I. I. ELECTRONIC COMMERCE IN GENERAL

This chapter is intended to provide a brief overview of the Brazilian legal framework regarding electronic contracts and electronic signatures as well as a comparison of such legal framework with the Model Law on Electronic Commerce 1996 (hereinafter referred to as "**ML 1996**") and Model Law on Electronic Signatures 2001 (hereinafter referred to as "**ML 2001**"), both issued by the United Nations Commission on Trade Law (hereinafter referred to as "**UNCITRAL**").

A. GENERAL

Legal Framework

It is important to point out that there is no federal statute in Brazil regarding electronic contracts. For this reason, it is not possible to either present Brazil's legal framework concerning e-commerce or, consequently, to compare it with ML 1996 and ML 2001.

Notwithstanding the above, some drafts of federal statutes have been proposed by Brazilian congressmen in the past few years, but as of today none of them have been voted by the Brazilian Congress.

From those drafts, Draft n. 1.483/1999 (hereinafter referred to as the "**Draft**") is at an advanced stage, since it has been approved by a special commission created by the Brazilian Congress to analyze its content[1].

As of today, the Draft is pending to be voted by the Brazilian Congress although there is

[1] Special Commission created by the Brazilian Congress to analyze the Draft number 1.483 and attached drafts (hereinafter referred to as the "**Special Commission**").

no reasonable expectation as to whether such fact will take place soon[2].

The Draft constitutes a complete legal framework for the e-commerce, and was prepared following a public hearing where many companies of the electronic sector as well as the judiciary power have been heard[3].

Thus, in this chapter, we will compare the dispositions of the Draft and the ML 1996 and ML 2001, eventually indicating, when appropriate, general contract rules that could be also applied to a specific situation.

Jurisprudence and scholars

In light of the fact that there is no legal framework in Brazil that specifically regulates e-commerce, Brazilian scholars have applied to this area Brazilian common contract law principles expressed in the Brazilian Civil Code, dated 10 January 2002 (hereinafter referred to as the "**Brazilian Civil Code**")[4].

Such scholars have defined electronic contracts as regular and normal contracts which, nevertheless, have the peculiarity of being formed through the internet. Thus, electronic contracts cannot be considered as a new type of contract[5].

By the same token, there is no leading case in Brazilian jurisprudence, whether from the Brazilian Superior Court of Justice or from the Brazilian Supreme Court regarding the

---

[2] This was the information received by the author on 6 August, 2004, from the cabinet of the Congressman Mr. Julio Semeghini who was the congressman designated by the Special Commission to elaborate the current final version of the Draft.

[3] For a complete overview of the parties which were heard in this public hearing, please refer to the report prepared by the Special Commission, Available at http://www.camara.gov.br/Internet/comissao/index/esp/CEPL1483_relatorio.htn (hereinafter referred to as the "**Report**").

[4] Available at <http://www.presidencia.gov.br/ccivil_03/LEIS/2002/L10406.htm>.

[5] MARQUES, CLÁUDIA LIMA. *Contratos no Código de Defesa do Consumidor o novo regime das relações contratuais*. 4. ed. São Paulo, Revista dos Tribunais, 2002, p. 103.

See also GRECO, Marco Aurélio, Martins; SILVA, Ives Gandra (Org.). *Direito e Internet: relações jurídicas na sociedade informatizada*. São Paulo. Revista dos Tribunais, 2001, p. 18.

legal framework applicable to electronic contracts.

1. Sphere of Application

The scope of the Draft, as per its Article 1 is to regulate: (i) the validity and strength as a means of evidence of data messages and of electronic signatures; (ii) the digital certification; and (iii) the e-commerce.

The regulation of e-commerce is applicable to any offer of goods, services and information, as per Article 25 of the Draft, which appears to meet the broad concept of commercial activities exposed and recommended by the ML 1996[6].

Moreover, as per the definition of data message mentioned in item (2) below, the Draft intends to cover all information generated, sent, received or stored by any electronic means, not including in its scope therefore, any kind of paper communication that will continue to be regulated by the Brazilian Civil Code.

It is also important to highlight that, according to the Draft, the Brazilian Civil Code will be applied subsidiarily[7].

2. Definitions

Data message is defined by Article 2.I of the Draft as the information generated, sent, received or stored by electronic, optical, optical-electronic or similar means. This definition is almost a literal translation of the definition provided in Article 2 of the ML 1996, except for the expression optical-electronic which, although not expressly mentioned in Article 2 of the ML 1996, is clearly included in its scope.

---

[6] As it is stated in the footnote **** to article 1 of the ML 1996, "*the term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not.*" See UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996, p. 4, available at <http://uncitral.org/english/texts/electcom/ml-ecomm.htm>.

[7] See article 26 of the Draft.

The other definitions provided by ML 1996 are not expressly contemplated by the Draft, which certainly makes the application of its dispositions more difficult.

Nevertheless, the definition of terms such as Originator, Addressee, Intermediary and Information System may be derived from the content of numerous clauses of the Draft[8].

3. Interpretation

There is no reference in the Draft regarding the interpretation of its dispositions, which leads us to the conclusion that the Draft's provisions will be construed by Brazilian Courts exclusively by reference to the concepts of Brazilian Law[9]. For that reason, it is not possible to assert that in the interpretation of the Draft, Brazilian Courts would take into account the international aspects and origin of the e-commerce and ML 1996's provisions itself.

Moreover, it should be noted that Article 3 of the ML 1996 is inspired by Article 7 of the United Nations Convention on Contracts for the International Sale of Goods, Vienna 1980[10], to which Brazil is not a party.

4. Variation by agreement

As a general rule, Brazilian law does not embrace the principle of party autonomy regarding the possibility of the parties to elect a determined applicable law to a contract nor to avoid the application of some provisions of a specific law[11].

---

[8] It is interesting to observe that even though the Special Commission expressly stated that the use of definitions in a federal statute is important, the Draft contains just a few. See Report, p. 18.

[9] For a complete overview regarding the interpretation methods that must be used by Brazilian Courts in the application of the rules foreseen in Brazilian federal statutes, see MAXIMILIANO, Carlos. *Hermenêutica e Aplicação do Direito*. 19 ed. São Paulo. Forense. 2000.

[10] Available at < http://www.uncitral.org/english/texts/sales/CISG.htm>.

[11] See ARAÚJO, Nádia de. *Contratos Internacionais*. 3 ed. São Paulo. Renovar. 2004.

In fact, in the past few years, Brazilian courts, in many cases, have not been applying any law, different from the Brazilian law, to a contract executed in Brazil. There are a number of reasons as to why this has been carried out[12].

Notwithstanding the above, the main exception for this principle takes place when the parties choose to resolve their controversies through an arbitration procedure[13].

Even in that case, the chosen law cannot contradict Brazilian public policy[14] and the parties cannot avoid the application of just some provisions of the chosen law.

With specific regards to the Draft, it has no provision whatsoever related to such matter nor has the doctrine faced such issue before, which makes it very difficult to foresee what would be the position of Brazilian Courts when facing a choice of law clause in an electronic contract.

Taking into account that as per the Brazilian jurisprudence the courts are very reluctant to accept the application of foreign laws, it is very likely that Brazilian Courts would apply the dispositions of the Draft to an electronic contract executed in Brazil[15], especially the Draft's provisions regarding the requirements for the validity of an offer[16].

B. APPLICATION OF LEGAL REQUIREMENTS TO DATA MESSAGES

[12] For a complete analysis, please see ARAÚJO, Nádia de. *Contratos Internacionais*. 3 ed. São Paulo. Renovar. 2004. This author has made extensive research about this matter and she has concluded that, as of today, Brazilian Courts have not directly faced this problem and they usually apply Brazilian Law for some procedural reasons, avoiding, therefore, the necessity to analyze the validity of a clause that determines the application of a foreign law to a contract executed in Brazil.

[13] Article 2.1. of the Federal Statute No. 9.307, dated 23 September 1996.

[14] Article 2.1. of the Federal Statute No. 9.307, dated 23 September 1996.

[15] Unless such electronic contract has an arbitration clause. Even in that case, the elected law could not contradict Brazilian public policy.

[16] Article 31 of the Draft.

1. Legal recognition of data messages

According to the Draft, an electronic document shall not be denied judicial effect, validity and enforceability solely because it is in an electronic form[17].

2. Incorporation by reference

The Draft does not contemplate the figure of the incorporation by reference. Thus, it is not certain whether the general rules regarding such matter and applicable to those contracts subject to Brazilian Law would be applicable in the electronic environment[18].

However, it is important to point out that the rules regarding consumer contracts, particularly the ones related to contracts of adhesion and the incorporation by reference issues derived thereto, will be applicable to electronic contracts as per Article 30 of the Draft[19].

3. Writing

Even though the Draft does not expressly refer to the data message as a written document, it is clear as per an interpretation of many dispositions of the Draft, that for legal purposes a data message is considered as information in writing.

---

[17] See Article 3 of the Draft. Such Article 3 is almost a reproduction of Article 5 of the ML 1996.

[18] According to Brazilian Law, incorporation by reference can be used in (a) adhesion agreements, (b) standard agreements or (c) in agreements executed with the Brazilian Public Government. Such incorporation by reference, in the first two cases mentioned above, will only be considered valid in the event it is mutually agreed among the parties.

In the scope of consumer law, the use of this kind of clause is submitted to the following conditions: (i) the consumer must have been informed, before signing the corresponding contract, of the existence of a incorporation by reference itself; (ii) the consumer must be informed of the content of what is going to be incorporated by reference; and (iii) the consumer must expressly accept such incorporation by reference.

In addition to this, Brazilian law establishes that the clauses negotiated between the parties shall always prevail over the ones incorporated by reference.

[19] For a more complete analysis of the application to the electronic contracts of the rules regarding consumer protection, please refer to section II.II.B. below.

For instance, Article 7 of the Draft stipulates that all evidence rules applicable for written documents and foreseen in Federal Statute 5.869, dated 11 January 1973 (hereinafter referred to as the "**Brazilian Civil Procedure Code**") will be applicable to data messages.

Such disposition clearly proves the legislator's intent to compare a data message to any other written document, as long as the requirements foreseen in the Draft and in this chapter explained are met (such as the existence of a valid electronic signature[20]).

Nevertheless, the fact that a data message is considered a written document does not mean that, whenever Brazilian law requires the validity of a specific document the adoption of a certain formality[21], such requirement could be met through the use of an electronic document. For example, any written document that must be formalized and executed as a notarial document[22] will not be valid if it is formalized in a data message.

4. Signature

General

The Draft, in its Article 4, adopts the idea contemplated in the ML 1996, especially in its Article 7, regarding the functions and effects of an electronic signature.

The Draft intends to create a secure and reliable system where the validity and enforceability of an electronic signature could prevail in the event the parties

[20] Please refer to section (4) below.

[21] See Article 104 of the Brazilian Civil Code.

[22] For an example of such requirement, please refer to Article 105 of the Brazilian Civil Code regarding the constitution of burdens over a real state.

would go to Court to contest an electronic signature validly executed. Moreover, the Draft, as it is going to be demonstrated below, maintains the idea that the electronic signature has as its main functions the identification of a person and the possibility to prove the person's involvement with the content of the data message that bears his electronic signature.

It is important to highlight that in order to achieve those purposes the Draft adopts a very conservative approach, conditioning the validity of an electronic signature to the existence of a corresponding digital certificate –what is not required in the ML 2001- and to the strict compliance of some specific requirements.

Legal Framework

Even though as a general rule Brazil does not have a regulation on electronic signatures, it should be noted that the *Medida Provisória* No. 2.200, dated 24 August, 2001, created the Public Key Infrastructure in Brazil (hereinafter referred to as "**ICP-BRAZIL**").

Such statute neither regulates the issues foreseen in the ML 2001 nor the ones expressed in the Draft since the above *Medida Provisória* No. 2.200 is limited to establish a basic framework for the technical procedures that must be adopted in order to guarantee the authenticity and integrity of data messages that use a digital certificate.

The ICP-BRAZIL was created by a presidential decree (*Medida Provisória*) that, as of today, have not been confirmed by the Brazilian Congress[23]. Moreover, the

[23] According to the text of the Brazilian Constitution that was enforceable by the time the *Medida Provisória No. 2.200* was issued, a *Medida Provisória* is an act issued by the Brazilian President that must be confirmed by the Brazilian congress within 30 days of its issuance date in order to be definitely considered inserted into Brazilian law. Notwithstanding the before mentioned, while the Brazilian Congress does not vote the *Medida Provisória*, the President is able to indefinitely prorogate its period of

Draft does not adopt all the concepts expressed in such presidential decree.

a. Sphere of Application

The Draft, as it is explained in the Report, intends to gather in only one federal statute all the regulations regarding data messages and electronic signatures. The rational behind this is to facilitate its application by the legal community as a whole and to avoid conflicts in the event those issues were regulated in two or more federal statutes.

The Draft has chosen the same approach of the ML 2001 regarding the sphere of application of its dispositions. According to the Draft, the regulation of electronic signatures are applicable to any kind of relationship, regardless of whether it is public or private, civil or commercial, such as it is foreseen in footnote ** to Article 1 of the ML 2001[24].

b. Definitions

The Report expressly refers, in its page 18, that the adoption of definitions in the text of the Draft is very important for the correct application of its dispositions since the Draft, at many times, deals with very complex and technical expressions that are unknown for many of those who are not familiar with e-commerce and electronic signature issues.

With specific regard to the electronic signature, the Draft adopts the following definitions:

---

validity. For a brief overview regarding this matter, please see ARAÚJO, Luiz Alberto David, and NUNES JÚNIOR, Vidal Serrano. *Curso de Direito Constitucional*. 3. ed. São Paulo, Saraiva, 1999, p. 281.

[24] As a matter of fact, the sphere of application will be the same in both cases (data messages and electronic signatures). For that reason, for a more detailed explanation regarding this matter, please refer to section I.I.a.I above.

(i) electronic signature: it is the result of an electronic data processing, based on an asymmetric cryptography system that proves the author and the integrity of a data message encrypted through the use of a private key.

(ii) asymmetric cryptography: a type of encoding that uses a pair of different and interdependent keys, denominated public and private keys, in such a way that a message encoded by one of the keys will only be decoded by the other key of the same pair.

(iii) certification service provider: a corporation that is able to issue a digital certificate and to offer or to facilitate services regarding the registry and dating of a transmission or reception of data messages.

(iv) digital certificate: a data message issued by a certification service provider which confirms the ownership of a public key.

c. <u>Treatment of various signature technologies</u>

The Draft partially adopts the principle contained in Article 3 of the ML 2001 and that intends to avoid the discrimination against methods that even if not expressly foreseen in a specific law, comply with the requirements established for the validity and enforceability of an electronic signature.

As it is clearly explained in the UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001[25], "*there should be no disparity of treatment between electronically signed messages and paper documents bearing handwritten signatures or between various types of electronically signed messages, provided that they meet the basic requirements set forth in Article 6,*

[25] Available at <http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf.>.

paragraph 1, of the Model Law[26] *or any other requirement set forth in applicable law*[27]".

The Draft partially incorporates this principle because even though it recognises the validity to the eventual application of a technology different from the one adopted by the Draft -asymmetric cryptography-, the Draft submits the application of such technology to a prior authorization of the public authorities[28].

d. Interpretation

Since Article 4 of the ML 2001 is a reproduction of Article 3 of the ML 1996, we refer to our comments in section I.I.a.3 above.

It is important to highlight again that there is no special reference in the Draft regarding the interpretation of any of its dispositions, including those related to electronic signatures.

e. Variation by Agreement

Again, given that Article 5 of the ML 2001 is a reproduction of Article 4 of the ML 1996, we refer to our comments in section I.I.a.4 above.

It is important to add that the rules regarding an electronic signature and foreseen in the Draft intend to provide certainty as to whether an electronic signature is valid or not and the consequences of that fact. Thus, some of those dispositions may constitute, as a matter of fact, evidential rules in the event a matter of such nature is brought to a Brazilian court and, therefore, the parties would not be able to alter such rules.

---

[26] It refers to the ML 2001.

[27] Page 48.

[28] See Article 2 of the Draft.

f. Compliance with a requirement for a signature

In effect, one of the most important goals that must be sought through the regulation of electronic signatures is the necessity of providing electronic signatures with the same legal effects provided by the law to handwritten signatures. As it is expressed in the UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001[29], "*where any legal consequences would have flowed from the use of a handwritten signature, the same consequence should flow from the use of a reliable electronic signature*"[30].

The Draft, that clearly contemplates such goal, establishes some requirements that must be met in order for an electronic signature to be considered valid and enforceable.

First, the electronic signature must be unique and exclusive to the data message to which such electronic signature is attached[31], in order to be able to unambiguously link the electronic signature to the content of the corresponding data message.

Second, the electronic signature must be able to permit its public verification by the relying party[32].

Third, it must be generated through a private key owned by the signatory and which is kept under his sole control and supervision[33]. This requirement is very important because in theory, there could be situations where the private key could be shared by several persons. The Draft, however, does not regulate the

[29] Available at <http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf.>.

[30] Page 52.

[31] Article 4.I of the Draft.

[32] Article 4.II of the Draft.

[33] Article 4.III of the Draft.

consequences that would arise in this situation, such as, for instance, that the reference to the signatory in the above situation would be a reference to the persons that shared the private key, which leads us to conclude that this third requirement would not be met in a shared private key context[34].

The fourth requirement sets forth that the electronic signature must be linked to the data message in such a way that in the event the data message's content is altered, the electronic signature would be automatically invalidated[35]. Even though a handwritten signature does not provide certainty as to the integrity of a written document, the Draft chooses to require not only that an alteration to the integrity of the data message must be detectable[36], but also requires that the integrity of the electronic signature and the integrity of the data message must be so related that an alteration in the second one automatically invalidates the first one by virtue of the hash function of the key pairs[37].

The fifth and last requirement sets forth that the electronic signature, in order to be valid, must not be issued after the expiration, suspension (temporary interruption of the operational period) or revocation (permanent invalidation) of the corresponding private key[38].

---

[34] For the legal consequences that would arise in the event an electronic signature is used by other person other than the owner of the private key, please refer to section (g) below.

[35] Article 4.IV.

[36] As it is required in the ML 2001, Article 6.3.(c) and 6.3.(d).

[37] "Hash function is a mathematical process, based on an algorithm wich creates a digital representation, or compressed form of the message, often referred to as a "message digest", or "fingerprint" of the message, in the form of a "hash value" or "hash result" of a standard length that is usually much smaller than the message but nevertheless substantially unique to it. Any change to the message invariably produces a different hash result when the same hash function is used. In the case of a secure hash function, sometimes called a "one-way hash function", it is virtually impossible to derive the original message from knowledge of its hash value". See UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, Available at <http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf.>.

[38] See Article 4.V.

The Draft stipulates all those requirements for the validity of an electronic signature in order to avoid the necessity of the parties to go to the court or to an arbitration procedure to require the declaration of such validity.

In addition to that, another measure adopted by the Draft that seems to seek the development of e-commerce, is the possibility of the parties to go to court in order to prove the validity of an electronic signature despite the signatory's private key not having been issued by a certification service provider that complies with the requirements foreseen in the Draft[39] and above mentioned.

g. Conduct of the signatory

The signatory, as the holder of a digital certificate, is obliged, according to Article 13 of the Draft[40], to keep the confidentiality of and the control over his private key, as well as to request to the certification service provider the revocation of such private key in the event he is aware of a violation of the private key's confidentiality or of the private key's security. In the event the signatory fails to fulfil such obligations, he will bear all civil and criminal, if applicable, consequences derived from such failure including, for instance, those related to the use by a non-authorised third party of his private key.

h. Conduct of the certification service provider and trustworthiness

Even though the need for a regulation over electronic signatures has been discussed in Brazil, including in the Brazilian Congress[41], it is quite undisputable that the development of the e-commerce depends upon the reliability on the

[39] See Article 5.

[40] Clearly inspired by Article 8 of the ML 2001.

[41] See Report, p. 2.

security and trustworthiness of the certification service provider that, in the end, will be the entity that will attest to the integrity of the data message and to the identity of its signatory (through the binding of a public key with a particular signatory).

According to the Draft, any corporation organized in accordance with Brazilian Laws and with its head office in Brazil is able to provide certification services, without any need to obtain any prior or *ex post* authorization before Brazilian authorities[42]. However, even though a registration before Brazilian Authorities is not necessary, the certification service provider must notify the competent authorities that it will start to perform such services in accordance with the Draft's dispositions.

In order to be able to obtain registration as a certification service provider, the Draft, in its Article 21, foresees that the entity must fulfil any and all requirements foreseen in the Draft. The enrolment's function is to somehow provide more comfort to the general public that the requirements foreseen in the Draft for the quality and security of the digital certificates (and summarized below) are met by the enrolled certification services provider and have actually been checked by the Brazilian public authorities.

The Draft strictly regulates the certification service provider's duties which can be summarized as follows:

(i) duty to have the necessary technical capacity to perform the certification services[43], human resources[44], hardware and software systems[45] together

[42] See Article 17 of the Draft.

[43] See Article 21.I of the Draft.

with the duty to be financially independent[46];[47]

(ii) duty to suspend a digital certificate whenever it has reasonable grounds to believe that such certificate was issued based on wrongful information or the corresponding private key had its confidentiality breached[48];

(iii) duty to cancel a digital certificate whenever the events described in paragraph (ii) above have been proved[49];

(iv) duty to preserve the privacy of the holder of the digital certificate[50], requesting from him only the essential information necessary to carry out the certification service and not using such information for other purposes, unless expressly authorized by such holder[51];

(v) duty to issue a digital certificate in the situations and in accordance with the conditions foreseen in the agreement executed with the corresponding holder[52]. In any case, the digital certification must, at least, indicate, according to Article 12 of the Draft, (a) the identification and electronic signature of the certification service provider, (b) the identification of the public key referred to in the digital certificate, (c) the digital certificate's

---

[44] Article 18.VI of the Draft.

[45] Article 18.II of the Draft.

[46] See Article 21.III and 21.IV of the Draft.

[47] The requirements foreseen in this paragraph (i) are similar to those foreseen in Article 9 of the ML 2001 and that are related to the trustworthiness of the certification service provider's systems, procedure and human resources.

[48] Article 14.II of the Draft. In those cases, the certification service provider must notify the corresponding holder that it suspended the validity of his digital certificate, indicating in such notification the grounds for such suspension.

[49] Article 15.III and IV of the Draft.

[50] Article 16.II. of the Draft.

[51] Article 16.1. of the Draft.

[52] Article 18.I. of the Draft.

issue date and its period of validity, (d) the name of the digital certificate holder and his/her date of birth, in the event it is an individual, and (e) the necessary elements to identify the used cryptography system;

(vi) duty to publish a list of the issued, suspended and cancelled digital certificates[53]; and

(vii) duty to keep and preserve the digital certificate registry for at least 20 years, unless a greater time period, if any, is foreseen in Brazilian law[54].

The Draft, in this matter, appears to be based on Article 9 of the ML 2001, since many of the certification service provider's duties foreseen in such Article 8 were translated to the Draft in some of its dispositions, particularly the ones related to the obligation of the certification service provider to act in accordance with the representations made by it with respect to its policies and practices[55] and the civil liability of the certification service provider whenever it fails to fulfil its duties[56].

i. <u>Conduct of the relying party</u>

The Draft, contrary to what is stated in Article 11 of the ML 2001, does not impose on the relying party any burden to verify the validity, suspension or cancellation of the digital certificate or the existence of any limitation expressed thereto.

In light of the above, the analysis of the legal consequences that would occur in the event the relying party does not make such verification will have to be made on a case by case basis according to Brazilian general contract law principles.

---

[53] Article 18.II. of the Draft.

[54] Article 20 of the Draft.

[55] See Article 9.1.a. of the ML 2001 and Article 10 of the Draft.

[56] See Article 9.2. of the ML 2001 and Article 19 of the Draft.

j. Recognition of foreign certificates and electronic signatures

Since the Draft submits the validity of an electronic signature to the existence of the corresponding digital certificate, the issue that must be addressed in this section is whether foreign certificates issued by companies that are not organized in accordance with Brazilian Laws and do not have their head office in Brazil would be binding upon Brazilian authorities. According to Article 47 of the Draft, such foreign digital certificates will only be enforceable in Brazil in the event the certification service provider has its head office in and is duly recognized as a valid certification service provider by a country that is a party to an international convention, executed and ratified by Brazil, that address this matter and stipulate the requirements and conditions for such recognition.

As can be seen, the Draft adopts a conservative approach to this matter, since for the ML 2001, for instance, a foreign digital certificate should be recognized as long as it offers a substantially equivalent level of reliability[57]. In other words, for the ML 2001, the determination of whether a digital certificate is capable of being legally effective should not depend on the place where the digital certificate was issued but on its technical reliability[58].

5. Original

Article 3.1. of the Draft sets forth that data messages digitally signed in accordance with the requirements foreseen in the Draft are considered as an original document. The simple text of such disposition does not address one of the main purposes of that kind of clause –that in ML 1996 is expressed in its Article

[57] See Article 12.2 of the ML 2001.

[58] Page 69 of the UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001 available at <http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf.>.

8- which is to regulate negotiable commercial instruments. The reason for that depends upon what is provided in Article 29 of the Draft that sets forth that negotiable commercial instruments, such as a letter of credit, whenever electronically issued, will follow the dispositions of the applicable commercial law.

Since a letter of credit, as it happens in many different countries, has its enforceability conditioned to the presentation, by the holder, of the original negotiable commercial instrument[59], it is uncertain whether a letter of credit electronically issued would be acceptable[60].

Notwithstanding the above, Article 3.1. of the Draft is a helpful tool in the development of e-commerce in Brazil given that, for the purposes of Brazilian Civil Procedure Law, an electronic contract digitally signed in due form will be considered as an original document and, therefore, will have the effects foreseen in Brazilian Civil Procedure Law for such kind of document[61].

6. Admissibility and evidential weight of data messages

The ML 1996, in its Article 9, intended to establish the admissibility of data

[59] For a complete overview of the Brazilian regulation regarding negotiable commercial instruments, please see ROSA JÚNIOR, Luiz Emigdio F. da. *Títulos de Crédito -Jurisprudência atualizada e Esquemas Explicativo*. 2. ed. São Paulo-Rio de Janeiro, Renovar, 2002.

[60] This Article's scope avoids an analysis of the legal regime in Brazil regarding negotiable commercial instruments issued by electronic means, particularly because such issue is rarely addressed in Brazilian federal statutes. For an intersting analysis of this issue, please see BINOTTI, Sérgio. *A Duplicata na era digital: do saque, endosso e protesto por meios virtuais*. In FERREIRA, Ivette Senise, BAPTISTA, Luiz Olavo Baptista (Org). *Novas Fronteiras do Direito na Era Digital*. São Paulo, Saraiva, 2002, 47-62.

[61] For instance, Article 614.I of the Brazilian Civil Procedure Code that requires the presentation of the original document in the event a lawsuit regarding rights or obligations derived from a contract is filed. For a complete overview regarding this matter, including the situations where the Brazilian jurisprudence has exceptionally accepted the presentation of a copy of the contract, please see ASSIS, Araken de. *Manual do Processo de Execução*. 8 ed. São Paulo, Editora Revista dos Tribunais, São Paulo, 2002, p. 153-155.

messages as evidence in legal proceedings and their evidential value[62] in order to avoid a court's rejection of a data message as evidence solely on grounds that a data message cannot, per se, be considered as evidence.

The Draft confers to data messages the same evidential value conferred by the Brazilian Civil Procedure Code to original written documents[63], as long as such data messages are electronically signed in accordance with the requirements foreseen in the Draft[64].

Moreover, according to Article 8 of the Draft, a judge is free to confer evidential value to a data message not issued in conformity with the Draft's disposition.

Notwithstanding the above, the Draft creates some specific rules of evidence that are applicable solely to data messages, such as:

(i) the public key's ownership cannot be determined based solely on witnesses[65];

(ii) in the event of expiration (termination of the validity period) or cancellation of a signatory's key, the party who would benefit from the data message has the burden of proving that the data message was generated before such expiration or cancellation[66].

7. Retention of data messages

[62] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996, p. 26, available at <http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>.

[63] See Articles 364 to 389 of the Brazilian Civil Procedure Code.

[64] See Article 7 of the Draft.

[65] See Article 5 of the Draft. Brazilian Civil Procedure Law has some exceptions where the witnesses cannot be taken into account by a judge. For example, please see Article 401 of the Brazilian Civil Procedure Code.

[66] See Article 6.1 of the Draft. For an overview of the Brazilian regulation regarding the admissibility of written documents as evidence, please see NEGRÃO, Theotônio. *Código de Processo Civil e Legislação Processual em vigor*. 34 ed. São Paulo, Saraiva, 2002, p. 426-433.

The Draft does not contain any rule regarding situations where it is necessary to retain data messages or to the conditions under what such retention would have to be made.

The retention of data messages is a very important issue in Brazil, particularly for tax and exchange control purposes. For example, according to Article 174 of the Brazilian Tax Code, dated 25 October 1966[67], a company will have to maintain, for a period of 5 (five)[68] years, the documents that support their annual income tax return.

As a general rule, there is no provision concerning the retention of data messages in electronic format and therefore, it is not possible to presently ascertain whether Brazilian Courts and authorities will require that data messages be kept in a proper format or not. However, one important exception is foreseen in administrative rule (*Circular*) No. 3.234, dated 24 April 2004, issued by the Brazilian Central Bank, which accepts the celebration of an exchange contract through electronic means[69] and therefore, accepts the retention of such electronic exchange contract by the financial institution for exchange control rules' purposes.

C. Communication of Data Messages

1. Formation and validity of contracts

As established in Article 12 of the ML 1996, the Draft, in its Article 26, recognises that an offer and an acceptance may be expressed by means of a data

[67] Please see also Article 265 of the Presidential Decree (*Decreto*) No. 3000, dated 26 March 1999.

[68] See Article 8 of Federal Statute 10.666, dated 8 May 2003, which stipulates that the time period must be 10 years in some specific situations.

[69] The electronic signature in the exchange contract must be made through digital certificates issued in accordance with the rules foreseen in the before mentioned Medida Provisória No. 2.200 that created the ICP-BRAZIL (please refer to section I.I.B.4 above).

message.

Said Article of the Draft expressly mentions that the rules regarding the formation of a contract will be those foreseen in the Brazilian Civil Code, which leads us to the conclusion that the intention here is to avoid any uncertainty regarding the possibility of the parties to express their will through data messages, unless any other form is expressly required by a mandatory rule[70].

2. Recognition by parties of data messages

Article 12 of the ML 1996 has as its purpose the recognition of the validity of any communication between contractual parties different from the communications relating to the execution of the contract itself (basically the offer and the acceptance). As an example, communications regarding notice of defective goods, offer to pay, recognition of a debt and notice of a place where a contract could be performed[71] could be highlighted.

The Draft, in Article 32, takes a similar view stating that for the accomplishment of the processes and time periods foreseen in consumer law, the acquirer of goods or services will be entitled to use data messages in order to make any notification related to the contract.

Two questions arise from such provision: first, that Article 32 is limited to consumer contracts and, therefore, it could be argued that it is not applicable to other types of contracts; second, only the acquirer of goods or services is entitled to make a notification through the use of a data message, which means, in other words, that the provider of such goods or services will have to use the regular

[70] Please refer to Section I.I.B.3 and footnote 22.

[71] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996, p. 29, available at <http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>.

means of communications accepted by Brazilian law (such as, e.g., a registered letter).

3. Attribution of data messages and acknowledgment of receipt

The Draft sets forth some specific rules regarding the steps that must be taken in order to conclude a contract through the use of data messages and electronic signatures.

First, the offeree of the goods or services must send his express acceptance of the conditions for the acquisitions of the goods or services offered[72]. Such communication must be made to the electronic address previously indicated by the offeror[73].

As can be seen, the Draft does not address the form by which the offer made by the offeror has to be made. It simply regulates the form pursuant to which the offeree must notify his acceptance to the offeror. Such fact leads us to the conclusion that the offeror may make his offer in any form, including in non-electronic means.

Notwithstanding the above, and with specific regard to providing certainty to electronic transactions, the Draft submits the validity of the acceptance made by the offeree to the sending, by the offeror to the offeree, of a data message (i) confirming the conditions previously accepted by the offeree and (ii) indicating the receipt by the offeror of the acceptance originally sent by the offeree[74]. Again,

[72] See Article 26.I of the Draft.

[73] See Article 27 of the Draft.

[74] See Article 26.II of the Draft.

such notice must be sent to the electronic address indicated by the offeree[75] [76].

It must be noted that, as per Article 26.1 of the Draft[77], in the event the offeror remits a data message with a contract proposal personally or through an information system programmed by him to operate automatically, he will be obliged by such proposal.

4. Time and place of dispatch and receipt of data messages

The date of a data message is, as between the parties, the date expressed thereto. Nevertheless, the parties have the right to prove, using any type of evidence accepted by Brazilian Civil Procedure Law, the effective date of such data message[78] if other than that expressed in the data message.

In relation to third parties, the date of the data message will be one of the following[79]:

(i) the date on which the data message was registered;

(ii) the date the data message was presented to a Brazilian governmental authority or to the Brazilian courts; or

(iii) the date of an act or fact that clearly establishes the formation of the data message and corresponding electronic signatures[80].

Regarding the place of dispatch for reasons of the determination of the place of

---

[75] See Article 27 of the Draft.

[76] Please note that differently from what is disposed in Article 13 of the ML 1996, the Draft does not regulate the situations where a data message must be deemed to have been sent by the originator.

[77] This article is almost a reproduction of Article 13.2.b. of the ML 1996.

[78] See Article 6 of the ML 1996.

[79] See Article 6.2. of the ML 1996.

[80] Contrary to what is stated in Article 15 of the ML 1996, the Draft has no disposition regarding the identification of the exact timing of a data message.

execution of an electronic contract, Article 435 of the Brazilian Civil Code will be applicable, which sets forth that such place will be the place where the offer has been issued.

II. II. ELECTRONIC COMMERCE IN SPECIFIC AREAS

A. CARRIAGE OF GOODS

There is no provision in the Draft regarding the carriage of goods.

Thus, any electronic contract regarding that matter will be regulated by the same legal framework applicable to the other types of electronic contracts –essentially the Draft and the Brazilian Civil Code-, except for that mentioned in sections (B) and (C) below.

B. CONSUMER CONTRACTS

The Draft, in its Article 30, expressly determines that all applicable rules regarding consumer protection will be applicable to electronic contracts.

All offers made to consumers must comply with the dispositions of the Draft, among which, it must be pointed out that the offeror must clearly and expressly indicate in the offer the following[81]:

(i) offeror's complete identification;

(ii) identification and indication of the registered address of the internet service provider involved in the transaction;

(iii) offeror's contact data;

(iv) explanation of the security system and technology used by the offeror in such transaction; and

[81] See Article 31 of the Draft.

(v) instructions for the consumer regarding the electronic file of the electronic contract and the steps that he must follow in order to obtain a copy of the electronic contract.

C. OTHER

In addition to what has been said above, it is important to highlight that the Brazilian Federal Revenue and Customs Secretariat (*Secretaria da Receita Federal*) has been permitting the use of data messages in many transactions within its jurisdiction.

In those cases, the Secretariat has requested compliance with the rules set forth in the ICP-BRAZIL environment and with its own rules[82].

*****

[82] Please refer to Presidential Decree (*Decreto*) 4.553, dated 27 December 2002.