number of academics. Firstly, the ‘general systems theory’ is revealed. It avers that every living organism is generally an open system. The systems that constitute this living organism generate various sub-systems. Therefore, a suitable method to regulate these organisms should aim to

control and manage their 'whole or wholeness'. Secondly, an approach which is modelled from the institutionalist label is discussed. It argues that systems generate their constituent parts by means of having relationships with each other. The Good Regulator Theorem is influenced by the idea that 'every good key must be a model of a lock it opens'. Following this idea the theorem argues that every regulatory scheme must be a reproduction of the scheme it seeks to regulate. For example, if regulations are designed to control a particular technology, a complete study of the nature and workings of such a technology is indispensable.

The theories above guide the manner of controlling recent forms of technologies and their associated challenges. In that regard, they accept that the law or legal rules regulates in a different way from regulations. A number of conclusions are reached that support this averment. However, it is submitted that an isolated or selective reading of the theories will not assist a regulator to fully understand their objectives. This is the case because the regulatory approaches that are followed by these theories differ in relation to the manner and structure of the control. Consequently, an attempt should be made to harmonise the differences in these theories in order to help establish, design and endorse a compact ICT regulatory structure.

5.4 CONCLUSION

It is revealed that, for purposes of regulating ICTs and their associated challenges, a clear distinction should be made between the law and regulations. This necessity is encouraged by the fact that a control of a particular occurrence should, in principle, be fit for its purpose. Accordingly, if the law is preferred as the fitting ICT regulatory mechanism then it should understand the dynamics of the technology. This entails being able to evolve with the changes that emanate from the technology. Having studied the law and regulations, regulations are found to be better suited to regulate recent forms of technologies. This selection is made because regulations are flexible[197] and easier to establish.[198] Therefore, regulators do not have to follow the inconvenient and rigid process of commencing legal rules if technology develops or a new

---

197 Murray *Legal futures* 288.

198 Barlow JP https://projects.eff.org/~barlow/EconomyOfIdeas.html (Date of use: 24 October 2012).

technology emerges. It is important to note that the law does not necessarily cease to have a role to play in ICT regulations. Specifically, the law retains a facilitative function. This means that it assists in channelling the nature and shape of ICT regulations.

There are differences which exist regarding the meaning and structure of ICT regulations. On the one hand, regulations are said to denote a form of command and control mechanism. The latter is enforced by means of legal rules.[199] In addition, the state plays an essential role.[200] On the other hand, it is argued that regulations follow a decentring stance. This entails that the essential role-players in regulatory regimes, for example, the state, society, regulated firms and Internet users are involved in the regulatory process.[201] This consideration particularly leads to what is referred to as *better regulation*.[202] *Better regulations* are products of a holistic approach to regulating whereby the idea of a single and supreme regulator is discarded. They assist in the study of certain selected ICT regulatory theories. The theories are the codes-based theory, the AIS theory, the systems theory and the 'Good Regulator Theorem'. These regulatory theories are not complete and exhaustive. However, they are essential in that they promote the hypothesis that every technology regulatory paradigm should generally be technology-neutral or independent.

For ICT regulatory purposes, it may be necessary to read the theories together in order to establish a complete comprehension of their objects or principles. In one case, the meaning of the codes-based theory may be lost if it is not read together with the systems theory or Good Regulator Theorem. It may thus be impossible or challenging for a regulator to establish a codes-based framework without following the steps that are set out in the systems theory. Accordingly, it may be necessary for a regulator to copiously understand the dynamics of ICT systems, such as the Internet and Web. These relate to the fact that these systems are connected to a living organism, like an operated computer.[203] A regulator may have to understand that in order to regulate

---

199 Coglianese and Mendelson *Handbook of regulation* 146.

200 Koops *Technology* 80-81.

201 Gunningham *Regulation* 131.

202 Gunningham *Regulation* 131.

203 Von Bertalanffy *Perspectives* 159. These systems can include a 'set of social, biological, technological or material partners' that collaborate on a common purpose. See Hjørland and Nicolaisen http://www.iva.dk/jni/lifeboat-_old/Positions/Systems%20theory.htm (Date of use: 10 December 2012).

these systems or networks it is essential to examine their 'whole or wholeness', that is, the ICT.[204] In other words, they may be required to model their ICT regulation from the 'whole or wholeness' of the technology to be regulated.[205] In other cases, the Good Regulator Theorem may assist regulators in establishing a structure of ICT regulation which is abstracted from the danger theory. The AIS theory is a biologically-inspired regulatory structure. It specifically uses the robustness, adaptability and autonomy of biological immune systems as a lead.[206] It then accepts that computer systems or networks also possess the characteristics that are comparable to those of a human body.[207] They are dynamic and developing.[208] Therefore, it may be necessary for the regulators that they develop frameworks that protect systems or networks from external attacks, such as e-crimes. These frameworks should follow the wording of the other ICT regulatory principles, for example the Good Regulator Theorem. In this instance, regulators may design regulations that conform to the principle that 'every good key must be a model of a lock it opens'.[209] In other words, it will have to acknowledge that a structure to regulate or control ICTs should be led by or founded from the manner in which ICTs are structured.

Having examined the need to regulate and control ICTs and their associated challenges, chapter 6 below investigates the current approaches to ICT regulation. It particularly accepts that e-crimes are one of the major challenges to an information society. Therefore, chapter 6 examines the overall approach or approaches to the control and management of e-crimes. These approaches form part of what is referred to as the 'System or Process of E-Authentication' or the 'E-Authentication System or Process'.[210]

---

204 Von Bertalanffy *Foundations* 5 and Von Bertalanffy *Perspectives* 157.

205 Conant and Ashby 1970 *International Journal of Systems Science* 89.

206 Hofmeyr and Forrest 1999 *Evolutionary Computation* 45.

207 Hofmeyr and Forrest 1999 *Evolutionary Computation* 46.

208 Hofmeyr and Forrest 1999 *Evolutionary Computation* 46.

209 Scholten DL http://www.goodregulatorproject.org/images/Every_Good_Key_Must_Be_A_Model_Of_The_Lock_It_Opens.pdf (Date of use: 18 December 2012).

210

CHAPTER 6

E-AUTHENTICATION

CHAPTER 6

E-AUTHENTICATION

6.1 INTRODUCTION

In chapter 5 answers or solutions to the questions regarding whether or not ICTs and their associated challenges can be regulated were sought. It was submitted that a difficulty generally exists regarding the regulation or not of ICTs. This challenge is partially associated with the uncertainty regarding whether or not the law or regulations are suitable for this control exercise. Given this uncertainty, different regulatory models were differentiated. These include those that are founded on legal rules and that which are abstracted from regulations. It was found that the role of law in ICT regulations should be to shape the structure of ICT regulations. This is the case because regulations in contrast to the legal rules are flexible and are able to evolve with the times.[1] More specifically, they are able to transform and improve with the variations and developments in contemporary technologies. Consequently, it was submitted that regulations are better suited to regulate ICTs and the ICT challenges. However, a question still remained relating to the manner of structuring or shaping such a regulatory framework. In responding to this question, a number of regulatory theories were discussed. These theories are not regulations as such. They simply support the view that a suitable ICT regulatory approach is the one that recognises the role of all the regulatory industries in the regulatory process. This type of approach is referred to as *Better Regulation* as opposed to *Less Regulation*.[2] The rationale for *better regulation* is to develop an all-encompassing regulatory structure which is attached to the technology and is able to evolve with it.[3]

---

1 Stenning PC et al "Controlling interests – two conceptions of order in regulating a financial market" in Friedland ML (ed) *Securing compliance: seven case studies* (University of Toronto Press Toronto 1990) 88-119 102.

2 Boyer R "The regulation approach as a theory of capitalism – a new derivation" in Labrousse A and Weisz JD (eds) *Institutional economics in France and Germany* (Springer Berlin 2001) 49-92 50. See also Baldwin R "Better regulation in troubled times" 2006 (1) *Health Economics, Policy and Law* 203-207 204-205.

3 Kirkpatrick and Parker *Regulatory Impact Assessment* 1-2.

Despite the difficulty in regulating ICTs and their associated challenges, the viewpoint that ICTs can be regulated is followed. It is particularly conceded that e-crimes pose a serious threat to the information society. Therefore, processes should be established that mitigate the risks and identify the measures to regulate e-crimes (e-crimes regulatory measures). The measures ought to generally be two-fold. They should provide, on the one hand, for the criminalisation of e-crimes. In one case, the accessing,[4] interception, interference with, modification or destroying of information without authority may be proscribed.[5] In other cases, the manufacturing, trading or offering to trade, possession or use of a contrivance (for example, a computer programme) in order to overcome or obstruct computer security measures may be made an offence. On the other hand, the measures should deal with the prevention of e-crimes and endorse a System of Authentication or, alternatively, an Authentication Structure. The abovementioned system may sometimes serve as the 'last line of defence'.[6]

It was indicated in chapter 1 of this research that e-authentication is not the only method that can be used in order to prevent e-crimes. Other methods, for example awareness programs, anti-viruses and building of firewalls may also be useful in deterring e-crimes. In this chapter, it is submitted that preventing e-crimes is better than dealing with or recovering from the consequences of this phenomenon. The phrase *prevention is better than cure* properly illustrates the significance of this form of prevention.[7] It specifically states that forestalling a wrong is usually better than dwelling on and making good its 'adverse effects after the event'.[8] Due to this importance, the

---

4 The term 'access' means, within the context of the ECT Act, the 'actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data'. See s 85 of the ECT Act.

5 See in general, Chapter XIII of the ECT Act.

6 Taylor A and Eder L "A comparison of authentication, authorisation and auditing in Windows and Linux" in Warkentin M and Vaughn RB (eds) *Enterprise information systems and assurance system security: managerial and technical issues* (Idea Group Publishing Hershey 2006) 326-342 327.

7 However, in this research it is argued that prevention is not always better than cure. For example, cutting off a person's head is not better than curing such a person's headache. See Chesterton GK *Eugenics and other evils* (Cassell and Company London 1922) 55.

8 Cane P *The Anatomy of tort law* (Hart Publishing Oxford 1997) 100.

process of authentication is selected as one of the effective measures to prevent e-crimes.

6.2 A THEORETICAL APPROACH TO AUTHENTICATION

The process of authentication is, in the main, an old phenomenon. Modes of authentication had long existed to support and preserve the credibility of a person or thing, for example a document. The notion credibility denotes the quality of being believable.[9] Hence the saying that: 'credible people are believable people….credible information is believable information'.[10] Credibility is sometimes associated with trust, not necessarily confidence.[11] Accordingly, it denotes the readiness to avail oneself to or accept a risk based on the positive expectations of or generated by the other person.[12] The notion of trust is one of the most important aspects of everyday life.[13] In their everyday lives people trust that their friends would be kind to them, they trust that motorists on the road would follow traffic rules and they trust that the goods that they buy have the quality that is commensurate with how much they pay for them.[14]

A multitude of methods are frequently used in order to establish the credibility of a person or a person's identity. Firstly, a person's face may be analysed. The instructive feature points that are found in a person's face, for example the eyes and mouth may assist in making this analysis.[15] Secondly, a person's finger prints may be inspected. This may be accomplished by scrutinising the uniqueness of the structures, that is, the

---

9 Fogg BF and Tseng H "The elements of computer credibility" in *Computing systems* (Papers delivered at the International Conference on Human Factors in Computing Systems 18-20 May 1999 Association of Computing Machinery Inc. New York 1999) 80-87 80.

10 Fogg and Tseng "Elements" 80.

11 Kim PH, Ferrin DL, Cooper CD and Dirks KT " Removing the shadow of suspicion – the effect of apology versus denial for repairing competence-versus integrity-based trust violations" in Costa AC and Anderson N (eds) *Trust and social capital organisations* (Sage Publications London 2013) 175-205 175-177 and Earle TC, Siegrist M and Gutscher H "Trust, risk perception and the TCC model of cooperation" in *Trust in risk management: uncertainty and the scepticism in the public mind* (Earthscan Publishing London 2010) 1-49 4.

12 Earle, Siegrist and Gutscher *TCC model* 4.

13 Selby-Bigge LA (ed) *A treatise on human nature by David Hume* (The Claredon Press Oxford 1896) 15-18.

14 Selby-Bigge *David Hume* 15-18.

15 Tistarelli M, Lagorio A and Grosso E "Understanding iconic image-based face biometrics" in Tistarelli M, Bigun J and Jain AK (eds) *Biometric authentication* (Springer Berlin 2002) 19-29 22.

global and local structures, in such a person's finger prints.[16] Thirdly, a person's signature may be verified or corroborated. The aforementioned is a complicated process. More specifically, the acceptance of a signature as one of the authentication means in legal discourse is usually debated. Studies relating to the validity of wills illustrate the aforementioned. In these readings, it is revealed that signatures are conventionally required to be handwritten, typewritten, or be in some form of a photographic procedure.[17] In some cases, thumb prints[18] and initials are accepted.[19] However, it has always been enquired whether a mark could or should be accepted as a signature or not. It is stated that a mark is, but does not necessarily entail, the making of a cross. It may be in a form of a 'thumbprint, rubber stamp or a seal-ring impression'.[20] In England, courts seem to agree that a mark satisfies the requirements of signing.[21] However, it must have been written or included in a document with an intention of making it a signature. However, South African courts and academics alike have always differed in relation to the aforementioned question.[22] These differences existed until the coming into operation of the Succession Amendment Act.[23] Section 1 of this Act expressly states that a signature includes the making of a mark. The said section partially followed the reasoning of the court in the case of *Putter v Provincial Insurance Co Ltd and Another*.[24] In this case, the court stated that 'any mark on a

---

16 Nilson K and Bigun J "Complex filters applied to fingerprint image detecting prominent symmetry points used for alignment" in Tistarelli M, Bigun J and Jain AK (eds) *Biometric authentication* (Springer Berlin 2002) 39-47 39.

17 Kerridge R and Brierley AHR *Parry and Kerridge: the law of succession* 12th ed (Sweet Maxwell London 2009) 43 and Barlow S, King LC and King AG *Wills, administration and taxation: a practical guide* 8th ed (Sweet Maxwell London 2003) 3.

18 *In the Estate of Finn* (1935) 105 L.J.P. 36.

19 S 1 of the Law of Succession Amendment Act 43 of 1992 (hereinafter referred to as the Succession Amendment Act).

20 De Waal MJ and Schoeman-Malan MC *Law of succession* 4th ed (Juta Cape Town 2008) 60.

21 *In the Goods of Savoy* (1851) 15 Jur. 1042, *In the Goods of Jenkins* (1863) 3 SW & Tr. 93 and *Thorn v Dickens* [1906] W.N. 54.

22 See in general *Ricketts v Byrne and Another* 2004 6 SA 474 CPD, *Jhajbhai and Others v Master and Another* 1971 (2) D. & C.L.D. 370 and *Ex Parte Goldman and Kalmer NN.O* 1965 1 W.L.D. 464.

23 This Act came into operation on 1 October 1992. See Paleker M "Succession" in du Bois F (ed) *Wille's principles of South African law* 9th ed (Juta Cape Town 2007) 666-731 668. See also Scalise Jr RJ "Testamentary formalities in the United States of America" in Reid KGC, de Waal MJ and Zimmermann R (eds) *Comparative succession law: testamentary formalities* (Oxford University Press Oxford 2011) 357-403 385.

24 *Putter v Provincial Insurance Co Ltd and Another* 1963 3 SA 145 (W)

document made by a person for the purpose of attesting the document, or identifying it as his act,…is his signature thereto'.[25]

Generally, a number of tests are used in order to determine the authenticity of a thing, such as a document. These tests are often referred to as the dual tests.[26] They are the authentication test and the best evidence test.[27] The authentication test avers that in circumstances where a thing is not or does not provide for self-authentication its credibility should be established separately.[28] The best evidence test regards a thing itself, for example a document, to be the best evidence.[29] Consequently, in cases where the authenticity of the contents of a document is in doubt the best evidence, for example the document itself, must be furnished.[30]

6.3 AUTHENTICATION – WHAT DOES IT MEAN?

The concept authentication is often confused with the notion authorisation.[31] It is sometimes presumed that these concepts share particular resemblances. However, an examination of these concepts illustrates that they are, in fact, different. The Commission of the European Communities'[32] particularly discloses these dissimilarities. The CEC states that a system of authentication encompasses 'a procedure which allows the payment service provider, i.e. bank, to verify that the payment service user (natural or legal person who has a right of disposal of funds and who allows them to be transferred to a payee) issuing the payment order is authorised to do so'.[33] Thus, it is proof that a certain attribute, namely the identity of a person,

---

25 See *Putter v Provincial Insurance Co Ltd and Another* 1963 3 SA 145 (W) 148E.

26 Klotter JC *Criminal evidence* 5th ed (Anderson Publishing Ohio 1992) 304.

27 Klotter *Evidence* 304.

28 Munday R *Evidence* (Oxford University Press Oxford 2007) 26-27.

29 Blond NC *Evidence* (Aspen Publishers New York 2009) 164. See also Murphy P and Baddour L "International criminal law and common law rules of evidence" in Khan KAA, Buisman C and Gosnell C (eds) *Principles of evidence in international criminal justice* (Oxford University Press Oxford 2010) 96-156 99.

30 Blond *Evidence* 164 and Murphy and Baddour *International criminal law* 99.

31 There is also another concept which precedes authentication and authorisation. This is referred to as auditing. It entails a process of investigating the activities that are carried out on a system in order to identify them by name and time.

32 Hereinafter referred to as the CEC.

33 Art 4(13) of the Commission of the European Communities "Proposal for a Directive of the European Parliament and of the Council on Payment Services in the Internal Market and amending Directive 97/7/EC, 2000/12/EC and 2002/65/EC" 1 December 2001.

exists.[34] From this analysis, it becomes evident that authorisation (or to authorise) succeeds the authentication process. It specifically denotes a practice to establish whether a person who has undergone or was subjected to an authentication procedure can access a particular resource or not.[35] For example, when access to a particular infrastructure is sought, authority to use that infrastructure is granted to those who possess proper authentication.[36] In contrast, access is denied to those with improper or insufficient authentication.[37]

Having examined the aforesaid differences, it is stated that the system of authentication supports or assists in supporting, by means of substantiation, a finding that a person or thing is what it claims.[38] This finding is established by verifying the identity of a person[39] and testing the credibility of a thing.[40]

6.4 SUMMARY

Authentication processes are old phenomena. A number of methods are customarily used in order to authenticate or establish the credibility of a person or thing (document). In one case, face images may be analysed, finger prints may be examined and signatures may be verified. In other cases, the authentication and best evidence tests may be applied. The basis is or should be to promote trust and believability of a person or thing. It is also demonstrated that a system of authentication does not necessarily imply an authorisation process. The former is a process which seeks to identify a person or document, whereas the last-mentioned attempts to establish whether or not a person should access a specific resource.

---

34 Camp LJ *The economics of identity theft: avoidance, causes and possible cures* (Springer Bloomington 2007) 13.

35 Todorov D *Mechanics of user identification and authentication: fundamentals of identity management* (Auerbach Publications Florida 2010) 7.

36 Todorov *Identity management* 4.

37 Todorov *Identity management* 4.

38 Andrews S "Building trust online – work at the OECD" in Schulz A (ed) *Legal aspects of an e-commerce transaction* (Sellier European Law Publishers München 2006) 243-247 243.

39 Oppliger R *Authentication systems for secure networks* (Artech House Publishers Boston 1996) 17-18.

40 Martin SE "Information controls and needs of information flow in representative democracies" in Lederman E and Shapira R (eds) *Law, information and information technology* (Kluwer Law International The Hague 2001) 369-389 386-388.

It is submitted that the achievements or successes of the authentication measures in offline settings have led to these mechanisms being used in online environments. In online settings, they are called e-authentication.

6.5 E-AUTHENTICATION

6.5.1 Background

E-authentication marks a progression from or is an online equivalent of offline authentication.[41] It connotes 'a process by (means of) which a person or legal entity seeks to verify the validity or genuineness of a particular piece of information'.[42] Alternatively, it encompasses a formal 'assertion of validity, such as the signing of a certificate: we authenticate what it certifies'.[43] It also responds to a need to promote trust in e-commerce.[44] Accordingly, it sets out legal rules that increase certainty and security in the use of ICT systems or networks.[45] These rules are designed to preserve the integrity of the information which is held by computer users.[46] In addition, the rules encourage responsible parties, for example banks to identify the legitimacy of the users.[47] Consequently, this identification helps to establish whether or not a particular user or information which is held by a user is known to a system or network.

A number of codes or devices are generally used in order to support a structure for e-authentication. The most significant of these include passwords, pins, digital or e-

---

41 Berinato http://www.csoonline.com/article/220784/FFIEC_Second_Thoughts_on_Second_Factors (Date of use: 22 April 2010).

42 See Article 3(5) Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014.

43 Mason S *Electronic signatures in law* 2nd ed (LexisNexis London 2007) 1.

44 United Nations Commission on International Trade Law (UNCITRAL) "Promoting confidence in electronic commerce: legal issues on international use of electronic authentication" 2009 35. To be accessed at http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf.

45 UNCITRAL 2009 35.

46 UNCITRAL 2009 17.

47 UNCITRAL "Legal guide on electronic funds transfer" 1987 7.

signatures that use public or private key infrastructures (PKIs), smart cards, one-time-passwords (OTPs),[48] USB plug-in devices or biometric identification.[49]

(a) Passwords or Codes

Passwords or codes are an assemblage of the technologies that are used to manage access to information systems or networks. They operate in a similar manner as a key.[50] They may also be used in order to sign a document or a communication, for example an online document.[51]

(b) E-Signatures

E-signatures include cryptographic codes or techniques.[52] They generally assist in ensuring that the original contents of information are protected from unwanted modifications or alterations.[53]

(c) PKIs

In cryptographic schemes different sets of keys are used in order to authenticate information.[54] The first key is referred to as a symmetric key. In this case, the same key is used both for encryption (a process of making information unintelligible to other computer users) and decryption (process of transforming information into becoming

---

48 OTPs are random numbers that are required to be used when entering into, for example e-transactions. They can only be used once and become inactive if the purpose for which they were initiated and issued has been achieved.

49 Grabosky PN and Smith RG *Crime in the digital age: controlling telecommunications and cyberspace illegalities* (Transaction Publishers New Jersey 1998) 152. See also Federal Financial Institutions Examination Council (FFIEC) http://www.ffiec.gov/pdf/authentication_guidance.pdf (Date of use: 13 July 2013).

50 Burnett M and Kleiman D (eds) *Perfect passwords: selection, protection, authentication* (Syngress Publishing Massachusetts 2006) 3-4.

51 UNCITRAL 2009 16.

52 Zhang F and Wang Y "Security fundamentals" in Kou W (ed) *Payment technologies for e-commerce* (Springer Berlin 1998) 7-38 24.

53 Zhang and Wang *Fundamentals* 24.

54 Zhang and Wang *Fundamental* 13.

intelligible). The second key is called an asymmetric key. In this instance, the key which is used for encryption differs from the one used for decryption.[55]

A difference is made between public-key cryptography and private-key cryptography. Pieprzyk, Hardjono and Seberry discuss this distinction and its importance to the e-authentication process.[56] In the former, two separate keys are used for e-authentication purposes. One key is referred to as the public key while the other is called the secret key. In the case of the latter, the keys are analogous and they are referred to as the secret keys.

(d) Smart Cards

Smart cards are comparable to computers. They have built-in computer chips. These chips record, compute and store sensitive information. The chips also assist in the verification and validation of information.[57]

(e) Biometrics Identification

In this category of identification, different technological devises are commonly used in order to identify a person or thing.[58] These technologies investigate a person's finger prints, hand geometry, retinal or iris scan, voice or facial features.[59] This identification is made possible by the idea that humans possess particular biological characters that are different from other persons.

However, it is accepted that certain constraints should be present before reliance can be placed on these characters. These are the following:

> *Universality*, which means that every person should have the characteristic, *uniqueness*, which indicates that no two (or more)

---

55 Zhang and Wang *Fundamentals* 13.

56 Pieprzyk J, Hardjono T, and Seberry J *Fundamentals of computer security* (Springer Berlin 2003) 69-218.

57 Whitman ME and Mattord HJ *Principles of information security* 4th ed (Cengage Learning Boston 2016) 241.

58 Reid P *Biometrics for network security* (Pearson New Jersey 2004) 3-5.

59 Pearson RL *Electronic security systems: a manager's guide to evaluation and selecting system solutions* (Elsevier Amsterdam 2007) 37 and Zhang D and Yu L "Biometrics for security in e-commerce" in Kou W (ed) *Payment technologies for e-commerce* (Springer Berlin 2003) 71-94 71.

> persons should be the same in terms of the characteristic, *permanence*, which means that the characteristic should be invariant with times, and *collectability*, which indicates that the characteristic can be measured quantitatively.[60]

The cryptograms as studied above are essential to the discussion of e-authentication. They are indispensable in carrying out the pillars of e-authentication. These are either a single pillar or multiple pillars of e-authentication.

6.5.2 E-Authentication Pillars

The pillars of e-authentication depend on the evidence of knowledge or something a person knows; confirmation of possession or something a person possesses, or proof by property or something a person is.[61] These are discussed below.

(a) Proof of Something

Proof of something is frequently associated with a single-factor e-authentication.[62] This is the case because only one factor, that is, a code, pin or password is used for e-authentication purposes. In this instance, a system validates a user, and not the other way around.[63] A user enters a code, pin or password to an allocated space on for example a webpage.[64] Thereafter, a system automatically verifies or matches a code, pin or password. This verification is made against the information of a user that is stored on a system. If a match is established, a system grants access to a user, that is, to authorise.

(b) Proof of Possession

---

60 Jain A, Bolle R and Pankanti S "Introduction to biometrics" in *Biometrics: personal identification in networked society* (Kluwer Academic Publishers Massachusetts 1999) 1-40 4.

61 Whitman and Mattord *Principles of information security* 240 and Reid *Network Security* 9.

62 Zhang and Wang *Fundamentals* 33.

63 Zhang and Wang *Fundamentals* 33.

64 UNCITRAL 2009 29.

This factor of e-authentication is also referred to as a multi or two-factor e-authentication.[65] Multi-factor e-authentication was established consequent to a need to develop a stronger e-authentication framework.[66] It was particularly felt that an e-authentication structure that depends solely on codes, pins and passwords is a 'joke'.[67] In particular, Nielsen and Vedel identify the conventional ways of compromising codes, pins or passwords.[68] In one case, crackers bribe victims of e-crimes in order to obtain the wanted codes, pins or passwords.[69] In others, computer crackers pay guards who protect the physical structures where the codes, pins and passwords are kept and stored in exchange for them to gain entry into the structures.[70]

With increases in online or e-transactions, another shortcoming of a single-factor e-authentication is identified. This relates to the fact that it places 'heavy loads (burden) on human memory'.[71] Consequently, the inability of other computer users to memorise long and complex codes, pins and passwords (strong e-authentication) lead them to take shortcuts and rely on simple-to-guess codes, pins and passwords (weak e-authentication).[72] In order to prevent the aforementioned, an e-authentication framework that relies on more than one e-authentication pillar was developed. This does not necessarily prevent the use of codes, pins and passwords in e-authentication structures. However, it accepts that, for purposes of establishing a stronger e-authentication framework, codes, pins and passwords should be supplemented by other tangible property. This property includes identity cards, smart cards, debit or credit cards.[73]

(c) Proof by Property

---

65 Allen R and Pickup A "Two-factor authentication" in Birch D (ed) *Digital identity management: technological, business and social implications* (Gower Publishing Limited Hampshire 2007) 113-120 113-119 and Schneier B "Two-factor authentication - too little, too late" 2005 (48) *Communications of the ACM* 136 136.

66 Reid *Network Security* 9-14.

67 See Huntington http://www.authenticationworld.com (Date of use: 13 February 2010).

68 Nielsen G and Vedel M *Improving usability of passphrase authentication* (Kongens Lyngby Denmark 2009) 11-12.

69 Nielsen and Vedel *Passphrase authentication* 11-12.

70 Nielsen and Vedel *Passphrase authentication 12*.

71 Ciampa M *Security awareness: applying practical security in your world* 4th ed (Cengage Learning Boston 2014) 40-41.

72 Ciampa *Security awareness* 40-41.

73 Oppliger *Secure networks* 18.

Proof by property refers to the characteristics or biometric features or credentials of a person.[74] These may be physiological or behavioural or both.[75] They include 'finger-scan, hand-scan or hand geometry, retina scan, iris-scan, facial-scan or facial geometry, signature-scan or dynamic signature verification, or voice scan or voice speaker or speaker verification'.[76] In more astute cases, they encompass an observance of keystroke dynamics. These are the characteristic keys and presses of person on a computer keyboard.[77]

6.5.3 Summary

E-authentication demonstrates a progression from the traditional forms of authenticating. It relies on e-codes in order to provide security and trust in electronic systems or networks. The symbols include passwords or codes, pins, digital or e-signatures that use public key infrastructures (PKIs), physical devises, for example smart cards, one-time-passwords (OTPs), USB plug-in devices or biometric identification. These cryptograms support the overall structure for e-authentication. They are also important to the performing of the e-authentication pillars, namely evidence of knowledge; confirmation of possession and proof by property.[78]

Carrying out the e-authentication pillars is generally a part of a county's broad cyber-security framework. In some cases, selected government agencies or institutions assume the duty to ensure that a proper e-authentication agenda is followed. In other cases, this obligation is delegated to certain responsible parties that constantly deal with e-authentication. Ordinarily, countries' e-authentication approaches may agree or differ depending on their overall cyber or information security structures. The section below illustrates these similarities or differences. This section is particularly selective. It only studies the United Kingdom and the European Union, Canada and South African approaches to e-authentication. This selection is made because the South African e-authentication agenda is, in many respects, similar to that of the United Kingdom and

---

74 Reid *Network security* 3-5.

75 Helou TJ "Introduction" in Coats WS, Bagdasarian A, Helou TJ and Lam T (eds) *The practitioner's guide to biometrics* (ABA Publishing Illinois 2007) 1-17 4-5.

76 Zhang and Yu *Biometrics* 71.

77 Jain, Bolle and Pankanti *Biometrics* 11.

78 Reid *Network security* 9.

Canada. In particular, the approaches of these jurisdictions build on the argument that is contained in chapter 5 above. Furthermore, they help in examining the risk sensitive-based e-authentication framework which is identified in chapter 7 below.

6.6 APPROACHES TO E-AUTHENTICATION

6.6.1 United Kingdom

A number of initiatives or directives are available in the UK that deals with e-authentication. The most significant of these are contained in the Electronic Communications Act,[79] Directive 2007/64/EC[80] and Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014. The said initiatives are founded from the premise that 'there is no such a thing as zero risks'.[81] Accordingly, it is sufficient to basically 'create a safe environment in which people…feel protected'.[82] In response to the latter, the initiatives address or seek to address the risks of computer networks[83] and information being used by criminals as instruments to commit e-crimes. This is done by mitigating cases of interference with information, interference with computer systems, misuse of information or systems and online theft or fraud. In terms of Regulation No 910/2014 of the European Parliament and of the Council, addressing the risks and discouraging the risks of interference with information are essential in building trust in electronic or e-transactions. This is the case because a

---

79 See Electronic Communications Act, 2000 (hereinafter referred to as the Communications Act).

80 See Directive of the European Parliament and of the Council on Payment Services in the Internal Market of 13 November 2007 (hereinafter referred to as Directive 2007/64/EC).

81 European Union https://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf (Date of use: 16 November 2015).

82 European https://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf (Date of use: 16 November 2015).

83 A computer network is defined in section 1 of the Cybercrime and Cybersecurity Bill of 2015 as meaning two or more inter-connected or related computer devices, which allows these inter-connected or related computer devices to exchange data or any other function with each other; exchange data or any other function with another computer network; or connect to an electronic communications network.

lack of trust in the security of systems generally results in consumers, businesses and public authorities becoming hesitant to carry out transactions electronically.[84]

This envisaged trust is encapsulated in Directive 2007/64/EC. Article 5(e) of this Directive requires the structure for e-authentication to be proportionate, sound and adequate.[85] This structure is intended to be comparable, commensurate or equivalent to the risks that are generated or potentially posed by e-crimes. In addition, it ought to be valid, reasonable and suitable for the aforesaid purpose. Furthermore, the e-authentication process should identify the person to be e-authenticated, his or her origin and the integrity of the data used or to be used during the e-authentication process.[86]

E-authentication in the United Kingdom is carried out as part of the United Kingdoms' ICT governance strategy and internal control principles.[87] The strategies and principles relate to administrative, risk management and accounting procedures.[88] Therefore, a number of relationships are created that support the United Kingdom's e-authentication structure. These relationships are exemplified below.

(a) Important Relationships

E-authentication in terms of Directive 2007/64/EC is based on the workings of certain relationships between different persons. In this chapter the interaction between a payer, payment system and payment institution is examined. A payer can be a natural or juristic person.[89] It holds a payment account with a payment institution and allows payment orders to be made from that account.[90] A payment account is held or kept in the name of a payer and is consequently used by it to execute e-transactions. Payment orders can be in the form of instructions by a payer for the execution of e-

---

84 See preamble to Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014.
85 Article 5(e) of Directive 2007/64/EC.
86 Article 3(5) of Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014.
87 Art 5(e) of Directive 2007/64/EC.
88 Art 5(e) of Directive 2007/64/EC.
89 See, Art 4(7) of Directive 2007/64/EC.
90 Art 4(7) of Directive 2007/64/EC.

transactions.[91] A payment system is simply a fund-transfer system. It has formal and pre-arranged rules for the processing, clearing and settlement of payment transactions.[92] Payment transactions refer to acts that are initiated by the payer or by the payee. They encompass the 'placing, transferring or withdrawal of funds, irrespective of any underlying obligations between the payer and the payee'.[93] Payment institutions are juristic or legal persons. They have the authority to provide and execute payment services.[94]

(b) E-Authentication Applied

In e-authentication schemes, a payer normally uses the payment systems that are offered by a payment institution in order to commence a payment transaction or transactions. A unique identifier, for example a code, pin or password is commonly used for the aforesaid reason. Generally, a payer gives or indicates its approval to carry out a payment transaction or transactions as prescribed in article 54 of Directive 2007/64/EC. Subsequent to that, a payment institution uses the unique identifier in order to identify a payer. A signature-verification data assists in this identification. They may be in the form of codes or public cryptographic keys[95] or a combination of letters, numbers or symbols.[96] For e-authentication purposes, they must be a valid means of 'establishing the authenticity and integrity of the communication or data'.[97]

Annexure IV of Directive 1999/93/EC sets out the steps that should be complied with for secure signature verification by stating the following:

> During the signature-verification process it should be ensured with reasonable certainty that the data used for verifying the signature correspond to the data displayed to the verifier; the signature is reliably verified and the result of that verification is correctly displayed; the verifier can, as necessary, reliably establish the

---

91 Art 4(16) of Directive 2007/64/EC.
92 Art 4(6) of Directive 2007/64/EC.
93 Art 4(5) of Directive 2007/64/EC.
94 See, Art 4 (4) of Directive 2007/64/EC.
95 Art 2(7) Directive 1999/93/EC.
96 Art 4(21) of Directive 2007/64/EC.
97 S 7(3) of the Communications Act.

> contents of the signed data; the authenticity and validity of the certificate required at the time of signature verification are reliably verified; the result of verification and the signatory's identity are correctly displayed; the use of a pseudonym is clearly indicated; and any security-relevant changes can be detected.[98]

Essentially, a signature-verification data amounts to what is referred to as an e-signature. It is the equivalence of offline signatures. Its legal status in law is regulated by Article 25 (Legal Effects of Electronic Signatures) of Regulation No 910/2014 of the European Parliament and of the Council. Article 25(1) of this Regulation specifically states the following:

> An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceeding solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.[99]

---

98 Annexure IV of Directive 1999/93/EC. In terms of Art 3(9) of Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 a signatory is a natural person who creates an e-signature.

99 A Qualified e-signature is an advanced e-signature that is created by qualified e-signature creation device, and which is based on a qualified certificate for e-signatures. See Art 3(12) of Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014. A qualified e-signature creation device is an e-signature creation device that meets the requirements that are laid down in Annexure II. See Art 3(23) of Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014. The said Annexure II states that a 'qualified e-signature creation device shall ensure, by appropriate technical and procedural means, that at least the confidentiality of the e-signature creation data used for e-signature creation is reasonably assured; the e-signature creation data used for e-signature creation can practically occur only once; the e-signature creation data used for e-signature creation cannot, with reasonable assurance, be derived and the e-signature is reliably protected against forgery using currently available technology; the e-signature creation data used for e-signature creation can be reliably protected by the legitimate signatory against use by others. Qualified e-signatures creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing. Generating or managing e-signature creation data on behalf of the signatory may only be done by a qualified trust service provider (that is, a trust service provider who provides one or more qualified trust services and is granted the qualified status by a supervisory body). Qualified trust service providers managing e-signature creation data on behalf of the signatory may duplicate the e-signature creation data only for back-up purposes provided that the security of the duplicated datasets must be at the same level as for

Section 2 of the Communications Act provides a definition of an e-signature. This section states that an e-signature includes anything in e-form which 'as is incorporated into or otherwise logically associated with any electronic communication, such as sound, images, or both and a communication effecting a payment[100] or electronic data; and purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both'.[101] The steps to create an e-signature are referred to as an identification process. The aforementioned is a process of using personal identification information that uniquely represents a person.[102] It is normally carried out using electronic identification means. Electronic identification means are defined as the 'material and/or immaterial unit containing a person identification data[103] and which is used for authentication for an online service'.[104]

Generally, the e-signature verification process should support the structure for advanced e-signatures.[105] Advanced e-signatures are used in electronic settings for purposes of achieving a number of objectives. In one instance, they may be used in order to establish with accuracy the identity of a person (signatory).[106] In other instances, they may be depended upon in order to guarantee the integrity of an e-document.[107] Srivastava identifies a digital signature with a PKI as the most important example of an advanced e-signature.[108] Regulation No 910/2014 of the European

---

the original datasets and the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

100 S 15(1) of the Communications Act.

101 S 2 of the Communications Act of 2003 and Art 3(10) of Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014.

102 Art 3(1) of Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014.

103 Person identification data is a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established. See Art 3(3) of Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014.

104 Art 3(2) of Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014.

105 Art 3(1) Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014.

106 Laborde CM *Electronic signatures in international contracts* (Internationaler Verlag der Wissenschaften Frankfurt 2010) 70.

107 Laborde *Signatures* 70.

108 Srivastava A *Electronic signatures for B2B contracts: evidence from Australia* (Springer Heidelberg 2013) 38.

Parliament and of the Council refers to PKIs as the 'electronic signature creation data'.[109] They include the unique data that is used by the signatory.[110] Following this, Article 26 of the aforementioned regulation sets out the requirements that an advanced e-signature should generally comply with. These requirements are that: it must be uniquely linked to a particular signatory; it must be capable of identifying the signatory; it must be created using e-signature creation data that the signatory can, with a high level of confidence, use under his sole control; and it must be linked to the data signed therewith in such a manner that any subsequent change in the data is easily detectable.[111]

6.6.2 Canada

The principles for secure information systems or networks are central to the overall approach to e-authentication in Canada. In one case, the principles set out the manner of performing certain e-authentication tasks. These include the provisions for risk management, the provisions for the security, privacy, and the requirements for certain disclosures and those that are related to the handling of complaints.[112] In other cases, they require a proper understanding of the risks to information systems or networks. This understanding assists in designing e-authentication frameworks that are comparable to the risks.[113] Various factors help in developing this understanding. These include an analysis of the description of the risks, an assessment of the levels or degrees of the risks and the likelihood of the risks occurring in the future. The principles also guarantee the authentication of a person and seek to ensure, that is, an assurance or measure of certainty that a statement or fact is true, that certain credentials are reliable. The notion credentials have to be understood within the context of what it

---

109 Art 3(13) of Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014.

110 Art 3(13) of Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014.

111 Art 26(a)-(d) of Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014.

112 Industry Canada "Principles for electronic authentication – a Canadian framework" May 2004 12-23. To be accessed at https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/Authentication.pdf/$file/Authentication.pdf.

113 Treasury Board of Canada Secretariat http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422 (Date of use: 13 June 2013).

implies in e-authentication schemes in Canada. It denotes a unique physical or electronic object (or identifier) which is issued to, or associated with, an individual, organisation or device.[114]

Three legal instruments are generally crucial to the application of the principles for secure information systems in Canada. These include the Canada Evidence Act,[115] the Personal Information Protection and Electronic Documents Act[116] and the Secure Electronic Signature Regulations.[117] The relevance of these laws in e-authentication settings is discussed below.

(a) The Evidence Act

The Evidence Act applies to or regulates the admission or admissibility of evidence in court. More specifically, section 31 of the Evidence Act deals with the admissibility of e-documents as evidence. It defines an e-document as data which is recorded or stored on any medium in or by a computer system or other similar device. In turn, the data must be capable of being read or perceived by a person or a computer system or other similar device or devices. It can be in the form of a display, print-out or other output of that data.[118] For admission purposes, the person who seeks to admit an e-document has to establish the authenticity of such a document.[119] In other words, he or she must demonstrate that the e-document is that which it purports to be.[120]

Furthermore, the Evidence Act requires that the best evidence rule should be followed during the process of authenticating an e-document. In particular, it has to be alleged and proved that the information or computer system, that is, an e-document system,[121] was used in order to record or store the e-document; that regulations were made that establish presumptions in respect of the e-documents that are signed with secure e-

---

114 Treasury Board of Canada Secretariat http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262 (Date of use: 6 June 2013).

115 Canada Evidence Act, 1985 (hereinafter referred to as the Evidence Act).

116 Personal Information Protection and Electronic Documents Act, 2000 (hereinafter referred to as the Documents Act).

117 Secure Electronic Signature Regulations, 2005 (hereinafter referred to as the Signature Regulations).

118 S 31.8 of the Evidence Act.

119 S 31.1 of the Evidence Act.

120 S 31.1 of the Evidence Act.

121 S 31.8 of the Evidence Act.

signatures, and an e-document in the form of a printout was or had been acted upon, relied on or used as a record of the information that is recorded or stored in it.[122]

(b) The Documents Act

The Documents Act covers a variety of issues. These comprise the protection of personal information in the private sector;[123] e-documents,[124] amendments to the Computer Evidence Act;[125] amendments to the Statutory Instruments Act;[126] and amendments to the Statute Revision Act.[127] The system of e-authentication is incorporated in Part 2 of the Documents Act. It is applied to e-signatures, for example letters, characters, numbers or symbols.[128] E-authentication endorses the establishment of a secure e-signatures' structure. This formation relates to a variety of things. Firstly, it has relations with the application of the hash function to the data. A hash function is an electronic one-way mathematical process.[129] In this process, hefty data is recorded into the system and smaller data is generated as an output.[130] For example, a plain text (B) may be divided into a number of blocks, for example 180 blocks.[131] Thereafter, the blocks may be ciphered or coded.[132] In addition, the data which is contained in an e-document are exchanged into a message digest.[133] Message digests should be unique to each specific example of information.[134] This uniqueness is ensured by allocating message digest algorithms that are distinct from others. For instance, MD6 = F1, F2 & F3 may be used to mean message digest 6 equals files 1, 2 and 3. The exchange of data should be such that if that data is to be

---

122 See ss 31.2(1)(a), 31.2(1)(b) read with s 31.4 and 31.2(2) of CEA.
123 Part 1 of the Documents Act.
124 Part 2 of the Documents Act.
125 Part 3 of the Documents Act.
126 Statutory Instruments Act, 1985. See also Part 4 of the Documents Act.
127 Statute Revision Act, 1985. See also Part 5 of the Documents Act.
128 S 31.1 of the Documents Act.
129 S 1 of the Signature Regulations.
130 Rogers DJ *Broadband quantum cryptography* (Morgan & Claypool Publishers Columbia 2010) 41. See also Radu C *Implementing electronic payment systems* (Artech House Boston 2003) 376-377.
131 Lefèbvre F *Message digests for photographic images and video contents* (Presses universitaires de Louvain CIACO University 2004)10-11.
132 Lefèbvre *Message digests* 10-11.
133 S 1 of the Signature Regulations.
134 S 1 of the Signature Regulations.

changed, it would, on conversion, result in a changed message digest.[135] Secondly, the creation of a secure e-signature must be linked to the application of a key to encrypt the message digest. This key can be a Pin, username or password. Thirdly, it can pertain to the transmission of an e-document and the encrypted message digest together with either a digital signature certificate or a means of accessing a digital signature certificate. Fourthly, it can require that the hash function be applied to the data which is contained in an e-document in order to generate a new message digest. The message digest may be verified or compared with the data and that the validity of the digital certificate is tested.[136]

Consequently, e-authentication must meet the requirements of section 48(2) of the Documents Act. These are that technologies or other processes should be used to create an e-signature; the e-signature must be unique to a person; the e-signature must be incorporated, attached or associated to an e-document; the e-signature must be under or subject to the sole control of a person (for example a computer user); the e-signature must identify the person; the e-signature must be such that it can be manifestly established whether or not it has been changed since its incorporation, attachment or association with the e-document.[137]

6.6.3 South Africa

The framework for e-authentication in South Africa can be abstracted from Chapter VI of the ECT Act. Also important for e-authentication purposes is the Draft National Cybersecurity Policy of South Africa of May 2011.[138] Before delving into these e-authentication instruments, it is important to note that a distinction generally exists between law and government policies. Policies are not law as such. They are merely plans of action that are chosen and adopted by a sitting government. They are introduced in order to respond to the imperatives of a particular legislation. In this instance, the Cybersecurity Policy gives effect to the ECT Act. Accordingly, the policy does not naturally have or carry the same weight as the promulgated statute laws.

---

135 S 1 of the Signature Regulations.
136 S 48.1 of the Documents Act.
137 S 48(2) of the Documents Act.
138 Hereinafter referred to as the Cybersecurity Policy.

However, this does not mean that decisions that are taken after following the wording of policies are meaningless.[139]

Given the aforementioned, a reference to the Cybersecurity Policy in this section is made only insofar as the policy complements, at least in part, the ECT Act. It does not imply that the provisions of the Cybersecurity Policy have similar importance for enforcement purposes as those of the ECT Act. Therefore, section (a) below covers the selected provisions of the Cybersecurity Policy. Thereafter, section (b) examines the e-authentication procedure that is abstracted from the ECT Act.

(a) The Cybersecurity Policy

The Cybersecurity Policy was drafted pursuant to Proclamation R118 *Government Gazette* 32963 of 19 February 2010. It came about following the decision by the Department of Justice to 'battle crime using technology-based solutions and partnerships'.[140] This decision culminated into the the adoption of the National Cybersecurity Policy Framework for South Africa of 4 December 2015.[141] The Policy aims to establish a 'secure, dependable, reliable and trustworthy cyber environment'.[142] It intends to do all this by ensuring confidence and trust in the secure use of ICTs. This confidence and trust is necessary in attaining the following objectives:

> To facilitate the establishment of relevant structures in support of cybersecurity; to ensure the reduction of cybersecurity threats and vulnerabilities; to foster cooperation and coordination between government and private sector; to promote and strengthen international cooperation; to build capacity and promoting a culture of

---

139 *Bato Star Fishing (Pty) Ltd v Minister of Environmental Affairs and Tourism and Others* 2004 4 SA 490 (CC) para [48].

140 Guy http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=13783 (Date of use: 16 November 2015).

141 Hereinafter referred to as the NCP Framework.

142 The Cybersecurity Policy 15.

> cybersecurity; and to promote compliance with appropriate technical and operational cybersecurity standards.[143]

The notion of cyber-security is defined very broadly in the Cybersecurity Policy. It refers to the collection of tools, policies, security concepts, safeguards and guidelines, risk management approaches, actions, training, best practices, assurances and technologies that are essential to the protection of the online environments in South Africa.[144]

The Cybersecurity Policy also recognises that cyber-crime, for example cyber espionage, cyber-terrorism, malware and e-crimes continue to pose a threat to South Africa's cyber-security structures.[145] Therefore, it recommends that an intelligible and integrated cyber-security approach in South Africa should be established.[146] The approach should specifically promote a culture of cyber-security in South Africa. Lastly, it demands compliance with certain minimum cyber-security standards. These include the strengthening of intelligence collection, investigation, prosecution and judicial processes in respect of preventing and addressing cybercrime, cyber terrorism and cyber warfare; establishing public-private partnerships for national and international action plans and ensuring the protection of national critical information infrastructures.[147]

For purposes of maintaining a culture of cyber-security in South Africa, national critical information infrastructures are described as the 'ICT systems, data systems, databases, networks (including people, buildings, facilities and processes), that are fundamental to the effective operation of the Republic'.[148]

(b) ECT Act

The ECT Act operates within a broader national cyber-security structure. For e-authentication purposes, sections 37 and 38 of this Act are particularly essential. These

---

143 The Cybersecurity Policy 5.
144 The Cybersecurity Policy 6. See also the NCP Framework 73.
145 The Cybersecurity Policy 9-10.
146 The Cybersecurity Policy 11.
147 The Cybersecurity Policy 11-12.
148 The Cybersecurity Policy 6. See also s 1 of the Draft Cybercrime and Cybersecurity Bill of 2015 (hereinafter referred to as the CaC Bill).

sections do not expressly provide for a system of e-authentication. They specifically regulate the accreditation of authentication products or services.[149] This accreditation is made in support of an advanced electronic signature.[150] The term accreditation for purposes of e-authentication is defined in section 33 of the ECT Act. It refers to the recognition of authentication products or services by an Accreditation Authority.[151] The authority that carries out the accreditation process is known as the .za Domain Name Authority.[152] The Director-General of the Department of Communications and Postal Services heads this Authority.[153]

Authentication products or services are described in section 1 of the ECT Act. They are the products or services that are designed to identify a holder of an e-signature from other persons.[154] These products or services may include the facilities, for example software or hardware that are used or intended for use in order to authenticate a person or thing. Within the context of the ECT Act, the e-authentication facilities are referred to as the signature creation data and the signature verification data.[155] Firstly, a signature creation data is a unique number.[156] This number is unique because it serves or should serve as a secret code or key that is exclusive to a computer user and which is used in order to create an e-signature.[157] Secondly, a signature verification data can be any data.[158] This data should be able to verify the e-signature that is exclusive to a computer user.[159]

---

149 See s 37(1) of the ECT Act. Notice 1537 of 2004 and Chapter II of GN 8701 *GG* 29995 of 20 June 2007 (hereinafter referred to as the Accreditation Regulations) deals with the application for accreditation, the manner of applying for accreditation, the information to be disclosed in such application, the submission of the application, the granting of the application, the publication of accreditation and the refusal of the application for accreditation.

150 See s 37(1) of the ECT Act.

151 S 33 of the ECT Act.

152 S 1 of the ECT Act.

153 South African Accreditation Authority http://www.saaa.gov.za/index.php/background.html (Date of use: 5 November 2015).

154 S 1 of the ECT Act.

155 S 1 of the Accreditation Regulations.

156 S 1 of the Accreditation Regulations.

157 S 1 of the Accreditation Regulations.

158 S 1 of the Accreditation Regulations.

159 S 1 of the Accreditation Regulations.

Section 38(2) of the ECT Act lists the factors that an Accreditation authority must consider before it accredits authentication products or services. These factors are the financial and human resources of the authentication product or service, including its assets; the quality of its hardware and software systems; its procedures for processing of products or services; the availability of information to third parties relying on the authentication product or service; the regularity and extent of audits by an independent body.[160] However, section 39(a) of the ECT Act provides that Accreditation Authority may suspend or revoke the accreditation if it is satisfied that the conditions that are specified in section 38 were not complied with.[161]

Having studied Chapter VI of the ECT Act, it becomes evident that e-signatures are distinguished from advanced e-signatures. On the one hand, e-signatures are a representation of data in an electronic form which is attached to or logically associated with other data and which serves as one of the methods of e-authentication.[162] The legal effect of e-signatures is dealt with in section 13 of the ECT Act. Section 13(2) states that an e-signature 'is not without legal force and effect merely on the grounds that it is in electronic form'. Accordingly, the requirement in relation to a data message[163] is considered to have been complied with if the following happens:

> If a method is used to identify the person and to indicate the person's approval of the information communicated; and having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.[164]

On the other hand, an advanced e-signature is an e-signature that results or has the potential to result from a process which has been accredited by the Accreditation

---

160 S 38(2)(a)-(d) of the ECT Act.

161 See s 39(2) of ECT Act for the conditions that have to be met before a suspension or revocation of an accreditation could be effected.

162 S 1 of the ECT Act. See also *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 (21 November 2014) 12 and Srivastava *Signatures* 38.

163 Data message, within the context of the ECT Act, means data that is generated, sent, received or stored by electronic means and includes a voice, where the voice is used in an automated transaction, and a stored record. See s 1 of the ECT Act.

164 S 13(3) of the ECT Act.

Authority as contemplated in section 37 of the ECT Act.[165] Primarily, an advanced e-signature facilitates the identification of a person.[166] Furthermore, it helps in determining the integrity and credibility of information.[167] Consequently, computer users should intend that the information which is a representation of their signatures will actually serve as an e-signature.[168] For purposes of e-authentication in South Africa, it has to be established that: the e-signature to which the product or service relate is inimitably connected to the holder of an e-signature or; is capable of identifying the holder of an e-signature; is generated using the means that can be maintained under the exclusive control of the holder of an e-signature; is attached to the data or data message to which it relates in such a manner that any consequent alteration of the data or data message is detectable, and is based on the face-to-face identification of the holder of an e-signature.[169]

The e-authentication process that is illustrated above must be carried out in specific 'trustworthy systems'.[170] This means that the computer hardware or software that is used for e-authentication purposes ought to be reasonably secure from computer cracking attacks.[171] Furthermore, the hardware or software must provide a sensible level of availability, reliability and correct operation.[172] In addition, the hardware or software must be reasonably suited to perform the e-authentication process.[173] Lastly, the hardware or software must conform to the existing and accepted ICT security procedures.[174] As the soon as the above-mentioned has been completed, the provisions of section 13(4) applies *mutatis mutandis*. This section states that 'where an advanced electronic signature has been used, such signature is regarded as a valid electronic signature and to have been applied properly, unless the contrary is proven'.

6.6.4 Summary

---

165 S 1 of the ECT Act.
166 Laborde *Signatures* 70.
167 Laborde *Signatures* 70.
168 S 1 of the ECT Act.
169 S 38(1)(a)-(e) of the ECT Act.
170 Accreditation Regulations.
171 S 38(3)(a) of the ECT Act.
172 S 38(3)(b) of the ECT Act.
173 S 38(3)(c) of the ECT Act.
174 S 38(3)(d) of the ECT Act.

The sections above discuss a number of approaches to e-authentication. Firstly, the United Kingdom perspective to e-authentication is studied. The provisions of the Communications Act, Directive 2007/64/EC and Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 are found to be significant. Firstly, the United Kingdom requires its e-authentication paradigm to be proportionate, sound and adequate.[175] It has to be designed in a manner that adequately responds to the risks that e-crimes pose to the information systems. Secondly, e-authentication in Canada is founded on the principles for secure or sheltered information systems. These principles guarantee the reliability of certain credentials. Thirdly, e-authentication in South Africa falls within a structure to establish a culture of cyber-security. This culture is propagated by certain provision of the ECT Act and the Draft National Cybersecurity Policy.

It is revealed that the United Kingdom, Canadian and South African perspectives to e-authentication differ in a number of respects. Although they all support the structure for advanced e-signatures, it is argued that some are elaborate and others are not. Furthermore, despite the fact that the aim is to guarantee the sustenance of secure e-authentication structures the selected countries adopt different approaches to achieving the aforementioned. For example, certain relationships are essential to the carrying out of e-authentication in the United Kingdom. These relationships are between a payer, payment system and payment institution. However, there are no such relationships that are expressly created by the Canadian and South African e-authentication frameworks.

Given the fact that the discussion above provides a descriptive study of e-authentication, it thus leaves open the question regarding the manner in which the system of e-authentication should be carried out. In view of this, the sections below respond to this fissure. More specifically, they examine some of the prevailing practices to e-authentication.

6.7 A PRACTICAL APPROACH TO AUTHENTICATION

---

[175] Art 5(e) of Directive 2007/64/EC.

This section continues from the viewpoint that maintaining the integrity, authenticity and trust in information systems or networks are essential. However, a different path is followed. Specifically, the practical operation and effects of e-authentication is investigated. This is done in order to provide meaning to the process of e-authentication. For its completion, this section depends upon certain diverse theories of e-authentication. The most important of these theories include the B2G online authentication standard theory,[176] the strand spaces theory,[177] the theories of trust or trust theories[178] and the remote authentication theory[179] Given the vastness of these

---

176 Campbell J "The development of a B2G authentication standard – a design perspective of the policy consultation process" 2007 (14) *Australasian Journal of Information Systems* 81-94.

177 Doghmi SF, Guttman JD and Thayer FJ "Completeness of the authentication tests" in Biskup J and López J (eds) *Computer security: ESORICS 2007* (Springer Berlin 2007) 106-121, Guttman JD "Authentication tests and disjoint encryption – a design method for security protocols" 2004 (12) *Journal of Computer Security* 409-433, Thayer FJ and Herzog JC "Strand spaces – proving security protocols correct" 1999 (7) *Journal of Computer Security* 191-230, Newe T and Coffey T "Realisation of a minimum-knowledge identification and signature scheme" 1998 (17) *Computers and Security Journal* 253-264, Burrows M, Abadi M and Needham R "Logic of authentication" 1990 (8) *ACM Transactions on Computer Systems* 18-36, Perring A and Song D "Looking for diamonds in the desert – extending automatic protocol generation to three-party authentication and key protocols" in *Computer Security* (Papers delivered at the Foundations Workshop on Computer Security 3-5 July 2000), Thayer FJ and Herzog JC "Strand spaces – why is a security protocol correct?" in *Security and Privacy* (Papers delivered at the IEEE Symposium on Security and Privacy 3-6 May 1998 IEEE Oakland) 160-171.

178 Ma J, Orgun MA and Sattar A "Analysis of authentication protocols in agent-based systems using labeled tableaux" 2009 (39) *IEEE Transactions on Systems, Man and Cybernetics* 889-900, Ma J and Orgun MA "Formalising theories of trust for authentication protocols" 2008 (10) *Information Systems Frontiers* 19-32, Ma J *et al* "Risk analysis in access control systems based on trust theories" in *Web intelligence and intelligent agent technology* (Papers delivered at the 2010 IEEE Conference on Web Intelligence and Intelligent Agent Technology 31 August-3 September 2010 IEEE Toronto) 415-418 and Harwood, Clark and Jacob http://www-users.cs.york.ac.uk/~jac/PublishedPapers/TrustNetworks_rev2.pdf (Date of use: 13 July 2013).

179 Chang CC and Lee JS "An efficient and secure remote authentication scheme using smart cards" 2006 (18) *International Journal of Information and Security* 122-133, Chen TH, Tsai DS and Horng G "Secure user-friendly remote authentication schemes" 2006 (18) *International Journal of Information and Security* 111-121, Wu ST and Chieu BC "A user-friendly remote authentication scheme with smart cards" 2003 *Journal of Computers and Security* 547-550, Wu TC and Sung HS "Authenticating passwords over insecure channels" 1996 *Journal of Computer and Security* 431-439, McElroy D and Turban E "Using smart cards in electronic commerce" 1998 *International Journal of Information Management* 61-72, Chang CC and Hwang KF "Some forgery attacks on a

theories, only the trust theories, the strand spaces theory and the remote authentication theory are discussed. This selection does not imply that the other theories are insignificant for e-authentication purposes. However, it is encouraged by the fact that the selected theories support the study of e-signatures and the structure for advanced e-signatures. The theories are motivated by the idea that three participants influence every system of e-authentication. Simmons refers to these participants as a transmitter, receiver and opponent (cracker).[180] The theories are mathematically or computationally inclined. They provide or seek to provide 'abstract descriptions of a more complex reality'.[181] This reality is, for purposes of this research, called e-authentication.

6.8 TRUST THEORY

6.8.1 Background

The trust theory holds the view that confidence in information systems or networks are essential to every e-authentication structure.[182] The notion of trust assumes a particular meaning. It denotes the opposite of distrust.[183] It has relations on the functions of an ICT system or network. Firstly, it is associated with the specification or specificity of the e-authentication protocols.[184] These include the keys or cryptograms that assist in e-authentication frameworks. Secondly, it is linked to the techniques that are essential to the implementation and management of the e-authentication protocols.[185] Trust is established from reason, knowledge and experience. It is not founded on presumptions or what is referred to as a hunch. It certifies or entitles computer users to have assurance that their online communications or interactions are secure from outside

---

remote user authentication scheme using smart cards" 2003 (14) *Journal of Informatica* 289-294.

180 Simmons GJ "Authentication theory/coding theory" in Blakley GR and Chaum D (eds) *Advances in cryptology – CRYPTO* (Springer Heidelberg 1985) 411-431 412-413.

181 Ryan PYA "Mathematical models of computer security" in Focardi R and Gorrieri R (eds) *Foundations of security analysis and design: tutorial lectures* (Springer Berlin 2001) 1-62 3.

182 Ma and Orgun 2008 *Information Systems Frontiers* 19-20.

183 Ma *et al* "Risk analysis" 415.

184 Ma, Orgun and Sattar 2009 *IEEE Transactions on Systems, Man and Cybernetics* 889.

185 Ma, Orgun and Sattar 2009 *IEEE Transactions on Systems, Man and Cybernetics* 889.

intrusions.[186] Lastly, it assists in creating a trustworthy relationship between computer users, computers, systems and other entities.[187]

Four steps are identified that assist in establishing the required trust.[188] They are an analysis of how e-communication systems operate; an inquiry into the existing security mechanisms and an identification of the agents that are attached to systems; a definition of the appropriate workings of computers; and a description of the rules that describe the functions and behaviours of systems.[189] These actions are given proper meaning by the creation of certain e-authentication models. In this chapter, the 'trust model for access control systems'[190] and the 'trust (and reputational) systems' are examined.[191]

6.8.2 The Trust Model

The trust model is generally a 6-turple or word, namely model or M = ‹U, R, A, O, P, AR›. In relation to the aforesaid, U refers to a set of users, R implies a set of roles (managers, admin or clerk), A means a set of actions (access, modify or approve), O denotes a set of objects (documents, records or data), P represents a set of permissions or pairs and AR connotes a set of assignment relations.[192] The trust model helps in estimating the levels of trust in a specific system and the tools that are used to operate such a system. Accordingly, accessing may be allowed or denied depending on the quality and intensity of the risks in accessing a system. Consequently, the higher the risks that trust is absent or low, the higher the chances that authority to access a system will be denied.

---

186 Ma and Orgun 2008 *Information Systems Frontiers* 19.

187 Ma and Orgun 2008 *Information Systems Frontiers* 19-20. See also Ma J and Orgun M "Managing theories of trust in agent based systems" in Yolum P, Güngör T, Gürgen f and Özturan C (eds) *Computer and information sciences – ISCIS 2005* (Springer Berlin 2005) 442-451 442.

188 Ma, Orgun and Sattar 2009 *IEEE Transactions on Systems, Man and Cybernetics* 893.

189 Ma, Orgun and Sattar 2009 *IEEE Transactions on Systems, Man and Cybernetics* 893.

190 Hereinafter referred to as the Trust Model.

191 Harwood, Clark and Jacob http://www-users.cs.york.ac.uk/~jac/PublishedPapers/TrustNetworks_rev2.pdf (Date of use: 13 July 2013).

192 Ma *et al* "Risk analysis" 415-416.

The figures below indicate an e-authentication method which is founded on the trust model for access control systems. These figures generally refer to the formulae that are abstracted from the trust model. Accordingly, an e-authentication agenda that is deduced from the trust model for access control systems will come across as follows:

Figure 6.8.2.1

$$\text{Holds}(U,R) \wedge \text{has permission}(R,A,O) \rightarrow$$

$$\text{user\_permission}(U,A,O)$$

This implies that in cases where *U* wishes to perform *A* on *O*, *U* should afterwards possess *R*. This possession should consequently lead to the granting of *P* to U.[193] It is also required that *R* should be appropriate in the circumstances.[194]

Figure 6.8.2.2

$$\text{is\_user}(U,AR) \rightarrow$$

$$\text{can\_approve}(U,O,P)$$

This means that *AR* may grant *P* to *U* in order that *U* may perform *A* on *O*. It is important to note that *U* does not have to access *O* himself or herself. In other cases, it may be possible for *U* to delegate *P* to another user, for example *Z*.[195]

Figure 6.8.2.3

$$\text{is\_in}(U, AR^1) \wedge \text{is\_in}(Y,AR^2) \rightarrow$$

$$\text{can\_co\_approve}(U,Y,P)$$

Figure 6.8.2.3 implies that if the scenario in 6.8.2.2 above takes place, two separate *AR*s (*AR*[1] and *AR*[2]) may then have to approve or grant *P* to *U* and *Z*.[196]

---

193 Ma *et al* "Risk analysis" 416.
194 Ma *et al* "Risk analysis" 416.
195 Ma *et al* "Risk analysis" 416.
196 Ma *et al* "Risk analysis" 416.

6.8.3 Trust Systems

Trust systems are sometimes associated with the reputational systems.[197] Trust, in this instance, is a model which should be used to exclude cases of deception.[198] This view is encouraged by the fact that a departure from agreed facts weakens the trust. Trust systems accept that a presence of trust depends on an existence of binary relationships. The first is a trust relationship. The second is a distrust relationship. Divergent paths determine whether these relationships are present or not.[199] These are a trust path, a given path and a distrust path.[200] A trust path demonstrates a sequence of trust pairs or agents to the extent that each and every pair or agent of a path is a trust.[201] Let us suppose that A trusts B, B trusts C, and C trusts D. In this example, it can be said that A also trusts C and D and vice-a-versa. A given path can either be a trust or distrust path. It particularly illustrates the different sets of users and their interaction in a path. A distrust path attacks the trust path or the paths upon which the trust is founded. Let us suppose again that D, in our example above, distrusts B, A trusts E and E distrusts D. The question then is: can it be said that A trusts C? In answering this question, the trust systems state that D's distrust of B defeats the chain which connects A and C. However, E's distrusts of D defeats the distrust and so 'cancels its effect'.[202] This then leaves A having trust in C. Consequently, A has trust in C because D's distrust of B leads to an attack path which is weaker than the trust path between A and C.[203]

---

197 Artz D and Gil Y "A survey of trust in computer science and the semantic web" 2007 (5) *Journal of Web Semantics* 58-71 60-61.

198 Artz and Gil 2007 *Journal of Web Semantics* 60-61.

199 Artz and Gil 2007 *Journal of Web Semantics* 58-59.

200 Harwood, Clark and Jacob http://www-users.cs.york.ac.uk/~jac/PublishedPapers/TrustNetworks_rev2.pdf (Date of use: 13 July 2013).

201 Bhuiyan T, Josang A and Xu Y "Managing trust in online social networks" in Furht B (ed) *Handbook of social network technologies and applications* (Springer New York 2010) 471-496 472.

202 Harwood, Clark and Jacob http://www-users.cs.york.ac.uk/~jac/PublishedPapers/TrustNetworks_rev2.pdf (Date of use: 13 July 2013).

203 Harwood, Clark and Jacob http://www-users.cs.york.ac.uk/~jac/PublishedPapers/TrustNetworks_rev2.pdf (Date of use: 13 July 2013).

A generic method on how these diverse paths work is commonly implemented. For example, user (*a)* sends or wishes to send a message (*msg X)* to another user (*b)*. It is common course that if *b* wants to access and read *X* he or she will then be required to encrypt *X* by using a particular key *ka.* In such a case, the trust theory will apply as follows:

Figure 6.8.2.4

$$(B^{a}\ \text{Secure}(ka) \wedge \text{Receive}(b, \{X\}ka) \leftrightarrow$$

$$B^{a}\ \text{Reliable}(X))$$

This means that in the event that *b* accepts that *k* is secure and consequently receives *X* as encrypted with *ka*, *b* then accepts that *X* is reliable.[204]

Figure 6.8.2.5

$$(\text{Receive}(a, \{X\ [T]\}ka) \wedge B^{a}\ \text{Duplicate}(T) \leftrightarrow$$

$$\text{Reject}(X\ [T])$$

This connotes that if *b* receives *X* containing a series of characters or codes that illustrates and identifies the e-authentication or encryption process, that is, timestamp *T* and it appears from *X* that *T* is a replica or is duplicated, *X* will be rejected.[205]

It is established from the above that the trust theory promotes the idea of trust in information systems or networks. The trust model and the trust or reputational systems are the models which are used to demonstrate the existence or not of trust in each case. The section below discusses the strand spaces theory. This theory focuses on the segments which constitute the whole or wholeness of systems. These segments are, for purposes of the strand spaces theory, referred to as the strands.

6.9 STRAND SPACES THEORY

---

204 Ma, Orgun and Sattar 2009 *IEEE Transactions on Systems, Man and Cybernetics* 894.

205 Ma, Orgun and Sattar 2009 *IEEE Transactions on Systems, Man and Cybernetics* 894.

6.9.1 Background

The strand spaces theory is one of the most widely used e-authentication models. It is relied upon to authenticate the infrastructure or architecture of a computer and to validate the tools for e-authentication.[206] It basically improves or serves as an improvement of the so-called *Needham-Schroeder Public Key Protocol*. The Needham-Schroeder Public Key Protocol was made famous by Needham and Schroeder in their article titled *Using Encryption for Authentication in Large Networks of Computers*.[207] It argues that secret keys are usually indispensable in every e-authentication framework.[208] For instance, they justify the authentication of a person or personal credentials. Some of these keys (short keys) are, according to the Needham-Schroeder Public Key Protocol, held by individual computer users.[209] Others (long keys) are kept and computed in an authentication server.[210] For e-authentication purposes, the Needham-Schroeder Public Key states that authentication servers are the final authority of e-authentication.[211] Accordingly, they validate a user's short key or keys by matching it or them with the long key or keys.[212]

Having examined the workings of the Needham-Schroeder Public Key, the strand spaces theory was incepted. It introduces an e-authentication framework which is founded on *strands*. Before the workings of this theory are examined, it is essential to discuss certain terms that are central to it. These include a strand, node, bundle and strand space. Firstly, a strand is a sequence of events that a computer user may undertake. These may be a series of message transmissions (send) and receptions (receive).[213] In this instance, it represents the local behaviours of principals in a session

---

206 Fröschke S "Adding branching to the strand space model" 2009 (242) *Theoretical Computer Science* 139-159 139.

207 See, Needham RM and Schroeder MD "Using encryption for authentication in large networks of computers" 1978 (21) *Communications of ACM* 993-999.

208 Needham and Schroeder 1978 *Communications of ACM* 993

209 Needham and Schroeder 1978 *Communications of ACM* 994

210 Needham and Schroeder 1978 *Communications of ACM* 999

211 Needham and Schroeder 1978 *Communications of ACM* 996.

212 Needham and Schroeder 1978 *Communications of ACM* 994-996.

213 Guttman JD "Key compromise, strand spaces, and the authentication tests" 2001 (45) *Theoretical Computer Science* 141-161 143-144 and Thayer F, Herzog JC and Guttman JD "Mixed strand spaces" in *Computer Security Fundamentals* (Papers delivered at the

or run, that is, the sending and receiving of messages. It also characterises the basic actions of encrypting and decrypting messages. It illustrates whether or not encryption or decryption is necessary in each case. Two categories of principals are created in a strand. Principals may either be legitimate users of computers (victims) or the penetrators or intruders (crackers) of computers.[214] In relation to the last-mentioned principal, a cracker uses what is referred to as a *penetrator set*.[215] This set encompasses the keys (*Kp*) that are originally known to a penetrator.[216] They are public, private or symmetric keys.[217]

Secondly, a node is the element of a strand. This element facilitates the transmission of messages between the principals.[218] Thirdly, the structure of a strand is referred to as a bundle. It generally combines the local view of a strand to form a global view. Fourthly, a strand space is or represents the coming together of strands.[219] For e-authentication purposes, a strand space may mean different things depending on whether or not a system is used by a victim or cracker. When used by a victim a strand space denotes a measure which illustrate the suitability of the existing e-authentication measures to withstand non-self intrusions.[220] However, in cases where a system is used by computer crackers it implies 'a sequence of message transmissions and receptions that model a basic capability a penetrator (computer cracker) should be assumed to possess'.[221] A difference is generally made between strand spaces. There is a 'secure strand spaces' and an 'intruder strand spaces'.[222] The first-mentioned strand space is

---

12th Computer Security Foundations Workshop 30 June 1999 IEEE Los Alamitos) 72-82 73.

214 Thayer Herzog and Guttman *Computer Security Foundations* 73.

215 Thayer FJ, Herzog JC and Guttman JD "Honest ideals on strand spaces" in *Computer Security* (Papers delivered at the 11th IEEE Computer Security Foundations Workshop 9-11 June 1998 The Institute of Electrical and Electronics Engineers Inc. Los Alamitos) 66-78 68.

216 Thayer Herzog and Guttman *Foundation Workshop* 68.

217 Thayer, Herzog and Guttman 1999 *Journal of Computer Security* 202.

218 Guttman JD and Thayer FJ "Authentication tests and the structure of bundles" 2002 (283) *Theoretical Computer Science* 333-380 336.

219 Syverson P "Towards a strand semantics for authentication logic" 1999 (20) *Theoretical Computer Science* 1-15 5.

220 Halpern JY and Pucella R "On the relationship between strand spaces and multi-agent systems" 2003 (6) *ACM Transactions on Information and System Security* 43-70 46.

221 Thayer, Herzog and Guttman 1999 *Journal of Computer Security* 194.

222 Caleiro C, Viganò L and Basin D "Relating strand spaces and distributed temporal logic for security protocol analysis" 2005 (13) *Logic Journal of the IGPL* 637-663 648.

sometimes called a standard or honest strand space. It contains both a legitimate and intruder strands.[223] The second-mentioned belongs or is controlled by a computer cracker and contains nodes that are known to and controlled by an intruder.[224]

6.9.2 Strand Spaces and E-Authentication

As is shown in the discussion above, the strand spaces theory is a development of the Needham-Schroeder Public Key. The Needham-Schroeder Public Key creates a scenario where *A* represents a set of messages (*msgs*).[225] These *msgs* are sent and received between principals. The elements of *A* are referred to as the *terms* (*t*). The *ts* are generated from two sets of *msgs* through encryption. There is *T* which represents the texts and *K*, which represents the key. For e-authentication purposes, the position will appear as follows:

Figure 6.8.2.6

$A , \{|B , N^a|\}\kappa$

This means that initiator *A* sends a *t* in order to commence an exchange of *msgs* with *B*.[226] During the time when *t* is sent, a *msg* is still in the form of a plaintext. Afterwards, a ciphertext is created on *msg*. A long key (*κ)* is used to create the ciphertext. Consequently, the encryption of a *msg* is in respect of *A*'s name.[227]

It is argued that the Needham-Schroeder Public Key has immeasurable drawbacks. For example, if we look at figure 6.8.2.6 above we can infer that *κ* was generated by *S* (denoting the Server). However, it cannot be said for certain how much time *S* took to complete the session. In other words, there is nothing available that measures the length of time between the sending of *t* and the creation of *κ*. This generates problems because a computer cracker may intercept the session and recover the generated *κ.*

---

223 Caleiro, Viganò and Basin 2005 *Logic Journal of the IGPL* 648.
224 Halpern and Pucella 2003 *ACM Transactions on Information and System Security* 46-47.
225 Needham and Schroeder 1978 *Communications of ACM* 994-995.
226 Needham and Schroeder 1978 *Communications of ACM* 995.
227 Needham and Schroeder 1978 *Communications of ACM* 995.

Thereafter, it may send a duplicate or wrong *κ* to *B*. In all this, *B* will not know that *k* is a duplicated or wrong key.

Having observed these shortcomings Guttman, Thayer and Herzog developed the strand spaces theory. It is founded on three principles.[228] Principle one states that a computer cracker must never know *k*.[229] Accordingly, the idea that *k* is generally good or safe should be approached with caution.[230] The second principle avers that *S* must never be allowed to re-use *k*.[231] Principle three asserts that a session *k* must never be similar to a long key.[232] Thus, *k* and *msg* must always be fresh. *K* or *msg* is deemed to be fresh if it is not a part of *k* or *msg* which was sent prior to the current epoch or session.[233] Accordingly, *k* or *msg* which was safe and good in the past session should not be regarded as such for purposes of current or future sessions.

In a strand, *A* denotes a set of *msgs* that can be sent between principles. The elements of *A* are called the *A* terms (*t*). The transmission of *t* is represented as *+t*. The reception of *t* is characterised as *–t*. For computational purposes, the terms will appear as follows:

Figure 6.8.2.7

$\{+t^1, +t^2....-t^1, -t^2\}$

In addition, if *s* is a strand, it then follows that $s \downarrow i$ is the 'i^{th} node (*n*) on *s*'.[234] The connection $n \Rightarrow n^1$ holds between nodes *n* and n^1 if $n = s \downarrow i$ and $n^1 = s \downarrow i + 1$. It is accepted that this working does not make sense to an ordinary reader. Therefore, it requires some unpacking or elaboration. The connection $n \rightarrow n^1$ represents the communication (or *msgs*) between strands (*s*).[235] When one *t* receives an *m* it is important that another *t* should also be allowed to receive a *msg*. This means that an

---

228 See Guttman 2001 *Theoretical Computer Science* 149-150.
229 Guttman 2001 *Theoretical Computer Science* 149.
230 Guttman 2001 *Theoretical Computer Science* 149.
231 Guttman 2001 *Theoretical Computer Science* 149.
232 Guttman 2001 *Theoretical Computer Science* 149.
233 Syverson 1999 *Theoretical Computer Science* 2.
234 Guttman and Thayer 2002 *Theoretical Computer Science* 335.
235 Thayer, Herzog and Guttman *Computer Security* 73-74.

occurrence of one event should also lead to the incidence of another.[236] Consequently, the situation is as demonstrated in formula 6.8.2.8 below:

Figure 6.8.2.8

$\{(n) = +t ..... (n^1) = -t\}$

Authenticating transmitted or outgoing *msgs* differs to the authentication of received or incoming *msgs*. In relation to outgoing *msgs*, a *msg* must be sent within a strand in an encrypted form and a *k* to decrypt it must be safe ($K \in S$). This assists in demonstrating whether or not a *k* is issued during the course of a session or is a result of a penetrated or cracked session. In relation to incoming *msgs*, the situation is complex. If a *msg* is encrypted and the encryption *k* was safe, then it can be said that a user was responsible for a session. This then leads to what is referred to as an honest session. A session is honest if it meets the following: 'The elements of that session cannot be synthesised by the penetrator. They cannot be guessed and a computer cracker cannot deduce them via a sequence of decryptions, encryptions, or separations'.[237] Nevertheless, in cases where a *msg* is encrypted and the encryption key (*k*) was unsafe, then it can be inferred that the session was penetrated.

It is argued above that the strand spaces theory adds on, supplements or complements the Needham-Schroeder Public Key. It mentions that *msgs* are communicated within a strand. Their encryption and decryption by principals depends on whether or not they are transmitted or received *msgs*.

6.10 REMOTE E-AUTHENTICATION THEORY

6.10.1 Background

Remote e-authentication implies an identification and verification of information remotely.[238] Remotely is here used in a selective manner. It denotes a procedure or

---

236 Thayer, Herzog and Guttman *Computer Security* 74.

237 Thayer, Herzog and Guttman *Computer Security* 75.

238 Hastings NE and Dodson DF "Qualifying assurance of knowledge based authentication" in Jones A and Remenyi D (eds) *Proceedings of the 3rd European conference on*

process (of e-authentication) which is undertaken over a system. Generally, a user enters or registers his or her particulars or credentials into a system. The system records these particulars or credentials and then uses them to authenticate a user at a later stage. Local area network (LAN) systems are particularly critical to the working of the remote e-authentication process. LAN systems are 'a collection of devices that are interconnected via a common transportation medium, for the purposes of transferring data'.[239] They ensure that information is verified without a need for direct engagements between a verifier (usually a remote server) and a user.[240] Furthermore, they help in the transfer of information from, for example a PC to a remote server.

A password table is commonly used in order to facilitate a smooth performing of remote e-authentication schemes. The table can look a lot like the one which is indicated below:

Password Table[241]

Codes	Narratives
U	A user
V	A value
ID	An identity of the user
Pw	A password of the user

information warfare and security (Academic Conference Limited Reading 2004) 109-116 109.

239 Miller P and Cimmins M *LAN technologies explained* (Digital Press Massachusetts 2000) 5.

240 Chen, Tsai and Horng 2006 *International Journal of Information and Security* 111.

241 Table 1 is an adapted version of the 'improvement of the secure dynamic ID-based remote user authentication' which is recommended by Hsiang and Shih. See Hsiang HC and Shih WK "Improvement of the secure dynamic ID-based remote user authentication for multi-server environment" 2009 (31) *Journal of Computer Standards and Interfaces* 1118-1123 119.

S	A server
R	A login request
Msg	A message
k	A secret key
rn	A random number
H	A one-way hash function
T	A time (operating like a time-stamp)
→	A common channel
═	A secure channel

Remote e-authentication can be based upon various cryptograms. It can be centred on passwords, smart cards or biometric data.[242]

6.10.2 Password-Based

This form of e-authentication is one of the most extensively used. It was made popular by Morris and Thompson in their 1979 paper.[243] In that paper, they found that passwords are one of the essential components in securing information.[244] They then argued that measures should be established to prevent attacks to remote-access systems.[245] In password-based remote e-authentication, it is necessary that the system or network should be able to perform the e-authentication process. In the absence of

---

242 For further interesting reading see Das AK, Sharma P, Chatterjee S and Sing JK "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks" 2012 (35) *Journal of Network and Computer Applications* 1646-1656.

243 See in general Morris S and Thompson K "Password security: a case history" 1979 (22) *Communications of the ACM* 594-597.

244 Morris and Thompson 1979 *Communications of the ACM* 594.

245 Morris and Thompson 1979 Communications *of the ACM* 594-596.

such ability, computer crackers could intercept the password and steal sensitive information. In authenticating a user, a remote system verifies and corroborates a password. Basically, a server searches a password from a password table (table that keeps or stores passwords). This searching is made with a view to establish whether a password matches that which is contained in a table or not.[246]

Two categories of password-based remote e-authentication are identified.[247] One uses a weak password, and the other relies on a strong password.[248] Advantages and disadvantages are attached to both these categories. On the one hand, weak-password authentication is easy to memorise, it is based on public-key cryptographic techniques and that remote systems do not have to keep a password table in order to authenticate user login details.[249] Nevertheless, weak-password authentication is easy to guess, inconveniences the e-authentication process (because the password table must be impenetrable) and requires that additional work be done to secure the password against computer crackers. On the other hand, strong-password e-authentication uses simple operations, for example a one-way hash function, easy to implement, and is less costly than weak-password authentication. However, a strong-password authentication is difficult to memorise.[250]

In addition, three phases are distinguished that characterises password-based remote e-authentication. These are a (i) registration phase; (ii) login phase, and (iii) authentication phase.[251] Chang, Tsu and Chen refer to the first-mentioned phase (registration phase) as the *Card Initiation Phase*.[252] This change in terminology does not alter the entire principles of password-based remote e-authentication. Conversely, the change emanates from the theory of *quadratic residues* which Chang, Tsu and

---

246 For criticism of this method of e-authentication see Li LH, Lin IC and Hwang MS "A remote password authentication scheme for multiserver architecture using neural networks" 2001 (12) *IEEE Transactions on Neural Networks* 1498-1504 1498.

247 Das LM, Saxena A and Gulati VP "A dynamic ID-based remote user authentication scheme" 2004 (50) *IEEE Transactions on Consumer Electronics* 629-631 629.

248 Das, Saxena and Gulati 2004 *IEEE Transactions on Consumer Electronics* 629.

249 Das, Saxena and Gulati 2004 *IEEE Transactions on Consumer Electronics* 629.

250 Li, Lin and Hwang 2001 *IEEE Transactions on Neural Networks* 1498.

251 Chen, Tsai and Horng 2006 International *Journal of Information and Security* 112-113 and Li, Lin and Hwang 2001 *IEEE Transactions on Neural Networks* 1499-1500.

252 Chang CC, Tsu SM and Chen CY "Remote scheme for password authentication based on theory of quadratic residues" 1995 (18) *Computer Communications* 936-942 937.

Chen propose. This theory contributes to the ideal to eliminate the chances that an eavesdropper or computer cracker may intercept a password.[253] There are also others who propose an additional phase to a password-based remote e-authentication.[254] They refer to this as the *Password Change Phase*.[255]

Despite these differences, the registration, login and authentication phases are discussed below.

(a) Registration Phase

In this phase *U* registers his or her information with *S*. This information can be in the form of an *ID* or a *Pw*. Chen, Tsai and Horng submit that only the hash value of an *ID* and *Pw* should be registered to *S*.[256] The registration ought to be carried out through a secure channel or, otherwise, to be done in neutral networks.[257] Neutral networks are referred to as the trained networks that facilitate a process of authenticating users online or remotely.[258] For computational purpose a registration phase will appear as follows:

Figure 6.8.2.9

$U = S \rightarrow$

$$h(ID);h(Pw)$$[259]

As soon as the registration is complete, *S* then computes *ID* and *Pw* and stores them remotely.

(b) Login Phase

---

253 Chang, Tsu and Chen 1995 *Computer Communications* 936.

254 Wen F and Li X "An improved dynamic ID-based remote user authentication with key agreement" 2012 (38) *Journal of Computers and Electrical Engineering* 381-387 382-383.

255 Wen and Li 2012 *Journal of Computers and Electrical Engineering* 383.

256 Chen, Tsai and Horng 2006 International *Journal of Information and Security* 114.

257 Li, Lin and Hwang 2001 (12) *IEEE Transactions on Neural Networks* 1499-1500.

258 Li, Lin and Hwang 2001 (12) *IEEE Transactions on Neural Networks* 1499.

259 Chen, Tsai and Horng 2006 International *Journal of Information and Security* 114.

In this phase *U* makes an *R*. This basically happens when *U* enters an *ID* and *Pw* in the spaces that are allocated for this purpose in a system or network. *R* is automatically transmitted to *S* at time (*T*), that is, the current date and time. *T* signifies the 'expected legal time interval for transmission delays between the login terminal and the system servers'.[260] These times are clearly defined or determined. Therefore, it is inevitable that they will defer from one e-authentication system to the other.

(c) Authentication Phase

In this phase *S* receives an *ID* and *Pw*. In addition, it accepts T^1 and T^2. T^1 refers to a time when an *R* was made. T^2 denotes a time when the *S* received an *R*. As soon as this happens, *S* establishes the format of an *ID* and *Pw*.[261] It also corroborates the time interval between T^1 and T^2.[262] This is made in order to ensure that the times are within the authorized acceptable level.[263] In other words, it is made with a view to guarantee that the delay in the times is not greater than is lawfully or reasonably expected to be. Accordingly, if T^1 is greater than T^2, *S* should reject *R*. Lastly, *S* should compute:

Figure 6.8.2.10

$$h(ID);h(Pw) =$$

$$T^1 \S T^2.$$[264]

6.10.3 Smart Cards-Based[265]

The idea of smart cards-based remote e-authentication is modelled from the approaches that Lamport used in one of his 1981 papers.[266] He argued for a remote e-

---

260 Li, Lin and Hwang 2001 (12) *IEEE Transactions on Neural Networks* 1499.

261 Chang, Tsu and Chen 1995 *Computer Communications* 937.

262 Wen and Li 2012 *Journal of Computers and Engineering* 383.

263 Chang, Tsu and Chen 1995 *Computer Communications* 937.

264 Chen, Tsai and Horng 2006 International *Journal of Information and Security* 115-116.

265 It is important to note the paper by Chang and Hwang which lists the manner of bypassing or attacking the e-authentication frameworks that are supported by the smart cards-based remote e-authentication. See Chang and Hwang 2003 *Journal of Informatica* 289-294.

266 See in general Lamport L "Password authentication with insecure communication" 1981 (24) *Communications of the ACM* 770-772.

authentication framework over insecure channels.[267] Following this development, these channels have become known as smart cards.[268] Smart cards-based remote e-authentication is based on the idea that remote servers are or should not be the sole keepers of user information. Accordingly, smart cards can also keep and store information. A smart card chip (memory and processor chips) facilitates this keeping and storage.[269]

Chen, Kuo and Wuu illustrate in what manner smart cards-based remote e-authentication works.[270] They say the following:

> In a smart-card-based (remote) authentication scheme, when (computer) users want to access resources on a secure sever, they insert their smart card into a card reader and then input a password for the card. The smart card takes the user's password, generates the user's login request, and sends the request to the secure server. Upon receiving the user's request, the server verifies the validity of the request.[271]

The use of smart cards in remote e-authentication schemes makes the keeping of a password table unnecessary.[272] However, it is conceded that caution should generally be exercised whenever they are relied upon.[273] For example, it should always be kept in mind that they do not possess the same memory or computational ability as remote servers. In particular, their memory is low as compared to that of remote servers.[274] Consequently, there is a danger that information may be lost or damaged due to this insignificant capacity.

---

267 Lamport 1981 *Communications of the ACM* 770-771.

268 Chang and 2006 *International Journal of Information and Security* 123.

269 Pfau A "Smart card solutions" in Fumy E and Sauerbrey J (eds) *Enterprise security: IT security solutions – concepts, practical experiences, technologies* (Publicis Corporate Publishing Erlangen 2006) 57-69 59-61.

270 See Chen BL, Kuo WC and Wuu LC "Robust smart-card-based remote user password authentication scheme" 2012 *International Journal of Communication Systems* http://onlinelibrary.wiley.com/doi/10.1002/dac.2368/pdf (Date of use: 09 October 2013).

271 Chen, Kuo and Wuu 2012 *International Journal of Communication Systems*.

272 Sun HM "An efficient remote use of authentication scheme using smart cards" 2000 (46) *IEEE Transactions on Consumer Electronics* 958-961 958.

273 Chang and Lee 2006 *International Journal of Information and Security* 123.

274 Chang and Lee 2006 *International Journal of Information and Security* 123.

(a) Registration Phase

In this phase, *U* submits his or her *ID* to the remote system or network. This relates to the *ID* that he or she chose himself or herself.[275] The system computes a *Pw* for *U*.[276] The *S* stores an *ID* and subsequently issues a smart card through a secure channel to *U*. The smart card contains *h*. Consequently, the computation is as follows:

Figure 6.8.2.11

Pw = $h(ID,k)$[277]

(b) Login Phase

This phase is used in cases when *U* wants to access the facilities that the remote system offers. These may be incidents wherein *U* wishes to make an electronic funds transfer (EFT) or buy property or goods online. Basically, *U* inserts the smart card into an allocated space on a system (input device). *U* will then be requested to enter his or her *ID* and *Pw*. Following this, the smart card will generate *rn*. *Rn* can only be used once. It also computes *h* and *Pw*. Thereafter, it sends a *msg* (*M*) which contains the ID and *rn* to the remote system (M = [ID, rn]).

(c) Authentication Phase

Immediately after receiving *M*, the system authenticates *U*. It verifies the validity of *U*'s *ID*. In cases where the format of the *ID* is incorrect, the remote system rejects the *R*. In addition, it corroborates the legitimacy of T^1 and T^2. If T^1 is greater than T^2, the system will reject *R*. Thereafter, the system computes $Pw = h(ID, k)$ and $M = h(T^1, Pw)$.[278] Accordingly, if *M* matches the *M* which was issued during the login phase the system

---

275 Chang and Lee 2006 *International Journal of Information and Security* 126.

276 It is important to note that there is nothing which prevents *U* from choosing an *ID* and PW.

277 Sun 2000 *IEEE Transactions on Consumer Electronics* 959 and Chen, Kuo and Wuu 2012 *International Journal of Communication Systems*.

278 Sun 2000 *IEEE Transactions on Consumer Electronics* 959.

will accept the *R*.[279] If the aforementioned does not ensue, the login request will be rejected.

6.10.4 Biometrics-Based

Biometrics-based e-authentication is generally one of the most secure ways of authenticating users. It specifically offers a cryptographically secure authentication of users.[280] This security is linked to the fact that a biometrics-based e-authentication use features that are inherent to users. These features are unique to users in that users cannot change or alter them during their lifetime. Hribernig and Weinzierl best describe the individuality of biometric data. They argue that it is 'singular within all humankind (past, present and future); stable from birth to dearth and independent of personal and environmental conditions'.[281] The use of biometrics-based e-authentication also excludes the possibility that the authentication cryptograms may be lost or destroyed. Therefore, users do have to remember or store IDs and passwords in a safe or protected place. Despite these advantages, two shortcomings of biometrics-based e-authentication are identified. Firstly, it is maintained that the distribution of the features is never identical or uniform. As a result, features that do not share particular resemblances may be used for e-authentication purposes. Secondly, it is often difficult to reproduce biometrics data.[282] This complexity is associated with the irregular and unbalanced nature of biometrics data.

In biometrics-based e-authentication schemes, four processes are distinguished. These are the capturing, encoding, storage and matching processes. Basically, a system captures biometric data. Usually, a sensor device is used for this purpose. Thereafter, a (raw) template of the data is produced which contains particulars, for example ID, username or password of a user.[283] The template together with the

---

279 Sun 2000 *IEEE Transactions on Consumer Electronics* 959.

280 Boyen X *et al* "Secure remote authentication using biometrics" in Cramer R (ed) *Advances in cryptology – Eurocrypt, lecture notes in computer science* (Springer Heidelberg 2005) 147-163 147-148.

281 Hribernig G and Weinzierl P "Biometric authentication" in Fumy E and Sauerbrey J (eds) *Enterprise security: IT security solutions – concepts, practical experiences, technologies* Publicis Corporate Publishing Erlangen 2006) 84-102 84.

282 Boyen *et al Remote Authentication* 147-148.

283 Hribernig and Weinzierl *Biometric* 88.

particulars is kept and stored in a system. Consequently, a user will have to possess the data and particulars that are similar or correspond with that which contained in the template.[284]

6.10.5 Summary

The manner in which the process of e-authentication operates is examined. This is made in order to ensure that the integrity and trust in information systems is preserved. With this in mind, various e-authentication theories are investigated. These are the trust theory, the strand spaces theory and the remote-e-authentication theory. The trust theory is founded on the idea to maintain trust in information systems. It relies on several trust models in order to achieve the aforementioned. Thus, the trust model and the trust or reputational systems are identified. The strand spaces theory is an addition to the Needham-Schroeder Public Key Protocol approach. It models its e-authentication structure from the workings of strands. It specifically argues that because strands are the key ingredients for the transmission and receiving of messages within a system, e-authentication processes should understand the workings and dynamics of strands. Remote e-authentication covers the identification of information using remote systems, for example a remote server. This e-authentication can be password-based, smart cards-based or biometrics-based.

E-authentication theories have certain benefits and drawbacks. For example, in the case of passwords-based remote e-authentication a distinction is made between weak and strong passwords. Weak passwords are easy to memorise and it is not necessary to keep a password table. However, they are easy to guess and thus added security measures are required in order to supplement them. Strong passwords use a hash function (which is a simple operation) and are inexpensive than weak passwords. However, they are difficult to remember and it is required that a password table should be kept. Smart cards-based remote e-authentication seeks to relieve remote servers as the only keepers of e-authentication information. However, it is conceded that smart cards have lesser or little memory as compared to that of remote servers. Consequently, there is a risk that information may be lost or destroyed. Biometrics-

---

[284] Hribernig and Weinzierl *Biometric* 88.

based remote e-authentication is the most sheltered e-authentication framework. This is the case because it uses for e-authentication purposes features (or biometric data) that are unique and inherent to a user. However, the dissemination of biometric data is never uniform. This then exposes the whole e-authentication process to a danger that distinct features may be used to identify a user. In addition, a process to make a replica of (or to replicate) the features is mostly a cumbersome activity

6.11 CONCLUSION

This chapter continues from the viewpoint that it is possible to regulate ICTs and their ensuing challenges. It then identifies e-crimes as one of the ICT challenges. More specifically, e-crimes generate risks to regulators and the overall information society. Therefore, it is necessary that structures should be created in order to avert this occurrence. On the one hand, acts or conducts that are associated with e-crimes may be criminalised. On the other hand, measures to prevent e-crimes may be introduced. In this chapter the measures to prevent e-crimes are discussed. They are studied as part of the system or process of authentication.

Authentication (and not authorisation) seeks to establish the credibility and dependability of a person or thing.[285] With respect to a person, this is made by analysing, inspecting and corroborating a person's face images, finger prints and signatures. In relation to a thing, the authentication and best evidence tests are commonly applied. The achievements of the system in offline frameworks have led to it being adopted in online environments. In online settings, the process is referred to as e-authentication. E-authentication uses certain electronic symbols (cryptograms) in order to provide security and trust in electronic systems. They are passwords or codes, pins, digital or e-signatures that use public key infrastructures, physical devises, for example smart cards, one-time-passwords, USB plug-in devices or biometric identification. The symbols are essential to the performing of the e-authentication pillars, for example evidence of knowledge; confirmation of possession, or proof by property.[286] Ensuring the performance of the pillars generally forms part of a country's

---

285 UNCITRAL 2009 35.

286 Reid *Network security* 9.

cyber-security paradigm. With this in mind, a selective study of the e-authentication measures in the United Kingdom, Canada and South Africa is made. It is found that these countries' e-authentication measures differ. Some are elaborate whilst others are not. For information security purposes, the practical approach to the e-authentication is also discussed. It relies on certain e-authentication theories. These are the trust, strand spaces and remote e-authentication theories. The theories are modelled from mathematics. They mathematically illustrate the manner of sending and receiving (strands) *msgs* online, the criteria for trusted e-authentication systems and how the process of e-authentication is or should be conducted.

Having examined the e-authentication measures, it becomes clear that the current e-authentication processes are inadequate. In particular, they are not strong enough to reasonably withstand cracking attacks. The vulnerability of these measures is not only limited to the weaknesses of weak or strong passwords. It also extends to the flaws of the existing e-authentication tools. For example, it was established from the e-authentication theories that e-authentication is usually carried out by a remote server (the *S*). In this instance, *U* submits an *ID* or *Pw* into an allocated space. The *S* verifies the *ID* or *Pw*. In the case of a smart cards-based remote e-authentication, a smart card which contains an *h* will generate an *rn*. It is submitted that this *rn* is analogous to an *OTP*. Thereafter, the *S* determines whether or not access should be accepted or denied to a user based on the information entered. Based on this, it is submitted that one of the purposes of e-authentication, that is, to prevent e-crimes cannot be achieved. By way of elaboration, chapter 4 revealed that computer crackers usually operate between computers. They target and attack computer (remote) servers and divert information stored in these servers into use other that intended by users. Accordingly, a use of servers (and in some cases smart cards) to authenticate users or their credentials online can be detrimental to users and the process of e-authentication as a whole. OTPs or *rns* cannot be expected to adequately prevent this damage. More specifically, cases have been reported in the past wherein the reliability or sufficiency of OTPs was questioned.[287] In these cases, consultants who, at the time, worked for

---

[287] BusinessDay http://www.bdlive.co.za/articles/2009/11/26/vodacom-accused-duped-lawyers-court-hears;jsessionid=5ADC6353F964516D33B8D9D2450B64DC.present2.bdfm (Date of use: 28 October 2013). See also Arde http://www.iol.co.za/business/personal-

certain cellular phone providers teamed up with criminals. This scheme was aimed at intercepting the OTPs before they reach the intended computer users. In each case, whenever a computer user requires the services of a particular service provider the consultants would open one sim-card for the computer user and a duplicate for themselves. For purposes of carrying out e-transactions, an OTP would be sent to a computer user's cellular phone or electronic mail and the designated duplicate sim-card. Consequently, the consultants would immediately use the OTP in order to access funds masquerading as users. Due to the fact that an OTP can only be used once, genuine users were prevented from accessing the funds or an account.

Given the identified shortcomings, chapter 7 introduces an elaborate framework to e-authentication. The framework is studied under the broad ambit of the *Precautionary Principle*. It does not necessarily segregate between the e-authentication theories. Simply, it argues that the e-authentication theories should be read together in order to establish appropriate e-authentication frameworks that responds to current and future e-crimes. This approach is part of customary international law,[288] and deals with the governance or regulation of risks to a particular phenomenon.[289] For e-authentication purposes, it contends that e-crimes pose grave risks to the sensitive information that belongs to computer users. Because of these risks, an ICT regulatory agenda should be a representation of the ICT and the risks that are posed to these recent forms of technologies.

---

finance/banking/how-crooks-use-sim-swaps-to-rob-you-1.1507185 (Date of use: 28 October 2013).

288 McIntyre O and Mosedale T "The precautionary principle as a norm of customary international law" 1997 (9) *Journal of Environmental Law* 221-241 235.

289 Sunstein CR "Beyond the precautionary principle" 2003 (151) *University of Pennsylvania Law Review* 1003-1058 1003.

CHAPTER 7

A PRECAUTIONARY APPROACH TO E-AUTHENTICATION

CHAPTER 7

A PRECAUTIONARY APPROACH TO E-AUTHENTICATION

7.1 INTRODUCTION

It was indicated above that property rights vest in information. These rights arise because users of information expend time and effort in gathering information. Consequently, information has become an essential asset of an information society. Given this importance, a risk exists that information may be appropriated by criminals illegally. Given this risk, it is then determined whether information is capable of being stolen. Having considered the developments of the law of theft in Roman-Dutch, English and South African law, it was argued that information can be stolen. The techniques that are used in e-crimes are discussed in order to demonstrate how the theft of information actually occurs. Because e-crimes have become more pervasive, it is then submitted that they pose grave challenges to the information society. The most pertinent of these challenges relate to whether it is possible to regulate ICTs or not, and whether the law is or legal rules are sufficient to adequately address ICTs and the challenges that are generated by these contemporary technologies or not. It was found that ICTs are spheres where regulations apply. However, it was argued that regulations could provide assistance to the ICT regulatory agenda. Thus, the role of the law should be to channel the nature and structure ICT regulations. In doing this, the state should, in incepting legal rules, be guided by the ICT regulatory theories that are discussed in chapter 5 above.

Having established that recent technologies can be regulated, ICT regulatory measures were examined in chapter 6. These measures were discussed as part of a broader System of Authentication. The discussion of the authentication measures was both theoretical and practical. The theoretical approach to authentication investigated the importance of authentication in offline settings. Accordingly, an overview of authentication and how it has come to be accepted as a model was illustrated. Given this acceptance, it was pointed out that the successes of offline authentication measures have led to these mechanisms being used in online environments, that is, the e-authentication process. Furthermore, it was stated that e-authentication does not necessarily mean the e-authorisation process. E-authentication has to do with the identification and verification of certain personal information online. However, e-

authorisation follows e-authentication and deals with the validation of the information that was identified and verified during the process of e-authentication. Therefore, it assists in arriving at the decision regarding whether or not a person who has been subjected to the e-authentication process should access a particular system or network. The study of the practical approach to authentication relied on a number of mathematical sketches or graphs. These sketches were extracted from certain selected e-authentication theories. The aforementioned theories included the trust, strand spaces and remote e-authentication theories. The rationale for examining the sketches was to give meaning to the theoretical aspects of e-authentication.

The study of the e-authentication measures in chapter 6 above revealed that the e-authentication process is founded on legal rules. These rules do not seem to have been modelled from the ICT regulatory concepts and theories that are discussed in chapter 5. Because of this, the e-authentication agenda that can be drawn from these legal rules is not bound to the technology to be regulated and is not capable of evolving with it. Specifically, it discards the fundamentals of the Good Regulator Theorem. Consequently, an ICT regulatory approach which is abstracted from these legal rules is one that is susceptible to continuous changing in so long as technologies develops. Following these limitations, a complementary e-authentication framework is proposed in this chapter. It builds on the investigation of risk regulation that was illustrated in the United Kingdom and Canada approaches to e-authentication. In this research, the proposed e-authentication structure is called the Precautionary Approach to E-Authentication or PAEA. It argues that the phenomena of risks should underpin every e-crimes controlling or regulatory exercise. For example, it regards e-crimes as one of the malicious threats that are generated by contemporary technologies. Because of this, PAEA supports the necessity to establish a risk or threat-based e-authentication framework. This framework responds or should respond to the existing uncertainties regarding how ICTs in general and e-crimes in particular should be regulated.

Furthermore, PAEA recommends a move from a point where regulators merely dwell on the influence or impact of the damages that are caused by e-crimes to a stage where regulators accept that the insufficiency, absence or uncertainty of science or scientific knowledge about the scale or degree of e-crimes does or should not prevent

the taking of measures to deter e-crimes.[1] This does not mean that science becomes insignificant to the study of risks to ICTs. Simply, the proposed move aims to demonstrate that a lack of certainty about the scale of the risks does or should not be taken to mean that risks do not exist.[2] Accordingly, regulators still need to exhaustively evaluate the scientific information which is related to the risks that are posed to contemporary technologies.[3]

The principle to exercise precaution or the so-called *Precautionary Principle* shapes the manner of studying PAEA. An examination of the precautionary principle is generally made in fields dealing with environmental studies. In this chapter these sources are then consulted in order to give meaning and substance to the precautionary approach to e-authentication. Thereafter, the manner in which PAEA operates or should operate for ICT regulatory purposes is demonstrated in chapter 8 below.

7.2 OVERVIEW OF THE PRECAUTIONARY PRINCIPLE

7.2.1 Background

A reference to the notion of precautionary principle was originally foreign in English literature. It is specifically a product of the events or debates that arose in the mid-1970s regarding the necessity to prevent environmental degradation or damage. During this time, it came to be accepted as an English term after the German word *Vorsorgeprinzip*. The concept of *Vorsorgeprinzip* is founded on good household management and it means 'to have foresight (*Vorsorge*) in planning'.[4] It is equated with the need to exercise caution, that is, to be cautious.[5] However, it is required that

---

1 Atapattu SA *Emerging principles of international environmental law* (Transnational Publishers New York 2006) 203.

2 Cox R *Environmental communication and the public sphere* 3rd ed (Sage Publications Los Angeles 2013) 324.

3 Commission of the European Communities "Communication from the Commission on the precautionary principle" 2 February 2000 14. To be accessed at http://ec.europa.eu/dgs/health_consumer/library/pub/pub07_en.pdf.

4 Williams MJ *NATO, Security, and risk management: from Kosovo to Kandahar* (Routledge Abington 2009) 97.

5 Holder J and Elworthy S "The BSE crisis – a study of the precautionary principle and the politics of science in law" in Reece H (ed) *Law and science: current legal issues Volume 1* (Oxford University Press Oxford 1998) 129-152 131.

Vorsorge or prudence (foresight principle)[6] should be at the centre of such an exercise.[7] This entails the avoidance of damage or a risk by 'careful forward planning, blocking the flow of potentially harmful activities'.[8]

Despite the novelty of the term, the taking or the practice of taking precautionary measures is an old phenomenon. Notions such as better safe than sorry, look before you leap, an ounce of prevention is worth a pound of cure[9] or prevention is better than cure characterise the acceptance of the practice in society. In some quarters, society associates the plea for the exercise of caution with human awareness or rationality. For instance, it has become rational to wear seat belts and motorcycle helmets in anticipation of an unproven event (accident) and to insure a building or life even in circumstances where there is no certainty regarding the cause and time of the risk (fire, accident or death). This analogy also has relevance to this research. In particular, it has relation to what may be referred to, in technological terms, as the action handling. Action handling has everything to do with preparedness – that is, being prepared for an imminent or eventual threat. It requires that one should design measures in order to respond to attacks in the future. Within the context of this research, it implies the introduction of certain regulatory or pre-emptive measures in order to alleviate forthcoming risks.

The origin and history of the precautionary principle is examined above. It is particularly illustrated that although the term precautionary principle is new in English literature, the practice of taking precautions or acting cautiously is an old phenomenon. Having studied the foundations of the precautionary principle, it becomes imperative to revise its meaning. The sections below therefore investigate this meaning.

7.2.2 What is the Precautionary Principle?

---

6 Resnik DB "Is the precautionary principle unscientific?" 2003 (34) *Studies in History and Philosophy of Biological and Biomedical Sciences* 329-344 329.

7 Holder and Elworthy *Precautionary principle* 131.

8 Tickner J and Raffensperger C *The Precautionary principle in action: a handbook* (Science and Environmental Health Network Windsor 1991) 2.

9 Bodansky D "Scientific uncertainty and the precautionary principle" 1991 (33) *Law, Environment: Science and Policy for Sustainable Development* 4-5 4.

There is no single description of the concept that exists in modern literature. In some cases, culture is used in order to give meaning to the precautionary principle. In other cases, the principle is affiliated with a particular discipline.[10] The absence of a precise definition does not imply however that the principle fails to possess a conceptual core.[11] Some argues that the principle conforms to the doctrine of *in dubio pro natura*.[12] This doctrine denotes that in cases where a doubt exists, natural surroundings or nature should be favoured.[13] For ICT regulatory purposes, this doctrine could be interpreted to mean that in cases of uncertainty regarding the possibilities of risks to ICTs or their regulation, any decision must be in favour of ICT protection.[14] Others state that the principle is necessary in dealing with or regulating modern setbacks to society.[15] Accordingly, they equate the principle with the rules of natural justice.[16] In this respect, it leads or can lead to the attainment of procedural fairness in decision-making.[17]

There are criticisms that may be levelled against the precautionary principle. On the one hand, there is the view that the principle is disjointed.[18] More specifically, it attacks and condemns the regulatory norms and standards that it seeks to uphold.[19] One of the most important of these norms goes something like: before regulations are commenced, steps should at least be taken in establishing the content and scale of the

---

10 Martin PH "If you don't know how to fix it, please stop breaking it! the precautionary principle and climate change" 1997 (2) *Foundations of Science* 263-292 266.

11 Trouwborst A *Precautionary rights and duties of states* (Martinus Nijhoff Publishers Leiden 2006) 2.

12 Trouwborst *Precautionary* 2.

13 Boyd DR *The environmental rights revolution: a global study of constitutions, human rights and the environment* (UBC Press Vancouver 2012) 224.

14 Boyd *Revolution* 224.

15 *Bridgetown Greenbushes Friends of the Forest Inc. v Executive Director of the Department of Conservation and Land Management* 2000 SOL Case 673, 1 December 2000 para 118.

16 *Bridgetown Greenbushes Friends of the Forest Inc. v Executive Director of the Department of Conservation and Land Management* 2000 SOL Case 673, 1 December 2000 para 118.

17 *Mohr v Great Barrier Reef Marine Park Authority* [1998] AATA 805 para 124

18 Sunstein http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1371&context=law_and_economics (Date of use: 18 January 2016).

19 Sunstein http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1371&context=law_and_economics (Date of use: 18 January 2016).

risks. On the other hand, it is said that the precautionary principle does not centre on the needs of society. In South Africa, this necessity is termed Batho Pele. Batho Pele is a South African imperative which translates in English to people first. It guarantees the promotion and maintenance of high standards of professional ethics; provision of services impartially, fairly, equitably and without bias; utilisation of resources efficiently and effectively; responding to people's needs; participation of citizens in policy-making and rendering an accountable, transparent, and development-oriented public administration.[20] With this in mind, it may be argued that a study of the precautionary principle should be made in consideration of the societal needs.

In this research, the need to preserve the principles for Batho Pele is advocated. Accordingly, it is argued that a discussion of the precautionary principle does not necessarily hamper the achievement of these principles. Conversely, it is closely linked with the regulation of risks or what is known as the process of risk regulation. Given this, it has to be acknowledged that risk regulation is concerned with the protection of one particular phenomenon (society) from the risks that arise or are perceived to ensue by reason of engaging in other activities – for example air pollution.[21]

Four elements or dimensions are identified within which the term precautionary principle is defined.[22] These are categorised as the risk or threat element, the uncertainty element, the action element and the command element.[23] These elements are in turn discussed in the sections below.

(a) Risk Element

In terms of the risk dimension, the principle is described by using phrases, for example a 'potentially dangerous or irreversible threat or damage'. The example of this can be

---

20 Independent Police Investigative Directorate of the Republic of South Africa http://www.ipid.gov.za/about%20us/batho_pele.asp (Date of use: 27 January 2014).

21 Fisher E "Is the precautionary principle justiciable?" 2001 (13) *Journal of Environmental Law* 315-334 317.

22 DeFur PL and Kaszuba M "Implementing the precautionary principle" 2002 (288) *The Science of Total Environment* 155-165 157 and Sandin P "Dimensions of the precautionary principle" 1999 (5) *Human and Ecological Risk Assessment* 889-907 890-891.

23 Sandin 1999 *Human and Ecological Risk Assessment* 890-891.

found in principle 15 of the Rio Declaration on Environment and Development (1992).[24] Principle 15 of the Rio Declaration states the following:

> In order to protect the environment, the precautionary approach shall be widely used by States according to their capabilities. Where there are *threats of serious or irreversible damage*, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation.[25]

The Science and Environmental Health Network in its so-called *Wingspread Statement on the Precautionary Principle (1998)* follows this particular line of reasoning. It provides that the adoption of the precautionary principle is sometimes indispensable in cases where 'an activity raises *threats of harm to human health or the environment*'.[26]

The connotation of a risk for purposes of examining the risk dimension needs further scrutiny. From the passages above it appears that a risk is normally associated with danger.[27] In other words, no distinction seems to be created or have been created between risks. Accordingly, a risk is regarded as a measure within which the likelihood or consequence of future events or damages is assessed.[28] Sunstein provides a philosophical dimension to the overall study of risk. This can be drawn from two of his works the working paper entitled "The Laws of Fear"[29] and the book which is titled *Laws of Fear: Beyond the Precautionary Principle*.[30] In his working paper Sunstein identifies what he refers to as the hysteria and neglect. Hysteria or neglect is,

---

24 Hereinafter referred to as the Rio Declaration.

25 The Ministerial Declaration of the Third International Conference on the Protection of the North Sea, The Hague, 8th March 1990. To be accessed at http://www.seas-at-risk.org/1mages/1990%20Hague%20Declaration.pdf. See also Santillo D *et al* "The precautionary principle – protecting against failures of scientific method and risk assessment" 1998 (36) *Marine Pollution Bulletin* 939-950 939-940.

26 Science and Environmental Health Network http://www.sehn.org/state.html#w (Date of use: 19 November 2013).

27 Van Asselt MBA *Perspectives on uncertainty and risk: the PRIMA approach to decision support* (Kluwer Academic Publishers Dordrecht 2000).

28 COMEST "The precautionary principles" March 2005 28. See also Yoe C *Principles of risk analysis: decision making under uncertainty* (CRC Press Boca Raton 2012) 1.

29 Sunstein CR "The laws of fear" 2001 (128) *John M. Olin Law & Economics Working Paper* 1-42.

30 Sunstein CR *Laws of fear: beyond the precautionary principle* (Cambridge University Press Cambridge 2005).

according to Sunstein, commonly used as an indication that a risk exists.[31] He alleges that some people resort to heuristics or mental shortcuts in order to establish whether or not risks exist.[32] Sunstein therefore warns against the abovementioned and say the following: People (generally) dislike losses far more than they like corresponding gains…. (They) tend to focus on the losses that are associated with some activity or hazard and to disregard the gains that might be associated with that activity or hazard.[33] The abovementioned arises because people focus on some risks because they are cognitively available.[34] This then enable them to disregard certain risks despite the fact that these risks are favoured by statistics.

Having examined the notion of risk, one thing becomes clear: the world (offline or online) is a very risky place.[35] More specifically, risks always characterise or pose a challenge to human life and natural resources. Nonetheless, this does or should not be construed as a justification for the taking of irrational decisions under the pretext of responding to a perceived risky state of affairs.

(b) Uncertainty Element

The notion that where there is a risk, there is uncertainty seems to be the basis upon which the uncertainty dimension is founded.[36] This viewpoint regards a risk as a chance of an uncertain outcome or situation. This chance can be precipitated by a suspicion of a dangerous situations[37] or a long-term hazard which, if action is postponed, can lead to a large-scale disaster. Uncertainty evidences an absence of or incomplete knowledge about a particular adverse event. In one case, phrases such as a lack of full scientific certainty[38] or 'before a causal[39] link has been established by

---

31 Sunstein 2001 *John M. Olin Law & Economics Working Paper* 2.

32 Sunstein 2001 *John M. Olin Law & Economics Working Paper* 3. See also Sutton IS *Process reliability and risk management* (Van Nostrand Reinhold New York 1992) 19.

33 Sunstein 2003 *University of Pennsylvania Law Review* 1008. See also Lofsterdt RE "The precautionary principle – risk, regulation and politics" 2003 (81) *Trans IChemE* 36-43 39.

34 Lofsterdt 2003 *Trans IChemE* 39.

35 Wilson R "Analysing the daily risks of life" 1979 *Technology Review* 41-46 41.

36 Bodansky 1991 *Law, Environment: Science and Policy for Sustainable Development* 4.

37 Vercelli A "From soft uncertainty to hard environmental uncertainty" 1995 (48) *Economie Appliquée* 251-269.

38 Art 3(3) of the UN Framework Convention on Climate Change of 1992.

absolute clear scientific certainty are mostly used to demonstrate the presence of uncertainty. In others, phrases like 'pending further scientific information for a more comprehensive risk assessment' are resorted to.[40]

Two sets of uncertainties are distinguished. They are a macro-level uncertainty and micro-level uncertainty.[41] Macro-level uncertainty is broader than micro-level uncertainty. It refers to doubts about the current structures, normative standards and the proper response(s) to be used to respond to the risks.[42] Micro-level uncertainty is subject-specific. It discusses the context (knowledge, models or information) within which particular decisions are made or actions are taken.[43]

(c) Element of Action

Uncertainty generally necessitates that particular decisions should be taken.[44] Loosely put, uncertainty justifies the taking of decisions to prevent a risk.[45] Seemingly, the viewpoint that 'decisions (or action) cannot wait until everything relevant is known' is maintained.[46] The decision or action to be taken in each case depends or should depend on the decision theory or theories that inform such an action. The theories respond to the dilemma which is associated with decision-making.[47] They include the behavioural (normative or descriptive), managerial, statistical, economic, administrative, conflict-minimisation model and casual or non-casual. The impasse or

---

39 Kant provides an illustrative philosophical argument about what is meant by the notion of 'cause' and its effect. See Kant I *Critique of pure reason* as translated by Müller FM *Immanuel Kant's critique of pure reason* (The MacMillan Company London 1922) 122.

40 Art 7 of Regulation EC/178/2002 (hereinafter referred to as the European Food Directive).

41 Yoe *Uncertainty* 23.

42 Yoe *Uncertainty* 23.

43 Yoe *Uncertainty* 23.

44 One of the refined definitions of the term 'decision' can be found in the book by Johnson Jr. and Kruse. They argue that a decision is a 'conscious choice (which is) made between two or more competing alternatives. (And) decision-making is not a robotic affair'. See Johnson Jr. BL and Kruse SD *Decision making for educational leaders: underexamined dimensions and issues* (State University of New York Press New York 2009) 13.

45 Lofsterdt 2003 *Trans IChemE* 37.

46 Corbett D *Australian public sector management* 2nd ed (Allen & Unwin Pty Ltd St. Leonards 1996) 62.

47 Berger JO *Statistical decision theory and the Bayesian analysis* 2nd ed (Springer New York 1985) 1.

improbability in decision making may be illustrated by examining certain questions. These questions relate to what or which decision to take, who should take such a decision and under which conditions will a decision work?

The element of action relates to the proper response to be applied to the looming risks.[48] Phrases such as 'cost effective measures to prevent….degradation, preventive measures or regulatory action are an expression of this element or dimension'.[49] The use of these phrases can be abstracted from various international instruments. In one case, it is said that preventive measures or regulatory action ought to be resorted to in cases where its costs are reasonably low. In other words, the action should generally be 'cost-effective so as to ensure global benefits at the lowest possible cost'.[50] In others, it is submitted that a lack of full scientific certainty should not be used as the basis for postponing the cost-effective actions.[51]

However, it is conceded that an absence of the phrases as aforesaid above in any instrument supporting the precautionary principle does not imply that action is not encouraged. This is the case because a threat commonly necessitates that action should be taken.

(d) Command Element

The strength of the command element varies. There is a weak version and a strong version.[52] The weak version is represented by words such as is justified or justifiable. Consequently, it may be said that 'it is justified or justifiable to control or inhibit a possibly hazardous situation before scientific certainty is established'. The strong version can be extracted from terms, for example should or ought. For example, it may be stated that measures or action to prevent or regulate the risks should or ought to be adopted even in cases where scientific proof regarding their nature and severity is

---

48 It is also acknowledged that not doing anything or non-action can, in certain limited circumstances, also amount to an action. See COMEST 2005 18.

49 Sandin 1999 *Human and Ecological Risk Assessment* 894.

50 Principle 3, Art 3 of the UN Framework Convention on Climate Change.

51 Principle 15 of the Rio Declaration.

52 Godard O "Social decision-making under scientific controversy, expertise, and the precautionary principle" in Joerges C, Ladeur KH and Vos E (eds) *Integrating scientific expertise into regulatory decision-making: national experiences and European innovations* (Nomos Baden-Baden 1997) 39-73 66-69.

lacking. Thus, a lack or insufficiency of science does not deter the taking of actions to prevent a risk or threat.[53]

7.2.3 Summary

It is stated above that society has reached a stage of development where a far-reaching framework to e-authentication should be adopted. Within the context of this research, this framework is referred to as the precautionary approach to e-authentication (or PAEA). The general ambit and scope of PAEA is drawn from the precautionary principle. The precautionary principle encourages regulators to exercise caution and foresight in regulatory planning (foresight principle).[54] In particular, it encourages regulators to adopt and embrace measures that are designed to circumvent the damage or risks by anticipating and blocking the envisaged flow of harmful activities.[55] The foresight principle does not imply that science is insignificant within a regulatory structure. Therefore, it is still necessary to conclusively demonstrate that risks exist or are imminent. However, the principle accepts that the uncertainty or lack of science does or should not be used as an excuse for inaction or a failure to commence regulations. For purposes of ICT regulation, this denotes that the existing (scientific) doubts regarding the scale of the measures to regulate ICTs and their associated challenges cannot or should not be a ground for postponing the application of PAEA.

In the section below, an analysis of the meaning and significance of the precautionary principle in e-authentication settings are scrutinised. The aim is to attempt to stay true to the object of this research. This relates to the necessity to discard the practice of re-inventing the ICT or technology regulatory wheel. Conversely, it supports the desire to (i) establish a suitable e-authentication regulatory framework which is (ii) attached or bound to the technology and is (iii) able to evolve with and respond to the developments in these technologies.

7.3 PRECAUTIONARY PRINCIPLE IN E-AUTHENTICATION FRAMEWORKS

---

53 DeFur and Kaszuba 2002 *The Science of the Total Environment* 157.
54 Williams *Risk management* 97.
55 *Mohr v Great Barrier Reef Marine Park Authority* [1998] AATA 805 para 124.

7.3.1 Background

Prevention is one of the essential ingredients in any ICT regulatory agenda. For purposes of prevention, regulators are enjoined to establish measures that forestall a wrong.[56] The mechanisms are aimed at preventing regulators from subsequently dealing with the adverse consequences (responsive measures) that are created by a wrong.[57] In practice, these prevention measures are referred to as the computer or information security mechanism. The most common are the awareness creation, management of patches,[58] installing antivirus software, configuring personal firewalls, using user account control (UAC), creating data backups and recovering from attacks.[59] Despite this, it is submitted that prevention can generate a number of drawbacks. This does not only lie in the fact of it being misconstrued sometimes - for example it being interpreted to mean that it deters a total use and access to modern forms of technologies. But it also relates to the fact that regulators may not have all the indispensable facts and figures regarding the extent and scale of that which is to be regulated. The presence of these figures is important to the regulatory agenda. It enables regulators to design measures that fully address a wrong, for example e-crimes. Specifically, it was submitted in the previous chapters that ICTs progress almost on a continuous basis. With these constant evolutions come the risks. Given this, regulators are or may be placed at a disadvantage if prevention is singularly used. This is the case because it is possible that other factors that are related to ICT regulation may be unknown or uncertain to regulators at the time that the prevention measures are devised. For example, regulators may not know the techniques that crackers are likely to use in the future, and they may not be able to identify with certainty the degree and scale of e-crimes and the technologies that may be exploited in order to commence e-crimes. Due to these uncertainties, it is almost guaranteed that

---

56 Cane P *The anatomy of tort law* (Hart Publishing Oxford 1997) 100.

57 Cane *Anatomy* 100.

58 From this, it may be distinguished between a security patch – that is, software which cover and address the identified risks or threats in a system or network– and a service patch – that is, software which provides security updates and their accompanying features on a continuous basis. See Nicastro FM *Curing the patch management headache* (Auerbach Publications Florida 2005) 18-22 and Jang M *Linux patch management: keeping Linux systems up to date* (Pearson Education Inc. New Jersey 2006) 9.

59 Ciampa M *Security awareness: applying practical security in your world* 4th ed (Cengage Learning Boston 2014) 88-96.

regulators may subsequently pass regulations that merely deal with the previous and present risks to ICTs. Consequently, the regulations may not be able to deal with forthcoming or future risks to ICTs.

In response to the identified inadequacy of prevention, an ICT regulatory framework which is referred to as PAEA is proposed. This structure accepts that e-authentication processes should generally lead the identity validation process. In other words, the process to verify the personal particulars of a user, for example ID, username and password or the user himself or herself should not be postponed until such a user registers or enters his or her identification particulars into a system. This does not entail a total exclusion of the identification particulars within the context of e-authentication. However, PAEA complements and promotes the need to amplify the current e-authentication approach. This extension should be in line with the necessity to establish a decentring analysis regarding the control and management of ICTs and its associated threats. The latter relates to the use of different role-players, for example a government, individual firms and community in regulatory schemes.

Furthermore, PAEA is suggested following the study of the regulatory theories in chapter 5. It accepts that ICTs produce their own languages. Sometimes, these languages develop separate or far apart from existing or foreseen legislations. Therefore, the whole or wholeness of these technologies ought to be studied before a regulatory structure which has relation to them is commenced. Consequently, this structure should be modelled on the technologies to be regulated and be a reproduction of it. The basis for this is that regulators should recognise that ICTs are a conglomeration of systems or networks many of which have sub-systems or sub-networks. These networks or sub-networks share similar characteristics. These characteristics have similar structures or shapes and others do not. Therefore, ICT regulations ought to be developed that appreciate the functioning or non-functioning of the systems or networks. The AIS theory is also relevant in this regard. This is the case because ICTs evolves. With these developments new forms of risks emerge. Therefore, it may be necessary for ICT regulators to rely on or study the dynamic behaviours of online users on or before the personal particulars of a computer user are

entered into a system. This examination should amount to what is referred to within the context of this chapter as the behavioural biometric.[60]

Behavioural biometric relies on the biometric data that are studied in chapter 6 above. It will be recalled that in chapter 6 the data was studied as one of the pillars (that is, proof by property) to e-authenticate a computer user or the particulars of a computer user. However, for purposes of PAEA the biometric data are examined in order to achieve a particular purpose. This is to support the view that an e-authentication framework which is modelled from the existing pillars of e-authentication is bound to fail. Accordingly, it is argued that e-authentication frameworks should be built on an ICT regulatory structure that accepts that ICTs evolve. Given this, it is necessary to rely on characters for e-authentication purposes that do not require to be changed following the developments in technologies. These characters should study the behaviour of a user online. They should exist even in cases where computer crackers devise techniques to intercept identifying information. Furthermore, they should amplify the already established incident-based forms of e-authentication. However, the effectiveness of behavioural characterisation must be tested against the convenience it affords to users. In other words, it has to be carried out in a manner that promotes the availability, accuracy, authenticity, confidentiality, integrity, utility and possession of information.

Within the context of this research, various methods are identified that assist in studying behavioural biometrics. These methods mimic the biometric data which is studied in chapter 6. This data includes signature dynamics, voice verification and keystroke dynamics. It is argued that these identification methods are by no means exhaustive. This is the case because other methods can also be found, for example the manner in which a user moves a computer mouse (mouse movements) - where the manner and sequence of moving a computer mouse are detected.[61]

---

60 See Whitman ME and Mattord HJ *Principles of information security* (Cengage Learning Australia 2012) 332-333.

61 Zheng N, Paloski A and Wang H "An efficient user verification system via mouse movements" in *Computer and communications security* (Papers delivered at 18th ACM conference on Computer and communications security 17-21 October 2011 ACM New York) 139-150, Purasa M and Brodley CE "User re-authentication via mouse movements" in *Visualization and Data Mining for Computer Security* (Papers delivered

In summary, a separation exists between the proposed behavioural biometrics and the biometrics data which is studied in chapter 6 above. The question is: what is it that distinguishes the two? Biometrics identification is examined as part of the prevention process, in this case, e-authentication. It helps in making an informed decision regarding whether a person should be granted authority to access a system or not. It has already been stated in chapter 6 above that prevention does not always yield positive results. Within the context of regulating modern forms of technologies, this means that there may be cases where ICT regulators may not have all the relevant facts and figures in terms of which the prevention measures could be based. In these instances, the measures may prove to be insufficient for ICT regulatory purposes. This position does not appear to be adequately resolved by the ICT regulatory theories. It is important to revert back to the Danger theory for a moment. The theory has to do with the creation of a systematised immune system. This system helps in identifying and discriminating between self and non-self attacks. Self attacks refer to the known or probed attacks. Whereas non-self attacks amount to unknown attacks that arise in the future as a result of the system being exposed to danger. It is argued that the position regarding the control of self attacks is straightforward. The system could with the help of the immune system fight these attacks and consequently repel them. However, a difficulty arises when it comes to the regulation of the non-self attacks. The AIS theory requires that a process of immunisation should follow. In other words, the system should be injected with new or modern defence mechanisms that are able to control emerging risks. In relation to this, a question is asked regarding what happens or should happen during the period between the emergence of novel risks and the injecting of the system? Behavioural biometrics provides an answer to this question. It requires that a framework should be created which studies and anticipates the risks. The smart regulation process, which involves the different role-players in ICT regulation, can be followed. The latter is a collaborative practice. In this process, the current scheme to prevent e-crimes is examined against the backdrop that ICT

---

at the 2004 ACM workshop on Visualization and Data Mining for Computer Security 29 October 2004 IEEE New York) 1-8 2-3 and Hashia, Pollett and Stamp http://www.cs.sjsu.edu/faculty/pollett/masters/Semesters/Spring04/Shivani/shivanipaper.pdf (Date of use: 13 November 2013).

evolves. With this development comes the danger that contemporary e-crimes will emerge.

(a) Signature Recognition

Studies that were aimed at addressing the issue of signature recognition initially came to the public domain during the 1960s.[62] These writings only dealt with one aspect of signature recognition. They focused on the symmetrical characteristics of a signature as opposed to its dynamic characteristics. It was during the 1980s that attempts were made to establish systems that assisted in monitoring the dynamics of signatures. Plamondon and Lorette are some of the writers who recognised this need.[63] They argued that users typically follow a particular pattern when writing their signatures.[64] This may relate to the appearance, shape, timing and pressure of writing.[65] Therefore, it is necessary to, they also argued, create systems that are able to pick up the aforementioned trends. These systems should, according to Plamondon and Lorette, be equipped with a 'digitiser or an instrument (or digitised) pen…and camera or scanner'.[66]

It is noteworthy that a number of papers have since been reported that follow some of the observations that were primarily made by Plamondon and Lorette.[67] For example,

---

62 Mauceri AJ "Feasibility studies of personal identification by signature verification" (Report No: SID 65 24RADC TR65 33, Space and Information Division, North American Aviation Company Anaheim 1965).

63 Plamondon R and Lorette G "Automatic signature verification and writer identification – the state of the art" 1989 (22) *Pattern Recognition* 107-131.

64 Plamondon and Lorette 1989 *Pattern Recognition* 107-108.

65 Bennet RF *Electronic authentication and digital signature: hearing before the Subcommittee on Financial Services and Technology of the Committee on Banking, Housing, and Urban Affairs United States* (US Government Printing Office Washington 1998) 53.

66 Plamondon and Lorette 1989 *Pattern Recognition* 108.

67 See, for example Dereli T and Tucker RW "Signature dynamics in general relativity" 1993 (10) *Classical and Quantum Gravity* 365-373, Yang L, Widjaja BK and Prasad R "Application of Hidden Markov Models for signature verification" 1995 (28) *Pattern Recognition* 161-170, Bajaj R and Chaudhury S "Signature verification using multiple neural classifiers" 1997 (30) *Pattern Recognition* 1-7, Huang K and Yan H "Off-line signature verification based on geometric feature extraction and neural network classification" 1997 (30) *Pattern Recognition* 9-17, Nelson W and Kishon E "Use of dynamic features for signature verification" in *Systems, management, and cybernetics* (Papers delivered at the IEEE International Conference on Systems, Management, and Cybernetics 17-20 October 1991 IEEE Le Touquet) 17-20 21-25.

Huang and Yan argue that calligraphic information or the geometric property of a signature is essential in identifying signature dynamics.[68] It particularly demonstrates the local and structural features of a particular signature. This identification consequently eases the process of extracting the least adjustable features of a signature.[69] The view by Huang and Yan seem to be followed by Bajaj and Chaudhury. According to Bajaj and Chaudhury, a signature entails a comprehensive carbon copy.[70] It is a representation of the different writing styles of users.[71] These styles can be recognised and verified by reliable systems that are created for this purpose.[72] These systems ought to be able to measure the outlook, form and compression of signatures.[73]

(b) Voice Verification

Preliminary attempts to establish a system for programmed voice verification can be traced to the 1970s. During that time the papers by Schafer and Rabiner,[74] Doddington[75] and Lummis[76] remained some of the reference point in this field. In the aforementioned papers it was accepted that the pitch of a voice (voice pitch) and its intensity (voice intensity) are some of the most significant features for voice verification.

Despite these developments, it is argued that one of the major breakthroughs on voice verification was the article by Furui which was published in 1981.[77] Firstly, Furui described voice (or speaker) verification as a process in terms of which the identity of a

---

68 Huang and Yan 1997 *Pattern Recognition* 9.
69 Huang and Yan 1997 *Pattern Recognition* 9-10.
70 Bajaj and Chaudhury 1997 *Pattern Recognition* 1.
71 Bajaj and Chaudhury 1997 *Pattern Recognition* 1.
72 Bajaj and Chaudhury 1997 *Pattern Recognition* 1.
73 Bennet *Electronic Authentication* 53.
74 Schafer RW and Rabiner LR "System for automatic format analysis of voiced speech" 1970 (47) *The Journal of the Acoustical Society of America* 634-648.
75 Doddington GR "A method of speaker verification" 1971 (49) *The Journal of the Acoustical Society of America* 139.
76 Lummis RC "Real-time technique for speaker verification by computer" 1971 (50) *The Journal of the Acoustical Society of America* 106 and Lummis RC "Implementation of an online speaker verification scheme" 1972 (52) *The Journal of the Acoustical Society of America* 181.
77 Furui S "Cepstral analysis technique for automatic speaker verification" 1981 (29) *IEEE Transactions on Accounts, Speech, and Signal Processing* 254-272.

narrator is established.[78] This identification is established or can be ascertained by calculating a narrator's expressions.[79] This calculation is intended to establish and identify a set of known voices or speakers.[80] The latter is mostly achieved by undertaking different tests or experiments. The most notable are the YOHO Corpus test (which is a combination of different phrases), baseline speaker verification test and voice-altered imposter test.[81] Secondly, Furui accepted that the pitch and intensity of a voice are essential in identifying a person using voice verification. However, he developed a (fresh) framework of voice verification which he called the identity claim and sample utterance.[82]

(c) Keystroke Dynamics

Keystroke dynamics became popular during the 1980s. The report that was prepared by Gaines, Lisowski, Press and Shapiro represent one of the early works which initiated a move to this form of biometric behaviour.[83] Keystroke dynamic is a convoluted process. Being a process, it encompasses a number of activities. Firstly, the ways in which a computer user types on a computer keyboard, that is, the rhythm of his or her keystrokes are analysed. Secondly, the rhythm of the key-presses is identified by relying on the habitual pattern of the keystrokes. Therefore, it may be

---

78 Furui 1981 *IEEE Transactions on Accounts, Speech, and Signal Processing* 254.

79 Furui 1981 *IEEE Transactions on Accounts, Speech, and Signal Processing* 254.

80 Reynolds DA "An overview of automatic speaker recognition technology" in *Acoustics, speech, and signal processing (ICASSP)* (Papers delivered at the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP) 13-17 May 2002 IEEE Florida) IV-4072-IV-4075 IV-4072. See also, Kinnunen T and Li H "An overview of text-independent speaker recognition – from features to supervisors" 2010 (52) *Speech Communication* 12-40 12-13.

81 Campbell JP "Testing with the YOHO CD-Rom voice verification corpus" in *Acoustics, speech, and signal processing* (Paper delivered at the International Conference on Acoustics, Speech, and Signal Processing, *1995* 9-12 May 1995 IEEE Detroit) 341-344 341-343 and Pellom BL and Hansen JHL "An experimental study of speaker verification sensitivity to computer voice-altered imposters" in *Acoustics, speech, and signal processing* (Papers delivered at the IEEE International Conference on Acoustics, Speech, and Signal Processing, 1999 15-19 March 1999 IEEE Phoenix) 837-840 839-840.

82 See the discussion in Furui 1981 *IEEE Transactions on Accounts, Speech, and Signal Processing* 255-265.

83 For a discussion of this principle see Gaines R *et al* "Authentication by keystroke timing – some preliminary results" May 1980 http://www.rand.org/content/dam/rand/pubs/reports/2006/R2526.pdf (Date of use: 13 March 2015).

argued that the principle that 'it is not what you type which is important, but the manner in which you type it' is upheld.[84]

Keystroke dynamics is motivated by the view that each computer user of a system follows a characteristic trend or pattern when typing particulars on a computer keyboard.[85] In other words, users' keystrokes are distinct, consistent or indiscriminate, and they follow a particular timing.[86] Therefore, these keystrokes can be used to identify a user online. A number of factors are important to the making of this determination. These include the timing of the keystrokes, the intervals of the keystrokes, the placement of fingers on the keys, the pressure that is being applied to each key.[87] Generally, a three-stage approach is commonly followed in order to establish a system to identify users using keystrokes dynamic. Firstly, keystroke data may be embedded into a system (data enrolment process). In this instance, the timing, pattern and consistency of the key-press are registered into a system. Secondly, a system to classify the keystrokes dynamics (classifier) is created. Thirdly, the captured data is extracted from a system and compared with other identifying information whenever the e-authentication process is possible.

7.3.2 Summary

Prevention is generally indispensable to an ICT regulatory agenda. It particularly deters and forestalls a wrong. However, it is argued that prevention may not fully address some of the challenges posed by ICTs in certain circumstances. More specifically, the

---

84 Monrose F and Rubin AD "Keystroke dynamics as a biometric for authentication" 2000 (16) *Future Generation Computer Systems* 351-359 353. See also, Shanmugapriya N and Padmavathi G "A survey of biometric keystroke dynamics – approaches, security and challenges" 2009 (5) *International Journal of Computer Science and Information Security* 115-119 116.

85 Robinson JA *et al* "Computer user verification using login string keystroke dynamics" 1998 (28) *IEEE Transactions on Systems, Man, and Cybernetics* 236-241 236.

86 Cho S and Hwang S "Artificial rhythms and cues for keystroke dynamics based authentication" in Zhang D and Jain AK (eds) *International conference on biometrics, 2006* (Springer Berlin 2005) 626-635 627-628 and Cho S *et al* "Web-based keystroke dynamics identity verification using neutral network" 2000 (10) *Journal of Organisational Computing and Electronic Commerce* 295-307 297-298.

87 Saevanee H and Bhattarakosol P "Authenticating user using keystroke dynamics and finger pressure" in *Consumer communications and networking* (Papers delivered at the 2009 6th IEEE consumer communications and networking conference 11-13 January 2009 Institute of Electrical and Electronic Engineers New York 2009) 1-2 1-2.

measures may be designed in a manner that only addresses the existing threats to ICTs.

Given the aforementioned, PAEA is recommended. It accepts that the starting point for e-authentication should not be at a stage when an identity of a user is validated. Systems should be created that help in identifying certain behaviours or characteristics of a user prior to the identifying information being entered into a system. For purposes of this chapter, this process is called behavioural biometric. It relies on a number of methods or techniques. These include the signature dynamics, voice verification and keystroke dynamics.

7.6 CONCLUSION

In this chapter a precautionary approach to e-authentication is examined. This method is referred to PAEA. PAEA is founded on the principles that govern the exercise of precaution or what is termed the Precautionary Principle. Regulators are, according to the precautionary principle, required to take anticipatory action in order to prevent a risk to ICTs that will accrue in the future. It particularly warns against the postponement of action for reasons such as that the action is not supported by scientific evidence. Furthermore, the precautionary principle enjoins regulators to have prudence and foresight in the manner in which they plan and design regulations. This entails a management of past and present risks, and also breaking-down or blocking the flow of potential or future risks.[88] It also accepts that prevention, although essential to a technology regulatory structure, may produce problems for purposes of managing ICTs. For instance, regulators may, due to developments in ICTs, not be able to know which risks are imminent and which ones are not. Consequently, they may implement regulatory frameworks that address or deal only with the past or present risks. The result of this can then be a constant or continuous creation of rules which seeks to repair the shortcomings of previous regulations.

By reason of the above, PAEA is developed. It is based on the idea that a study of systems, the dynamics of systems and how systems are connected online is necessary for any technology regulation. In other words, technology regulations should be

---

[88] Tickner and Raffensperger *Handbook* 2.

designed in such a manner that they are bound to ICTs and are able to develop with it. In this chapter biometric dynamic is introduced as one of the means to respond to the aforementioned necessity. Biometrics dynamic requires an identification of certain user characteristics, for example signature recognition, voice verification, keystroke dynamics or computer mouse movements. The basis for introducing biometric dynamic is that a change or development in ICTs will almost always necessitate a relook of existing regulations that pertains to those technologies. In fact, it happens mostly that developments in ICTs also expose these technologies to harm or exploitation by criminals. An example of this is the combination or use of the Web and the Internet. However, it is argued that such a change does or will not require a modification of a user's biometric characters.

Given the need for PAEA, chapter 8 illustrates the general outlook of PAEA for regulatory purposes. It specifically exposes the fallacies in the current e-authentication approaches (United Kingdom, Canada and South Africa). Thereafter, it provides a framework within which e-authentication measures should be founded.

CHAPTER 8

PAEA – THE PROPOSED E-AUTHENTICATION APPROACH

CHAPTER 8

PAEA – THE PROPOSED E-AUTHENTICATION APPROACH

8.1 SUMMARY OF THE FINDINGS

In this research e-crimes are identified as one of the main barriers to the ICT regulatory agenda. Accordingly, a focus is made on e-crimes as a specific crime which is related to the traditional crimes of theft. Because e-crimes involve an appropriation of information, it is enquired whether information is property which is capable of being stolen. This then requires an investigation to be made of the law of property. The basis for this scrutiny is to establish if information is property for purposes of law. From this discussion, it is observed that the objects of rights do not always remain stationary. More specifically, rights in property vest in those things that a particular society during a specific period in the history of the law of property regards as worthy of being legally protected. This view was substantiated in chapter 2 above when a study of the Roman-Dutch law of property was made. For example, old Roman law recognised that ownership in property was only vested in corporeals. The latter view was discarded in pre-classical Roman law. Specifically, it was argued that both corporeal and incorporeal things were the object of rights, but not ownership. This view seemed to have been followed and developed by the jurists of the Roman law of property. In particular, a distinction was made in Dutch law between private and public rights.[1] Private rights were said to be vested in property. These relates to the right to use and enjoy property.

The notion of private rights forms the basis of the South African law of property. In South Africa, it is required that some form of legal relationship must exist between a person and a thing before an object can be regarded as property in law. This is to say that a person should, at least, have some form of a justified entitlement or interest (*res in* commercio) in the thing.[2] Following this, a case is made that the emergence of an information society makes real rights in information possible. This is the case because information is one of the essential assets of an information society. The importance of

---

1 Grotius H *De Jure Belli ac Pacis* (Clarendon Press London 1625) II.II.II.1.

2 Van der Walt AJ and Pienaar GJ *Introduction to the law of property* 6th ed (Juta & Co Claremont 2009) 13.

information is drawn not only on the fact that it mimics real property, but also on that users of this information expend time, effort and money in gathering it. Consequently, a reasonable expectation ensues that this information is or should be property for legal purposes.

Given the fact that property rights in information are possible, chapter 3 examined whether or not a *contrectatio* over information exist. In that chapter, the Roman-Dutch, English and South African law approaches to theft were examined. This examination revealed that the principles of theft are founded on a flexible system of legal rules. Society adapts and modifies these principles in such a manner that the current demands or challenges are met. For example, the Dutch law of theft deviated from the viewpoint that was held in classical and post-classical Roman law of theft that a physical *contrectatio* must result in a permanent deprivation of property. In particular, it was accepted in Dutch law that a temporary *contrectatio* is also possible. The latter view seems to have been followed in South Africa. In South Africa, the principles of theft have been modified. Specifically, it is contended that *contrectatio* is too rigid in dealing with the challenges that are inimical to a modern society. Accordingly, appropriation of property is accepted as the flexible alternative. Furthermore, it is acknowledged that theft does not always result in a permanent deprivation of property. There are incidents wherein the deprivation may be temporal or partial.

The development of the principles of theft supports the view that appropriation does not necessarily have to result in the owner being permanently deprived of property, for example information. Consequently, theft could still arise in situations where an owner has, consequent to his or her computer being cracked, been deprived of the control, use and enjoyment of the rights to his or her information. For this reason, the fact that only a copy of the information is available to or has been appropriated by a computer cracker does or should not make a difference.

Having accepted that information can be the object of theft, a study of the conventional risks that ICTs generate is made. Specifically, it is argued that there is a risk of ICTs being the object of e-crimes, in cases where a hardware or software is appropriated illegally, and there is a risk that ICTs may become a tool in order to appropriate

information unlawfully.[3] Accordingly, it is that argued e-crimes are pervasive. The scale and impact of these crimes far exceeds those of the offline crimes, for example theft or fraud. Sometimes, computer crackers collaborate with criminals in remote jurisdictions in order to frustrate the detection of e-crimes. The pervasive nature of these risks lies in the fact that they extend beyond borders and their future and impact is difficult to reasonably predict. In chapter 5 it is submitted that the scale of e-crimes is bound to continue if the so-called button-pushers or computer morons are involved in the ICT regulatory agenda. Because of this, it is inquired whether ICTs can be regulated. If so, how should an ICT regulatory framework be structured? It is submitted that ICTs are spheres where regulations apply. However, *better regulations* are appropriate in dealing with the dynamics of the technologies. This means that the regulatory industries, for example the state, businesses and computer users should be particularly involved in establishing ICT regulations. These regulations should generally understand the existing e-authentication measures. Furthermore, they should be modelled from the regulatory theories that are discussed in chapter 6 above. The theories include the codes-based theory, systems theory, AIS theory and the Good regulator Theorem. The rationale for all this is to establish a holistic approach to e-authentication. This approach has to be in keeping with the proposed *Precautionary Approach to E-Authentication* or *PAEA*.

8.2 THE PROPOSED PAEA

PAEA supplements the existing e-authentication measures. It uses the process of risk regulations as the yardstick upon which ICT regulations should be measured. It argues that because e-crimes generate risks to the information society regulators should then study these risks and design regulations that reasonably respond to these risks. In addition, ICT regulators should recognise that risks are uncertain and that their realm and latitude cannot be proved conclusively. Furthermore, ICT regulators should acknowledge that the existing e-authentication measures are not enough to alleviate the existing risks. This insufficiency exists whether or not biometric data is used as part of the e-authentication agenda. In one case, computer crackers can send emails to a

---

[3] Cassim F "Formulating specialised legislation to address the growing spectre of cybercrime – A comparative study" 2009 (12) *PER* 36-79 36.

number of targeted victims. These are emails which prompt or could prompt victims to follow a particular URL hyperlink. In those links victims may be requested to enter their e-authentication data or particulars (pins, username or password) in certain allocated spaces. As soon as they are entered, computer crackers will interrupt and block the online session, appropriate the particulars in order to use them for criminal purposes. In other cases, computer crackers can follow the steps that are shown in chapter 4, figure 4.4 in order to crack a system and appropriate sensitive information. In this instance, a victim or user could be directed to a replica (dummy) website where he or she may be asked to enter his or her particulars. This entering of particulars and his or her biometric data could then be studied and retrieved from there. Thereafter, the recorded particulars and data could be used in order to circumvent the e-authentication process. In particular, they may serve as a key in order to unlock a system or network for purposes of gaining authority to access it.

The manner in which regulators should apply PAEA is illustrated in the sections below. Firstly, the related aspects of the aforesaid approach are exemplified. These aspects are technology neutrality, good regulations, equity and the regulatory instruments. Secondly, the outlook of PAEA as a possible regulatory measure is discussed. This discussion continues from the premise that a framework to regulate ICTs and their associated risks should generally be risk-sensitive based. This process enjoins or should enjoin ICT regulators to examine the past and current forms of e-crimes while at the same forecasting the imminent trends that computer crackers are likely to follow in the future. Thirdly, a summary of the facts regarding the process of regulating by risk is made.

8.3 ASPECTS OF PAEA

8.3.1 Technology Neutrality

PAEA is founded on a technology-neutral or technology-independent regulatory framework. Accordingly, this structure accepts that e-authentication processes should generally be commenced from the computer user to the machine (computer or system) interface. Furthermore, it recognises that technologies evolve and that this evolution of change necessitates the creation of innovative forms of regulatory tools and, in technological terms, technological toolkits.

8.3.2 Good Regulations

The starting point towards the establishment of good or better regulatory frameworks is to accept that regulations as opposed to the law are better suited to regulate ICTs and the risks that ICTs generate. This does not then mean that the law becomes irrelevant for ICT regulatory purposes. More specifically, legal rules influence or may influence the structure of the good regulations. However, they do not determine the meaning and construction of good regulations.

Consequently, a regulatory framework which is abstracted from good regulations entails a shift or move from fewer or no regulation. It ensures that regulations are both effective and efficient.

8.3.3 Equity

Equity is here used in order to denote the principles such as good governance, accountability, fairness, openness, suitable expertise and efficiency.[4] This is the case because regulations or ICT regulatory frameworks should be appropriate and just. Accordingly, ICT regulators should adopt expediential ICT controlling measures. This has to be done in manner which recognises and is mindful of the exponential increases in the costs involved in regulating ICTs. Furthermore, it accepts that ICT regulations should general include a study of the technology and the systems or sub-systems that compose the technology.

8.3.4 Regulatory Instruments

PAEA accepts that different instruments are indispensable in order to commence a technology regulatory framework. They include legal rules, social norms, market and nature or architecture.[5] These apparatus are equal or function on an equal basis. Accordingly, their meaning and significance for technology controlling purposes should be evaluated by examining the contribution or influence of the different role-players

---

4 Baldwin R and Cave M *Understanding regulation: theory, strategy, and practice* (Oxford University Press Oxford 1999) 76.

5 Lessig "The law of the horse – what cyberlaw might teach" 1999 (113) *Harvard Law Review* 501-549 507.

(that is, the state or government, the regulated industries or firms and society)[6] in the overall regulatory agenda.

8.3.5 Summary

The aspects of PAEA are discussed above. The features serve as a guide to ICT regulators in establishing risk-sensitive based e-authentication measures. Accordingly, they are not intended to be exhaustive. Regulators may update or revises these aspects whenever possible.

The sections below discuss the proposed fundamentals to a precautionary approach to e-authentication. These are behavioural characterisation, risk control, education or awareness, and monitoring and evaluation. In this chapter, the essentials are investigated following a wide-ranging scrutiny of a system or process of risk regulation. It will be established that the notion of risk or risks dominates the study of the aforesaid system. This dominance exists because e-crimes are generally construed as the threat to the overall security of information systems or networks. Therefore, it is argued that a meaningful way to address the scourge of e-crimes should generally be risk-sensitive based.

8.4 PAEA REGULATORY OUTLOOK

8.4.1 Background

A process of risk regulation or regulation by risks is proposed a one of the measures to control ICTs and to curb e-crimes. In chapter 7 this process was discussed as part of the precautionary approach. It is conceded that an approach to regulation by risk is generally not foreign to South Africa. Ordinarily, it is accepted that circumstances may arise wherein it may be necessary to introduce regulations that manage a threat which may or is likely to occur in the future. These regulations are not necessarily founded on a clear scientific assurance that risks will ensue. However, they are based on the fact that under normal circumstances risks occur or ordinarily occur if regulations are withheld or suspended. The controlling exercise in terms of the Financial Intelligence

---

[6] Hereinafter referred to as the ‘regulatory industries’.

Centre Act[7] can be used as an illustration for process of risk regulation. In terms of this Act, certain institutions, that is, accountable institutions,[8] must perform certain functions.[9] These tasks are enumerated in chapter 3 of FICA. They are: a duty to identify clients;[10] duty to keep records;[11] reporting duties and access to information;[12] measures to promote compliance by accountable institutions,[13] and referral and supervision.[14] For example, section 21 of FICA requires accountable institutions to identify and verify the personal particulars of a person.[15] These persons are referred to as those who are about to establish or have established a business relationship[16] or about to conclude or have concluded a single transaction[17] with an accountable institution.[18] Furthermore, the particulars to be identified and verified can be a person's full names; date of birth; identity numbers; income tax registration numbers (if issued), and residential addresses.[19] The functions as stated above are performed or they should be carried out in anticipation of an indeterminate threat or risk to an accountable

---

7 See the Financial Intelligence Centre Act 38 of 2001 (hereinafter referred to as FICA).

8 Accountable institutions are the institutions that are listed in Schedule 1 of FICA. See, s 1 of FICA. The list include, attorneys, board of executors, estate agents, financial instrument traders, management companies, persons who carry on the business of banks, mutual banks, persons who carry on long-term insurance businesses, persons who carry on business in respect of which gambling licences are required to be issued by a provincial licencing body, persons who carry on businesses of dealing in foreign exchange, persons who carry on the business of lending money against the security of securities, persons who carry on the businesses of rendering investment advices or investment broking services, persons who issue, sell or redeem travellers' cheques, money orders or similar instruments, Postbanks, members of a stock exchange, the Ithala Development Finance Corporation Limited, persons who have been approved or fall within a category of persons approved by the Registrar of Stock Exchanges, persons who have been approved or fall within a category of persons approved by the Registrar of Financial Markets and persons who carry on business of a money remitter. See Schedule 1 of FICA.

9 S 21 of FICA.

10 Part 1 of Chapter 3 of FICA.

11 Part 2 of Chapter 3 of FICA.

12 Part 3 of Chapter 3 of FICA.

13 Part 4 of Chapter 3 of FICA.

14 Part 5 of Chapter 3 of FICA.

15 S 21 of FICA.

16 In terms of section 1 of FICA, a business relationship amounts to an arrangement between a client (person) and an accountable institution for the purpose of concluding transactions on a regular basis.

17 A single transaction is a transaction other than a transaction which is concluded in the course of a business relationship. See s 1 of FICA.

18 S 21(1) and (2) of FICA.

19 Reg 3(1)(a)-(e) of the exemptions in terms of the Financial Intelligence Centre Act 38 of 2001 (GN R1596 *GG* 24176 of 20 December 2002).

institution's integrity. Within the context of FICA, money laundering[20] and terrorism are identified as some of these risks.[21]

Having examined the structure to regulate ICTs in South Africa, it does not appear the essence of risk regulation is sufficiently captured. The ECT Act simply states that a method which is intended to regulate or control ICTs for example, the e-authentication process should be technologically neutral.[22] It should be safe, secure and effective. Most importantly, it should be responsive to the needs of computer users. Following this, it is then postulated that the e-authentication structures that are modelled from sections 37 and 38 of the ECT Act fully respond and address this technology neutrality.[23]

Given the above-mentioned, it is submitted that the structure to regulate ICTs in South Africa is only founded on an inflexible framework which promotes the re-invention of the ICT regulatory wheel. One of the examples of the re-invention of the ICT regulator wheel is demonstrated in the proposed Draft Cybercrime and Cybersecurity Bill of 2015.[24] The CaC Bill is an attempt to address some of the shortcomings of the ECT Act, especially those relating to e-crimes.[25] By so doing, it lists a multitude of activities and defines these as e-crimes.[26] The list of e-crimes in the CaC Bill is so long that it contributes to the danger that Von Bertalanffy warned ICT regulators that they should guard against.[27] This is the danger of becoming a computer moron, button-pusher or learned idiot. The aforementioned danger manifests itself in situations where regulators simply concern themselves with the immediate or existing risks. In this respect, they fail

---

20 For a definition of the crime of money laundering see s 1 of FICA. See also, Njotini M "The transaction or activity monitoring process: an analysis of the customer due diligence (CDD) systems of the United Kingdom and South Africa" 2010 (31) *Obiter* 556-573 558-559.

21 The crime of terrorism and related activities is defined in section 4 of the Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004. See also *Shaaban Bin Hussein v Chonk Fook Kam* [1969] 3 All ER 1626 1631, *Powell v van der Merwe* [2005] 1 All SA 149 (SCA) 162 [37] and Proc R309 *GG* 30873 of 14 March 2008.

22 See 2(f) of the ECT Act.

23 S 2(k) of the ECT Act.

24 Hereinafter referred to as the CaC Bill.

25 See Preamble to the CaC Bill.

26 Chapter 2 of the CaC Bill.

27 Von Bertalanffy L *General system theory: foundations, development, applications* (George Braziller Inc. New York 1968) 10.

to contribute anything to ICT regulation and the control of the imminent challenges that are posed by contemporary technologies.[28] Instead, they adopt methods that are suited to regulate offline occurrences and hope that those methods will function well in controlling online phenomenon, for example e-crimes. Immediately when technologies innovate, these button-pushers re-thing their strategy and introduce legal rules that address existing challenges.

8.4.2 Behavioural Characterisation

It has already been illustrated in the previous chapters that behavioural characterisation supports a precautionary approach to e-authentication. The justification for this view was discussed in chapter 7 of this research. It was submitted that although PAEA relies on biometric data which is relevant to the e-authentication process, it differs from the latter in number of respects. For example, biometric data is used as part or as an aspect of the e-authentication process. In particular, it supports the third pillar of e-authentication, which is proof by property. From this, biometrics data is e-authentication itself. However, biometric characterisation follows or is modelled from risk control or analysis. It requires a scientific examination of the risks and the evaluation of the potential scale of the consequences of those risks. It accepts that because characters for example keystrokes or e-signatures are developed by or for ICTs, then they can assist in the e-authentication process. In cases where these characters are used in e-authentication frameworks, it does not, in turn, mean that the manner of operation of the technologies which developed these characters will have to be modified or altered. Simply put, the effectiveness of the characters in e-authentication schemes is not affected by peripheral innovations in recent technologies. By the same token, a change or development in ICTs does or will not essentially imply a modification of the biometric characters.

Having exemplified the above-mentioned, it may then be asked: what this means for ICT regulatory purposes? The answer to this is simple. Biometric characters do not replace the identification particulars. They merely supplement and amplify existing e-authentication structures. Pins, usernames, passwords and even biometric data, are

---

[28] Von Bertalanffy *Foundations* 10.

still essential to the e-authentication agenda. Accordingly, ICT regulators should apply these characters in order to complement the authentication of computer users or the particulars of computer users online. For example, a scenario or situation should be created where a user (*U*) subjects or will present himself or herself to a system (*Ts*). The *Ts* should be equipped with a number of technological applications or devices. These may a digitiser which is able to transform physical gestures into digital signals, camera or scanner. These signals, camera and scanner should capture or ought to be capable of capturing the image of *U*. Furthermore, a digitiser could be any online monitoring device which identifies the patterns of *U*'s behaviour or activities online for example, keystrokes.

In the case where signals, camera and scanner are used in e-authentication schemes, *Ts* should be able to identify *U*'s signature. The signature ought to then be changed into computer data and thereafter be securely stored in the computer server (*S*). Furthermore, in circumstances where a voice is e-authenticated, then the manner and sequence of the speech (*Seq*) can or should be detected. Seq^1, Seq^2, Seq^3, etc. may consequently be used and computed in order to demonstrate the similarities or differences in the sound, loudness or a pitch of a voice. Lastly, in the case of keystrokes, the system should identify the timing of a keystroke (*kst*). These can be the key-presses and key-releases. The measurements that ought to be used include kst^1, kst^2, kst^3, etc. The number of *Es* in or between every *kst* should also be recorded, if there are any.

8.4.3 Risk Control

Risk control was introduced in chapter 7 of this research. It was submitted that the control of risks, in this case, e-crimes, is essential to the idea of a precautionary approach to e-authentication. This introduction does not imply that PAEA is not without its own limitations.[29] This view is based on the fact that only an *all or nothing approach* to regulation could generate absolute regulatory frameworks. Within the context of regulating ICTs, this could mean a scenario where ICTs are used only for the purpose

---

[29] See Jablonowski M *Precautionary risk management: dealing with catastrophic loss potentials in business, the community and society* (Palgrave Macmillan New York 2006) 25.

for which they were designed (this then excludes them being exploited by computer crackers) or to, given the vastness and perverse nature of e-crimes, encourage the regulatory industries to discontinue the use of the recent forms of technologies.

The object of risk control, and ultimately PAEA, is to establish a framework in terms of which a balance is struck or sought to be struck between the detriments that are created by e-crimes and the benefits that recent technologies generate. The latter amounts to a process and requires an identification of past, present and forthcoming risks. Risk control has to be carried out at a particular level.[30] This is referred to as a level (which) is suitable for analysis. The ultimate goal thereof is to measure and moderate the risks. The success of the measuring and mitigating process depends on the complexity of the detail in identifying the risks. However, it should be remembered that certain risks are more perverse and complicated than others. This is especially so given the constant developments in modern technologies. Therefore, it may be difficult and, sometimes, impossible to forecast future or upcoming risks.

8.4.4 Education or Awareness

In this research the necessity for education or awareness was initially acknowledged in chapter 1. In that chapter it was argued that education and awareness are some of the indispensable measures to prevent e-crimes. The aforementioned importance was also reiterated in chapter 7 where an investigation of the precautionary principle was made. In this chapter education and awareness are examined as a precautionary measure against e-crimes. They are ordinarily carried out by instituting programs (awareness programs) that are aimed at informing, teaching or alerting the regulatory industries about certain uncertain or indeterminate risks. Information is consequently disseminated which identifies these potential threats. From this information, the industries remain acquainted and cautious of the possible threats to their sensitive information. They then establish programs (security education, training and awareness

---

30 Hopkinson M *The project risk maturity model: measuring and improving risk management capability* (Gower Publishing Surrey 2011) 113.

programs) that are designed to enhance their existing ICT infrastructure.[31] This can be done in the following manner:

> Improving awareness of the need to protect system resources, developing skills and knowledge so (that) computer users can perform their jobs more securely and building in-depth knowledge, as needed, to design, implement, or operate security programs for organisations and systems.[32]

However, it is argued that foresight in identifying risks is not a factor in the current education and awareness programmes. Firstly, these programmes inform the public about the risks that have already been identified. By so doing, they ignore the fact that a change in ICTs usually translate to a change in the techniques that are used to commit e-crimes. Secondly, the programmes are meaningless if they are not acted upon. Ignorance and lack of practical skills to effect action can be identified as the factors that contribute to this insignificance. Therefore, PAEA argues that e-crimes (would) flourish in environments where both the institutions that are charged with or responsible for creating the awareness or education and the users who should act on it (awareness) fail to take measures to alleviate the risks of e-crimes. Therefore, it is necessary for the industries to take ownership and control of the structures that are designed for awareness and education.

8.4.5 Monitoring and Evaluation

Risk monitoring and evaluation has to be understood against the background of chapter 5 above. Chapter 5 promotes or seeks to promote a holistic approach to ICT regulation. It does not embody a top-down or aggregation valuation[33] (where the state or government champions regulations) nor does this encourage a bottom-up or disaggregation approximation[34] (where regulatory industries determine regulations) regulatory agenda. However, it is a structure which recognises that all the affected

---

31 Whitman ME and Mattord HJ *Principles of information security* 4th ed (Cengage Learning Australia 2012) 203.
32 Whitman and Mattord *Principles of information security* 203.
33 Michaels JV *Technical risk management* (Prentice Hall New Jersey 1996) 287-288.
34 Michaels *Technical* 289-292.

industries (the state, regulated industries and computer users) can produce better or good ICT regulations. This amounts to what is referred to as co-regulations. Furthermore, it ensures that the industries are continuously aware and remain vigilant over the state of the ICT environment.

Risk monitoring and evaluation denotes risk analysis. Risk analysis encompasses three aspects. These are risk assessment, risk management and risk communication.[35] Thus, it requires a study to be made of the context of the risks, the source of the risks and the consequences that the risks may have to the affected industries. It does not necessarily amount to the control of all the risks. Generally, it has to be remembered that not all the risks are worthy of being controlled. Certain risks are so insignificant and meaningless that the taking of the measures to control and manage them would be a total waste of time and resources.[36] Therefore, it has to be investigated whether a risk is acceptable or not,[37] or is so unsafe that it merits some action.[38] The *de minimis non curat lex* rule can be used as a guide when analysing the risks. This rule states that the law does not concern itself with trifles. What this entails for ICT regulatory purposes is that the risks and the degree of the risks should be segregated. Risk matrixes (or Probability-Impact-Matrix or PIM) could be used in order to assist in making this separation. Thereafter, the risks that can be established in real time (foreseen or foreseeable risks) may be separated from unforeseen or unforeseeable risks. This could be done by studying contemporary risks and thus observing their long-run comparative regularity or predictabilities.

Because ICT regulations are a product of this proposed all-inclusive approach, the regulated or affected industries should assume the role of the enforcers of these regulations. Accordingly, they have to determine the future that ICTs have to the

---

35 See Button C *The power to protect: trade, health and uncertainty in the WTO* (Hart Publishing Oxford 2004) 95. Fisher adds a fourth element to risk analysis. This, he says, is the 'cost-effective analysis'. See Fisher RP *Information systems security* (Prentice-Hall New Jersey 1984) 80.

36 See *S v Kgogong* 1980 (3) SA 600 (A), *S v Nedzamba* 1993 1 SACR 673 (V) and *R v Dane* 1957 2 SA 472 (N).

37 See Douglas M *Risk acceptability according to the social sciences* (Routledge London 1985).

38 See Rayner S and Cantor R "How fair is safe enough? – the cultural approach to societal technology choice" 1987 (7) *Risk Analysis* 3-9.

information society; the effect that ICTs are likely to have to the information society; the structure to be followed in controlling that envisaged effect; and the consequences that a change in ICTs is likely have to the computer users, businesses and governments. Furthermore, the industries must effect a change in ICT regulations whenever possible. This means that they should seek to establish and maintain an effective ICT regulatory framework, and take measures to preserve and protect the integrity and stability of information systems in South Africa.

8.4.6 Summary

A structure to e-authenticate a computer user or the particulars of a computer user is not fully or sufficiently addressed in South Africa. Despite the acceptance of the precautionary measures in other cases (for example, those relating to anti-money laundering or anti-terrorism), the ECT Act seems to ignore the importance of risk regulations. Furthermore, it is not clear from the ECT Act whether or not the exercise of precaution in e-authentication schemes could be delegated to the proposed ICT regulatory industries. In this chapter, behavioural characterisation, risk control, education or awareness and monitoring and evaluation assists in rectifying the aforementioned vacuum in the ECT Act. Firstly, behavioural characterisation signifies a move beyond the use of biometric data. It accepts that identifying particulars and biometric data are essential to the e-authentication agenda. However, it recognises that the particulars and data can be or are more effective if they are used as part of PAEA as opposed to them as e-authentication themselves. Secondly, risk control does not imply an all or nothing ICT regulatory structure. It only necessitates that past, present and future risks should be identified.

Thirdly, education or awareness are measures that are aimed at teaching and alerting the regulatory industries about e-crimes and the consequences that e-crimes have or can have to their information. Therefore, the regulatory industries ought to take ownership of the initiatives created for this purpose. Fourthly, monitoring and evaluation amount to risk analysis. It acknowledges that some risks of are perverse whereas others are not. Therefore, the nature, context and foreseen or foreseeable consequences of the risks should be examined. The basis for this is to enable the regulatory industries to separate significant from insignificant risks. Accordingly, they can use the *de minimis non curat lex* rule as a guide.

Figure 8.1 below contains a summary of the proposed precautionary approach to e-authentication. This summary demonstrates the meaning of the aforementioned approach for ICT regulatory purposes. It also evidences the element and the effectiveness of PAEA.

Proposed PAEA	**Meaning**	**Essential Elements**	**Effectiveness**
Behavioural Characterisation	- Relates to the examination of the behavioural characters of user - Relies on proof by property (biometric data) - Fosters existing e-authentication measures - Biometric data supplements identifying particulars (ID, username and password) - Modelled from risk control	- Biometric data - Keystroke dynamics and e-signatures - System and system dynamics - Technological applications or devices	- Technologically neutral - Available to use - It is attached to the technology - It develops with innovations in ICTs - It not affected by external developments in technology - It can be operated at a user-to-machine
Risk Control	- Relates to the management of risks - It seeks to balance the risks and the benefits - Recognises that risks should be segregated – certain risks are high as opposed to others.	- Builds on behavioural characterisation - Supports precautionary approach to risk regulation - Good regulations	- Technologically neutral - Founded on the principle for good regulations - Legal rules influence and not determine the structure of ICT regulations - Risk evaluation - ICT regulations to be commensurate to the risks
Education or Awareness	- Conducting awareness programmes - Disseminate information to designated groups / industries - Identify current and future risks	- Foresight in risks identification - Ensure that there is response following the programmes - Devise measures to curtail current, future, certain and uncertain risks - Be responsive to the programmes	- The programmes are fairly and equitable communicated to the identified industries - Records are kept and stored - Improve areas where risks are uncertain
Monitoring and Evaluation	- It involves risk analysis - The context of the risks is investigated - The source of the risks is determined - The potential consequences that the risks could cause to a system are analysed - No amount of work should be expended on insignificant risks - Resort to the creation of a risk matrix in order to determine the scale of the risk	- Risk assessment - Risk management - Risk communication - Risk matrixes to be used	- Holistic approach to risk identification - Promotes an all-inclusive ICT regulatory agenda - It is referred to as co-regulation - Industries communicate and seek to find solutions

Figure 8.1: Summary of the proposed precautionary approach to e-authentication

8.5 CONCLUSION

In this chapter a precautionary approach to e-authentication is discussed. This method is referred to as PAEA. PAEA argues that a suitable method of regulating technologies

should not only be drawn from legal rules. Flexible regulations could provide a suitable framework within which ICTs and their accompanying risks are controlled. Furthermore, it accepts that the state is or ought not to be a single role-player in ICT regulations.[39] Social norms, market and nature or architecture are also important in this regard.[40] A number of aspects are discussed which determine the meaning and structure of the proposed precautionary approach to e-authentication. These include technology neutrality or independence, good or better regulations, equity and a system of regulatory instruments.

The effectiveness of PAEA is evaluated by examining the existing structures to e-authentication. The United Kingdom, Canada and South African arrangements to e-authentication provide a lead. It is established that the structure for risk regulation or regulation by risk is encouraged by the United Kingdom and Canada e-authentication measures. This structure is discussed fully and elaborated. However, South Africa omits to provide measures dealing with a precautionary approach to e-authentication. In particular, there is no mention being made of PAEA in sections 37 and 38 of the ECT Act. Although the Cybersecurity Policy refers to a process of risk management, it is argued that this process is not comparable to PAEA. Even if the opposite is true, the Cybersecurity Policy, in any event, fails to provide substance to the proposed risk management process. Consequently, the challenges that are created by e-crimes remain as they were despite the provisions of the Cybersecurity Policy. Lastly, it is argued that the outlook of PAEA for ICT regulatory purposes should be influenced by, at least, four fundamentals. These are behavioural characterisation, risk control, education or awareness and monitoring and evaluation.

---

39 Lessig 1999 *Harvard Law Review* 507.

40 Lessig 1999 *Harvard Law Review* 507.

BIBLIOGRAPHY, TABLE OF STATUTES, TABLE OF CASES, INTERNATIONAL CONVENTIONS OR DIRECTIVES AND LIST OF ABBREVIATIONS

BIBLIOGRAPHY

1. BOOKS

A

Adeley G, Acquah-Dadzie K, Sienkewicz TJ and McDonough JT *World dictionary of foreign expressions: a resource for readers and writers* (Bolchazy-Carducci Publishers Wauconda 1999)

Anders PC and Ellson SE *The criminal law of South Africa* (Hortor Johannesburg 1917) 264-265

Anderson P *Passages from antiquity to feudalism* (Verso London 1974)

Angelus Carletus de Clavasio *Summa angelica* (1488)

Anson S, Bunting S, Johnson R and Pearson S *Mastering windows networks forensics and investigation* (John Wiley Indianapolis 2012)

Aquinas *Summa theologiae* 66.9.1.

Ardy JT and Walker B *The commentaries of Gaius and Rules of Ulpian* 3rd ed (The Law Book Exchange New Jersey 2005)

Atapattu SA *Emerging principles of international environmental law* (Transnational Publishers New York 2006)

Aulus Gellius, *Noctes atticae* 11.18.20.22.23

Austin G *Shaping church law around the year 1000: the Decretum of Burchard of Worms* (Ashgate Publishing Surrey 2009)

Austin J *Lectures on jurisprudence or the philosophy of positive law* (Spottiswoode London 1879)

B

Badenhorst PJ, Pienaar JM and Mostert H *Silberberg and Schoeman's the law of property* 5th ed (LexisNexis Durban 2006)

Baldwin R and Cave M *Understanding regulation: theory, strategy, and practice* (Oxford University Press Oxford 1999)

Barlow S, King LC and King AG *Wills, administration and taxation: a practical guide* 8th ed (Sweet Maxwell London 2003)

Bartolus ad D 51.2.17.1.

Bennet RF *Electronic authentication and digital signature: hearing before the Subcommittee on Financial Services and Technology of the Committee on Banking, Housing, and Urban Affairs United States* (US Government Printing Office Washington 1998)

Bentham J *Of the limits of the penal branch of jurisprudence* (Clarendon Press Oxford 2010)

Berger JO *Statistical decision theory and the Bayesian analysis* 2nd ed (Springer New York 1985)

Berman HJ *Law and revolution - the formation of the Western legal tradition* (Harvard University Press Cambridge 1983)

Best RB *Identity theft: a legal research guide* (Buffalo New York 2004)

Biegel S *Beyond our control?: confronting the limits of our legal systems in the age of cyberspace* (The MIT Press Cambridge 2003)

Biegelman MT *Identity theft handbook: detection, prevention, and security* (John Wiley New Jersey 2009)

Birke L *Feminism and the biological body* (Edinburgh University Press Edinburgh 1999)

Black J *Critical reflections on regulation* (Centre for Analysis of Risk and Regulation London 2002)

Blackstone W *Commentaries on laws of England* 18th ed (Sweet Maxwell London 1836)

Blackstone W *Commentaries on the laws of England: a facsimile of the first edition of 1765-1769* (The University of Chicago Press London 1972)

Blackstone W *Commentaries on the laws of England: in four books; with an analysis of the work, by Sir William Blackstone, KNT, one of the Justices of the Court of Common Pleas* 18th ed (Sweet and Maxell London 1829)

Blond NC *Evidence* (Aspen Publishers 2009)

Boczek BA *International law: a dictionary* (Scarecrow Press Maryland 2005)

Bonnici JPM *Self-regulation in cyberspace* (TMC Asser Press The Hague 2008)

Boyd DR *The environmental rights revolution: a global study of constitutions, human rights and the environment* (UBC Press Vancouver 2012)

Bracton H *On the laws and customs of England* (Harvard University Press Cambridge 1968)

Brett AS *Liberty, right and nature: individual rights in later scholastic thought* (Cambridge University Press Cambridge 1997)

Brissaud J *A History of French public law* (as translated by Garner JW) (Augustus M. Kelly Publishers New York 1969)

Brody DC and Acker JR *Criminal law* 2nd ed (Aspen Publishers Gaithersburg 2001)

Brown BC *How to stop e-Mail spam, spyware, malware, computer viruses and hackers from running your computer or network: the complete guide for your home and work* (Atlantic Publishing Group Florida 2011)

Bryant BH and Krause MS *John* (College Press Publishing Missouri 1998)

Buckland WW *A textbook of Roman law: from Augustus to Justinian* 3rd ed (Cambridge University Press Cambridge 1963)

Buckland WW *The main institutions of Roman private law* (Cambridge University Press 1931)

Buckland WW *The Roman law of slavery: the condition of the slave in private law from Augustus to Justinian* (Cambridge University Press Cambridge 2010)

Burchell J and Milton J *Principles of criminal law* 2nd ed (Juta Kenwyn 1997)

Burchell J and Milton J *Principles of criminal law* 3rd ed (Juta & Co Lansdowne 2005)

Burchell J and Milton J *Principles of criminal law* 3rd ed (Juta Lansdowne 2005)

Burdick WL *The principles of Roman law and their relation to modern law* (The Lawbook Exchange New Jersey 2004)

Burnett M and Kleiman D (eds) *Perfect passwords: selection, protection, authentication* (Syngress Publishing Massachusetts 2006)

Button C *The power to protect: trade, health and uncertainty in the WTO* (Hart Publishing Oxford 2004)

C

Calisse C *A history of Italian law* (Augustus M. Kelly Publishers New York 1969)

Camp LJ *The economics of identity theft: avoidance, causes and possible cures* (Springer Bloomington 2007)

Cane P *The anatomy of tort law* (Hart Publishing Oxford 1997)

Castells M *The internet galaxy: reflections on the internet, business, and society* (Oxford University Press Oxford 2001)

Castronova E *Synthetic worlds: the business and culture of online games* (University of Chicago Press Chicago 2005)

Chesterton GK *Eugenics and other evils* (Cassell and Company London 1922)

Ciampa M *Security awareness: applying practical security in your world* 4th ed (Cengage Learning Asia 2014)

Cohen D *Münchener Beiträge zur Papyrusforschung Heft 74: Theft in Athenian Law* (C.H. Beck'sche Verlagsbuchhandlung München 1983)

Cohen D *Theft in Athenian law* (C.H. Beck'sche Verlagsbuchhandlung Müchen 1983)

Collins JM *Preventing identity theft in your business* (John Wiley New Jersey 2005)

Colquhoun PMC *A summary of the Roman civil law, illustrated by commentaries on and parallels for the Mosaic, Canon, Mohammedan, English and Foreign law* (William Benning London 1860)

Corbett D *Australian public sector management* 2nd ed (Allen & Unwin Pty Ltd St. Leonards 1996)

Cox R *Environmental communication and the public sphere* 3rd ed (Sage Publications Los Angeles 2013)

D

Davies W and Fouracre P (eds) *Property and power in the early middle ages* (Cambridge University Press Cambridge 1995)

De Revigny J *Lectura supra Codice* on C 4.65.5.

De Waal MJ and Schoeman-Malan MC *Law of succession* 4th ed (Juta Cape Town 2008)

De Zulueta F *The Institutes of Gaius: part ii commentary* (Oxford University Press London 1953)

Declareuil J *Rome the law-giver* (Greenwood Press Westport 1927)

Decock W *Theologians and Contract Law: The Moral Transformation of the Ius Commune (ca. 1500-1650)* (Koninklijke Brill Leiden 2013)

Descheemaeker E *The division of wrongs: a historical comparative study* (Oxford University Press Oxford 2009)

Diamond AS *Primitive law, past and present* (Routledge London 1971)

Digest

Douglas M *Risk acceptability according to the social sciences* (Routledge London 1985)

Dressler J *Understanding criminal law* 3rd ed (Lexis Publications New York 2001)

Drew KF *The laws of the Salian Franks* (University of Pennsylvania Press Philadelphia 1991)

Du Plessis JP *Barkowski's textbook on Roman law* 4th ed (Oxford University Press Oxford 2010)

Du Plessis P *Borkowski's textbook on Roman law* 5th ed (Oxford University Press Oxford 2015)

Dubrawsky I *How to cheat at securing your network* (Syngress Publishing Burlington 2007)

Dunham K (ed) *Mobile malware attacks and defence* (Syngress Publishing Inc Burlington 2009)

Durrani S *Information and liberation: writings on the politics of information and librarianship* (Library Juice Press Duluth 2008)

E

Elkin-Koren N and Salzberger EM *Law, economics and cyberspace: the effects of cyberspace on the economic analysis of law* (Edward Elgar Cheltenham 2004)

Emery JC *Management information systems: the critical strategic resource* (Oxford University Press Oxford 1987)

Erlank W *Property in virtual worlds* (LLD Thesis Stellenbosch University 2012)

F

Fisher RP *Information systems security* (Prentice-Hall New Jersey 1984)

Fletcher GP *Rethinking criminal law* (Little, Brown Boston 1978)

Forst ML *Cybercrime: Appellate court interpretations* (Montclair Enterprises San Francisco 1999)

Franklin CJ *The investigator's guide to computer crime* (Charles C Thomas Publisher Ltd Illinois 2006)

Frier BW and McGinn TAJ *A casebook on Roman family law* (Oxford University Press Oxford 2004)

G

Ganshof FL *Feudalism* (as translated by Grierson P) (Medieval Academy of America New York 1996)

Gardiner FG *Gardiner and Lansdown: South African criminal law and procedure* 6th ed (Juta Cape Town 1957)

Garner BA *Garner's dictionary of legal usage* 3rd ed (Oxford University Press Oxford 2011)

Garnsey P *Thinking about property: from Antiquity to the Age of Revolution* (Cambridge University Press Cambridge 2007)

Gatian *Decretum magistri Gratiani* 2.37.2.

Gattiker UE *The information security dictionary: defining the terms that define security for e-business, internet, information and wireless technology* (Kluwer Academic Publishers New York 2004)

Genesis 27

Glanville W *Textbook of Criminal Law* 2nd ed (Stevens & Sons London 1983)

Goddu A *Copernicus and the Aristotelian tradition: education, reading, and philosophy in Copernicus's path to Heliocentrism* (Koninklijke Brill Leiden 2010)

Gordley J *The Jurists: a critical history* (Oxford University Press Oxford 2013)

Grabosky PN and Smith RG *Crime in the digital age: controlling telecommunications and cyberspace illegalities* (Transaction Publishers New Jersey 1998)

Graham J, Howard R and Olson R (eds) *Cyber security essentials* (Auerbach Publishers Florida 2011)

Green DH *Language and history in the early Germanic world* (Cambridge University Press New York 1998)

Griew E *The theft acts* 7th ed (Sweet Maxwell London 1995)

Grossi P *A history of European law* (Blackwell Publishing West Sussex 2010)

Grotius, *De Jure Belli ac Pacis* (Clarendon Press 1625)

Guillaume HM and Posthumus M *Hugo Grotius: meletius, sive de IIS quae inter Christianos conveniunt epistola* (E.J. Brill Leiden 1988)

Gupta MS *Cyber crimes* (Centrum Press New Delhi 2013)

H

Hahlo HR and Kahn E *The union of South Africa: the development of its laws and constitution* (Juta London 1960)

Hall DE *Criminal law and procedure* 6th ed (Delmar Cengage Learning New York 2012)

Hall J *Theft, law and society* 2nd ed (Bobbs-Merrill Indianapolis 1952)

Harris EM *The rule of law in action in democratic Athens* (Oxford University Press Oxford 2013)

Hebbert C *The introduction to Dutch jurisprudence of Hugo Grotius* (John van Voorst London 1945)

Hoffman SK and McGinley TG *Identity theft* (Greenwood Publishing Group 2010)

Holmes OW *The common law* (The Lawbook Exchange New Jersey 2005)

Honoré T *Justinian's digest: character and compilation* (Oxford University Press Oxford 2010)

Hood CC and Margetts HZ *The tools of government in the digital age* (Palgrave MacMillan New York 2007)

Hopkinson M *The project risk maturity model: measuring and improving risk management capability* (Gower Publishing Surrey 2011)

Hosten WJ, Edwards AB, Bosman F and Church J *Introduction to South African law and legal theory* 2nd ed (Butterworths Publishers Durban 1997)

House of Commons Regulatory Reform Committee *Getting results: the better regulation executive and the impact of the regulatory reform agenda* (The Stationery Office Limited London)

Howes RB and Davis RPB *The elements of Roman law: being selections from the Institutes of Justinian, with explanatory notes, for the use of students* (Juta Cape Town 1923)

Huard RL *Plato's political philosophy: the cave* (Algora Publishing New York 2007)

Hübner R *A history of Germanic private law* (Augustus M Kelly Publishers New York 1968)

Hüebner R *A history of Germanic private law* (The Lawbook Exchange New Jersey 2000)

Hull E *The institution and abuse of ecclesiastical property* (T. Cadell, Strand London 1831)

I

Ignatieff M and Hont I (eds) *Wealth and virtue: the shaping of political economy in the Scottish enlightenment* (Cambridge University Press Cambridge 1983)

Institutes of Gaius

Institutes of Justinian

J

Jablonowski M *Precautionary risk management: dealing with catastrophic loss potentials in business, the community and society* (Palgrave Macmillan New York 2006

James L *Phishing exposed* (Syngress Publishing Rockland 2005)

Janczewski LJ and Colarik AM *Cyber warfare and cyber terrorism* (Information Science Reference London 2008)

Jang M *Linux patch management: keeping Linux systems up to date* (Pearson Education Inc. New Jersey 2006)

Jasper MC *Identity theft and how to protect yourself* 2nd ed (Oceana Oxford 2006)

Johnson D *Roman law in context* (Cambridge University Press Cambridge 1999)

Johnson Jr. BL and Kruse SD *Decision making for educational leaders: underexamined dimensions and issues* (State University of New York Press New York 2009)

Jolowicz HF and Nicholas B *Historical introduction to the study of Roman law* 3rd ed (Cambridge University Press Cambridge 1972)

Jolowicz HF *Digest XLVII.2 De furtis* (Cambridge University Press Cambridge 1940)

K

Kaken H *Information and self-organisation: a macroscopic approach to complex systems* 3rd ed (Springer Berlin 2006)

Kant I *Critique of pure reason* as translated by Müller FM *Immanuel Kant's critique of pure reason* (The MacMillan Company London 1922)

Kapoor N *Computerised banking system in India* 1st ed (Sublime Jaipur 2008)

Kaser M *Roman private law* (translated by Dannenbring R) (University of South Africa Pretoria 1980)

Kaser M *Roman private law* (translated by Dannenbring R) 2nd ed (Butterworths Durban 1968)

Keenan D *Smith and Keenan's English law* 8th ed (Pitman Publishing Ltd London 1986)

Kerridge R and Brierley AHR *Parry and Kerridge: the law of succession* 12th ed (Sweet Maxwell London 2009)

Kidder DS and Oppenheim NO *The intellectual devotional: American history* (TID Volumes New York 2007)

Kiralfy AKR *Potters historical introduction to English law and its institutions* 4th ed (Sweet Maxwell London 1962)

Klotter JC *Criminal evidence* 5th ed (Anderson Publishing Ohio 1992)

Knittel J Soto M *Everything you need to know about the dangers of hacking* (The Rosen Publishing Group New York 2003)

Korkunov NM and Hastings WG *General theory of law* (The Boston Book Company Washington 1909)

Kruger H and Skelton A (eds) *The law of persons* (Oxford University Press Southern Africa Cape Town 2010)

L

Laborde CM *Electronic signatures in international contracts* (Internationaler Verlag der Wissenschaften Frankfurt 2010)

Lafargue P *The evolution of property from savagery to civilisation* (New Parks London 1975)

Larson M, Liu C and Allen R *Mastering the domain name system: DNS on windows server 2003* (O'Reilly Media Inc Sebastopol 2004)

Lastowka G *Virtual justice: the new laws of online worlds* (Yale University Press New Haven 2010)

Lawson FH and Rudden B *The law of property* 3rd ed (Oxford University Press Oxford 2002)

Leary MS *Quantifying the discoverability of identity attributes in internet-based public records: impact on identity theft and knowledge-based authentication* (Ph.D thesis Capella University for CHE 2008)

Lefèbvre F *Message digests for photographic images and video contents* (Presses universitaires de Louvain 2004)

Lessig L *Code and other laws of cyberspace* (Basic Books New York 1999)

Levy E *West Roman vulgar law: the law of property* (American Philosophical society Philadelphia 1951)

LIoyd I *Legal aspects of the information society* (Butterworths London 2000)

Loubser MM *The theft of money in South African law: with a comparison of other legal systems* (LLD Thesis University of Stellenbosch 1978)

Luschnig CAE *An introduction to ancient Greek: a literary approach* 2nd ed (Hackett Publishing Indianapolis 2007)

Lyon BD *The Middle ages in recent historical thought: selected topics* (American Historical Association Washington DC 1965)

M

Maasdorp AFS *Institutes of South African law* 10th ed (Juta Cape Town 1976)

Maasdorp AFS *The institutes of Cape Town: being a compendium of the common law, decided cases and statute law of the colony of the Cape of Good Hope* (Juta Cape Town 1923)

Maasdorp AFS *The institutes of South Africa: being a compendium of the common law, decided cases, and statute law of the Union of South Africa* 5th ed (Juta Cape Town 1929)

MacKenzie L *Studies in Roman law with comparative views of laws of France, England and Scotland* (Gaunt Holmes Beach 1991)

Macpherson CB *Democratic theory* (Claredon Press Oxford 1973)

Maine HS *Ancient law: its connection with the early history of society and its relation to modern ideas* (Spottiswoode London 1897)

Mann I *Hacking the human: social engineering techniques and security countermeasures* (Gower Publishing Hampshire 2008)

Manning T *Radical strategy: How South African companies can win against global competition* (Zebra Press Sandton 1997)

Mansell R and Wehn U *Information technology for sustainable development* (Oxford University Press Oxford 1998)

Dixon R *Karl Marx, Frederick Engels: collected works* (International Publishers New York 1975)

Mason S *Electronic signatures in law* 2nd ed (LexisNexis London 2007)

Matthaeus A *De criminibis* (Hoogenhuysen Vesaliæ 1672)

McCraw TK *Regulation in perspective: historical essays* (Harvard University Press Boston 1981)

McLynn F *Crime and punishment in the eighteenth-century England* 1st ed (Routledge London New York 1989)

Michaels JV *Technical risk management* (Prentice Hall New Jersey 1996)

Miller P and Cimmins M *LAN technologies explained* (Digital Press Massachusetts 2000)

Milton JRL *South African criminal law and procedure* (3rd ed (Juta Cape Town 1996)

Mitnick BM *Planning regulation: a framework for the analysis of regulatory possibilities* (University of Pittsburgh Pittsburgh 1979)

Mitnick BM *Regulation and the theory of agency: incentives, control, and reform in regulation* (University of Pittsburgh Pittsburgh 1979)

Mommsen T *The Digest of Justinian* (University of Pennsylvania Press Philadelphia 1985)

Moore R *Cybercrime: investigating high-technology computer crime* 2nd ed (Anderson Publishing Oxford 2011)

Morgan B and Yeung K *An introduction to law and regulation: text and materials* (Cambridge University Press Cambridge 2007)

Mostert H *The constitutional protection and regulation of property and its influence on the reform of private law and landowners in South Africa and Germany* (Springer Berlin 2002)

Moussourakis G *Fundamentals of Roman private law* (Springer Berlin 2012)

Moyle JB *The Institutes of Justinian* 5th ed (Clarendon Press Oxford 1913)

Muirhead J *Historical introduction to the private law of Rome* (Gaunt Inc. Florida 1998)

Muirhead J *Historical introduction to the private law of Rome* 3rd ed (A & C Black Ltd London 1916)

Munday R *Evidence* (Oxford University Press Oxford 2007)

Murray AC *Germanic kinship structure: studies in law and society in Antiquity and the early Middle ages* (Pontifical Institute of Medieval Studies Toronto 1983)

Murray AD *The regulation of the internet: control in the online environment* (Routledge-Cavendish Abington 2007)

N

Nasmith D *Outline of Roman history from Romulus to Justinian (including translation of the Twelve Tables, the Institutes of Gaius, and the Institutes of Justinian), with special reference to the growth, development and decay of Roman jurisprudence* (The Lawbook Exchange New Jersey 2006)

Nathan M *The common law of South Africa: a treatise based on Voet's commentaries on the Pandects, with reference to the leading Roman-Dutch authorities, South African decisions, and statutory enactments in South Africa* (Africa Book Company London 1904)

National Research Council *Computers at risk: safe computing in the information age* (National Academy Press Washington DC 1991)

Neethling J, Potgieter JM and Visser PJ *Law of delict* 2nd ed (Butterworths Durban 1994)

Neethling J, Potgieter JM and Visser PJ *Law of delict* 2nd ed (Butterworths Durban 1994)

Neff SC (ed) *Hugo Grotius on the law of war and peace: student edition* (Cambridge University Press Cambridge 2012)

Nicastro FM *Curing the patch management headache* (Auerbach Publications Florida 2005)

Nicholas B *Introduction to Roman law* (Oxford University Press Oxford 1987)

Nielsen G and Vedel M *Improving usability of passphrase authentication* (Kongens Lyngby Denmark 2009)

O

Okey R *Eastern Europe 1740-1980* (Hutchinson Minneapolis 1982)

Okin JR *The internet revolution: the not-for-dummies guide to the history, technology, and use of the internet* (Ironbound Press Winter Harbor 2005)

Ong RYC *Mobile communication and the protection of children* (Leiden University Press Leiden 2010)

Oosthuizen AJ *The law of property* (Juta Cape Town 1981)

Oppliger R *Authentication systems for secure networks* (Artech House Publishers Boston 1996)

Ortolan J *The history of Roman law from the text of Ortolan's histoire de la legislation Romaine et généralisation du droit* (Butterworths London 1871)

P

Paré DJ *Internet governance in transition: who is the master of this domain?* (Rowman Littlefield Publishers Maryland 2003)

Paton GW and Derham DP (eds) *A textbook of jurisprudence* 4th ed (Claredon Press Oxford 1972)

Pearson RL *Electronic security systems: a manager's guide to evaluation and selecting system solutions* (Elsevier Amsterdam 2007)

Pejovich S *The economics of property rights: towards a theory of comparative systems* (Kluwer Academic Publishers Dordrecht 1990)

Pieprzyk J, Hardjono T, and Seberry J *Fundamentals of computer security* (Springer Berlin 2003)

Plucknett TFT *A concise history of the common law* 5th ed (The Law Book Exchange New Jersey 2001)

Pollock F and Maitland FW *The history of English law before the time of Edward I* 2nd ed (The Lawbook Exchange New Jersey 2008)

Pollock F and Maitland FW *The history of English law before the Time of Edward I* 2nd (Cambridge University Cambridge 1968)

Pound R and Plucknett T *Readings on the history and systems of the common law* 3rd ed (WM.W. Gaunt Florida 1993)

Pratt D *The political thought of King Alfred the great* (Cambridge University Press Cambridge 2007)

R

Radin MJ *Reinterpreting property* (The University of Chicago Press London 1993)

Radu C *Implementing electronic payment systems* (Artech House Bostons 2003)

Raff M *Private property and environmental responsibility: a comparative study of German real property law* (Kluwer Law International The Hague 2003)

Raymond ES *The cathedral and the baazar: musings on linux and open source by an accidental revolutionary* (O'Reilly and Associates Beijing 2001)

Raymond ES *The cathedral and the bazaar: musings on linux and open source by an accidental revolution* (O'Reilly Beijing 1999)

Reed C *Internet law: text and materials* 2nd ed (Cambridge University Press Cambridge 2004)

Reeves J *History of English law, from the times of saxons, to the end of the reign of Philip and Mary* 2nd ed (Temple-Bar London 1787)

Reid P *Biometrics for network security* (Pearson New Jersey 2004)

Robinson JW *William of Ockham's early theory of property rights in context* (Koninkljke Brill Leiden 2008)

Roby HJ *Roman private law in the times of Cicero and of the Antonines* (Gaunt Inc. Florida 1998)

Rogers DJ *Broadband quantum cryptography* (Morgan & Claypool Publishers Columbia 2010)

Rolfe JC *The attic nights of Aulus Gellius* (Harvard University Press Cambridge 1927)

Ross A *On law and justice* (The Law Book Exchange Ltd New Jersey 2004)

Ross RA, Mortinger S, Christ R, Scelsi C and Alemi F (eds) *Computer games and virtual worlds: a new frontier in intellectual property law* (ABA Publishing Illinois 2010)

Rowe GW *Theoretical models in biology: the origin of life, the immune system and the brain* (Oxford University Press Oxford 1994)

S

Samuel G "The many dimensions of property" in McLean J (ed) *Property and the constitution* (Hart Publishing Oxford 1999)

Saunders CJ *Rape and ravishment in the Literature of medieval England* (Boydell & Brewer Ltd Cambridge 2001)

Scheb JM *Criminal law and procedure* 4th ed (Wadsworth Thomson Belmont 2002)

Schulz F *Classical Roman law* (Oxford University Press London 1961)

Schwabach A *Internet and the law: technology, society and compromises* (ABC-CLIO California 2006)

Scott SP *The civil law including the Twelve Tables, the Institutes of Gaius, the rules of Ulpian, the opinions of Paulus, the enactments of Justinian, and the constitutions of Leo* Vol 1 (AMS Press New York 1973)

Selby-Bigge LA (ed) *A treatise on human nature by David Hume* (The Claredon Press Oxford 1896)

Shaffern RW *Law and justice form antiquity to enlightenment* (Rowman & Littlefield Publishers 2009)

Shogimen T *Ockham and political discourse in the late Middle ages* (Cambridge University Press Cambridge 2007)

Siltala R *Law, truth, and reason: a treatise on legal argumentation* (Springer Dordrecht 2011)

Simon HA *The sciences of the artificial* 3rd ed (The MIT Press Cambridge 1996)

Simpson DP *Cassell's new Latin-English English-Latin Dictionary* (Cassell & Co London 1959)

Singer H (ed) *Die summa decretorum des Magister Rufinus* (Ferdinand Schöningh Paderborn 1902)

Singer JW *Property law: rules, policies, and practices* 3rd ed (Aspen Publishers New York 2002)

Singer RG and La Fond JQ *Criminal law* 5th ed (Wolters Kluwer Austin Boston 2010)

Skoudis ED and Zeltser L *Malware: fighting malicious code* (Pearson Education New Jersey 2004)

Smith K and Keenan DJ *English law* 2nd ed (Sir Isaac Pitman London 1966)

Smith W and Anthon C (eds) *A dictionary of Greek and Roman antiquities* (American Book New York 1843)

Smith W and Anthon C (eds) *A dictionary of Greek and Roman antiquities* 3rd ed (Harper New York 1870)

Snyman CR *Criminal Law* 5th ed (LexisNexis Durban 2008)

Snyman CR *Strafreg* (LexisNexis Durban 2012)

Soete L *Building the European information society for use al: final policy report of the high level expert group* (European Communities Brussels 1997)

Sohm R *The institutes: a text-book of the history and systems of Roman private law* 2nd ed (Gaunt Inc. Florida 1901)

Sohm R *The institutes: a textbook of the history and the system of Roman private law* 3rd ed (The Clarendon Press London 1907)

Solomon RC and Higgins KM *The Big questions: a short introduction to philosophy* 8th ed (Cengage Learning Wadsworth 2010)

Solove DT, Rotenberg M and Schwartz PM *Privacy, information, and technology* (Aspen Publishers New York 2006)

Srivastava A *Electronic signatures for B2B contracts: evidence from Australia* (Springer Heidelberg 2013)

Stavroulakis P and Stamp M (eds) *Handbook of information and communication Security* (Springer Heidelberg 2010)

Stein P *Roman law in European history* (Cambridge University Press Cambridge 1991)

Stephen JF *A Digest of the criminal law (Crimes and Punishments)* 5th ed (MacMillan & Co New York 1894)

Stewart JM, Chapple M and Gibson D *Cissp: certified information systems security professional study guide* (John Wiley San Francisco 2005)

Strebe M *Network security jumpstart: computer and network security basics* (SYBEX Inc Alameda 2002)

Strömholm S *A short history of legal thinking in the West* (Norstedts Stockholm 1985)

Stump E *Aquinas* (Routledge London 2003)

Sullivan D *The definitive guide to controlling malware, spyware, phishing, and spam* (Realtime publishers 2006)

Summers D (ed) *Longman dictionary of contemporary English* 3rd ed (Longman Harlow Essex 1995)

Sunstein CR *Laws of fear: beyond the precautionary principle* (Cambridge University Press Cambridge 2005)

Susskind RE *The future of law: facing the challenges of information technology* (Clarendon New York 1996)

Sutton IS *Process reliability and risk management* (Van Nostrand Reinhold New York 1992)

T

Tamm D *Roman law and European legal history* (Djøf Publishing Copenhagen 1997)

Thomas JAC *The Institutes of Justinian: text, translation and commentary* (Juta & Co Ltd Cape Town 1975)

Tickner J and Raffensperger C *The precautionary principle in action: a handbook* (Science and Environmental Health Network Windsor 1991)

Todorov D *Mechanics of user identification and authentication: fundamentals of identity management* (Auerbach Publications Florida 2010) 7

Tomkins FJ and Jencken HD *A compendium of the modern Roman law founded upon the treatises of Puchta, Von Vangerow, Arndts, Franz Moehler, and the Copus Juris Civilis* (Butterworths London 1870)

Torfing J *Politics, regulation and modern welfare state* (MacMillan Press Ltd Hampshire 1998)

Treviño AJ *The sociology of law: classical and contemporary perspectives* (Transaction Publishers New Brunswick 1996)

Trouwborst A *Precautionary rights and duties of states* (Martinus Nijhoff Publishers Leiden 2006)

Tuck R *Natural rights theories: their origin and development* (Cambridge University Press Cambridge 1979)

Turner JWC and Armitage A *Cases on criminal law* 3rd ed (Cambridge University Press London 1964)

Turner JWC *Russell on crime* 12th ed (Stevens London 1964)

V

Vacca JR *Identity theft* (Pearson Education New Jersey 2003)

Valpy FEJ *An etymological dictionary of the Latin language* (Baldwin London 1828)

Van Asselt MBA *Perspectives on uncertainty and risk: The PRIMA approach to decision support* (Kluwer Academic Publishers Dordrecht 2000)

Van Caenegem RC *An historical introduction to private law* (Cambridge University Press Cambridge 1992)

Van der Merwe C and Verbeke AL (eds) *Time-limited interests in law* (Cambridge University Press Cambridge 2012)

Van der Merwe CG and De Waal M *The law of things and servitudes* (Butterworths Publishers Durban 1993)

Van der Merwe CG *Sakereg* 2nd ed (Butterworths Durban 1987)

Van der Merwe CG *The law of things* (Butterworths Durban 1987)

Van der Merwe DP *Information and communication technology law* (LexisNexis Durban 2008)

Van der Walt AJ and Pienaar GJ *Introduction to the law of property* 2nd ed (Juta Kenwyn 1997)

Van der Walt AJ and Pienaar GJ *Introduction to the law of property* 6th ed (Juta Claremont 2009)

Van der Walt AJ *Constitutional property law* (Juta Cape Town 2005)

Van der Walt AJ *Die ontwikkeling van houerskap* (LLD Thesis Potchefstroom University 1985)

Van der Walt AJ *The constitutional property clause: a comparative analysis of section 25 of the South African Constitution of 1996* (Juta Kenwyn 1997)

Van der Walt JGW *The twilight of legal subjectivity: towards a deconstructive republican theory of law* (LLD Thesis RAU Johannesburg 1995)

Van Klink BMJ and Prins JEJ *Law and regulation: scenarios for the information age* (IOS Press Amsterdam 2002)

Van Leeuwen S *Commentaries on Roman-Dutch law* (Stevens and Haynes London 1886)

Van Warmelo P *An introduction to the principles of Roman civil law* (Juta Cape Town 1976)

Van Zyl DH *Geskiedenis van die Romeins-Hollandse Reg* (Butterworths Durban 1979)

Vinogradoff P *Roman law in medieval Europe* 3rd ed (Oxford University Press Oxford 1929)

Visser C, Pretorius JT, Sharrock R and Van Jaarsveld M *South African mercantile and company law* 8th ed (Juta Cape Town 2003)

Voet J *Commentarius ad Pandectas* (1698)

Voet J *Commentarius ad Pandectas* (Juta Cape Town 1902)

Voet J *De furti*

Von Bar L *A history of continental criminal law* (Augustus M. Kelley Publishers New York 1968)

Von Bertalanffy L *General system theory: foundations, development, applications* (George Braziller Inc New York 1968)

Von Bertalanffy L *Perspectives on general system theory: scientific-philosophical studies* (George Braziller Inc. New York 1975)

Von Klink BMJ and Prins JEJ *Law and regulation: scenarios for the information age* (IOS Press Amsterdam 2002)

W

Waite M (ed) *Oxford paperback thesaurus* 4th ed (Oxford University Press Oxford 2012)

Wallace-Hadrill JM *The long-haired kings and other studies in Frankish history* (Methuen & Co Ltd London 1962)

Watson A *Roman law and comparative law* (The University of Georgia Press Athens 1991)

Watson A *The evolution of western private law* (Johns Hopkins University Press Baltimore 2001)

Watson A *The nature of law* (Edinburgh University Press Edinburgh 1977)

Watson A *The spirit of Roman law* (University of Georgia Press Georgia 1995)

Weber RH *Shaping internet governance: regulatory challenges* (Springer Heidelberg 2009)

Webster F *Theories of the information society* 3rd ed (Routledge Abington 2006)

Wehmeier S, McIntosh C, Turnbull J and Ashby M *Oxford advanced learner's dictionary of current English* 7th ed (Oxford University Press Oxford 2005)

Whitman JQ *The legacy of Roman law in the German Romantic era: historical vision and legal change* (Princeton University Press New Jersey 1990)

Whitman ME and Mattord HJ *Principles of information security* 4th ed (Cengage Learning Australia 2012)

Williams G *Textbook of criminal law* 2nd ed (Stevens and Sons London 1983)

Williams MJ *NATO, Security, and risk management: from Kosovo to Kandahar* (Routledge Abington 2009)

Wilson E *Savage Republic: De Indis of Hugo Grotius, republicanism, and Dutch hegemony within the early modern world-system* (Martinus Nijhoff Publishers Leiden 2008)

Windscheid B *Lehrbuch des Pandektenrechts* 7th ed (Buddesus Düsseldorf 1863)

Woolgar S (ed) *Virtual society? technology cyberbole, reality* (Oxford University Press Oxford 2002)

Woollfson J *Padua and the Tudors: English students in Italy, 1485-1603* (James Clarke & Co Cambridge 1998)

World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) *The precautionary principle* (United Nations Educational, Scientific and Cultural Organisation Paris 2005)

Y

Yoe C *Principles of risk analysis: decision making under uncertainty* (CRC Press Boca Raton 2012)

Z

Zimmerman R *The law of obligations: Roman foundations of the civilian tradition* (Juta Cape Town 1990)

2. CHAPTERS IN BOOKS

A

Aickelin U, Bentley P, Cayzer S, Kim J and McLeod J "Danger theory - the link between AIS and IDS?" in Timmis J, Bentley P and Hart E (eds) *Artificial immune systems* (Springer Berlin 2003) 147-155

Allen R and Pickup A "Two-factor authentication" in Birch D (ed) *Digital identity management: technological, business and social implications* (Gower Publishing Limited Hampshire 2007) 113-120

Andrews S "Building trust online – work at the OECD" in Schulz A (ed) *Legal aspects of an e-commerce transaction* (Sellier European Law Publishers München 2006) 243-247

B

Bhuiyan T, Josang A and Xu Y "Managing trust in online social networks" in Furht B (ed) *Handbook of social network technologies and applications* (Springer New York 2010) 471-496

Blöcher U "Network and system security" in Fumy W and Sauerbrey J (eds) *Enterprise security - IT solutions: concepts, practical experiences technologies* (Publicis Corporate Publishing Erlangen 2006) 44-56

Bossler AM and Burruss GW "The general theory of crime and computer hacking - low self-control hackers?" in Holt TJ and Schell BH (eds) *Corporate hacking and technology-driven crime: social dynamics and implications* (Information Science Reference Hershey 2011) 38-67

Bowling B, Marks A and Murphy CC "Crime control technologies – towards an analytical framework and research agenda" in Brownsword R and Yeung K (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart Publishing Oxford 2008) 51-78

Boyen X, Dodis Y, Katz J, Ostrvsky R and Smith A "Secure remote authentication using biometrics" in Cramer R (ed) *Advances in cryptology – eurocrypt, lecture notes in computer science* (Springer Heidelberg 2005) 147-163

Boyer R "The regulation approach as a theory of capitalism – a new derivation" in Labrousse A and Weisz JD (eds) *Institutional economics in France and Germany* (Springer Berlin 2001) 49-92

Brenner SW "History of computer crime" in de Leeuw K Bergstra J (eds) *The history of information security: a comprehensive handbook"* (Elsevier Amesterdam 2007) 705-721

Brown I, Edwards L and Marsden C "Information security and cyberspace" in Edwards L and Waelde C (eds) *Law and the internet* (Hart Publishing Oxford 2009) 671-684

Brownsword R "So what does the world need now? - reflections on regulating technologies" in Brownsword R and Yeung K (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart Publishing Oxford 2008) 23-48

Brownsword R and Yeung K "Regulating technologies – tools, targets and thematic" in *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart Publishing Oxford 2008) 3-22

Burchell J "Criminal law" in Van der Merwe CG and du Plessis JE (eds) *Introduction to the law of South Africa* (Aspen Publishers The Hague 2004) 447-492

C

Cairns JW "Craig, Cujas and the definition of *feudum*" in Birks P (ed) *New Perspectives in the Roman law of property: essays for Barry Nicholas* (Claredon Press Oxford 1989) 75-84

Cairns JW “The definition of slavery in eighteenth-century thinking” in Allain J (ed) *The legal understanding of slavery* (Oxford University Press Oxford 2012) 61-84

Carver CS and Scheier MF “Self-regulation of action and affect” in Vohs KD and Baumeister RF (eds) *Handbook of self-regulation, second edition: research, theory, and applications* (The Guilford Press New York 2011) 3-21

Cho S and Hwang S “Artificial rhythms and cues for keystroke dynamics based authentication” in Zhang D and Jain AK (eds) *International conference on biometrics, 2006* (Springer Berlin 2005) 626-635

Coglianese C and Mendelson E “Meta-regulation and self-regulation” in Baldwin R, Cave M and Lodge M (eds) *The oxford handbook of regulation* (Oxford University Press Oxford 2010) 146-168

Costa AM “Emerging challenges” in Savona EU (ed) *Crime and technology: new frontiers for regulation, law enforcement and research* (Springer Dordrecht 2001) 1-6

D

Di Pietro R and Verde NV “Digital forensic techniques and tools” in Jahankhani H, Watson DL, Me G and Leonhardt F (eds) *Handbook of electronic security and digital forensics* (World Scientific Publishing New Jersey 2010) 321-356

Ding J “Internet regulation” in Campbell D, Bán C, Bán S and Szabo S (eds) *Legal issues in the global information society* (Oceana Publications New York 2005) 279-351

Doghmi SF, Guttman JD and Thayer FJ “Completeness of the authentication tests” in Biskup J and López J (eds) *Computer security: ESORICS 2007* (Springer Berlin 2007) 106-121

Downing RW “Shoring up the weakest link – what lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime” in Carr I (ed) *Computer crime* (Ashgate Publishing Limited Surrey 2009) 4-72

Du Plessis PJ “Towards the medieval law of hypothec” in Cairns JW and du Plessis PJ (eds) *The creation of the ius commune: from Casus to Regula* (Edinburgh University Press Edinburgh 2010) 159-175

E

Earle TC, Siegrist M and Gutscher H "Trust, risk perception and the TCC model of cooperation" in *Trust in risk management: uncertainty and the scepticism in the public mind* (Earthscan Publishing London 2010) 1-49

F

Fantham E "With malice aforethought – the ethic of *militia* on stage and law" in Sluiter I and Rosen RM (eds) *Kakos: badness and anti-value in classical antiquity* (Brill Leiden 2008) 319-334

Febbrajo A "The rules of the game in the welfare state" in Teubner G (ed) *Dilemmas of law in the welfare state* (De Gruyte Berlin 1986)

Feenstra "*Dominium* and *ius in re aliena* - the origins of a civil law distinction" in P Birks (ed) *New perspectives in the Roman private law of property: essays for Barry Nicholas* (Clarendon Press Oxford 1989) 111-122

Finch E "The problem of stolen identity and the Internet" in Jewkes Y (ed) *Crime online* 1st ed (Willan Devon 2007) 29-43 29-31

Fraud Advisory Panel Cybercrime Working Group "Recent attack trends" in Reuvid J (ed) *The secure online business handbook: a practical guide to risk management and business continuity* 4th ed (Kogan Page Limited London 2006) 5-10

G

Godard O "Social decision-making under scientific controversy, expertise, and the precautionary principle" in Joerges C, Ladeur KH and Vos E (eds) *Integrating scientific expertise into regulatory decision-making: national experiences and european innovations* (Baden-Baden Nomos 1997) 39-73

Gordon BJ "Internet criminal law" in Buys (ed) *Cyberlaw @ SA: the law of the Internet in South Africa* (Van Schaik Publishers Pretoria 2000)

Gorge M and Brudenall P "Phishing, pharming and the requirement for strong user authentication" in Reuvid J (ed) *The secure online business handbook: a practical*

guide to risk management and business continuity 4th ed (Kogan Page London 2006) 91-94

Gregersen B "The public sector as a pacer in national systems of innovation" in Lundvall BÅ (ed) *National systems of innovation: toward a theory of innovation and interactive learning* (Anthem Press London 2010) 133-150

Gunningham N "Enforcement and compliance strategies" in Baldwin R, Cave M and Lodge M (eds) *The oxford handbook of regulation* (Oxford University Press Oxford 2010) 120-145

Gunningham N "Regulating biotechnology – lessons from environmental policy" in Somsen H (ed) *The regulatory challenge of biotechnology: human genetics, food and patents* (Edward Elgar Publishing Ltd Cheltenham 2007) 3-18

H

Hastings NE and Dodson DF "Qualifying assurance of knowledge based authentication" in Jones A and Remenyi D (eds) *Proceedings of the 3rd European conference on information warfare and security* (Academic Conference Limited Reading 2004) 109-116

Heldeweg MA "Legal design of smart rules and regimes – regulating innovation" in Heldeweg MA and Kica E (eds) *Regulating technological innovation: a multidisciplinary approach* (Palgrave Macmillan Hampshire 2011) 52-76

Helmholz RH "Human rights in the Canon law" in Witte J and Alexander FS (eds) *Christianity and human rights: an introduction* (Cambridge University Press Cambridge 2010) 99-112

Helou TJ "Introduction" in Coats WS, Bagdasarian A, Helou TJ and Lam T (eds) *The practitioner's guide to biometrics* (ABA Publishing Illinois 2007) 1-17

Hirschfeld M "How a Thomistic model framework can take social causality seriously" in Finn DK (ed) *Distant markets, distant harms: economic complicity and Christian ethics* (Oxford University Press Oxford 2014) 146-172

Holder J and Elworthy S "The BSE crisis – a study of the precautionary principle and the politics of science in law" in Reece H (ed) *Law and science: current legal issues Volume 1* (Oxford University Press Oxford 1998) 129-152

Hosten WJ and Schoeman J "Private law – law of things" in Hosten WJ, Edwards AB, Bosman F and Church J (eds) *Introduction to South African law and legal theory* (Butterworths Durban 1997) 622-659

Hrabok M and Kerns KA "The development of self-regulation – a neuropsychological perspective" in Solok BW, Müller U, Carpendale JIM, Young AR and Iarocci G (eds) *Self and social regulation: social interaction and the development of social understanding and executive functions* (Oxford University Press Oxford 2010) 129-154

Hribernig G and Weinzierl P "Biometric authentication" in Fumy E and Sauerbrey J (eds) *Enterprise security: IT security solutions – concepts, practical experiences, technologies* Publicis Corporate Publishing Erlangen 2006) 84-102

J

Jain A, Bolle R and Pankanti S "Introduction to biometrics" in *Biometrics: personal identification in networked society* (Kluwer Academic Publishers Massachusetts 1999) 1-40

Joskow PL and Rose NL "The effects of economic regulation" in Armstrong M and Porter RH (eds) *Handbook of industrial organization* (Elsevier Amsterdam 1989) 1450-1506

K

Kessler GC and Levine DE "Denial-of-service attacks" in Bosworth S, Kabay ME and Whyne E (eds) *Computer security handbook* 5th ed (John Wiley and Sons New Jersey 2009) 18.1-18

Kim PH, Ferrin DL, Cooper CD and Dirks KT " Removing the shadow of suspicion – the effect of apology versus denial for repairing competence-versus integrity-based trust violations" in Costa AC and Anderson N (eds) *Trust and social capital organisations* (Sage Publications London 2013) 175-205

Kirkpatrick C and Parker D "Regulatory impact assessment – an overview" in *Regulatory impact assessment: towards better regulation* (Edward Elgar Publishing Cheltenham 2007) 1-16

Knoll PW "*Nationes* and other bonding groups at late medieval central European universities" in van Deusen N and Koff LM (eds) *Mobs: an interdisciplinary inquiry* (Koninklijke Brill Leiden 2010) 79-94

Koops BJ "Criteria for normative technology – the acceptability of 'Code as Law' in light of democratic and constitutional values" in Brownsword R and Yeung K (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart Publishing Portland 2008) 157-174

Koops BJ "Should ICT regulation be technology neutral?" in Koop BJ, Lips M, Prins C and Schellekens M (eds) *Starting points for ICT regulation: deconstructing prevalent policy one-liners"* (Asser Press The Hague 2006) 77-108

Koster R "Declaring the rights of players" in Balkin JM and Noveck BS (eds) *The State of Play: Law, Games, and Virtual Worlds* (2006) 55-67

L

Lee H, Kim W and Hong M "Biological inspired computer virus detection system" in Ijspeert AJ, Murata M and Wakamiya M (eds) *Biologically inspired approaches to advanced information technology* (Springer Berlin 2004) 153-165

Lee O and Lee W "Mobile commerce and national IT infrastructure" in Pour MK (ed) *Information technology and organisations: trends, issues, challenges and solutions* (Idea Groug Publishing Hershey 2003) 352-354

Lee S "In the prison of the mind – punishment, social order, self-regulation" in Saral A, Douglas L and Umphrey MM (eds) *Law as punishment or law as regulation* (Stanford University Press California 2011) 124-154

Lessig L "The laws of cyberspace" in Spinello RA and Tavani HT (eds) *Readings in cyberethics* (Jones Bartlett Sudbury 2004) 134-144

Leventhal H, Brissette I and Leventhal EA "The common-sense model of self-regulation of health and illness" in Cameron LD and Leventhal H (eds) *The self-regulation of health and illness behaviour* (Routledge London 2003) 42-65

Levi-Faur D "Regulation and regulatory governance" in *Handbook on the politics of regulation* (Edward Elgar Publishing Ltd Cheltenham 2011) 3-21

M

Ma J and Orgun M "Managing theories of trust in agent based systems" in Yolum P, Güngör T, Gürgen F and Özturan C (eds) *Computer and information sciences – ISCIS 2005* (Springer Berlin 2005) 442-451

MacQueen HL "Two toms and the ideology for Scots Law – TB Smith and Lord Cooper of Culross" in Reid E and Miller DLC (eds) *A mixed legal system in transition: TB Smith and the process of Scots law* (Edinburgh University Press Edinburgh 2005)

Maré MC "Public law – criminal law" in Hosten WJ, Edwards AB, Bosman F and Church J *Introduction to South African law and legal theory* 2nd ed (Butterworths Durban 1995) 1082-1125

Martin SE "Information controls and needs of information flow in representative democracies" in Lederman E and Shapira R (eds) *Law, information and information technology* (Kluwer Law International The Hague 2001) 369-389

McHarg A "Devolution and the regulatory state – constraints and opportunities" in Oliver D, Prosser T and Rawlings R (eds) *The regulatory state: constitutional implications* (Oxford University Press Oxford 2010) 67-91

McIntyre TJ and Scott C "Internet filtering – rhetoric, legitimacy, accountability and responsibility" in Brownsword R and Yeung K (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart Publishing Oxford 2008) 109-124

Moore T and Edelman B "Measuring the perpetrators and funders of typosquatting" in Sion R (ed) *Financial cryptography and data security* (Springer Berlin Heidelberg 2010) 175-191

Murphy P and Baddour L "International criminal law and common law rules of evidence" in Khan KAA, Buisman C and Gosnell C (eds) *Principles of evidence in international criminal justice* (Oxford University Press Oxford 2010) 96-156

Murray AD "Conceptualising the post-regulatory (cyber) state" in Brownsword R and Yeung K (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart Publishing Portland 2008) 287-315

Myers S "Introduction to phishing" in Jakobsson M and Myers S (eds) *Phishing and counter-measures: understanding the increasing problem of online identity theft* (John Wiley New Jersey 2007) 1-30

N

Nigri DF "Theft of information and the concept of property in the information age" in Harris JW (ed) *Property problems: from genes to pension funds* (Kluwer Law International London 1997) 48-60

Nilson K and Bigun J "Complex filters applied to fingerprint image detecting prominent symmetry points used for alignment" in Tistarelli M, Bigun J and Jain AK (eds) *Biometric authentication* (Springer Berlin 2002) 39-47

P

Paleker M "Succession" in du Bois F (ed) *Wille's principles of South African law* 9th ed (Juta Cape Town 2007) 666-731

Papadopoulos S "An introduction to cyberlaw" in Papadopoulos S and Snail S (eds) *Cyberlaw @SA III: The law of the internet in South Africa* (Van Schaik Publishers Hatfield 2012) 1-8

Perens B "The Open Source definition" in DiBona C, Ockman S and Stone M (eds) *Open sources: voices from the open source revolution* (O'Reilly and Associates Beijing 1999) 171-188

Perez FX "Risk regulation, precaution and trade" in Wüger D and Cottier T (eds) *Genetic engineering and the world trade system: World Trade Forum* (Cambridge University Press Cambridge 2008) 246-284

Pfau A “Smart card solutions” in Fumy E and Sauerbrey J (eds) *Enterprise security: IT security solutions – concepts, practical experiences, technologies* Publicis Corporate Publishing Erlangen 2006) 57-69

Pottage A and Sherman B “On the prehistory of intellectual property” in Howe HR and Griffiths J (eds) *Concepts of property in intellectual property law* (Cambridge University Press Cambridge 2013) 11-28

R

Raab CD and De Hert P “Tools for technology regulation – seeking analytical approaches beyond Lessig and Hood” in Brownsword R and Yeung K (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart Publishing Portland 2008) 263-285

Raymond ES “The revenge of the hackers” in DiBona C, Ockman S and Stone M (eds) *Open sources: voices from the open source revolution* (O’Reilly and Associates Beijing 1999) 207-219

Roux T “Property” in Cheadle MH, Davis DM and Hayson NRL (Eds) *South African constitutional law: the Bill of Rights* (Butterworths Durban 2002) 429-472

Ryan PYA “Mathematical models of computer security” in Focardi R and Gorrieri R (eds) *Foundations of security analysis and design: tutorial lectures* (Springer Berlin 2001) 1-62

S

Samuelson P “Five challenges for regulating the global information society” in Marsden CT (ed) *Regulating the global information society* (Routledge London New York 2000) 317-319

Savona EU and Mignone M “The fox and the hunters - how ICT technologies change the crime race” in Savona EU (ed) *Crime and technology: new frontiers for regulation, law enforcement and research* (Springer Dordrecht 2004) 7-28

Scalise Jr RJ “Testamentary formalities in the United States of America” in Reid KGC, de Waal MJ and Zimmermann R (eds) *Comparative succession law: testamentary formalities* (Oxford University Press Oxford 2011) 357-403 385

Sieber U “The emergence of information law - object and characteristics of a new legal order” in Lederman E and Shapira R (eds) *Law, information and information technology* (Kluwer Law International The Hague 2001) 1-30

Simmons GJ “Authentication theory/coding theory” in Blakley GR and Chaum D (eds) *Advances in cryptology –CRYPTO* (Springer Heidelberg 1985) 411-431

Sinatambou E “The approach of mixed legal systems – the case of Mauritius” in Bowman M and Bole A (eds) *Environmental damages in international and comparative law: problems of definition and valuation* (Oxford University Press Oxford 2002) 271-280

Singh N “Digital economy” in Bidgoli H (ed) *Handbook of information security: threats, vulnerabilities, prevention, detection, and management* (John Wiley New Jersey 2006) 15-36

Smith M “Capital punishment and burial in the Roman empire” in Ellens J H (ed) *Bethsaida in archaeology, history and ancient culture: a festschrift in honour of J.T Greene* (Cambridge Scholars Publishing Newcastle 2014) 395-436

Stenning PC, Shearing CD, Addario SM and Condon MG “Controlling interests – two conceptions of order in regulating a financial market” in Friedland ML (ed) *Securing compliance: seven case studies* (University of Toronto Press Toronto 1990) 88-119

Sullins LL “’Phishing’ for a solution – domestic and international approaches to decreasing online identity theft” in Carr I (ed) *Computer crime* (Ashgate Publishing Limited Surerey 2009) 73-109

Sussmann MA “The critical challenges from international high-tech and computer-related crime at the millennium” in Carr I (ed) *Computer crime* (Ashgate Publishing Limited Surerey 2009) 379-418 379-381

T

Taylor A and Eder L "A comparison of authentication, authorisation and auditing in Windows and Linux" in Warkentin M and Vaughn RB (eds) *Enterprise information systems and assurance system security: managerial and technical issues* (Idea Group Publishing Hershey 2006) 326-342

Tiagha E "Technology management and technology transfer in Africa" in Waiguchu JM, Tiagha E and Mwaura M (eds) *Management of organisations in Africa: A handbook and reference* (Quorum Books Westport 1999) 243-263

Tistarelli M, Lagorio A and Grosso E "Understanding iconic image-based face biometrics" in Tistarelli M, Bigun J and Jain AK (eds) *Biometric authentication* (Springer Berlin 2002) 19-29

Todeschini G "The origin of medieval anti-Jewish stereotype – the Jews as the receivers of stolen goods (twelfth to thirteenth centuries) in Adams J and Hanska J (eds) *The Jewish-Christian encounter in medieval preaching* (Routledge New York 2015) 240-252

V

Van der Merwe CG "Law of property" in Van der Merwe CG, Du Plessis JE and Zimmermann R (eds) *Introduction to the law of South Africa* (Kluwer Law International The Hague 2004) 201-242

Van der Merwe CG and Pope A "Property" in Du Bois F (ed) *Willie's Principles of South African Law* 9th ed (Juta Cape Town 2007) 405-732

Van der Vyver JD "The doctrine of private law rights" in Straus SA (ed) *Huldigingsbudel vir W.A. Joubert: aan hom aangebied by geleentheid van sy sewentigste verjaardag op 27 Oktober 1988* (Butterworths Durban 1988) 201-246

Van der Walt AJ and Kleyn DG "Duplex dominium – the theory and significance of the concept of divided ownership" in Visser DP (ed) *Essays on the history of law* (Juta Cape Town 1989) 213-260

Van Hoecke M “Legal doctrine - which method(s) for what kind of discipline?” in *Methodologies of legal research: what kind of methods for what kind of discipline* (Hart Publishing Oxford 2011) 1-18

Vinogradoff P “The organisation of Kinship” in Krader L (ed) *Anthropology and early law* (Basic Books Inc. New York 1966) 57-74

W

Watney M “Cybercrime and the investigation of cybercrime” in Papadopoulos S and Snail S (eds) *Cyberlaw @SA III: The law of the internet in South Africa* (Van Schaik Publishers Hartfield 2012) 333-351

Williams MR “A preview of things to come - some remarks on the first generation of computers” in Rojas R and Hashagen U (eds) *The first computers: history and architectures* (Massachusetts Institute of Technology Massachusetts 2000) 1-16

Wyatt S, Thomas G and Terranova T “They came, they surfed, they went back to the beach - conceptualising use and non-use of the Internet” in Woolgar S (ed) *Virtual society? technology cyberbole, reality* (Oxford University Press Oxford 2002) 23-40

Y

Yeung K “Towards an understanding of regulation by design” in Bownsword R and Yeung K (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* ((Hart Publishing Portland 2008) 79-107

Z

Zhang D and Yu L “Biometrics for security in e-commerce” in Kou W (ed) *Payment technologies for e-commerce* (Springer Berlin 2003) 71-94

Zhang F and Wang Y “Security fundamentals” in Kou W (ed) *Payment technologies for e-commerce* (Springer Berlin 1998) 7-38

3. JOURNAL ARTICLES

A

Artz D and Gil Y "A survey of trust in computer science and the semantic web" 2007 (5) *Journal of Web Semantics* 58-71

B

Bajaj R and Chaudhury S "Signature verification using multiple neural classifiers" 1997 (30) *Pattern Recognition* 1-7

Baldwin R "Better regulation in troubled times" 2006 (1) *Health Economics, Policy and Law* 203-207

Bazelon E, Dana L, Choi YJ and Conaty JF "Computer crimes" 2006 (43) *The American Criminal Law Review* 260-308

Beck U "From industrial society to the risk society – questions of survival, social structure and ecological enlightenment" 1992 (9) *Theory, Culture and Society* 97-123

Benson BL "It takes two invisible hands to make a market – *Lex Mercatoria* (Law Merchant) always emerges to facilitate emerging market activity" 2010 (3) *Studies in Emerging Order* 100-128

Berg T "The changing face of cybercrime – New Internet threats create challenges to law enforcement" 2007 (86) *Michigan Bar Journal* 18-22

Birks P "The Roman Law concept of *dominium* and the idea of absolute ownership" 1985 *Acta Juridica* 1-37

Bodansky D "Scientific uncertainty and the precautionary principle" 1991 (33) *Law, Environment: Science and Policy for Sustainable Development* 4-5

Bouckaert B "What is property?" 1990 (13) *Harvard Journal of Law and Public Policy* 775-816

Braithwaite J “The new regulatory state and the transformation of criminology” 2000 (40) *British Journal of Criminology* 222-238

Bretscher P and Cohn M “A theory of self-non-self discrimination” 1970 (169) *Science* 1042-1049

Brickey KF “The jurisprudence of larceny – an historical inquiry and interest analysis” 1980 (33) *Vanderbilt Law Review* 1101-1142

Brown EAR “The Tyranny of a construct – feudalism and historians of mediaeval Europe” 1974 (79) *The American Historical Review* 1063-1088

Brownsword R “Code, control, and choice – why East is East and West is West” 2005 (25) *Journal for Legal Studies* 1-21

Burchell J “Criminal justice at the crossroads” 2002 (119) *South African Law Journal* 579-602

Burrows M, Abadi M and Needham R “Logic of authentication” 1990 (8) *ACM Transactions on Computer Systems* 18-36

C

Caleiro C, Viganò L and Basin D “Relating strand spaces and distributed temporal logic for security protocol analysis” 2005 (13) *Logic Journal of the IGPL* 637-663

Campbell J “The development of a B2G authentication standard – a design perspective of the policy consultation process” 2007 (14) *Australasian Journal of Information Systems* 81-94

Canguilhem G “Regulation” 1985 (XV) *Encyclopedia Universalis* 797-799

Cassim F “Formulating specialised legislation to address the growing spectre of cybercrime – A comparative study” 2009 (12) *PER* 36-79

Chang CC and Hwang KF “Some forgery attacks on a remote user authentication scheme using smart cards” 2003 (14) *Journal of Informatica* 289-294

Chang CC and Lee JS “An efficient and secure remote authentication scheme using smart cards” 2006 (18) *International Journal of Information and Security* 122-133

Chang CC, Tsu SM and Chen CY “Remote scheme for password authentication based on theory of quadratic residues” 1995 (18) *Computer Communications* 936-942

Chen BL, Kuo WC and Wuu LC “Robust smart-card-based remote user password authentication scheme” 2012 *International Journal of Communication Systems* http://onlinelibrary.wiley.com/doi/10.1002/dac.2368/pdf (Date of use: 09 October 2013)

Chen TH, Tsai DS and Horng G “Secure user-friendly remote authentication schemes” 2006 (18) *International Journal of Information and Security* 111-121

Cho S, Han C, Han DH and Kim H “Web-based keystroke dynamics identity verification using neutral network” 2000 (10) *Journal of Organisational Computing and Electronic Commerce* 295-307

Chroust AH and Affeldt RJ “The problem of private property according to St. Thomas Aquinas” 1950-1951 (34) *Marquette Law Review* 151-182

Chung M and Solum LB “The layers principle – internet architecture and the law” 2004 (79) *Notre Dame Law Review* 815-948

Conant RC and Ashby WR “Every good regulator of a system must be a model of that system” 1970 (1) *International Journal of Systems Science*

D

Das AK, Sharma P, Chatterjee S and Sing JK “A dynamic password-based user authentication scheme for hierarchical wireless sensor networks” 2012 (35) *Journal of Network and Computer Applications* 1646-1656

Das LM, Saxena A and Gulati VP “A dynamic ID-based remote user authentication scheme” 2004 (50) *IEEE Transactions on Consumer Electronics* 629-631

Dasgupta D, Yu S and Nino F “Recent advances in artificial immune systems – models and applications 2011 (1) *Applied Soft Computing* 1574-1587

De Araujo M “Hugo Grotius, contractualism, and the concept of private property – an institutionalist interpretation” 2009 (26) *History of Philosophy Quarterly* 353-371

DeFur PL and Kaszuba M “Implementing the precautionary principle” 2002 (288) *The Science of Total Environment* 155-165

Dereli T and Tucker RW “Signature dynamics in general relativity” 1993 (10) *Classical and Quantum Gravity* 365-373

Doddington GR “A method of speaker verification” 1971 (49) *The Journal of the Acoustical Society of America*

Duff PW “*Furtum* and Larceny” 1954 (12) *The Cambridge Law Journal* 86-88

E

Erlank W “Acquisition of ownership inside virtual worlds” 2013 *De Jure* 770-782

F

Fisher E “Is the precautionary principle justiciable?” 2001 (13) *Journal of Environmental Law* 315-334

Fletcher GP “The metamorphosis of larceny” 1976 (89) *Harvard Law Review* 469-530

Ford CL “New governance, compliance, and principles-based securities regulation” 2008 (45) *American Business Law Journal* 1-60

Forrester JW “Industrial dynamics - a major breakthrough for decision makers” 1958 (36) *Harvard Business Review*

Frazel TD “’Furtum’ and the description of stolen objects in Cicero ‘In Verrem’’ 2005 (126) *The American Journal of Philosophy* 363-376

Fröschke S “Adding branching to the strand space model” 2009 (242) *Theoretical Computer Science* 139-159

Furui S “Cepstral analysis technique for automatic speaker verification” 1981 (29) *IEEE Transactions on Accounts, Speech, and Signal Processing* 254-272

G

Garber L “Denial-of-service attacks rip the Internet” 2000 *Technology news* 1-17

Gilad S “It runs in the family – meta-regulation and its sibling” 2010 (4) *Regulation and Governance* 485-506

Granova P and Eloff JHP “A legal overview of phishing” 2005 *Computer Fraud and Security* 6-11

Gray K “Property in thin air” 1991 (50) *Cambridge Law Journal* 252-307

Greenleaf G “An endnote on regulating cyberspace – architecture vs law” 1998 (21) *UNSW Law Journal* 593-622

Griemmelmann JTL “Virtual worlds as comparative law” 2004 (49) *New York Law School Law Review* 147-184

Grimmelmann J “Regulation by software” 2005 (114) *The Yale Law Journal* 1719-1758

Guttman JD “Authentication tests and disjoint encryption – a design method for security protocols” 2004 (12) *Journal of Computer Security* 409-433

Guttman JD “Key compromise, strand spaces, and the authentication tests” 2001 (45) *Theoretical Computer Science* 141-161

Guttman JD and Thayer FJ “Authentication tests and the structure of bundles” 2002 (283) *Theoretical Computer Science* 333-380

H

Halpern JY and Pucella R “On the relationship between strand spaces and multi-agent systems” 2003 (6) *ACM Transactions on Information and System Security* 43-70

Henning JJ and Ebersöhn GJ “Insider trading, money laundering and computer crime” 2001 *Transactions of the Centre for Business Law* 105-152

Hofmeyr SA and Forrest S “Architecture for an artificial immune system” 1999 (7) *Evolutionary Computation* 45-68

Horowitz SJ “Competing Lockean claims to virtual property” 2007 (20) *Harvard Journal of Law & Technology* 443-458

Howells M “Beware cybersquatters and typosquatters” 2002 (20) *Ancestry Magazine* 55-58

Hsiang HC and Shih WK “Improvement of the secure dynamic ID-based remote user authentication for multi-server environment” 2009 (31) *Journal of Computer Standards and Interfaces* 1118-1123

Huang K and Yan H “Off-line signature verification based on geometric feature extraction and neural network classification” 1997 (30) *Pattern Recognition* 9-17

J

Jankowich AE “Property and democracy in virtual worlds” 2005 (11) *Boston University Journal of Science and Technology Law* http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume112/JankowichArticleWEB.pdf%3Fq%3Dproperty-and-democracy-in-virtual-worlds (Date of use: 04 December 201)

Johnson DR and Post D “Law and borders – the rise of law in cyberspace” 1996 (48) *Stanford Law Review* 1366-1402

K

Kerr C “The origin and development of the Law Merchant” 1929 (15) *Virginia Law Review* 350-364

Kesan JP and Shah JC “Deconstructing code” 2003 (6) *Yale Journal of Law and Technology* 277-389

Kim K “Mixed systems in legal origins analysis” 2010 (83) *Southern California Law Review* 693-730

Kinnunen T and Li H “An overview of text-independent speaker recognition – from features to supervisors” 2010 (52) *Speech Communication* 12-40

Kroeze IJ “Legal research methodology and the dream of interdisciplinarity” 2013 (16) *Potchefstroom Electronic Law Journal* 36-65

L

Lamport L “Password authentication with insecure communication” 1981 (24) *Communications of the ACM* 770-772

Lastowka FG and Hunter D “The laws of the virtual worlds” 2004 (92) *California Law Review* 1-75

Lederman L “Stranger than fiction – Taxing virtual worlds” 2007 (82) *New York University Law Review* 1620-1672

Lessig L “The law of the horse – what cyberlaw might teach” 1999 (113) *Harvard Law Review* 501-549

Lessig L “The New Chicago School” 1998 (27) *The Journal of Legal Studies* 661-691

Lessig L “The path of cyberlaw” 1995 (104) *The Yale Law Journal* 17-46

Li LH, Lin IC and Hwang MS “A remote password authentication scheme for multiserver architecture using neural networks” 2001 (12) *IEEE Transactions on Neural Networks* 1498-1504

Lofsterdt RE “The precautionary principle – risk, regulation and politics” 2003 (81) *Trans IChemE* 36-43

Lummis RC “Implementation of an online speaker verification scheme” 1972 (52) *The Journal of the Acoustical Society of America*

Lummis RC “Real-time technique for speaker verification by computer” 1971 (50) *The Journal of the Acoustical Society of America*

M

Ma J and Orgun MA “Formalising theories of trust for authentication protocols” 2008 (10) *Information Systems Frontiers* 19-32

Ma J, Orgun MA and Sattar A “Analysis of authentication protocols in agent-based systems using labelled tableaux” 2009 (39) *IEEE Transactions on Systems, Man and Cybernetics* 889-900

Martin PH “If you don’t know how to fix it, please stop breaking it! the precautionary principle and climate change” 1997 (2) *Foundations of Science* 263-292

Martinez MG, Fearne A, Caswell JA and Henson S “Co-regulation as a possible model for food safety governance - opportunities for public–private partnerships” 2007 (32) *Food Policy* 299-314

Matzinger P “The danger model – a renewed sense of self” 2002 (296) *Science* 301-305 301

McElroy D and Turban E “Using smart cards in electronic commerce” 1998 *International Journal of Information Management* 61-72

McIntyre O and Mosedale T “The precautionary principle as a norm of customary international law” 1997 (9) *Journal of Environmental Law* 221-241

McSweeney TJ “Property before property – Romanising the English law of land” 2012 (60) *Buffalo Law Review* 1139-1199

Mefford A “*Lex Informatica* – foundations of law on the Internet” 1997 (5) *Indiana Journal of Global Legal Studies* 211-237

Minnaar A “You’ve received a greeting e-card from.... – the changing face of cybercrime email spam scams” 2008 (2) *Acta Criminologica* 92-116

Monrose F and Rubin AD “Keystroke dynamics as a biometric for authentication” 2000 (16) *Future Generation Computer Systems* 351-359

Morgan B “The economisation of politics – meta-regulation as a form of nonjudicial legality” 2003 (12) *Journal of Social and Legal Studies* 489-523

Moringiello JM “What virtual worlds can do for property law” 2010 *Widener University School of Law* 1-50

Morris S and Thompson K “Password security: a case history” 1979 (22) *Communications of the ACM* 594-597

N

Needham RM and Schroeder MD “Using Encryption for Authentication in Large Networks of Computers” 1978 (21) *Communications of ACM* 993-999

Newe T and Coffey T “Realisation of a minimum-knowledge identification and signature scheme” 1998 (17) *Computers and Security Journal* 253-264

Njotini M “The transaction or activity monitoring process: an analysis of the customer due diligence (CDD) systems of the United Kingdom and South Africa” 2010 (31) *Obiter* 556-573

O

O’Rahilly A “S. Thomas’s theory of property” 1920 (9) *Studies: An Irish Quarterly Review* 337-354

Oghenerukeybe EA “Customers perception of security indicators in online banking sites in Nigeria” 2009 (14) *Journal of Internet Banking and Commerce* 1-15

P

Plamondon R and Lorette G “Automatic signature verification and writer identification – the state of the art” 1989 (22) *Pattern Recognition* 107-131

R

Rapalje S “Larceny distinguished from other offences” 1892 (14) *The Criminal Law Magazine and Reporter*

Rasdale M “Denial of service attacks - legislating for robots and zombies” 2006 (22) *Computer Law and Security Report*

Rayner S and Cantor R “How fair is safe enough? – the cultural approach to societal technology choice” 1987 (7) *Risk Analysis* 3-9

Reidenberg JR “*Lex Informatica* – the formulation of information policy rules through technology” 1998 (76) *Texas Law Review* 553-584

Resnik DB “Is the precautionary principle unscientific?” 2003 (34) *Studies in History and Philosophy of Biological and Biomedical Sciences* 329-344

Robinson JA, Liang VM Chambers JA and MacKenzie CL “Computer user verification using login string keystroke dynamics” 1998 (28) *IEEE Transactions on Systems, Man, and Cybernetics* 236-241

S

Samuel G “Is law really a social science? – a view from comparative law” 2008 (67) *The Cambridge Law Journal* 288-321

Samuelson P “Is information property?” 1991 (34) *Communications of the ACM* 15-18

Sandin P “Dimensions of the precautionary principle” 1999 (5) *Human and Ecological Risk Assessment* 889-907

Santillo D, Stringer RL, Johnson PA and Tickner J “The precautionary principle – protecting against failures of scientific method and risk assessment” 1998 (36) *Marine Pollution Bulletin* 939-950

Schafer RW and Rabiner LR “System for automatic formant analysis of voiced speech” 1970 (47) *The Journal of the Acoustical Society of America* 634-648

Schneier B “Two-factor authentication - too little, too late” 2005 (48) *Communications of the ACM* 136

Schraw G, Crippen KJ and Hartley K “Promoting self-regulation in science education - metacognition as part of a broader perspective on learning” 2006 (36) *Research in Science Education* 111-139

Sciglimpaglia RJ “Computer hacking - a global offense” 1991 (3) *Pace International Law Review* 199-266

Scott H “Absolute ownership and legal pluralism in Roman law – two arguments” 2011 *Acta Juridica* 23-34

Scurlock J “The element of trespass in larceny at Common Law” 1948 (22) *Temple Law Quarterly* 12-45

Shanmugapriya N and Padmavathi G “A survey of biometric keystroke dynamics – approaches, security and challenges” 2009 (5) *International Journal of Computer Science and Information Security* 115-119

Stuart D “An entrenched bill of rights best protects against law and order expediency” 1998 (11) *South African Journal of Criminal Justice* 325-336

Sun HM “An efficient remote use of authentication scheme using smart cards” 2000 (46) *IEEE Transactions on Consumer Electronics* 958-961

Sunstein CR “Beyond the precautionary principle” 2003 (151) *University of Pennsylvania Law Review* 1003-1058

Sunstein CR “The laws of fear” 2001 (128) *John M. Olin Law & Economics Working Paper* 1-42

Syverson P “Towards a strand semantics for authentication logic” 1999 (20) *Theoretical Computer Science* 1-15

T

Thayer FJ and Herzog JC “Strand spaces – proving security protocols correct” 1999 (7) *Journal of Computer Security* 191-230

Tierney B “Permissive natural law and property – Gratian to Kant” 2001 (62) *Journal of the History of Ideas* 381-399

Trakman LE “From the medieval Law Merchant to E-Merchant Law” 2003 (53) *University of Toronto Law Journal* 265-304

V

Van der Walt AJ “The enforceability of tenant’s rights” 2012 (1) *TSAR* 35-52

Van der Walt AJ “Towards a theory of rights in property - exploratory observations on the paradigm of post-apartheid property law” 1995 (10) *SA Public Law* 298-345

Vandevelde KJ “The new property of the nineteenth century – the development of the modern concept of property” 1980 (29) *Buffalo Law Review* 325-367

Vercelli A “From soft uncertainty to hard environmental uncertainty” 1995 (48) *Economie Appliquée* 251-269

Vick DW “Interdisciplinarity and the discipline of law” 2004 (31) *Journal of Law and Society* 163-193

Visser DP “The ‘absoluteness’ of ownership – the South African common law perspective” 1985 *Acta Juridica* 39-52

Volokh A “Property rights and contract form in Medieval Europe” 2009 (VII) *American Law and Economics Review* 399-459

W

Watney M “Identity theft - the mirror reflects another face” 2004 (3) *TSAR* 511-519

Watson A “The Definition of Furtum and the Trichotomy” 1960 (28) *Tijdschrift voor Rechtsgeschiedenis* 197-210

Weinrib AS “Information and property” 1988 (38) *The University of Toronto Law Journal* 117-150

Wen F and Li X “An improved dynamic ID-based remote user authentication with key agreement” 2012 (38) *Journal of Computers and Electrical Engineering* 381-387

Westbrook TJ “Owned – finding a place for virtual world property rights” 2006 (779) *Michigan State Law Review* 779-812

Whitson JR “Identity theft and the challenge of caring for your virtual self” 2000 (51) *British Journal of Sociology* 605-622

Wiener JB “The regulation of technology, and the technology of regulation” 2004 (26) *Journal of Technology in Society* 483-500

Wilson R “Analysing the daily risks of life” 1979 *Technology Review* 41-46 41

Wu ST and Chieu BC “A user-friendly remote authentication scheme with smart cards” 2003 *Journal of Computers and Security* 547-550

Wu TC and Sung HS “Authenticating passwords over insecure channels” 1996 *Journal of Computer and Security* 431-439

Y

Yang L, Widjaja BK and Prasad R “Application of Hidden Markov Models for signature verification” 1995 (28) *Pattern Recognition* 161-170

4. CONFERENCE PROCEEDINGS

A

Aickelin U and Cayzer S “The danger theory and its application to artificial immune systems” (Papers delivered at the 1st Intentional Conference on ARtificial Immune Systems (ICARIS-2002), 2002 Canterbury) 141-148

C

Campbell JP “Testing with the YOHO CD-Rom voice verification corpus” in *Acoustics, speech, and signal processing* (Paper delivered at the International Conference on Acoustics, Speech, and Signal Processing, *1995* 9-12 May 1995 IEEE Detroit) 341-344

F

Fogg BF and Tseng H “The elements of computer credibility” in *Computing systems* (Papers delivered at the International Conference on Human Factors in Computing Systems 18-20 May 1999 Association of Computing Machinery Inc New York 1999) 80-87

H

Hofmeyr SA and Forrest S “Immunity by design - an artificial immune system” in *Genetic and evolutionary computation* (Papers presented at the Genetic and Evolutionary Computation Conference (GECCO-99) Orlando, Florida 1999) 1289-1296

M

Ma J, Logrippo L, Adi K and Mankovski S “Risk analysis in access control systems based on trust theories” in *Web intelligence and intelligent agent technology* (Paper delivered at the 2010 IEEE Conference on Web Intelligence and Intelligent Agent Technology 31 August-3 September 2010 IEEE Toronto) 415-418

Mauceri AJ “Feasibility studies of personal identification by signature verification” (Report No: SID 65 24RADC TR65 33, Space and Information Division, North American Aviation Company Anaheim 1965)

N

Nelson W and Kishon E “Use of dynamic features for signature verification” in *Systems, management, and cybernetics* (Papers delivered at the IEEE International Conference on Systems, Management, and Cybernetics 17-20 October 1991 IEEE Le Touquet) 17-20

P

Pellom BL and Hansen JHL “An experimental study of speaker verification sensitivity to computer voice-altered imposters” in *Acoustics, speech, and signal processing* (Papers delivered at the IEEE International Conference on Acoustics, Speech, and Signal Processing, 1999 15-19 March 1999 IEEE Phoenix) 837-840

Perring A and Song D “Looking for diamonds in the desert – extending automatic protocol generation to three-party authentication and key protocols” in *Computer Security* (Papers delivered at the Foundations Workshop on Computer Security 3-5 July 2000)

Purasa M and Brodley CE “User re-authentication via mouse movements” in *Visualization and Data Mining for Computer Security* (Papers delivered at the 2004 ACM workshop on Visualization and Data Mining for Computer Security 29 October 2004 IEEE New York) 1-8

R

Reynolds DA “An overview of automatic speaker recognition technology” in *Acoustics, speech, and signal processing (ICASSP)* (Papers delivered at the IEEE International

Conference on Acoustics, Speech, and Signal Processing (ICASSP) 13-17 May 2002 IEEE Florida) IV-4072-IV-4075

S

Saevanee H and Bhattarakosol P "Authenticating user using keystroke dynamics and finger pressure" in *Consumer communications and networking* (Papers delivered at the 2009 6th IEEE consumer communications and networking conference 11-13 January 2009 Institute of Electrical and Electronic Engineers New York 2009) 1-2

T

Thayer F, Herzog JC and Guttman JD "Mixed strand spaces" in *Computer Security Fundamentals* (Papers delivered at the 12th Computer Security Foundations Workshop 30 June 1999 IEEE Los Alamitos) 72-82

Thayer FJ and Herzog JC "Strand spaces – why is a security protocol correct?" in *Security and Privacy* (Papers delivered at the IEEE Symposium on Security and Privacy 3-6 May 1998 IEEE Oakland) 160-171

Thayer FJ, Herzog JC and Guttman JD "Honest ideals on strand spaces" in *Computer Security* (Papers delivered at the 11th IEEE Computer Security Foundations Workshop 9-11 June 1998 The Institute of Electrical and Electronics Engineers Inc. Los Alamitos) 66-78

V

Vacca RG "Viewing virtual property ownership through the lens of innovation" in *Virtual property* (Papers delivered at the 2008 Cornell Law Student Inter-University Graduate Student Conference Paper 3 June 2008 Carnell University) 1-28

Van der Merwe D "Criminal law – your partner in preventing information loss" (Paper presented at the *Lex Informatica* Conference on 23 May 2008)

Z

Zheng N, Paloski A and Wang H "An efficient user verification system via mouse movements" in *Computer and communications security* (Papers delivered at 18th ACM

conference on Computer and communications security 17-21 October 2011 ACM New York) 139-150

5. ARTICLES

C

COMEST “The precautionary principle” March 2005

Commission of the European Communities “Communication from the Commission on the precautionary principle” 2 February 2000

Commission of the European Communities “Proposal for a Council framework decision on attacks against information systems” 19 April 2002

Commission of the European Communities “Proposal for a Directive of the European Parliament and of the Council on Payment Services in the Internal Market and amending Directive 97/7/EC, 2000/12/EC and 2002/65/EC” 1 December 2001

E

European Commission “Smart regulation in the European Union” 8 October 2010

G

Gaines R, Lisowski W, Press S and Shapiro N “Authentication by keystroke timing – some preliminary results” May 1980

I

Industry Canada “Principles for electronic authentication – a Canadian framework” May 2004

U

UNCITRAL “Legal guide on electronic funds transfer” 1987

UNCITRAL “Promoting confidence in electronic commerce: legal issues on international use of electronic authentication” 2009

6. INTERNET SOURCES

A

APWG “Global phishing survey – trends and domain name use in 2h2011” http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2011.pdf (Date of use: 22 July 2012)

APWG “Phishing activity trends report – 1st quarter 2012” http://www.antiphishing.org/reports/apwg_trends_report_q1_2012.pdf (Date of use: 22 July 2012)

APWG “Uniting the global response to cybercrime” http://www.antiphishing.org/ (Date of use: 13 September 2012)

Arde A “How crooks use SIM swaps to rob you” http://www.iol.co.za/business/personal-finance/banking/how-crooks-use-sim-swaps-to-rob-you-1.1507185 (Date of use: 28 October 2013)

B

Barlow JP “Selling wine without bottles - the economy of mind on the global net” http://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/idea_economy_article.html (Date of 13 October 2012)

Barlow JP “The economy of ideas - selling wine without bottles on the global net” https://projects.eff.org/~barlow/EconomyOfIdeas.html (Date of use: 24 October 2012)

Berinato S “FFIEC: Second Thoughts on Second Factors” http://www.csoonline.com/article/220784/FFIEC_Second_Thoughts_on_Second_Factors (Date of use: 22 April 2010)

BusinessDay “Vodacom accused duped lawyers, court hears” http://www.bdlive.co.za/articles/2009/11/26/vodacom-accused-duped-lawyers-court-hears;jsessionid=5ADC6353F964516D33B8D9D2450B64DC.present2.bdfm (Date of use: 28 October 2013)

BusinessWeek “This bug is nasty, brutish, and sneaky” http://www.businessweek.com/magazine/content/06_15/b3979068.htm (Date of use: 14 January 2010)

Byrne E “What is internet infrastructure?” http://edbyrne.me/what-is-internet-infrastructure/ (Date of use: 26 September 2012)

C

Center for Strategic and International Studies “Net losses – estimating the global cost of cybercrime” http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf (Date of use: 13 April 2016).

CIFAS “Digital thieves – a special report on online fraud” http://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/Digital_Thieves_October2010.pdf (Date of use: 20 August 2012)

CIFAS “Fraudscape – depicting the UK’s fraud landscape” https://www.cifas.org.uk/secure/contentPORT/uploads/documents/reports/Confidential-%20Fraudscape%202011.pdf (Date of use: 13 July 2012)

CIFAS “The anonymous attacker – a special report on identity fraud and account take over” http://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/The_Anonymous_Attacker_CIFAS_Special_Report_Oct_2009.pdf (Date of use: 13 June 2012)

Click2Houston.com http://www.click2houston.com/rducation/4152951/detail.html (Date of use: 14 January 2010

Consumer Report http://www.consumerreports.org/cro/magazine-archive/2010/june/electronics-computers/social-insecurity/state-of-the-net-2010/index.htm (Date of use: 24 July 2012)

Consumer Report Magazine “State of the net 2009” http://www.consumerreports.org/cro/magazine-archive/june-2009/electronics-computers/state-of-the-net/state-of-the-net-2009/state-of-the-net-2009.htm (Date of use: 24 July 2012)

Council of the European Union and Commission of the European Communities (2000) "Digital agenda for Europe – a Europe 2020 initiative" http://ec.europa.eu/information_society/eeurope/2002/action_plan/pdf/actionplan_en.pdf (Date of use: 16 June 2012)

D

Dutton WH and Shepherd A "Confidence and risk on the Internet" http://www.bis.gov.uk/files/file15271.pdf (Date of use: 13 May 2013)

E

Estes A and Jan T "Boston Latin teen is accused of hacking" http://www.boston.com/news/local/articles/2006/04/29/boston_latin_teen_is_accused_of_hacking/ (Date of use: 14 January 2010)

European Commission http://ec.europa.eu/governance/better_regulation/documents/brochure/br_brochure_en.pdf (Date of use: 13 November 2012)

European Consumer Organisation "Smart regulation – BEUC response to the stakeholder consultation" http://ec.europa.eu/smart-regulation/consultation_2012/docs/registered_organisations/beuc_en.pdf (Date of use: 13 March 2016).

European Union (EU) Fraud Prevention Expert Group (FEPG) "Preventing payment fraud in Europe" http://ec.europa.eu/internal_market/fpeg/identity-theft_en.htm (Date of use: 20 July 2012)

European Union "Internal security strategy for the European Union – towards a European security model" https://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf (Date of use: 16 November 2015)

F

Federal Financial Institutions Examination Council (FFIEC) “Authentication in an internet banking environment” http://www.ffiec.gov/pdf/authentication_guidance.pdf (Date of use: 13 July 2013)

Flemming RA “The importance of smart regulation” https://www.sec.gov/news/speech/importance-of-smart-regulation.html (Date of use: 13 March 2016).

Fripp C “Cybercrime costs South Africa about R5.8 billion a year” http://htxt.co.za/2014/11/11/cybercrime-costs-south-africa-about-r5-8-billion-a-year/ (Date of use: 13 April 2016).

G

Guy M “Cyber security policy will go before cabinet for approval this year” http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=13783 (Date of use: 16 November 2015)

H

Hjørland B and Nicolaisen J “Systems theory” http://www.iva.dk/jni/lifeboat-_old/Positions/Systems%20theory.htm (Date of use: 10 December 2012)

Huntington “The business of authentication” http://www.authenticationworld.com (Date of use: 13 February 2010)

HPCSA “Vision and mission” http://www.hpcsa.co.za/About/VisionMission (Date of use: 13 April 2016)

I

Independent Police Investigative Directorate of the Republic of South Africa “Batho Pele Principles” http://www.ipid.gov.za/about%20us/batho_pele.asp (Date of use: 27 January 2014)

M

MarkMonitor “Corporate overview” https://www.markmonitor.com/company/overview.php (Date of use: 13 September 2012)

MarkMonitor “Typosquatting continues to pose dangers to enterprises, consumers” https://www.markmonitor.com/mmblog/typosquatting-continues-to-pose-dangers-to-enterprises-consumers/ (Date of use: 20 August 2012)

Military Analysis Network “TRW” http://www.fas.org/man/company/trw.htm (Date of use: 13 June 2012)

O

OECD “About the OECD” http://www.oecd.org/about/ (Date of use: 13 September 2012)

OECD Directorate for Science, Technology and Industry Committee on Consumer Policy Committee for Information, Computer and Communications Policy http://www.oecd.org/dataoecd/63/28/36494147.pdf (Date of use: 13 May 2012)

Ornaghi A “Man in the middle attacks – demos” http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-ornaghi-valleri.pdf (Date of use: 13 August 2013)

P

Parliamentary Monitoring Group (PMG) http://www.pmg.org.za/parlinfo/sectionb3 (Date of use: 2 November 2012)

R

Reid CE “History of phishing” http://www.allspammedup.com/2009/02/history-of-phishing/ (Date of use: 22 April 2010)

S

Scholten DL “A primer for Conant and Ashby’s ‘Good Regulator Theorem’” http://www.goodregulatorproject.org/images/A_Primer_For_Conant_And_Ashby_s_Good-Regulator_Theorem.pdf (Date of use: 18 December 2012)

Scholten DL “Every good key must be a model of the lock it opens – (The Conant and Ashby Theorem revisited) http://www.goodregulatorproject.org/images/Every_Good_Key_Must_Be_A_Model_Of_The_Lock_It_Opens.pdf (Date of use: 18 December 2012)

Science and Environmental Health Network “The Wingspread statement on the precautionary principle” http://www.sehn.org/state.html#w (Date of use: 19 November 2013)

Scott WR “Institutional theory – contributing to a theoretical research program” http://icos.groups.si.umich.edu/Institutional%20Theory%20Oxford04.pdf (Date of use: 13 May 2011)

Securelist “Changing threats, changing solutions – a history of viruses and antivirus” http://www.securelist.com/en/analysis/204791996/Changing_threats_changing_solutions_A_history_of_viruses_and_antivirus (Date of use: 5 July 2010)

South African Accreditation Authority “Functions and powers” http://www.saaa.gov.za/index.php/background.html (Date of use: 5 November 2015)

South African Law Commission “Computer-related crime – options for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects” http://www.justice.gov.za/salrc/dpapers/dp99_prj108_comp_2001jul.pdf (Date of use: 13 May 2012)

Sunstein CR “Precautions against what? – the availability heuristic and cross-cultural perceptions” http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1371&context=law_and_economics (Date of use: 18 January 2016)

T

The Javelin Strategy and Research “2010 identity fraud survey report – consumer version” https://www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveyConsumer.pdf (Date of use: 13 May 2012)

Treasury Board of Canada Secretariat “Framework for the management of risk” http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422 (Date of use: 13 June 2013)

U

UK Cabinet Office “Making travel safer in cyberspace” http://www.cabinetoffice.gov.uk/news/making-travel-safer-cyberspace (Date of use: 18 July 2012)

UK Cabinet Office “The UK cyber security strategy – protecting and promoting the UK in a digital world” http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf (Date of use: 10 May 2012)

TABLE OF STATUTES

1. CONSTITUTIONS

Constitution of the Republic of South Africa, 1996

2. STATUTES

Canada Evidence Act, 1985

Civil Proceedings Evidence Act 25 of 1965

Communications Act of 2003

Computer Evidence Act 57 of 1983

Copyright Act 98 of 1978

Cybercrime and Cybersecurity Bill of 2015

Draft Cybercrime and Cybersecurity Bill of 2015

Drugs and Drug Trafficking Act 120 of 1992

Dutch Policy Memorandum Legislation for the Electronic Highways of 1998

Electronic Communications Act, 2000

Electronic Communications and Transactions Act 25 of 2002

Electronic Communications and Transactions Amendment Bill, 2012

Fair Credit Reporting Act, 1996

Financial Intelligence Centre Act 38 of 2001

Game Theft Act 105 of 1991

Larceny Act of 1916

Law of Succession Amendment Act 43 of 1992

Personal Information Protection and Electronic Documents Act, 2000

Proceeds of Crime Act 76 of 1996

Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004

Protection of Personal Information Act 4 of 2013

Secure Electronic Signature Regulations, 2005

State Information Technology Agency Act 88 of 1998

The Law of the Twelve Tables

Theft Act of 1968

3. REGULATIONS AND PROCLAMATIONS

Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014

GN R1596 *GG* 24176 of 20 December 2002

GN R8701 *GG* 29995 of 20 June 2007

Proc R309 *GG* 30873 of 14 March 2008

4. POLICIES AND NOTICES

Draft National Cyber-security Policy of South Africa of May 2011

Notice 1537 of 2004

TABLE OF CASES

In the Goods of Savoy (1851) 15 Jur. 1042

Investgold CC v Uys & Another (686/2013) [2014] ZASCA 166 (1 October 2014)

Isaacman v Miller 1922 TPD 56

Jajbhay v Cassim 1939 AD 537

Jhajbhai and Others v Master and Another 1971 2 D. & C.L.D. 370

Kazazis v Georghiades 1979 3 TPD 886

Lawrence v Commissioner of the Police for the Metropolis [1971] 2 All ER 1253

Liebenberg v Koster Village Council 1935 TPD 413

Lozentz v Melle 1978 3 SA 1044 (T)

Macduff & Co Ltd (in liquidation) v Johannesburg Consolidated Investment Co Ltd 1924 AD 573

McAdams v Fiander's Trustee & Bell NO 1919 AD 207

Millar v Taylor (1769) 98 E.R. 201

Mohr v Great Barrier Reef Marine Park Authority [1998] AATA 805

Naidoo v Moodley 1982 4 SA 82 (TPD)

Ndlovu v Minister of Correctional Services 2006 (4) SA 165 (W)

Nissan South Africa (Pty) Limited v Marnitz No and Others (stand 1 at 6 Aeroport (Pty) Limited intervening), 2005 1 SA 441 (SCA)

O'Keeffe v Argus Printing and Publication Co Ltd 1954 (3) SA 244 (C)

Odendaalsrus Gold, General Investments and Extensions Ltd v Registrar of Deeds 1953 1 SA 600 (O)

Oxford v Moss (1979) 68 Cr. App. R. 183

Pearly Beach Trust v Registrar of Deeds 1990 4 SA 614 (C)

Phame (Pty) Ltd v Paizes [1973] 3 All SA 501 (A) 514

Powell v van der Merwe [2005] 1 All SA 149 (SCA) 162

Preller v Jordaan 1956 1 AD 483

Putter v Provincial Insurance Co Ltd and Another 1963 (3) SA 145 (W)

R v Ashwell 16 Q. B. D. 190

R v Dane 1957 2 SA 472 (N)

R v Dier (1883-1884) 3 EDC 436

R v Fortuin (1880-1884) 1 Buch AC 290 299

R v Herholdt and Others [1957] 3 All SA 105 (A)

R v Holloway 1 Den. C.C. 370

R v Hudson [1943] 1 K. B. 458

R v Laforte 1922 CPD 487

R v Lawrence [1970] 3 All ER 933

R v Lessing (1907) 21 EDC 220

R v Makogo 1915 TPD 516

R v Mtshali [1960] 4 All SA 156 (N) 158

R v Murphy and Another (1990) 20 EDC 62

R v Offley (1986) 45 Alta. L.R. (2d) 23

R v Olivier and Others 1921 TPD 120

R v Sibiya [1955] 4 All SA 312 (A) 418

R v Stanbridge [1959] 3 All SA 218 (C)

R v Umfaan 1908 TS 62

Regina v Stewart 149 D.L.R. (3d) 583

Ricketts v Byrne and Another 2004 (6) SA 474 CPD

S v A 1971 (2) TPD 293

S v Graham [1975] 3 All SA 572 (A)

S v Harper and another 1981 2 SA 638 (D)

S v Kgogong 1980 3 SA 600 (A)

S v Kotze 1961 (1) SA 118 (SCA)

S v Mashiyi 2002 (2) SACR 387 (Tk)

S v Mintoor 1996 1 SASV 514 (K)

S v Ndebele and Others 2012 1 SACR 245 (GSJ)

S v Ndiki 2008 (2) SACR 252 (Ck)

S v Nedzamba 1993 1 SACR 673 (V)

S v Van den Berg 1991 (1) SACR 104 (T)

Shaaban Bin Hussein v Chonk Fook Kam [1969] 3 All ER 1626

Spring Forest Trading v Wilberry (725/13) [2014] ZASCA 178 (21 November 2014)

Thomas Marshall (Exports) Ltd. v Guinle [1978] 3 All E.R. 193

Thorn v Dickens [1906] W.N. 54

TRW v Andrews, 534 U.S. 19 (2001)

INTERNATIONAL CONVENTIONS OR DIRECTIVES

Council of Europe's Convention on Cybercrime of 23 November 2001

Directive of the European Parliament and of the Council on a Community Framework for Electronic Signatures of 13 December 1999

Directive of the European Parliament and of the Council on Payment Services in the Internal Market of 13 November 2007

Dutch Policy Memorandum Legislation for the Electronic Highways of 1998

European Food Directive, 2002

Ministerial Declaration of the Third International Conference on the Protection of the North Sea, The Hague, 8th March 1990

Rio Declaration on Environment and Development (1992)

The United Kingdom's (the UK) E-Principles

UN Framework Convention on Climate Change, 1992

LIST OF ABBREVIATIONS

AIS	-	Artificial Immune System
AOL	-	American Online
APWG	-	Anti-Phishing Working Group
ATM	-	Auto Teller Machine
BC	-	Behaviour Characterisation
BIS	-	Biological Immune System
CEC	-	Commission of the European Communities
COMEST	-	World Commission on the Ethics of Scientific
		Control Protocol
CPIC	-	Canadian Police Information Centre
DDOS	-	Distributed Denial of Service Development
EFT	-	Electronic Funds Transfer
HTTP	-	Hypertext Transfer Protocol
ICT	-	Information and Communication Technology
IP	-	Internet Protocol Knowledge and Technology
LAN	-	Local Area Network
NCII	-	National Critical Information Infrastructure
NSPKP	-	Needham-Schroeder Public Key Protocol
OECD	-	Organisation for Economic Co-Operation and
OTP	-	One-Time-Password

PA	-	Payment Order
PAEA	-	Precautionary Approach to E-Authentication
PC	-	Personal Computer
PI	-	Payment Institution
PKI	-	Public Key Infrastructure
PO	-	Payment Order
PP	-	Precautionary Principle
PS	-	Payment System
PT	-	Payment Transaction
SA	-	South Africa
TCP	-	Transmission Connection Protocol or Transport
TMACS	-	Trust Model for Access Control Systems
UK	-	United Kingdom
URL	-	Uniform Resource Locator
USA	-	United State of America
USB	-	Universal Serial Bus