

2. ENABLING ELECTRONIC TRANSACTIONS: BASIC PRINCIPLES

THE BASIC PRINCIPLES

Electronic contracts are concluded through data messages which are defined by section 1 ECTA as

“data generated, sent, received or stored by electronic means and includes (a) voice, where the voice is used in an automated transaction; and (b) a stored record”.

Certain principles have been expounded in order to ensure that laws originally crafted for the physical environment are meaningfully transposed onto the digital environment. The aim of these principles is to ensure that, as far as possible, data messages are afforded legal validity and that rules are developed to facilitate the application of ‘traditional’ laws to the digital environment. The relevant basic principles may be summarised as follows:

Non-discrimination: This ensures that data messages (even where incorporated by reference) have legal validity (see subsection entitled ‘Legal recognition of data messages’ below).

Media and technology neutrality: This ensures that the use of electronic technology does not result in unequal treatment of transactions because of the platform on which they are concluded.

Functional equivalence: The development of rules applicable to electronic communications to facilitate e-commerce by adapting existing [paper-based environment] legal requirements. The functional-equivalent approach has been taken in articles 6 to 8 of the Model Law with respect to the concepts of writing, signature and original respectively and not with other concepts. This is incorporated into South African law by ECTA sections 12 (writing), s13 (signature) and s14 (original).

Party autonomy: This affords parties to electronic transactions the freedom to agree on appropriate ecommerce facilities and levels of security to suit their circumstances. This autonomy may be restricted or limited by statutory provisions.

per Luca Castellani ‘UNCITRAL legislative standards on electronic communications and electronic signatures: an introduction’ (2010)

<http://www.itu.int/oth/T1508000002/en>

THE FUNCTIONAL EQUIVALENT APPROACH

Legal requirements prescribing the use of traditional paper-based documentation are considered to be the main obstacle to the development of e-commerce. Requirements in national laws for trade-related documents and communications relating to "writing", "signature" and "original" restrict e-commerce unless there are recognized computer-based equivalents.



Electronic Transactions Law, compiled by Caroline B Ncube, Department of Commercial Law, UCT, 2012 is licensed under a Creative Commons Attribution Non-commercial Share-Alike 2.5 South Africa License

Functional equivalence “involves an examination of the function fulfilled by traditional form requirements (‘writing’, ‘signature’, ‘original’, ‘dispatch’ and ‘receipt’) and a determination as to how the same function could be transposed, reproduced, or imitated in a dematerialized environment” (JAE Faria ‘E-commerce and international legal harmonization: Time to go beyond functional equivalence?’ (2004) 16(4) *SA Merc LJ* 529, 531 note 9). For example, among the functions served by a paper document are the following:

- a) to provide that a document would be legible by all;
- b) to provide that a document would remain unaltered over time;
- c) to allow for the reproduction of a document so that each party would hold a copy of the same data;
- d) to allow for the authentication of data by means of a signature; and
- e) to provide that a document would be in a form acceptable to public authorities and courts.

See Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996) par 16.

Par agraph 16 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996) emphasises that:

“it should be noted that in respect of all of the above-mentioned functions of paper, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met. However, the adoption of the functional-equivalent approach should not result in imposing on users of electronic commerce more stringent standards of security (and the related costs) than in a paper-based environment”.

Hierarchy of form requirements

A data message, in and of itself, cannot be regarded as an equivalent of a paper document. It is of a different nature and does not necessarily perform all conceivable functions of a paper document. There is an existing hierarchy of form requirements, which provides distinct levels of reliability, traceability and unalterability with respect to paper-based documents. For example, the requirement that data be presented in written form (which constitutes a "threshold requirement") is not to be confused with more stringent requirements such as "signed writing", "signed original" or "authenticated legal act". The Model Law provides criteria which, once they are met by data messages, enable such data messages to enjoy the same level of legal recognition as corresponding paper documents performing the same function.



Electronic Transactions Law, compiled by Caroline B Ncube, Department of Commercial Law, UCT, 2012 is licensed under a Creative Commons Attribution Non-commercial Share-Alike 2.5 South Africa License

NB the functional-equivalent approach has been taken in articles 6 to 8 of the Model Law with respect to the concepts of “writing”, “signature” and “original” and not with other concepts (Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996) par 18). Each of these is discussed below:

Writing

Writing is “the lowest layer in a hierarchy of form requirements”, its main function is the reproduction of information so that it can be read and the objective criteria set by the Model Law for data messages to fulfil this function is that they “must be accessible so as to be usable [by computers and humans] for subsequent reference” (Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996) par 49 -50).

Article 6 of the Model Law provides:

“ (1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing”.

Following suit section 12 ECTA provides:

“A requirement in law that a document or information must be in writing is met if the document or information is—

(a) in the form of a data message; and

(b) accessible in a manner usable for subsequent reference.”

Signature

Signatures perform a variety of functions (e.g. identification, certification, confirmation of intent to be bound by, or to endorse, the contents of a document)

The Model Law “focuses on the two basic functions of a signature, namely to identify the author of a document and to confirm that the author approved the content of that document” (Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996) par 56 -57).

Therefore article 7 (1)(a) provides that, in an electronic environment, these functions are performed by way of a method that identifies the originator of a data message and confirms that the originator approved the content of that data message.



Article 7 (1)(b) establishes a flexible approach to the level of security to be achieved by the method of identification used under paragraph (1) (a).

In determining whether the method used under paragraph (1) is appropriate, legal, technical and commercial factors that may be taken into account include the following: (1) the sophistication of the equipment used by each of the parties; (2) the nature of their trade activity; (3) the frequency at which commercial transactions take place between the parties; (4) the kind and size of the transaction; (5) the function of signature requirements in a given statutory and regulatory environment; (6) the capability of communication systems; (7) compliance with authentication procedures set forth by intermediaries; (8) the range of authentication procedures made available by any intermediary; (9) compliance with trade customs and practice; (10) the existence of insurance coverage mechanisms against unauthorized messages; (11) the importance and the value of the information contained in the data message; (12) the availability of alternative methods of identification and the cost of implementation; (13) the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and (14) any other relevant factor (Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996) par 58).

Section 13 ECTA provides:

“(1) Where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used.

(2) Subject to subsection (1), an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form.

(3) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if—

(a) a method is used to identify the person and to indicate the person’s approval of the information communicated: and

(b) 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.

(4) Where an advanced electronic signature has been used, such signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved.



Electronic Transactions Law, compiled by Caroline B Ncube, Department of Commercial Law, UCT, 2012 is licensed under a Creative Commons Attribution Non-commercial Share-Alike 2.5 South Africa License

(5) Where an electronic signature is not required by the parties to an electronic transaction, an expression of intent or other statement is not without legal force and effect merely on the grounds that—

- (a) it is in the form of a data message; or
- (b) it is not evidenced by an electronic signature but is evidenced by other means from which such person's intent or other statement can be inferred".

ECTA also provides for advanced electronic signatures which are defined in section 2 as "an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37". Sections 37 – 41 regulate accreditation and are supplemented by the Accreditation Regulations, GN 504 of 20 June 2007. The South African Accreditation Authority has been established (www.saaa.gov.za) and is constituted by the Director-General of the Department of Communications, who is assisted by a Deputy and officers. The first accreditation was given to LAWtrust in 2012 for its digital certificate (AeSign) an advanced electronic signature (see <http://www.lawtrust.co.za/?q=aesign>)

Original

In the bricks and mortar world, an original is defined as a medium on which information was fixed for the first time. Originals are required to lessen the chance that they have been altered. The Model Law provides for originality of data messages in cases where originality is important or required e.g. for documents of title, negotiable instruments, weight certificates. It sets criteria to ensure the integrity of data messages.

Article 8 of the Model Law provides:

- "(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:
- (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and
 - (b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented".

This is incorporated into South African law by ECTA section 14 which provides:

- "(1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if—



Electronic Transactions Law, compiled by Caroline B Ncube, Department of Commercial Law, UCT, 2012 is licensed under a Creative Commons Attribution Non-commercial Share-Alike 2.5 South Africa License

- (a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and
- (b) that information is capable of being displayed or produced to the person to whom it is to be presented”.

Integrity

Both the Model Law and ECTA provide criteria for ensuring the integrity of signatures as shown below:

Model Law, article 8(3):

“For the purposes of subparagraph (a) of paragraph (1):

- (a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and
- (b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances”.

ECTA, section 14(2):

“For the purposes of subsection 1 (a), the integrity must be assessed—

- (a) 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;
- (b) in the light of the purpose for which the information was generated; and
- (c) having regard to all other relevant circumstances”.

LEGAL RECOGNITION OF DATA MESSAGES

Data messages may not be denied legal force and effect merely on the grounds that they are wholly or partly in the form of a data message and in the context of contract formation, *unless otherwise agreed by the parties*, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose (s 11(1) ECTA).

In *Sihlali v SABC* [2010] ZALC 1; (2010) 31 ILJ 1477 (LC) , an employee who was required by law to tender his resignation in writing sent an sms to his employer stating that he was terminating his employment with immediate effect. Thereafter, he sought to nullify this resignation by arguing that the sms was not ‘writing’ and therefore he had not resigned. The



Electronic Transactions Law, compiled by Caroline B Ncube, Department of Commercial Law, UCT, 2012 is licensed under a Creative Commons Attribution Non-commercial Share-Alike 2.5 South Africa License

court held that an sms message (a data message) meets the requirement of writing and that the employee had validly resigned.

Information that is incorporated in a data message is valid (section 11 (2) ECTA). Where information that is not in the public domain (or freely accessible) is incorporated into an agreement, such incorporation is only valid if it is-

(a) referred to in a way in which a reasonable person would have noticed the reference thereto and incorporation thereof; and

(b) accessible in a form in which it may be read, stored and retrieved by the other party, whether electronically or as a computer printout as long as such information is reasonably capable of being reduced to electronic form by the party incorporating it' (section 11 (3) ECTA).

These provisions enable the incorporation of information by reference in the digital environment to approximate what happens in the physical environment where this is done using annexures or appendices to written documents. In the digital environment, in numerous instances parties often incorporate information by reference. For example, many employers require their employees to affix or append an email disclaimer to email sent using their work email addresses. The email disclaimer is not spelt out in full, but a link is provided to a webpage where the full disclaimer is available. For example, UCT's disclaimer is phrased as follows:

"This e-mail is subject to the UCT ICT policies and e-mail disclaimer published on our website at <http://www.uct.ac.za/about/policies/emaildisclaimer/> or obtainable from +27 21 650 9111."

Data messages are also valid expressions of intent or other statements between contracting parties even if they are not evidenced by an electronic signature (section 24 ECTA).

Recommended Reading

Luca Castellani 'UNCITRAL legislative standards on electronic communications and electronic signatures: an introduction' (2010) <http://www.itu.int/oth/T1508000002/en>

José Angelo Estrella Faria 'e-Commerce and International Legal Harmonization: Time To Go Beyond Functional Equivalence?' (2004) 16 *SA Merc LJ* 529 – 555

Chris Reed 'Taking Sides on Technology Neutrality' (2007) 4:3 *SCRIPT-ed* 265

Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)



Electronic Transactions Law, compiled by Caroline B Ncube, Department of Commercial Law, UCT, 2012 is licensed under a Creative Commons Attribution Non-commercial Share-Alike 2.5 South Africa License