United Nations A/CN.9/WG.IV/WP.104/Add.3

General Assembly

Distr.: Limited
15 September 2003

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Forty-second session
Vienna, 17-21 November 2003

Legal aspects of electronic commerce

Electronic contracting: background information

Note by the Secretariat*

Addendum

Contents

* Submission of the present document by the secretariat of the United Nations Commission on International Trade Law was delayed by a few days owing to shortage of staff.

V.03-87972 (E) 290903 300903

III. Issues related to the use of data messages in international contracts

1. The following sections deal with issues that are either specific to contracting through electronic means or may be rendered particularly conspicuous by the use of modern means of communication. In section C issues related to the appropriateness of authentication methods and criteria for attribution of data messages are discussed, while in section D legal questions arising out of the use of fully automated systems used in electronic commerce, including mistake and error, are examined. Availability of contract terms and information obligations that might be imposed upon parties using electronic information systems are dealt with in section E. Both sections D and E appear in a further addendum (A/CN.9/WG.IV/WP.104/Add.4).

C. Form requirements

2. The preliminary draft convention on electronic contracting follows the general principle of freedom of form enshrined in the United Nations Convention on Contracts for the International Sale of Goods ("the United Nations Sales Convention")[1] and extends it to all contracts falling within its sphere of application. However, it is recognized that form requirements may exist under the applicable law as writing or signature requirements, for example when a State party to the United Nations Sales Convention has made a reservation under article 96 of the Convention.[2] Even where form requirements as such do not exist, obstacles to the use of data messages may derive from rules on evidence that expressly or implicitly limit the parties' ability to use data messages as evidence to demonstrate the existence and content of contracts.

1. Writing requirements and evidentiary value of electronic records

3. Despite the wide acceptance that the UNCITRAL Model Law on Electronic Commerce ("the Model Law") has found and the increasing number of States that have based their legislation on electronic commerce on it, an international instrument on electronic contracting could not be based on the assumption that the principles of the Model Law have already achieved universal application. It seems, therefore, useful for the new instrument to establish the conditions under which form requirements may be met by equivalent electronic methods.

4. There are not many court decisions on the legal value of electronic records. The few reported cases show an evolution towards legal recognition of electronic records and data messages, but also some uncertainty as to their admissibility both as a means for the formation of contracts and as evidence of the content of contracts.

5. In the United States of America, the courts seem to have taken a liberal approach to the admissibility of electronic records, including electronic mail (e-mail), as evidence in civil proceedings.[3] Courts in the United States have dismissed arguments that e-mail messages were inadmissible evidence because they were unauthenticated and parol evidence.[4] The courts have found instead that e-mails obtained from the plaintiff during the discovery process were self-authenticating, since "the production of documents during discovery from the parties' own files is sufficient to justify a finding of self-authentication".[5] The

courts tend to take into account all available evidence and do not reject electronic records as being prima facie insufficient evidence.

6. However, in some countries that have not adopted the Model Law, electronic records, in particular those resulting from Internet transactions, have been said to be "devoid of legal value".[6] Moreover, concerns about the risk of manipulation in electronic records have led to court decisions that dismiss the value, for instance, of e-mails as evidence in court proceedings on the grounds that e-mails do not offer adequate guarantees of integrity.[7]

7. Case law on this issue is still at an incipient stage and, given the small number of court decisions to date, does not provide a sufficient basis to draw firm conclusions. Nevertheless, it could be argued that international commerce might benefit from the enhanced legal certainty that would result from uniform provisions that offered criteria for the recognition of electronic records and data messages in international trade. Article 9, paragraph 2, of the preliminary draft convention reproduces, for that purpose, the criteria contained in article 6 of the Model Law for the legal recognition of data messages as "writings".

2. Attribution of messages and signature requirements

8. The use of electronic methods of identification involves two aspects that may deserve consideration by the Working Group. The first aspect relates to the general issue of attribution of a message to its purported originator. The second aspect relates to the appropriateness of the identification method used by the parties for the purpose of meeting legal form requirements, in particular signature requirements. Also relevant are legal notions that imply the existence of a handwritten signature, as is the case for the notion of "document" in some legal systems. Even though these two aspects may often be combined or, depending on the circumstances, may not be entirely distinguishable one from another, an attempt to analyse them separately may be useful, as it appears that courts tend to reach different conclusions according to the function being attached to the identification method.

(a) Attribution of data messages

9. The Model Law deals with attribution of data messages in its article 13. That provision has its origin in article 5 of the UNCITRAL Model Law on International Credit Transfers, which defines the obligations of the sender of a payment order. Article 13 is intended to apply where there is a question as to whether a data message was really sent by the person who is indicated as being the originator. In the case of a paper-based communication the problem would arise as the result of an alleged forged signature of the purported originator. In an electronic environment, an unauthorized person may have sent the message but the authentication by code, encryption or the like would be accurate. The purpose of article 13 is not to assign responsibility. It deals rather with attribution of data messages by establishing a presumption that under certain circumstances a data message would be considered a message of the originator.

10. Article 13, paragraph 1, of the Model Law recalls the principle that an originator is bound by a data message if it has effectively sent that message. Paragraph 2 refers to a situation where the message was sent by a person other than the originator who had the authority to act on behalf of the originator. Paragraph 3

deals with two kinds of situation in which the addressee could rely on a data message as being that of the originator: firstly, situations in which the addressee properly applied an authentication procedure previously agreed to by the originator; and, secondly, situations in which the data message resulted from the actions of a person who, by virtue of his or her relationship with the originator, had access to the originator's authentication procedures.

11. A number of countries have adopted the rule in article 13 of the Model Law, including the presumption of attribution established in paragraph 3 of that article.[8] Some countries expressly refer to the use of codes, passwords or other means of identification as factors that create a presumption of authorship.[9] There are also more general versions of article 13, in which the presumption created by proper verification through a previously agreed procedure is rephrased as an indication of elements that may be used for attribution purposes.[10]

12. Other countries, however, have adopted only the general rules in article 13 that a data message is that of the originator if it was sent by the originator itself or by a person acting on the originator's behalf, or by a system programmed by or on behalf of the originator to operate automatically.[11] Lastly, a few countries that have implemented the Model Law have not included any specific provision based on article 13.[12] The assumption in those countries was that no specific rules were needed and that attribution was better left to ordinary methods of proof, the same way as attribution of documents on paper: "The person who wishes to rely on any signature takes the risk that the signature is invalid, and this rule does not change for an electronic signature."[13]

13. In countries that have not adopted the Model Law, there seem to be no specific legislative provisions dealing with attribution in an analogous fashion. In those countries, attribution is typically a function of the legal recognition of electronic signatures and the presumptions attached to records authenticated with particular types of electronic signature.

14. Thus far, the preliminary draft convention has not included specific rules on attribution on the basis of article 13 of the Model Law. The Working Group may wish to consider, however, whether it might be useful to consider formulating provisions on attribution separately from provisions on electronic signatures. The reason for such an approach is that signatures are not the only method of identification recognized by law to attribute documents and records to a given person, as the official comments to the relevant provision of the United States Uniform Electronic Transactions Act (UETA) explain:[14]

> "1. Under subsection (a) [of UETA section 9], so long as the electronic record or electronic signature resulted from a person's action it will be attributed to that person—the legal effect of that attribution is addressed in subsection (b). This section does not alter existing rules of law regarding attribution. The section assures that such rules will be applied in the electronic environment. A person's actions include actions taken by human agents of the person, as well as actions taken by an electronic agent, i.e., the tool, of the person. Although the rule may appear to state the obvious, it assures that the record or signature is not ascribed to a machine, as opposed to the person operating or programming the machine.

"In each of the following cases, both the electronic record and electronic signature would be attributable to a person under subsection (a):

"A. The person types his/her name as part of an e-mail purchase order;

"B. The person's employee, pursuant to authority, types the person's name as part of an e-mail purchase order;

"C. The person's computer, programmed to order goods upon receipt of inventory information within particular parameters, issues a purchase order which includes the person's name, or other identifying information, as part of the order.

"In each of the above cases, law other than [UETA] would ascribe both the signature and the action to the person if done in a paper medium. Subsection (a) expressly provides that the same result will occur when an electronic medium is used.

"2. Nothing in [UETA section 9] affects the use of a signature as a device for attributing a record to a person. Indeed, a signature is often the primary method for attributing a record to a person. In the foregoing examples, once the electronic signature is attributed to the person, the electronic record would also be attributed to the person, unless the person established fraud, forgery, or other invalidating cause. However, a signature is not the only method for attribution.

"3. The use of facsimile transmissions provides a number of examples of attribution using information other than a signature. A facsimile may be attributed to a person because of the information printed across the top of the page that indicates the machine from which it was sent. Similarly, the transmission may contain a letterhead which identifies the sender. Some cases have held that the letterhead actually constituted a signature because it was a symbol adopted by the sender with intent to authenticate the facsimile. However, the signature determination resulted from the necessary finding of intention in that case. Other cases have found facsimile letterheads NOT to be signatures because the requisite intention was not present. The critical point is that with or without a signature, information within the electronic record may well suffice to provide the facts resulting in attribution of an electronic record to a particular party.

"In the context of attribution of records, normally the content of the record will provide the necessary information for a finding of attribution. It is also possible that an established course of dealing between parties may result in a finding of attribution. Just as with a paper record, evidence of forgery or counterfeiting may be introduced to rebut the evidence of attribution.

"4. Certain information may be present in an electronic environment that does not appear to attribute but which clearly links a person to a particular record. Numerical codes, personal identification numbers, public and private key combinations all serve to establish the party to whom an electronic record should be attributed. Of course security procedures will be another piece of evidence available to establish attribution.

> "The inclusion of a specific reference to security procedures as a means of proving attribution is salutary because of the unique importance of security procedures in the electronic environment. In certain processes, a technical and technological security procedure may be the best way to convince a trier of fact that a particular electronic record or signature was that of a particular person. In certain circumstances, the use of a security procedure to establish that the record and related signature came from the person's business might be necessary to overcome a claim that a hacker intervened. The reference to security procedures is not intended to suggest that other forms of proof of attribution should be accorded less persuasive effect. It is also important to recall that the particular strength of a given procedure does not affect the procedure's status as a security procedure, but only affects the weight to be accorded the evidence of the security procedure as tending to establish attribution."

15. It also seems important to bear in mind that a presumption of attribution would not by itself displace the application of rules of law on signatures, where a signature is needed for the validity or proof of an act. Once it is established that a record or signature is attributable to a particular party, "the effect of a record or signature must be determined in light of the context and surrounding circumstances, including the parties' agreement, if any" as well as of "other legal requirements considered in light of the context".[15]

16. Examples of a more restrictive approach to attribution can be found in recent cases involving Internet auctions, in which courts have applied a high standard for attribution of data messages. Those cases have typically involved suits for breach of contract on grounds of lack of payment for goods allegedly purchased in Internet auctions. Claimants maintained that defendants were the buyer, as the highest bid for the goods had been authenticated with the defendant's password and had been sent from the defendant's e-mail address. The courts have found that those elements were not sufficient to firmly conclude that it was in fact the defendant who had participated in the auction and submitted the winning bid for the goods. The courts have used various arguments to justify that position. For example, passwords were not reliable because anyone who knew the defendant's password could have used its e-mail address from anywhere and participated in the auction using the defendant's name,[16] a risk that some courts, on the basis of expert advice on security threats to Internet communications networks, in particular through the use of so-called "Trojan horses" capable of "stealing" a person's password, estimated as "very high".[17] The risk of unauthorized use of a person's identification device (password) should be borne by the party that offered goods or services through a particular medium, as there was no legal presumption that messages sent through an Internet web site with recourse to a person's access password to such web site were attributable to that person.[18] Such a presumption might conceivably be attached to an "advance electronic signature", as defined in law, but the holder of a simple "password" should not bear the risk of its being misused by unauthorized persons.[19]

17. Uniform rules for attribution of data messages may be useful to enhance legal certainty as to the elements upon which a party may rely for the attribution of responsibility for data messages. Such rules could be formulated as a presumption, using the elements of article 13 of the Model Law. They may have the additional

advantage of limiting the scope of issues expected to be solved by common standards on electronic signatures, which often serve a different purpose.

(b) Signature requirements

18. As regards signature requirements, one question that the Working Group needs to consider is whether the preliminary draft convention should limit itself to a general provision on the recognition of electronic signatures or whether it should spell out the conditions for the legal recognition of electronic signatures in a greater level of detail. Under the first option, the Working Group might wish to introduce in the new instrument a provision along the lines of article 7, paragraph 1, of the Model Law. That option is reflected in variant A of paragraph 3 of draft article 9. Under the second option, the Working Group would use more detailed language along the lines of article 6, paragraph 3, of the UNCITRAL Model Law on Electronic Signatures. That option is reflected in variant B of paragraph 3 of draft article 9. It should be noted these options are not mutually exclusive, since article 7, paragraph 1, of the Model Law on Electronic Commerce was the basis for the more detailed rules in article 6, paragraph 3, of the Model Law on Electronic Signatures.

19. Ultimately, the choice between the two variants involves a decision on the desirable level of detail in order to provide meaningful guidance and an acceptable level of uniformity. In any event, it seems important that the rules preserve the appropriate degree of flexibility so as to allow the parties and the courts to assess the adequacy and reliability of the authentication methods used in the light of all relevant circumstances.

20. In some countries, the courts have been inclined to interpret signature requirements liberally. Courts in the United States have been receptive to legislative recognition of electronic signatures, admitting their use also in situations not expressly contemplated in the enabling statute, such as in judicial warrants.[20] More importantly for a contractual context, the courts have also assessed the adequacy of the identification in the light of the dealings between the parties, rather than using a strict standard for all situations. Thus, where the parties had regularly used e-mail in their negotiations, the courts have found that the originator's typed name in an e-mail satisfied statutory signature requirements.[21] A persons "deliberate choice to type his name at the conclusion of all e-mails" has been considered to be valid authentication.[22] A similarly liberal approach is taken by courts in Colombia that have confirmed the admissibility of judicial proceedings conducted entirely by electronic communications. The submissions exchanged during such proceedings were valid, even if they were not signed with a digital signature,[23] as the electronic communications used methods that allowed for the identification of the parties.[24]

21. However, in other countries, such as France, courts have been reluctant to accept electronic means of identification as equivalent to handwritten signatures prior to the adoption of legislation expressly recognizing the validity of electronic signatures.[25] At the same time, however, there are decisions that accept the electronic filing of administrative complaints for the purpose of meeting a statutory deadline, at least as long as they are subsequently confirmed by regular mail.[26]

22. In contrast to their restrictive approach to the attribution of data messages in the formation of contracts, German courts have been liberal in the acceptance of identification methods as equivalent to handwritten signatures in court proceedings.

The debate in Germany has evolved around the increasing use of scanned images of legal counsel's signature to authenticate computer facsimiles containing statements of appeals transmitted directly from a computer station via modem to a court's facsimile machine. In earlier cases, courts of appeal[27] and the Federal Court (*Bundesgerichtshof*)[28] had held that a scanned image of a handwritten signature did not satisfy existing signature requirements and offered no proof of a person's identity. An identification might conceivably be attached to an "advance electronic signature", as defined in German law. Generally, however, it was for the legislator and not the courts to establish the conditions for the equivalence between writings and intangible communications transmitted by data transfers.[29] That understanding was eventually reversed in view of the unanimous opinion of the other high federal courts that accepted the delivery of certain procedural pleas by means of electronic communication of a data message accompanied by a scanned image of a signature.[30]

23. It is not suggested that the considerations that justify a liberal approach in the context of judicial or administrative appeals can be transposed directly to the context of international contracts. Indeed, while in a contractual context a party might be faced with the risk of repudiation of the agreement by the other party, in the context of civil proceedings it is typically the party using electronic signatures or records that is interested in confirming its approval of the record and its contents. Nevertheless, the above discussion shows how courts may be inclined in practice to assess the reliability of authentication methods in the light of the purposes for which they are used.

24. Another aspect that the Working Group may wish to bear in mind in its discussions is that under both article 7, paragraph 3, of the Model Law on Electronic Commerce and article 6, paragraph 5, of the Model Law on Electronic Signatures an enacting State has the possibility to exclude the recognition of electronic signatures in specific situations to be set forth in domestic legislation. Ideally, international legal harmonization would be best served by a commonly agreed list of exclusions. It is recognized, however, that such a result might not easily be achieved. One possible alternative, which the Working Group may wish to consider, might be to exclude only those situations where domestic laws either categorically exclude electronic signatures or where they prescribe the use of a particular type of electronic signature ("advanced signature" or "secure signature").

Notes

[1] United Nations, *Treaty Series*, vol. 1489, No. 25567, p. 3 (also available at www.uncitral.org/english/texts/sales/CISG.htm).

[2] Under that provision:

> "A Contracting State whose legislation requires contracts of sale to be concluded in or evidenced by writing may at any time make a declaration in accordance with article 12 that any provision of article 11, article 29, or Part II of this Convention, that allows a contract of sale or its modification or termination by agreement or any offer, acceptance, or other indication of intention to be made in any form other than in writing, does not apply where any party has his place of business in that State."

[3] *Commonwealth Aluminum Corporation v. Stanley Metal Associates*, United States District Court for the Western District of Kentucky, 9 August 2001, Federal Supplement, 2nd series, vol. 186, p. 770; and *Central Illinois Light Company (CILCO) v. Consolidation Coal Company (Consol)*,

United States District Court for the Central District of Illinois, 30 December 2002, Federal Supplement, 2nd series, vol. 235, p. 916.

[4] In *Sea-Land Service, Inc. v. Lozen International, Llc.*, for example, a court of appeal reversed a decision by a district court that had excluded an internal company e-mail authored by one plaintiff's employees. The district court excluded this evidence on the ground that the defendant "makes no argument, nor does it present any evidence indicating the identity or job title of [the] employee" who authored the e-mail. The court of appeal noted that the original e-mail, an internal company memorandum, closed with an electronic "signature" indicating the name and function of the drafter. The district court had therefore abused its discretion when it excluded the e-mail as evidence (United States Court of Appeals for the Ninth Circuit, 3 April 2002, Federal Reporter, 3rd series, vol. 285, p. 808).

[5] *Superhighway Consulting, Inc. v. Techwave, Inc.*, United States District Court for the Northern District of Illinois, Eastern Division, 16 November 1999, U.S. Dist. LEXIS 17910.

[6] (Undated) statement by Judge Ruy Rosado de Aguiar Jr. of the Brazilian Superior Tribunal de Justiça ("*Comércio eletrônico não tem valor jurídico*", at www.trabalhodeeconomia.hpg.ig.com.br/juri.html, accessed on 12 September 2003).

[7] Amtsgericht Bonn, Case No. 3 C 193/01, 25 October 2001, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 332/2002 (available at www.jurpc.de/rechtspr/20020332.htm, accessed on 11 September 2003). In this case, the claimant sued the defendant demanding payment of a broker's fee for acting as an intermediary in a bulk sale of cigarettes. The court dismissed the claim for lack of proof of an agreement for the payment of a fee. The court held that the e-mail printouts produced by the claimant and repudiated by the defendant had no value as evidence, as it is "generally known" that ordinary e-mails can be easily altered or forged.

[8] See Colombia (*Ley Número 527 de 1999: Ley de comercio electrónico*, art. 17); Ecuador (*Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, 2002, art. 10); Jordan (Electronic Transactions Law (No. 85) of 2001, art. 15); Mauritius (Electronic Transactions Act, 2000, section 12(2)); Philippines (Electronic Commerce Act, 2000, sect. 18, para. (3)); Republic of Korea (Framework Law on Electronic Commerce, 1999, art. 7, para. (2)); Singapore (Electronic Transactions Act, 1998, subsect. 13 (3)); Thailand (Electronic Transactions Act, 2002, sect. 16); and Venezuela (*Decreto nº 1024 de 10 de febrero de 2001—Ley sobre mensajes de datos y firmas electrónicas*, art. 9). The same rules are also contained in the laws of the British Crown Dependency of Jersey (Electronic Communications (Jersey) Law 2000, art. 8), and the British overseas territories of Bermuda (Electronic Transactions Act, 1999, sect. 16, para. 2) and Turks and Caicos (Electronic Transactions Ordinance, 2000, sect. 14).

[9] Mexico (*Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal* of 26 April 2000, art. 90, para. I).

[10] For example, the United States Uniform Electronic Transactions Act (UETA), provides in section 9 (a) that an electronic record or electronic signature "is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable". Section 9 (b) provides further that the effect of an electronic record or electronic signature attributed to a person under subsection (a) "is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law".

[11] Australia (Electronic Transactions Act, 1999, sect. 15, subsect. (1)); essentially in the same manner, India (Information Technology Act, 2000, sect. 11); Pakistan (Electronic Transactions Ordinance, 2002, sect. 13 (2)); Slovenia (Electronic Commerce and Electronic Signature Act, 2000, art. 5); in the British Crown Dependency of the Isle of Man (Electronic Transactions Act, 2000, sect. 2); and in the Hong Kong Special Administrative Region of China (Electronic Commerce Ordinance, 2000, sect. 18).

[12] For example, Canada, France, Ireland, New Zealand and South Africa.

[13] Uniform Law Conference of Canada, *Uniform Electronic Commerce Act (Annotated)*, commentary to section 10 (2) (available at www.ulcc.ca/en/poam2/index.cfm?sec=1999&sub=1999ia, accessed on 11 September 2003).

[14] National Conference of Commissioners on Uniform State Laws, *Uniform Electronic Transactions Act (1999)*, approved and recommended for enactment in all the states at its 108th annual conference meeting (Denver, Colorado, 23-30 July 1999), with prefatory note and comments (available at www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm, accessed on 11 September 2003).

[15] Ibid.

[16] Amtsgericht Erfurt, Case No. 28 C 2354/01, 14 September 2001, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 71/2002 (available at www.jurpc.de/rechtspr/20020071.htm, accessed on 25 August 2003).

[17] Landgericht Konstanz, Case No. 2 O 141/01 A, 19 April 2002, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 291/2002 (available at www.jurpc.de/rechtspr/20020291.htm, accessed on 25 August 2003).

[18] Landgericht Bonn, Case No. 2 O 450/00, 7 August 2001, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 136/2002 (available at www.jurpc.de/rechtspr/20020136.htm, accessed on 25 August 2003).

[19] Oberlandesgericht Köln, Case No. 19 U 16/02, 19 April 2002, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 291/2002 (available at www.jurpc.de/rechtspr/20020291.htm, accessed on 25 August 2003).

[20] *Department of Agriculture & Consumer Services v. Haire*, Court of Appeal of Florida, Case Nos. 4D02-2584 & 4D02-3315, 15 January 2003 (available at www.4dca.org/Jan2003/01-15-03/4D02-2584op.pdf, accessed on 12 September 2003).

[21] *Cloud Corporation v. Hasbro, Inc.* involved a suit for breach of contract in which the defendant denied having placed a number of purchase orders. The parties had communicated through e-mail. It appeared that some of the correspondence exchanged contained no signature. The district court entered judgement in favour of the defendant for lack of proof of the alleged purchase commitments. The court of appeal reversed that judgement, holding that the sender's name on an e-mail satisfied the signature requirement of the statute of frauds. The court of appeal held further that neither common law nor the Uniform Commercial Code required a handwritten signature, "even though such a signature is better evidence of identity than a typed one". The purpose of the statute of frauds according to the court "is to prevent a contracting party from creating a triable issue concerning the terms of the contract—or for that matter concerning whether a contract even exists—on the basis of his say-so alone. That purpose does not require a handwritten signature, especially in a case in which there is other evidence, and not merely say-so evidence, of the existence of the contract besides the writings" (United States Court of Appeals for the Seventh Circuit, 26 December 2002, Federal Reporter, 3rd series, vol. 314, p. 296).

[22] *Jonathan P. Shattuck v. David K. Klotzbach*, Superior Court of Massachusetts, 11 December 2001, 2001 Mass. Super. LEXIS 642. In this case, the buyer filed an action to enforce a contract for the sale of real property and to recover damages arising out of an alleged breach of that contract against the sellers. The sellers filed a motion to dismiss alleging that there was no written and signed sales contract that met the form requirements of the laws of Massachusetts. The parties had negotiated the sale of real estate through the exchange of e-mails. All e-mail correspondence between the parties contained a typewritten signature at the end. The court held that the parties had formed an agreement as to the essential terms of the land sale contract: the parties, the locus, the nature of the transaction and the purchase price, satisfying the statute of frauds. Moreover, the court held that the e-mails sent by the seller regarding the terms of the

sale of the property were intended to be authenticated by the seller's typed name at the closing of his mails.

[23] Colombia has adopted the UNCITRAL Model Law on Electronic Commerce. Although the law contains a general provision similar to article 7 of the Model Law, the law establishes a legal presumption of authenticity only in respect of digital signatures (*Ley Número 527 de 1999: Ley de comercio electrónico*, article 28).

[24] *Juan Carlos Samper v. Jaime Tapias*, Juzgado Segundo Promiscuo Municipal Rovira Tolima, 21 July 2003, Rad. 73-624-40-89-002-2003-053-00 (available at www.alfa-redi.org/documento/alexdiaz.pdf, accessed on 12 September 2003).

[25] The Cour de Cassation rejected the receivability of a statement of appeal signed electronically, because there were doubts as to the identity of the person who created the signature and the appeal had been signed electronically before entry into force of the law of 13 March 2000, which recognized the legal effect of electronic signatures (Cour de Cassation, Second Civil Chamber, 30 April 2003, *Société Chalets Boisson v. M. X.*, available at www.juriscom.net/jpt/visu.php?ID=239, accessed on 12 September 2003).

[26] Conseil d'État, 28 December 2001, N° 235784, *Élections municipales d'Entre-Deux-Monts* (available at www.rajf.org/article.php3?id_article=467**,** accessed on 12 September 2003).

[27] For instance, Oberlandesgericht Karlsruhe, Case No. 14 U 202/96, 14 November 1997, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 09/1998 (available at www.jurpc.de/rechtspr/19980009.htm, accessed on 12 September 2003).

[28] Bundesgerichtshof, Case No. XI ZR 367/97, 29 September 1998, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 291/2002 (available at www.jurpc.de/rechtspr/19990005.htm, accessed on 12 September 2003).

[29] The Bundesgerichtshof recognized that case law had for some time accepted the use of facsimile for transmission of pleas. In such cases, however, the original document had to be signed by hand by counsel and such signature usually appeared in the facsimile copy received by the courts. Facsimiles generated and transmitted directly by a computer, however, did not produce an original document in tangible form. Neither was the document signed by counsel by hand. Only the printout of the facsimile by the court's facsimile machine generated a tangible paper document. Accepting computer facsimiles would ultimately mean waiving the writing requirements created by statute. The legislator was called upon to establish the conditions for the equivalence between writings and intangible communications transmitted by data transfers. That result, in the view of the Bundesgerichtshof, could only be achieved by statute and not by case law (see note 28).

[30] In a decision on a case referred to it by the Bundesgerichtshof (see note 26 above), the Joint Chamber of the Highest Federal Courts of Germany (Gemeinsamer Senat der obersten Gerichtshöfe des Bundes) noted that form requirements in court proceedings were not an end in themselves. Their purpose was to ensure a sufficiently reliable ("*hinreichend zuverlässig*") determination of the content of the writing and the identity of the person from whom it emanated. The Joint Chamber noted the evolution in the practical application of form requirements, so as to accommodate earlier technological developments, such as telex or facsimile. The Joint Chamber held that accepting the delivery of certain procedural pleas by means of electronic communication of a data message with a scanned image of a signature would be in line with the spirit of existing case law (Gemeinsamer Senat der obersten Gerichtshöfe des Bundes, GmS-OGB 1/98, 5 April 2000, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 160/2000 (available at www.jurpc.de/rechtspr/20000160.htm, accessed on 12 September 2003).