CHAPTER 14

PROVING CYBER CRIME

14.1 INTRODUCTION

Evidence is the material used by the State to prove that the perpetrator committed a cyber crime.[1] The State must prove *all* the elements of the cyber crime.[2] The State must prove all the elements of the offence beyond a reasonable doubt, which is a very high standard of proof to meet.[3] The accused is presumed to be innocent until proven guilty[4] and bears no onus[5]. One should clearly distinguish between the admissibility requirements for evidence and the weight or probative value that should be attached to admissible evidence.[6]

The first requirement for evidence to be admissible is that it should be relevant to the specific case.[7] Secondly each specific form of evidence has specific requirements in respect of admissibility that has to be met.[8] Thirdly evidence should be obtained in a constitutional manner having

---

[1] Schmidt & Rademeyer *Bewysreg* (2000) 3; Schmidt & Zeffertt (Revised by D P van der Merwe) *Evidence* (1997) 1.

[2] Schmidt & Rademeyer (footnote 1 *supra*) 52 *et seq*.

[3] Schmidt & Rademeyer (footnote 1 *supra*) 82 *et seq*.

[4] Section 35(3)(h) of the Constitution of the Republic of South Africa, Act 108 of 1996.

[5] Schmidt & Rademeyer (footnote 1 *supra*) 83.

[6] Schmidt & Zeffertt (footnote 1 *supra*) 5.

[7] Schmidt & Rademeyer (footnote 1 *supra*) 387 *et seq*.

[8] Schmidt & Rademeyer (footnote 1 *supra*) 387 *et seq*.

due regard to a person's constitutionally entrenched rights.[9] Section 35(5) of the Constitution[10] states:

> "Evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice."

Unconstitutionally obtained evidence *must* be excluded if the admission of such evidence will render the trial unfair or detrimental to the administration of justice. The court has no discretion in this regard and must exclude the evidence.[11] However the court still has a discretion when determining whether the admission of the evidence will render the trial unfair or detrimental to the administration of justice.[12] Prejudice to the accused, the nature of the prejudice to the accused and public policy are all factors that may assist the court to establish whether the admission of the evidence will render the trial unfair or detrimental to the administration of justice.[13]

Computers, attachments and related components thereto may constitute real evidence. Evidence in computer crimes may also vary from documentary evidence in the form of computer printouts to data contained in a computer system. The data could be encrypted and documents could be digitally signed. In fact a cyber criminal could hide

---

[9] Schmidt & Rademeyer (footnote 1 *supra*) 376 *et seq*.

[10] Act 108 of 1996.

[11] Schmidt & Rademeyer (footnote 1 *supra*) 378.

[12] Schmidt & Rademeyer (footnote 1 *supra*) 378.

[13] Schmidt & Rademeyer (footnote 1 *supra*) 378 *et seq*.

his criminal conduct by making use of cryptography. An expert may be required to explain certain procedures and evidence of a technical nature.

14.2 DOCUMENTARY EVIDENCE, REAL EVIDENCE AND HEARSAY

14.2.1 International position

In an article entitled *Proposed changes to the federal rules of evidence as applied to computer-generated evidence*, Paula N Singer addresses the main problems in respect of the admissibility of computer-generated documents in the United States namely authentication, hearsay and the best evidence rule.[14] Kelman & Sizer suggested *the seven statements* in order to establish the reliability of computer evidence and printouts.[15] This included the qualifications and experience of the person in charge of the computer; a description of the computer system; quality of the individual components, testing and documentation standards of software programs; procedures for logging updates to the software and the qualifications of the staff working with the system; physical and electronic security features; and how did the particular piece of evidence come into existence.[16]

Internationally many countries enacted legislation to provide for the admissibility requirements of computer-generated evidence. For instance

---

[14] (1979) Rutgers Journal of Computers, Technology, and the Law Vol. 7 No. 1 157 *et seq.* Bart D Cohen in *Computer Crime* (1988) American Criminal Law Review Vol. 25 No. 3 369 wrote that the authentication rule, the hearsay rule and the best evidence rule are obstacles in respect of the admission of computer generated evidence.

[15] Kelman & Sizer *The Computer in Court* (1982) 70 *et seq*.

[16] Footnote 15 *supra*.

the Singapore Computer Misuse Act contains specific provisions in respect of the admissibility of computer-generated evidence.[17]

14.2.2 South African responses

It has been said that in a modern technological era one should not force technologically advanced appliances and devices into limited categories such as real evidence and documentary evidence.[18] Many authors rather deal with these types of evidence in a separate category relating to devices and appliances with its own specific requirements of admissibility.[19] Some authors are of the view that when a computer collects information without human intervention, the output of that computer will constitute real evidence.[20] The only requirement in order to prove admissibility is to prove that the computer was reliable and working properly.[21]

Some argue that due to the aspect of human intervention and thought, the output of a computer will constitute documentary evidence.[22] Documentary evidence "consists of statements made in writing which are

---

[17] See Katherine S Williams & Indira Mahalingam Carr *The Singapore Computer Misuse Act – Better Protections for the Victims?* (1994) Journal of Law and Information Science Vol. 5 No. 2 215 *et seq*.

[18] Schmidt & Rademeyer (footnote 1 *supra*) 358; Schmidt & Zeffertt (footnote 1 *supra*) 112.

[19] See footnote 18 *supra* as well as Schwikkard *et al Principles of evidence* (1997) 267 *et seq*.; Van der Merwe (footnote 22 *infra*) 77.

[20] See the case of *The Statute of Liberty* [1968] 2 All ER 195 where the film of radar echoes of ships was found to be real evidence. Since the film was created by mechanical means without human intervention it did not constitute hearsay (A St Q Skeen *Evidence and Computers* (1984) SALJ 680).

[21] *S v Fuhri* 1994 (2) SACR 829 (A).

[22] See in general Dana van der Merwe *Documentary evidence (with specific reference to hearsay)* (1994) Obiter 67.

intended to be relied upon".[23] A document was defined in *S v Daye*[24] as "any written thing capable of being evidence". Section 33 of the Civil Procedure and Evidence Act[25] defines a *document* as including any book, map, plan, drawing or photograph. The requirements for admissibility of documentary evidence are firstly that the document must be relevant and admissible. In other words this means that the document must for example not contain inadmissible hearsay evidence. Secondly the authenticity of the document must be proved.[26] Thirdly the original document must usually[27] be produced.[28]

The Appellate Division held in the case of *Narlis v South African Bank of Athens*[29] that a computer printout was inadmissible in terms of section 34 of the Civil Procedure and Evidence Act.[30] The Court held that a computer is not a person.[31] This decision led to the Law Commission investigating whether legislation was required in respect of computer-

---

[23] Schwikkard et al *Principles of evidence* (1997) 260.

[24] 1908 (2) KB 333 at 340.

[25] Act 25 of 1965. Section 222 of the Criminal Procedure Act provides for the incorporation of the provisions of the Civil Procedure and Evidence Act.

[26] Schwikkard (footnote 23 *supra*) 263; Schmidt & Rademeyer (footnote 1 *supra*) 339 *et seq*.; Schmidt & Zeffertt (footnote 1 *supra*) 104; Van der Merwe *Documentary evidence (with specific reference to hearsay)* (1994) Obiter 68.

[27] There are exceptions to the rule. See footnote 28 *infra*.

[28] "Best evidence rule". See Schwikkard (footnote 23 *supra*) 261-263; Schmidt & Rademeyer (footnote 1 *supra*) 344 *et seq*.; Schmidt & Zeffertt (footnote 1 *supra*) 105 *et seq*.

[29] 1976 (2) SA 573 (A).

[30] See D P van der Merwe *Onlangse ontwikkelinge op die raakvlak tussen rekenaars en die reg* (1991) 54 THRHR 96.

[31] at page 577. Also see *Ex Parte Rosch* [1998] 1 All SA 319.

generated evidence.[32] The Computer Evidence Act[33] was then enacted and was only applicable in civil cases.[34] It made provision for an authenticating affidavit in order to authenticate a computer printout[35], which will then be admissible in civil proceedings.[36] The Act was widely criticised[37] and was finally repealed by the Electronic Communications and Transactions Act[38].

The information and data that is contained in a computer or system are usually entered into the computer or system by a human being. If the person does not testify the information contained in the printout constitutes hearsay, which in principle is inadmissible as evidence in a criminal trial. The Law of Evidence Amendment Act[39] deals with the admissibility of hearsay evidence and provides that subject to certain statutory provisions hearsay evidence may not be admitted as evidence in criminal or civil proceedings.[40] The court may however, having regard to various factors, admit hearsay evidence in the interests of justice.[41] These

---

[32] South African Law Commission *Report on the Admissibility in Civil Proceedings of Evidence Generated by Computers* Project 6 (1982).

[33] Act 57 of 1983.

[34] Preamble as well as section 3 of Act 57 of 1983.

[35] Sections 1 and 2 of Act 57 of 1983.

[36] Section 3 of Act 57 of 1983.

[37] A J Ebden *Computer evidence in court* (1985) SALJ 687. He states "when your house is not in order, do you put it in order, or do you change the law so as to define it as being in order". Also see A st Q skeen *Evidence and Computers* (1984) SALJ 675 on 683 *et seq*.; J T Delport *Die Wet op Rekenaargetuienis* (1983) Obiter 140 *et seq*.; D P van der Merwe *Computers* in W A Joubert(ed) in LAWSA Vol. 5 11; Schwikkard (footnote 23 *supra*) 270 *et seq*.

[38] Section 92 of Act 25 of 2002.

[39] Act 45 of 1988.

[40] Section 3(1) of Act 45 of 1988. In general see Eiselen *Elektroniese dataverwisseling (EDV) en die bewysreg* (1992) 55 THRHR 217; Van der Merwe (footnote 22 *supra*) 70 *et seq*.

[41] Section 3(1)(c) of Act 45 of 1988.

factors include the nature of the proceedings; the nature of the evidence; the purpose for which the evidence is tendered; the probative value of the evidence; the reason why the evidence is not given by the person upon whose credibility the probative value of such evidence exist; any prejudice to a party if the evidence is admitted; and any other relevant factor.[42]

Sections 221 and 236[43] of the Criminal Procedure Act constitute statutory exceptions to the hearsay rule. Section 236(5) of the Criminal Procedure Act provides that a *document* will include a "recording or transcribed computer printout produced by any mechanical or electronic device and any device by means of which information is recorded and stored". Section 221 of the Criminal Procedure Act provides:

> "(1) In criminal proceedings in which direct oral evidence of a fact would be admissible, any statement contained in a document and tending to establish that fact shall, upon production of the document, be admissible as evidence of that fact if-
>
> (a) the document is or forms part of a record relating to any trade or business, from information supplied, directly or indirectly, by persons who have or may reasonably be supposed to have personal knowledge of the matters dealt with in the information they supply;
>
> (b) the person who supplied the information recorded in the statement in question is dead or outside the Republic or is unfit by reason of his physical or mental condition to attend as a witness or cannot with reasonable diligence be

[42] Section 3(1)(c) of Act 45 of 1988.

[43] Section 236 of Act 51 of 1977 provides for the proof of accounting records and documentation of banks accompanied by an affidavit that indicates that these entries were made in the ordinary course of business.

> identified or found or cannot reasonably be expected, having regard to the time which has elapsed since he supplied the information as well as all the circumstances to have any recollection of the matters dealt with in the information he supplied."[44]

A court should estimate the weight to be attached to the statement with reference to *inter alia* accuracy of the statement.[45] Section 221(5) of the Criminal Procedure Act defines *document* as including any device by means of which information is stored or recorded. In the case of *S v Harper and Another* [46] it was decided that a computer printout was a document within the ordinary grammatical meaning of the word document and would therefore fall within the ambit of section 221 of the Criminal Procedure Act.[47] In other words the ordinary meaning of document is wide enough to include computer printouts since it contains letters and symbols in a readable format.

In the case of *S v De Villiers*[48] the Namibian High Court held that a computer printout produced by a computer that sorts and collates information is admissible provided that it is certified as authentic. Some authors argue that a computer printout is merely a copy of the information that is stored in the computer and that the original "document" is the hard drive of the computer. The Court held in the *De Villiers-case*[49] that

---

[44] In general see Eiselen (footnote 40 *supra*) 214; A St Q Skeen *Evidence and computers* (1984) SALJ 675; A st Q Skeen *The admissibility of computer output in evidence* (1981) 7 SACC 229 *et seq*.

[45] Section 221(3) of Act 51 of 1977.

[46] 1981 (1) SA 88 (D).

[47] Eiselen (footnote 40 *supra*) 215.

[48] 1993 (1) SACR 574 (NM).

[49] (Footnote 48 *supra*) on page 579.

computer printouts are in fact *duplicate originals* and admissible provided that is has been proven to be authentic.

However, in the case of *S v Mashiyi and Another*[50] the Transkei Division of the High Court of South Africa held that documents that contain information that has been processed or generated by a computer are not admissible in a criminal trial. The court further held that documents that have been scanned to produce an *exact* electronic image of the original are admissible. The Honourable Judge Miller stated:

> "All that I can do is add my voice to the call that this *lacunae* in our law be filled and for new legislation relating specifically to computer evidence in criminal cases be considered and promulgated."[51]

In South Africa computers and information technology are increasingly being used in all sectors of society. Clarity in relation to the admissibility requirements of computer-generated evidence was necessary. In 2002 the Electronic Communications and Transactions Bill came to light.[52] The Act came into operation on 30 August 2002 and extensively dealt with the issue of evidence in the milieu of cyber space and computer-generated documents.[53] The Act states that "information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of

---

[50] 2002 (2) SACR 387 (TkD).

[51] (Footnote 50 *supra*) on page 393.

[52] 2002.

[53] In general see Jacques Jansen *A new era for e-commerce in South Africa* (2002) October De Rebus 17; John Peter *The Electronic Communications and Transactions Act* (2003) April Advocate 31 *et seq*.; Buys(ed) *Cyberlaw @ SA II* (2004) 335.

a data message".[54] Information in electronic form has now been given legal status.

A requirement that information or a document must be in writing is met if the information or document is in the form of a data message (thus in electronic format) and accessible in any manner suitable for subsequent reference.[55] A data message is defined as "data generated, sent, received or stored by electronic means".[56] Where it is required by a law that information must be presented in its original form, a data message will be admissible if the integrity of the data or information is unaffected[57] and the information can be displayed or produced.[58]

The Act provides for the admissibility of data messages in any legal proceedings, including criminal cases.[59] This is a welcome addition to our law since the Computer Evidence Act was only applicable in civil cases. The Act further states that a data message is admissible even if it is not in its original form provided that it is the best evidence that the person adducing it could reasonably be expected to obtain.[60] This means that computer printouts of data messages are admissible in criminal cases provided that all the other requirements are met. Section 15(4) of the Act provides that a data message made by a person in the ordinary course of

[54] Section 11(1) of Act 25 of 2002.

[55] Section 12 of Act 25 of 2002; See Jansen (footnote 53 *supra*) 17.

[56] Section 1 of Act 25 of 2002.

[57] The information has remained complete and unaltered – see section 14(2) of Act 25 of 2002.

[58] Section 14 of Act 25 of 2002.

[59] Section 15(1) of Act 25 of 2002.

[60] Section 15(1) of Act 25 of 2002.

business or a copy or printout of such a data message certified to be correct by an officer in the service of such a person is on mere production admissible as evidence. It will constitute rebuttable proof of the information contained in such a document and will be admissible in criminal proceedings as well.[61] Since this provision places a reverse onus on the accused to rebut the information contained in such a data message, this provision may be constitutionally challenged on the basis of an accused person's fundamental right to be presumed innocent, to remain silent, and not to testify during the proceedings[62].

The next question is what weight should be attached to the information and the Act states that: "information in the form of a data message must be given due evidential weight"[63] When a court assesses the evidential weight of a data message it must have regard to the reliability of the manner in which the data message was generated, stored or communicated; the reliability of the manner in which the integrity of the data message was maintained; the manner in which its originator was identified; and any other relevant factor.[64]

14.3 ENCRYPTION

Encryption is the process of converting readable information into unreadable or unintelligible code. The readable information or text is called *plaintext* and the encrypted information is called *cipher text.*[65] A

[61] Section 15(4) of Act 25 of 2002.

[62] As contained in section 35(3)(h) of Act 108 of 1996.

[63] Section 15(2) of Act 25 of 2002.

[64] Section 15(3) of Act 25 of 2002.

[65] Buys(ed) *Cyberlaw @ SA* (2000) 209; Buys(ed) *Cyberlaw @ SA II* (2004) 114.

code or cipher is used to encrypt the information into characters or code. *Decryption* is the process of converting the cipher text back to the readable plaintext form. The purpose of encryption is to ensure confidentiality, authenticity, integrity and non-repudiation[66].[67] A definition of a decryption key is found in the Regulation of Interception of Communications and Provision of Communication-Related Information Act:

> "…any key, mathematical formula, code, password, algorithm or any other data which is used to-
> (a) allow access to encrypted information; or
> (b) facilitate the putting of encrypted information into an intelligible form"[68]

There are two basic forms of encryption. *Symmetric or private key encryption* entails that both parties must have the same encryption key in order for the sending party to encode the data and for the receiving party to decode the information.[69] Van der Merwe is of the view that there are many problems associated with symmetric encryption which include *inter alia* that symmetric encryption will only work between two parties that regularly exchange information.[70] The private key can also easily be

---

[66] Non- repudiation ensures that the transaction is binding and cannot be denied.

[67] Buys(ed) *Cyberlaw @ SA II* (2004) 114; Richard Harrison *Public Key Infrastructure: The Risks of being Trusted* (2000) Computers & Law Vol. 11 Issue 3 28; Stewart A. Baker & Paul R Hurst *The Limits of Trust Cryptography, Governments, and Electronic Commerce* (1998) 2 *et seq*.

[68] Section 1 of Act 70 of 2002. At the time of writing the Act was not yet in operation.

[69] Buys(ed) *Cyberlaw @ SA* (2000) 210; D P van der Merwe *Die regsimplikasies van elektroniese handeldryf ("E-Commerce") met besondere verwysing na die bewysreg* (1999) THRHR 230. In Buys(ed) *Cyberlaw @ SA II* (2004) it is called secret key cryptography.

[70] Dana van der Merwe *Computers and the law* (2000) 231; Van der Merwe (footnote 69 *supra*) 230

intercepted by third parties.[71] It is therefore of the utmost importance that the key is secure.[72]

Asymmetric encryption is also known as *public key infrastructure*. The transmitting party uses two keys. The private key is used to encrypt the message and digitally sign it. The private key is known only to the transmitter. The public key is mathematically related to the private key although the one cannot be discovered from the other. The public key is given to third parties so that they can decode the message and ascertain whether it is authentic. The public key may be published on the Internet.[73]

Early in 1997 the OECD[74] published a document entitled *Recommendation of the Council Concerning Guidelines for Cryptography Policy*[75] that establishes certain guidelines in respect of cryptography policies and regulation. In the United Kingdom the Electronic Communications Act[76] provides that cryptography support services must be approved and registered.[77] Cryptography support service is in essence defined as services using cryptography techniques to ensure

---

[71] Van der Merwe (footnote 70 *supra*) 231; Van der Merwe (footnote 69 *supra*) 230; Harrison (footnote 67 *supra*) 28.

[72] John T Soma *Encryption, Key recovery, and commercial trade secret assets: A proposed legislative model* (1999) Rutgers Computer and Technology Law Journal Vol. 25 No. 1 102.

[73] In respect of public key encryption see Buys(ed) *Cyberlaw @ SA* (2000) 210 – 211; Buys *Cyberlaw @ SA II* (2004) 115; Van der Merwe (footnote 70 *supra*) 231; Van der Merwe (footnote 69 *supra*) 230; Harrison (footnote 67 *supra*) 28; Stewart & Hurts (footnote 67 *supra*) 1 *et seq*.; Soma (footnote 72 *supra*) 102; Benjamin Wright *Alternatives for signing electronic documents* (1995) 11 The Computer Law and Security Report 136.

[74] Organisation for Economic Co-operation and Development.

[75] Dated 27 March 1997. Also see Buys(ed) *Cyberlaw @ SA II* (2004) 112-113; Stewart & Hurts (footnote 67 *supra*) 513 *et seq*.

[76] 2000.

[77] Harrison (footnote 67 *supra*) 28.

confidentiality, integrity and authenticity of electronic communications and data.[78]

In South Africa the Electronic Communications and Transactions Act contains provisions in respect of encryption. A *cryptography product* is defined as:

> "any product that makes use of cryptography techniques and is used by a sender or recipient of data messages for the purpose of ensuring-
> a. that such data can be accessed only by relevant persons;
> b. the authenticity of the data;
> c. the integrity of the data; or
> d. that the source of the data can be correctly ascertained"[79]

Cryptography service is defined as:

> "any service which is provided to a sender or a recipient of a data message or to anyone storing a data message, and which is designed to facilitate the use of cryptography techniques for the purpose of ensuring-
> a. that such data or data message can be accessed or can be put into an intelligible form only by certain persons;
> b. that the authenticity or integrity of such data or data message is capable of being ascertained;
> c. the integrity of the data or data message; or
> d. that the source of the data or data message can be correctly ascertained"[80]

---

[78] Harrison (footnote 67 *supra*) 29.

[79] Section 1 of Act 25 of 2002. See Buys(ed) *Cyberlaw @ SA II* (2004) 117.

[80] Section 1 of Act 25 of 2002. See Buys(ed) *Cyberlaw @ SA II* (2004) 117.

The Act is widely defined and will include all forms of cryptography including symmetric as well as asymmetric encryption.

A Cryptography provider[81] may not provide cryptographic services or products in South Africa unless the provider has registered with the Department of Communications.[82] The Director-General of the Department of Communications must maintain a register of cryptography providers.[83] A cryptography provider must furnish the Director-General with the required information in the prescribed manner.[84] The name and address of the cryptography provider and a description of the cryptography service or product provided must be recorded in the register.[85] The Act provides that it is not required of a cryptography provider to disclose confidential information or trade secrets.[86]

Section 30(3) of the Act provides that a cryptography service or product is regarded as being provided in South Africa when it is provided:

1.) from premises in South Africa;
2.) to a person who is present in South Africa and that person makes use of the service or product;

---

[81] A cryptography provider is defined in section 1 of Act 25 of 2002 as "any person who provides or who proposes to provide cryptography services or products in the Republic".

[82] Section 30(1) of Act 25 of 2002. See Buys(ed) *Cyberlaw @ SA II* (2004) 120.

[83] Section 29(1) of Act 25 of 2002.

[84] Section 30(2) of Act 25 of 2002. A prescribed administrative fee is also payable. See Buys(ed) *Cyberlaw @ SA II* (2004) 118.

[85] Section 29(2) of Act 25 of 2002.

[86] Section 29(3) of Act 25 of 2002.

3.) to a person who uses the service or product for the purposes of a South African business.[87]

These are very wide jurisdictional provisions and may have vast implications for overseas cryptography products that are used in South Africa. A cryptography provider who fails to register in terms of this Act is guilty of an offence and may be sentenced to a fine or imprisonment not exceeding two years.[88]

A cyber criminal could encrypt certain data that has bearing on, or may constitute evidence in respect of the commission of an offence. A perpetrator could hide his criminal actions by encrypting information.[89] Without the decryption key the data would be unintelligible which will render it useless to law enforcement agencies. A *key recovery* mechanism will assist the police and other parties to investigate crime.[90] The Regulation of Interception of Communications and Provisions of Communication-Related Information Act provides for a *decryption direction* which is a directive in terms of which the decryption key holder is directed to disclose a decryption key or provide decryption assistance[91]

---

[87] These provisions in respect of jurisdiction are in essence similar to those in the Electronic Communications Act 2000 in the United Kingdom. See Harrison (footnote 67 *supra*) 29.

[88] Section 32(2) of Act 25 of 2002.

[89] Yaman Akdeniz, Nicholas Bohm & Prof Clive Walker *Internet Privacy: Cyber Crimes vs Cyber-Rights* (1999) Computers and Law Vol. 10 Issue 1 35.

[90] In the United Kingdom the recovery of decryption keys in regulated by the Regulation of Investigatory Powers Act 2000. See Rico Calleja *The Regulation of Investigatory Powers Act 2000* (2000) Computers & Law Vol. 11 Issue 3 21 *et seq*. Also see Buys(ed) *Cyberlaw @ SA II* (2004) 118 *et seq*.

[91] Decryption assistance means to allow access to encrypted information or to facilitate the putting of encrypted information into an intelligible readable form – section 1 of Act 70 of 2002. Also see section 29 of Act 70 of 2002.

in respect of encrypted information.[92] Only certain police officers[93] may apply to a designated judge for such a directive and detailed procedures and prerequisites are required by the Act.[94]

The suspect or accused may be the decryption key holder. In terms of the South African Constitution an accused has the right to a fair trial which includes the rights to be presumed innocent, to remain silent[95] and not to be compelled to give self-incriminating evidence[96]. The right to a fair trial also extends to pre-trial investigations. It may be argued that these provisions in respect of a decryption directive are unconstitutional in as far as it also infringes the constitutionally protected right to privacy. The rights in the Bill of Rights may be limited under certain circumstances.[97] An accused may argue that evidence obtained through a decryption directive that directed an accused to decrypt information, are unconstitutional or violates his right to a fair trial and must be excluded.[98]

---

[92] Section 1 of Act 70 of 2002.

[93] An officer referred to in section 33 of the South African Police Service Act as well as written approval in advance of at least an Assistant Commissioner. Other applicants are also identified. See section 1 of Act 70 of 2002.

[94] Section 21 read with section 16 of Act 70 of 2002.

[95] Section 35(3)(h) of the Constitution of the Republic of South Africa, Act 108 of 1996.

[96] Section 35(3)(j) of the Constitution of the Republic of South Africa, Act 108 of 1996.

[97] See section 36 of the Constitution of the Republic of South Africa, Act 108 of 1996. Fundamental rights may be limited to the extent that the limitations are reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom.

[98] In terms of section 35(5) of the Constitution.

14.4 ELECTRONIC SIGNATURES

Electronic signatures are sometimes referred to as digital signatures. Digital signatures ensure data integrity, non-repudiation and guarantee authenticity.[99] One should distinguish between the term *electronic signature* and the term *digital signature*.[100] A digital signature is a type of electronic signature and involves the use of encryption or keys to guarantee authenticity.[101] An electronic signature is not necessarily a digital signature and includes the PIN code and the mere click of the mouse on acceptance terms on a web page.[102]

The European Union released a directive entitled "Directive on a Community framework for electronic signatures".[103] The directive distinguishes between electronic signatures and advanced electronic signatures.[104] An electronic signature is advanced if it is uniquely linked to the signatory, capable of identifying the signatory, using means that is under the sole control of the signatory and subsequent changes can be

---

[99] In general see Hofmeyr Herbstein & Gihwala Inc *Questions and answers* at http://www.hofmeyr.co.za/legal questions and answers.htm

[100] Nigel Miller *Electronic Signatures – much ado?* (2002) Computers & Law Vol. 13 Issue 2 36; Stephen Mason *The evidential issues relating to electronic signatures –part 1* (2002) Computer Law and Security Report Vol. 18 No. 3 176; Aalberts & Van der Hof *Digital Signature Blindness Analysis of Legislative Approaches to Electronic Authentication* (2000) The EDI Law Review Vol. 7 No. 1 2; Stewart & Hurst (footnote 67 *supra*) 248.

[101] Miller (footnote 100 *supra*) 36; Stewart & Hurts (footnote 67 *supra*) 249; Aalberts & Van der Hof (footnote 100 *supra*) 2.

[102] Miller (footnote 100 *supra*) 36; Stewart & Hurst (footnote 67 *supra*) 249; Aalberts & Van der Hof (footnote 100 *supra*) 2.

[103] See Harrison (footnote 67 *supra*) 29; Miller (footnote 100 *supra*) 36; Van der Merwe (footnote 69 *supra*) 231 *et seq*.

[104] Harrison (footnote 67 *supra*) 29.

detected.[105] According to the Directive an advanced electronic signature is admissible as evidence.

In the United Kingdom electronic signatures is governed by the Electronic Communications Act[106] and Electronic Signatures Regulations[107]. The Regulations implemented the Directives of the European Union in respect of electronic signatures.

It was the subject of much debate whether digital signatures are legally recognised in South African law.[108] Certain writers used the law of succession in respect of the signing of testaments in order to investigate the legality of digital signatures.[109] In the case of *Jhajbay v The Master*[110] the court held that the test that should be applied is whether the testator intended that a mark or signature must serve as his or her signature. This liberal approach could have been useful to argue the legality of digital signatures.[111] However the Electronic Communications and Transactions Act put an end to the debate by legalising digital signatures.[112] The Act was assented to on 31 July 2002 and the President of South Africa signed

---

[105] Harrison (footnote 67 *supra*) 29.

[106] 2000. See Mason (footnote 100 *supra*) 176 *et seq*.; Mason *The evidential issues relating to electronic signatures –part II* (2002) Computer Law and Security Report Vol. 18 No. 4 243 *et seq*.

[107] 2002. See Miller (footnote 100 *supra*) 36.

[108] See Hofmeyr Herbstein & Gihwala Inc *Is a digital signature legal?* at http://www.hofmeyr.co.za/digital signature legal.htm

[109] Dana van der Merwe *Computers and the Law* (2000) 232 *et seq*.; Van der Merwe (footnote 69 *supra*) 236 *et seq*.

[110] 1971 (2) SA 370 (D); See J C Sonnekus *Dempers and Others v The Master and Others (1) 1977 4 SA 44 (SWA)* (1978) TSAR 175 on page 178.

[111] Also see Van der Merwe (footnote 69 *supra*) 237; Van der Merwe (footnote 70 *supra*) 234.

[112] In general see Jansen (footnote 53 *supra*) 18 and Buys(ed) *Cyberlaw @ SA II* (2004) 121 *et seq*.

the English text of the Act with his own advanced electronic or digital signature![113]

The Act defines an *electronic signature* as "data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature".[114] An electronic signature is now recognised in our law and the Act states that "an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form".[115] However, the legislator provided for the concept of advanced electronic signatures. When the law requires the signature of a person but does not specify the type of signature, an electronic signature will only be recognised if an *advanced electronic signature* is used.[116] These provisions accord with the Directives of the European Union on Electronic Signatures. The Act provides that where an advanced electronic signature is used it is presumed that the electronic signature is valid and has been properly applied.[117] This statutory presumption may however be rebutted in proving the contrary.[118]

An advanced electronic signature "means an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37".[119] The Accreditation Authority may accredit

---

[113] Photograph published in the Citizen 1 August 2002.

[114] Section 1 of Act 25 of 2002. See in general Buys(ed) *Cyberlaw @ SA II* (2004) 132 *et seq.*

[115] Section 13(2) of Act 25 of 2002.

[116] Section 13(1) of Act 25 of 2002.

[117] Section 13(4) of Act 25 of 2002. Also see Jansen (footnote 53 *supra*) 17.

[118] Footnote 85 *supra.*

[119] Section 1 of Act 25 of 2002.

authentication products and services in respect of advanced electronic signatures.[120] Section 38 stipulates the criteria for accreditation.[121] Section 38(1) provides that:

> "The Accreditation authority may not accredit authentication products or services unless the Accreditation Authority is satisfied that an electronic signature to which such authentication products relate-
>
> a. is uniquely linked to the user;
> b. is capable of identifying that user;
> c. is created using means that can be maintained under the sole control of that user; and
> d. will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable;
> e. is based on the face-to-face identification of the user."

The Accreditation Authority may consider factors such as the financial and human resources of an authenticating service provider who applies to have their authentication products or services registered.[122] Further factors would include the quality of its hardware and software systems, availability of information to third parties relying on these services, the regularity and extent of audits by an independent body and any other relevant factor.[123] The hardware and software systems of an authenticating service provider must:

- be reasonably secure from intrusion and misuse;

---

[120] Section 37(1) of Act 25 of 2002.

[121] See in general Jansen (footnote 53 *supra*) 18 and Buys(ed) *Cyberlaw @ SA II* (2004) 126.

[122] Section 38(2) of Act 25 of 2002.

[123] Section 38(2) of Act 25 of 2002.

- provide reasonable levels of availability, reliability and correct operation;
- be reasonably suited to perform their intended functions;
- adhere to generally accepted security procedures.[124]

The Accreditation Authority may also stipulate certain minimum prerequisites in respect of technical requirements, responsibilities and liabilities before accrediting authentication products and services provided by a certification service provider.[125] A certification service provider is defined as "a person providing an authentication product or service in the form of a digital certificate attached to, incorporated in or logically associated with a data message".[126]

When accrediting an authentication product or service any condition or restriction may be imposed by the Accreditation Authority.[127] The Accreditation Authority may suspend or revoke an accreditation in certain instances.[128] A person that falsely holds out that his authentication products or services have been accredit by the Accreditation Authority is guilty of an offence[129] and liable upon on conviction to a fine or a period of imprisonment not exceeding 12 months.[130]

---

[124] Section 38(3) of Act 25 of 2002. See Jansen (footnote 53 *supra*) 18.

[125] Section 38(4) of Act 25 of 2002; See Jansen (footnote 53 *supra*) 18.

[126] Section 1 of Act 25 of 2002.

[127] Section 38(5) of Act 25 of 2002.

[128] Section 39 of Act 25 of 2002.

[129] Section 37(3) of Act 25 of 2002.

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

It would appear that the South African legislation in respect of electronic signatures accord in great detail with the European Union's directives in respect of electronic signatures.