The Electronic Communications and Transactions Act

John Peter, Johannesburg Bar

Introduction

On 31 July 2002 the Electronic Communications and Transactions Act, 25 of 2002, was passed in parliament. The Act came into operation on 30 August 2002 by proclamation in the Gazette. The stated objects in section 2 of the Act are "... to enable and to facilitate electronic communications and transactions in the public interest."

This Act is the long overdue legislative attempt to deal with the internet and its related computer and electronic issues which have had an explosive impact on our everday lives since the 1990's.

The purpose of this article is to provide a brief overview of the Act and to highlight some of the more critical issues which are likely to have a significant impact on the practice of law, specifically in the field of litigation.

Before delving into any scrutiny of the provisions of the Act, it is worthwhile reflecting that the internet, e-mail, computerised and electronic communications and the concepts with which the Act has to deal, are nothing more than a new form of communication and but another step in the march of technological process. There are still members of the legal profession, and no doubt not a few members of the Bench, who are able to recall what it was like to practise in a time before the photocopier. Multiple carbon copies on tissue thin paper were left behind in the march to the wet process photocopier with its murky reproductions. The mail and communications by post yielded to the fax machine not so long ago with its thermal paper which faded over time. The advanced state-of-the-art golf ball typewriter yielded to the word processor, which in turn was superseded by the PC. Similarly, in antiquity, no doubt incantations before the *pontifex maximus* for the grant of a rustic servitude were at some stage rendered obsolete by the eminently more modern facility of parchment.

By far the most significant feature of the internet is that it provides a medium of communication which is both paperless and soundless. This medium of communication provides the opportunity for people to communicate and transact business over great distances almost instantaneously without requiring to have two people interacting simultaneously with each other. It further provides new opportunities for anti-social and criminal behaviour.

General overview

The Act is a fairly lengthy document, comprising 95 sections divided into 14 chapters.

Chapter 1 of the Act deals with interpretation, the objects and application of the Act. The most significant definition is a "data message". This is the key to the understanding of the Act and the nucleus of the paperless and soundless information in electronic form, which is what the Act seeks to regulate. The Act applies in respect of any "electronic transaction" (not defined) or "data message". There appears to be no express territorial limitation to the Republic. The Act specifically does not apply to statutes and matters referred to in the two schedules to the Act. These principally relate to the execution of wills and codicils, the alienation of land, execution of bills of exchange and stamp duties.

Chapter 2 of the Act provides for the creation of a national e-strategy (not defined), together with an accompanying policy framework to be developed by the Minister of Communications within two years after the commencement of the Act.

The Minister is additionally charged with the formulation of an electronic transactions policy. In so doing, he or she is to have due regard to the objects of the Act, the nature, scope and impact of electronic transactions, international best practice and conformity with laws and guidelines of other jurisdictions and international bodies and existing laws in the administration in the Republic. Although the Minister is required to publish policy guidelines in the Gazette, no doubt the formulation of this policy is most likely to give rise to further legislation related to electronic transactions as the flaws and weaknesses in the Act are exposed over time.

Chapter 3 of the Act, which is directed at facilitating electronic transactions, is the most important chapter for the purpose of this article and for litigation. It is dealt with further below.

Chapter 4 of the Act deals with what is termed "e-government services". It provides, in respect of public bodies which accept the filing of documents, issue permits and provide for payment, to do so in electronic form.

Chapter 5 of the Act provides for the registration of cryptography providers. Cryptography is, broadly, the software technique of encoding or encrypting data for purposes of security and ensuring the authenticity and integrity of the data message.

Chapter 6 provides for the registration and accreditation of authentication service providers. Authentication is tied up with the concept of an "advanced electronic signature". The product or service of such provider is one which ensures that an electronic signature is unique to a particular user.

Chapter 7 of the Act deals with the subject of consumer protection. It provides for disclosure requirements by suppliers offering goods or services for sale, hire or exchange by way of an electronic transaction. Consumers are entitled to a "cooling-off" period during which they may cancel an electronic transaction without penalty. This "cooling-off" period does not apply to certain kinds of transactions, including financial services, auctions, supply of foodstuffs and other transactions where a right to resile after seven days would be impractical or unfair to the providers of the goods and services.

Importantly, the chapter contains a provision dealing with electronic "junk mail". A person sending unsolicited commercial communications must provide the addressee with an option to cancel his or her subscription to the mailing list and, on the request of the consumer, provide the identifying particulars of the source from which that consumer's personal information was obtained. There is an express prohibition on the conclusion of an agreement where the consumer has failed to respond to an unsolicited communication. Persistence in despatching unsolicited commercial communications to a person who has advised the sender that such commu-

nications are unwelcome is criminalised.

Chapter 8 of the Act deals with the protection of personal information obtained through electronic transactions. Importantly, data collectors must have the express written permission of the data subject for the collation, processing or disclosure of personal information relating to the person who is the subject of the data, unless the data controller is permitted or required to do so by law. Precisely how this is to be regulated and enforced remains to be seen.

Chapter 9 of the Act deals with the protection of critical data bases. "Critical data" is data declared by the Minister to be of importance for the protection of the national security of the Republic and the economic and social wellbeing of its citizens. This chapter deals with the registration of critical data bases, permits the Minister to prescribe standards and prohibitions in respect of the management and administration of critical data bases and provides for the inspection of such data bases.

By far the most controversial chapter which attracted a blaze of publicity and strong criticism of the government, is chapter 10 dealing with the Domain Name Authority and Administration. This chapter provided for the establishment of a juristic person to be known as the ".za Domain Name Authority" to assume responsibility for the ".za Domain Name". Although the Authority was vested with the juristic personality from the date of the promulgation of the Act, the Minister is required to take the steps necessary for the incorporation of the Authority as a company, contemplated in section 21(1) of the Companies Act.

Chapter 11 provides for the limitation of liability for service providers, who are defined as persons providing information system services. This is a welcome provision, defining the roles and extent of responsibilities of service providers. Service providers have no general obligation to monitor the data which they transmit or store, nor do they have the obligation actively to seek facts or circumstances indicating unlawful activity. However, on receipt of a complaint or notice of unlawful activity received in writing, they must act expeditiously to remove or disable access to the data complained of.

Chapter 12 provides for the appointment of government employees in the Department of Communications as cyber inspectors for the enforcement and administration of the Act. Their powers include powers to search and seize upon a warrant, the provisions of the Criminal Procedure Act 51 of 1977 being made applicable.

Chapter 13 is a chapter devoted to "cyber crime". This chapter formally creates a range of offences directed at computer hackers. It criminalises, subject to the Interception and Monitoring Prohibition Act 127 of 1992, the accessing or interception of any data without authority or permission. Intentional and unauthorised interference with data which causes it to be modified, destroyed or otherwise rendered ineffective, is made an offence. Further offences include the unlawful production, sale, distribution or possession of any device or computer program to overcome security measures for the protection of data and the utilisation of any device or computer programme in order to overcome such security measures. The threat of computer hacking for the purpose of extortion is also criminalised.

Chapter 14 contains general provisions. A court in the Republic trying an offence in terms of the Act has jurisdiction where the offence was committed in the Republic, where any act or preparation towards the offence or any part of the offence was committed in the Republic or where the result has an effect in the Republic. Jurisdiction exists in respect of any offences committed aboard any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time the offence was committed.

The Act remarkably includes jurisdiction if the offence was committed by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic, irrespective of where the offence was committed. This overreaching extension of jurisdiction may give rise to the following difficulty. It is conceivable that a South African citizen or resident (or someone carrying on business in the Republic) might perpetrate certain conduct which has no connection whatsoever with the Republic. It would be difficult to imagine that the unlawful access and cracking of the password and corruption of data on someone's personal computer in the United Kingdom (physical access being obtained in the United Kingdom) ought to be treated as an offence for the purpose of the South African Act, simply because such conduct was perpetrated by a South African abroad. The narrow application of this section will beg the question as to whether the conduct is an offence in South Africa.

The chapter, however, does not affect the criminal or civil liability in terms of the common law.

The Minister is empowered to make regulations necessary or expedient for the proper implementation or administration of the Act.

Chapter 3

The most important chapter to the legal profession and in particular those dealing with litigation and commercial transactions, is chapter 3. This chapter is directed at the facilitation of electronic transactions.

The key to this chapter (and the Act more generally) is the concept of a "data message". This is defined as data generated, sent, received or stored by electronic means and includes (a) voice, where voice is used in an automated transaction, and (b) a stored record. An "automated transaction" is an electronic transaction conducted or performed in whole or in part by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment. A good example of an automated transaction, is that once exciting experience of drawing money from an ATM after hours on the weekend when all the banks have closed.

The Act accords legal recognition to data messages. Section 11 provides that information is not without legal force or effect, merely on the grounds that it is wholly or partly in the form of a data message. The section further provides for legal force and effect of information which is incorporated by reference in a data message which purports to give rise to such legal force and effect. When information which is not in the public domain is incorporated into an agreement, it is regarded as having been incorporated into a data message if the information is referred to in the data message in such a way that a reasonable person would have noticed the reference and the incorporation and if such information is accessible in a form in which it may be read, stored or retrieved by the addressee. This provision would enable vendors to incorporate by reference their standard terms of sale where the provisions are not in the document,

but may be accessed by a highlighted button which provides a link to such standard terms.

Section 12 of the Act provides that where a document or information is required by law to be in writing, the requirement will be met where the document or information is in the form of a data message and accessible in a manner usable for subsequent reference.

The Act further deals with signatures. In this regard there are two types of signatures, an electronic signature and an advanced electronic signature. The advanced electronic signature is a signature which results from a process which has been accredited by the Accreditation Authority charged by law with the accreditation of authentication products and services. Where the signature of a person is required by a law which does not specify the type of signature, then in relation to a data message the requirement of a signature is met only if an advanced electronic signature is used. When an electronic signature is used by the parties to an electronic transaction and there is no agreement as to the type of signature that is required, then an electronic signature other than an advanced electronic signature may be used.

The requirements for an electronic signature in relation to a data message, are (a) a method used to identify the author and to indicate the persons approval of the information communicated, and (b) having regard to all the relevant circumstances at the time the method was used, a method that was reliable and appropriate for the purposes for which the information was communicated. Presumably, in a contract concluded by the exchange of e-mail correspondence, the requirement of a signature will be satisfied by the simple typing of the parties names. Provision is made for a rebuttable presumption of validity in respect of an advanced electronic signature, which is not the case in respect of other electronic signatures. Accordingly, in any litigation to prove the existence of such a contract, the authenticity of an ordinary electronic signature would still have to be proved and may not be presumed.

Section 14 provides that where a law requires information to be presented or retained in its original form, this requirement is met by a data message if the information is capable of being displayed or produced to the person to whom it is presented, and if the integrity of the information at the time when it was first generated in its final form as a data massage, or otherwise, has passed an assessment. The integrity must be assessed by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display, in the light of the purpose for which the information was generated and having regard to all other relevant circumstances. It is an important provision in providing for the admissibility of a data message as evidence, without being excluded as not being the original document under the best evidence rule.

For the purposes of admissibility and evidence in ligation, section 15 is the most important section in this chapter. This section must be read with section 92, which repeals the Computer Evidence Act 57 of 1983. The admissibility of computer evidence is now governed by section 15 and its concept of a data message. The section provides that the rules of evidence in any legal proceedings must not be applied so as to deny the admissibility of a data message in evidence merely on the grounds that it is constituted by a data message, or if it is the best evidence that the person producing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

Information in the form of a data message must be given due evidential weight. In assessing evidential weight of a data message, regard must be had to the reliability of the manner in which the data message was generated, stored or communicated and further to the manner in which it was maintained. Regard must also be had to the manner in which the originator was identified and "any other relevant factor".

Most importantly, a data message made by a person in the ordinary course of business or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, will be admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, or printout. This provision is a welcome innovation to overcome the practical difficulties encountered in *Narlis v The South African Bank of Athens* 1976 (2) SA 573 (A), and further the shortcomings of the now repealed Computer Evidence Act. Nevertheless the practitioner wishing to prove the balance of a bank overdraft should be weary of merely producing the printouts and expect them to be received into evidence without further ado. The printouts would have to be certified and the status of the person certifying the document ought to be proved as that of an officer in the service of the bank. Furthermore, evidence ought to be led that the printouts are printouts of data messages made by persons in the ordinary course of the business of the bank. This provision is also a development of the inroads made against the rule against hearsay by section 34 of the Civil Proceedings Evidence Act 1965, which has become inadequate in meeting the exigencies of modern commerce.

Section 18 of the Act provides that where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met in an advanced electronic signature of the person authorised to perform the notarising, acknowledgement, verification or administration of the oath, is attached to, incorporated in or logically associated with the electronic signature or data message which is authenticated.

Conclusion

As the Act presently stands, two important considerations must be borne in mind. First, at the time of writing, the Minister has not exercised his power granted to him/her, in terms of section 94 of the Act, to make regulations. Accordingly, there are no regulations regarding the accreditation of authentication products and services and accordingly provisions relating to advanced electronic signature cannot be given effect. Secondly, the application of data messages and the elevation of their status to writing are not universal. Hard copy paper and conventional signatures are required in matters relating to wills and codicils, the alienation of land and long-term leases, bills of exchange and stamp duties.

On the whole, this Act must be seen as the first attempt to catch up with the technological leap brought about by the internet and electronic communication. No doubt in the future there will be much further legislation, as the Act is refined by amendment, its shortcomings and gaps exposed, and as technology changes.