O documento eletrônico e sua implicação no Direito

Adriano Roberto Vancim[*]

Sumário: 1 Conceito de documento eletrônico. 2 Validade do documento eletrônico. 3 Mecanismos de segurança. 3.1 Assinatura eletrônica. 3.2 Assinatura digital. 3.3 Assinatura criptográfica. 3.4 Autenticação e certificação digital. 4 Considerações finais. 5 Referências bibliográficas.

"Cada forma de vida inventa seu mundo (...) e, com esse mundo, um espaço e um tempo específicos [...]. A virtualização por desconexão em relação a um meio particular não começou com o humano. Ela está inscrita na própria história da vida." (Pierre Lévy)

1 Conceito de documento eletrônico

Em princípio, não fugindo do tradicional conceito atribuído, documento seria simplesmente qualquer declaração escrita, hábil a demonstrar a realidade de algum fato. Entrementes, tal conceito apresenta-se impreciso, na medida em que não somente as declarações escritas podem provar a realidade de algum fato, mas também as declarações por meio de sinais, símbolos, etc.

Giuseppe Chiovenda o define de forma muito ampla, como sendo "toda representação material destinada a reproduzir determinada manifestação do pensamento, como uma voz fixada duradouramente *(vox mortua)* (1945, p. 183).

Não basta, no entanto, para a perfeita caracterização do documento, aliás, como meio de prova, a mera manifestação do pensamento, devendo também representar um fato juridicamente relevante. Dessarte, o conceito que nos parece mais categórico é o de Francesco Carnelutti, ao qual *"il documento non é soltanto una cosa, mas una cosa rappresentativa, cio é capace di rappresentare un fatto"* (1947, p. 183).

Por conseguinte, documento seria qualquer declaração escrita ou não, capaz de representar um fato juridicamente relevante, hábil a instruir o processo como prova, influenciando no livre convencimento do magistrado.

Tratando-se do documento eletrônico, a doutrina nacional, bem como a doutrina estrangeira, insistem em apresentar diferenças quanto à terminologia empregada, às vezes classificando como documentos informáticos, telemáticos, computadorizados, mas que, na sua essência, todos se materializam num computador.

---

[*] Ex-Advogado em Ribeirão Preto/SP. Autor de inúmeros artigos jurídicos publicados em revistas especializadas, inclusive com citação pelo Superior Tribunal de Justiça - STJ. Pós-graduando em Direito Privado. Autor da disciplina Direito Internacional Público e Privado na obra *Curso preparatório para o exame de Ordem – prova objetiva e parte teórica*, 4. ed. Editora Tático. Co-autor da disciplina Direito Internacional Público e Privado na obra *Coleção sinopses jurídicas*, Editora Tático, e da disciplina Direito do Consumidor (no prelo). Servidor público vinculado ao Juizado Especial Cível e Criminal da Comarca de Guaxupé/MG.

Como dito em linhas anteriores, sendo o documento qualquer meio de representar um fato, por razões óbvias, o documento eletrônico não foge à regra, sendo por conseguinte a representação de um fato materializado não em uma cártula, mas sim armazenado na memória de um computador.

Não queremos com isso ser simplistas, muito pelo contrário; a definição do que venha ser documento eletrônico não é tarefa das mais fáceis e é extremamente importante, na medida em que poderemos verificar sua eficácia probatória frente o contrato pactuado.

A Lei Modelo da Uncitral, em seu art. 2, "a", define de forma concisa o que vem a ser "mensagem de dados" ou "mensagem eletrônica", que, na verdade, consoante o texto legal, consubstancia o próprio documento eletrônico, a partir do momento em que recebido e armazenado no computador.

> Por 'mensagem de dados' se entenderá a informação gerada, enviada, recebida ou arquivada ou comunicada por meios eletrônicos, óticos ou similares, como podem ser, entre outros, o intercâmbio eletrônico de dados (EDI), o correio eletrônico, o telegrama, o telex ou o telefone.

Diante dos conceitos supramencionados e de vários outros que poderíamos expor, mas que não nos parece necessário, temos que o grande incômodo não é determinar o que vem a ser documento eletrônico, mas sim saber exatamente qual a sua eficácia como meio de prova e sua implicação no Direito.

Isso porque é abstratismo para muitos a utilização de "uma seqüência de *bits*" como prova da avença. Ademais, corroborando para a majoração de tal ceticismo, a aceitação de tais documentos ainda está na fase embrionária em nosso país, muito aquém das legislações alienígenas que dispõem com muita propriedade sobre sua utilização e eficácia, fator esse que deve ser relevado para que possam ter o mesmo reconhecimento e transmitir a mesma segurança de imutabilidade própria dos documentos tradicionalmente conhecidos.

Vale a pena afirmar que a mensagem eletrônica, diversamente do que ocorre com as mensagens tradicionais, uma vez emitida pelo "iniciador" e recebida pelo "destinatário", é traduzida e armazenada no computador em forma de *bits,* de forma que sua composição não será em letras ou algarismos.

Importante aduzir, porém, não em demasia, que a palavra *bit,* de origem inglesa, significa "dígito binário", sendo que para cada dígito utilizado há apenas duas possibilidades de variação, 0 (zero) ou 1 (um).

Pode-se observar hodiernamente que o documento eletrônico está muito vulnerável, suscetível a fraudes e falhas do computador onde está armazenado, mas que, como veremos em momento oportuno, observados certos requisitos, torna-o com validade e eficácia jurídicas.

2 Validade do documento eletrônico

Alguns problemas surgem em relação a admitir como prova o documento eletrônico, em razão de não preencher certos requisitos necessários à sua validade, visualizados mais facilmente nos documentos tradicionais, tais como a autenticidade, a integridade e a confidencialidade da declaração.

Todavia, não podemos deixar de mencionar algumas legislações que dispõem a respeito, admitindo e atribuindo força probante a tais documentos, vejamos:

Dispõe o art. 9.1, *a*, da Lei Modelo da Uncitral:

> Em todo trâmite legal, não se dará aplicação a regra alguma da prova que seja óbice para a admissão como prova de uma mensagem de dados:
> a) pela simples razão de que se trata de uma mensagem de dados.

Art. 9.2:

> Toda informação apresentada em forma de mensagem de dados gozará da devida força probatória. Ao valorar a força probatória de uma mensagem de dados se terá presente a fiabilidade da forma em que se tenha gerado, arquivado ou comunicado a mensagem, a fiabilidade da forma em que se tenha conservado a integridade da informação, a forma em que se identifique o seu iniciador e qualquer outro fator pertinente.

No mesmo sentido, dispõe o art. 225 do *Codex* Civil:

> As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte contra quem foram exibidos não lhes impugnar a exatidão.

E, mais, prescreve o art. 332 do Código de Processo Civil:

> Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa.

Em decorrência da análise de tais dispositivos legais, torna-se superada a discussão acerca da sua admissibilidade como prova de um contrato convencionado entre as partes contratantes ou de um contrato em que inexista o consentimento mútuo em sua formação.

Verifica-se que a Lei Modelo da Uncitral assim como a nossa legislação civil e processual civil estão intimamente entrelaçadas, uma a confirmar a outra, razão pela qual negar admissibilidade jurídica aos documentos eletrônicos é ir de encontro aos primados do Direito.

A questão reside em situar a validade jurídica de tais documentos, ao passo que somente será plena, produzindo os efeitos que deles se esperam, a partir do instante em que estiverem preenchidos os seus requisitos de validade, quais sejam autenticidade, integridade e confidencialidade.

3 Mecanismos de segurança

3.1 Assinatura eletrônica

Inicialmente, o exame acerca da assinatura é de suma importância, na medida em que é o fator preponderante para se admitir o documento eletrônico como válido e seguro, pois identifica o autor do documento, um elo objeto de incansáveis discussões, mas que superado em razão de a assinatura dar presunção de autenticidade ao documento.

A assinatura tradicional, manuscrita, aposta num documento cartáceo, é o ato de *discrímen* e que identifica seu autor como sendo o legítimo titular do documento, ou por meio de símbolos, brasões, aliás, diga-se de passagem, comumente utilizado na Idade Média.

Já a assinatura eletrônica, diversamente da assinatura tradicional, não é manuscrita no documento eletrônico, mas se dá por meio de senhas, números, códigos, sempre com cunho confidencial, exclusiva de seu proprietário, o que o legitima a realizar diversas transações e, fornecendo sua senha comparada com seus dados já cadastrados, o identifica como subscritor de tal transação ou documento.

Não se pode perder de vista que a finalidade do documento tradicional assim como do documento eletrônico é a mesma, vale dizer, visa identificar o legítimo subscritor do documento ou da transação realizada, atribuindo-se os efeitos legais inerentes à assinatura, quais sejam a autoria de quem o subscreveu, a aquiescência quanto ao documento ou à transação efetuada e o conhecimento pleno de seu conteúdo, fator esse que motivou o indivíduo a perpetrar o documento ou a transação.

Ressalte-se que utilizamos o termo transação, tal como utilizado por diversos autores, e não negócio jurídico, pois, em se tratando do contrato – negócio jurídico por excelência –, a assinatura a ser utilizada é mais complexa, de forma a dar maior confiabilidade e autenticidade ao negócio jurídico, denominada assinatura digital, a qual analisaremos *a posteriori*.

O art. 7 da Lei Modelo da Uncitral discorre sobre a assinatura, e o transcrevemos devido a sua importância jurídica.

> 7.1 - Quando a lei requeira a assinatura de uma pessoa, esse requisito ficará satisfeito em relação a uma mensagem de dados:
> 7.1 *a* - Se se utiliza um método para identificar a essa pessoa e para indicar que essa pessoa aprova a informação que figura na mensagem de dados; e
> 7.1 *b* - Se esse método é tão fiável como seja apropriado aos fins para os quais se gerou ou comunicou a mensagem de dados, à luz de todas as circunstâncias do caso, incluído qualquer acordo pertinente.
> 7.2 - O parágrafo 1) será aplicável tanto se o requisito nele previsto esteja expresso em forma de obrigação quanto se a lei simplesmente preveja conseqüências no caso de que não exista uma assinatura...

Dentre os vários comentários que podemos tecer, alguns se tornam pertinentes.

Primeiramente, tal artigo preocupou-se em manter e reconhecer os atributos legais da assinatura, ou seja, identificar o documento a uma pessoa, dar certeza à participação pessoal dessa pessoa no ato de assinar e associar a essa pessoa o conteúdo de um documento.

Secundariamente, a assinatura *de per si* não é o bastante para dar total validade jurídica ao documento, sendo necessária igualmente a utilização de métodos que assegurem a total

identificação do subscritor ao documento, e que este aprove as informações constantes no documento.

Por fim, num terceiro instante, será exigida a assinatura, se constante como obrigação pactuada pelas partes, ou se a lei prever que sua não-utilização acarretará conseqüências (GARCIA JÚNIOR, 2001, p. 220-34).

A assinatura eletrônica seria, portanto, o meio pelo qual, através da utilização de senhas, códigos, números, seu legítimo proprietário é identificado como tal, livre a efetuar qualquer transação débito-crédito ou formular qualquer documento.

Sendo assim, o art. 2º, 1, da Diretiva 1999/93/CE define o que vem a ser assinatura eletrônica, entendendo-se como sendo:

> 'Assinatura eletrônica', os dados sob forma eletrônica, ligados ou logicamente associados a outros dados eletrônicos, e que sejam utilizados como método de autenticação.

Em outras linhas, é o que ocorre, corriqueiramente, com a utilização dos cartões de crédito como meio de pagamento de uma transação, seja ela de pequeno ou médio valor, dos quais, às vezes se pede a senha ou às vezes somente o número do cartão de crédito.

Ainda não é com a assinatura eletrônica que o documento eletrônico estará totalmente seguro no que tange à sua utilização. Mecanismos mais exatos, complexos, atribuem a tal documento uma autenticidade insuscetível, a nosso ver, de falhas bruscas, capazes de criar óbices à utilização do documento como prova do contrato.

É o que veremos a seguir com a assinatura digital, instituto esse utilizado com muita freqüência nos contratos eletrônicos, e que propicia uma confiabilidade e autenticidade quase que absolutas do documento eletrônico, em razão de se tratar de um sistema muito seguro, sujeito ao crivo da criptografia.

3.2 Assinatura digital

A assinatura digital, espécie do gênero assinatura eletrônica, é aquela submetida ao controle da criptografia, em que, grosso modo, consiste em ser o ato de tornar aparentemente ininteligível uma mensagem, texto, som, imagem, com uso da técnica de se escrever em código ou cifra.

Definição que nos parece mais completa e que elucida de forma bem cristalina a assinatura digital, esta prevista na Diretiva 1999/93 do Parlamento Europeu, já mencionada em linhas anteriores, mas que se torna necessário renová-la em função de sua enorme importância ao tratar especificamente da assinatura digital e de outros assuntos a ela inerentes, como a sua autenticação e certificação.

Dispõe o art. 2º, 2:

> 'Assinatura eletrônica avançada', uma assinatura eletrônica que obedeça aos seguintes requisitos:

a) estar associada inequivocadamente ao signatário;
b) permitir identificar o signatário;
c) ser criada com meios que o signatário pode manter sob seu controle exclusivo; e
d) estar ligada aos dados a que diz respeito, de tal modo que qualquer alteração subseqüente dos dados seja detectável.

Importa identificar o que venham significar as expressões "dados de criação de assinaturas" e "dados de verificação de assinaturas", como forma de, com total certeza, afirmar que a assinatura digital está associada ao uso da criptografia.

> Art. 2º, "4: 'Dados de criação de assinaturas', um conjunto único de dados, como códigos ou chaves criptográficas privadas, usado pelo signatário para a criação de uma assinatura eletrônica".

> Art. 2º, "7: 'Dados de verificação de assinaturas', um conjunto de dados, como códigos ou chaves criptográficas públicas, usado para verificar a assinatura eletrônica".

Infere-se da definição apresentada que a assinatura digital decorre do procedimento de criptografia; para ser mais preciso, ela é verificada durante o processo da criptografia, da seguinte forma:

Remetente e destinatário de uma mensagem utilizam-se de chaves (simétrica - privada, assimétrica - privada e pública), para que possam, respectivamente, cifrar (tornar ininteligível a mensagem) e decifrar a mensagem desejada (tornar inteligível a mensagem aparentemente ininteligível).

Nesse interstício, é inserido no arquivo eletrônico um código identificador da chave que fora utilizada pelo remetente para cifrar aquela determinada mensagem, sendo que esse código consiste em ser a assinatura digital própria do documento eletrônico cifrado.

Não perdendo de vista que o documento eletrônico trata de ser uma "seqüência de *bits*", a assinatura digital é gerada a partir dos mesmos *bits* contidos no documento eletrônico cifrado.

Dessa forma, estando indissociáveis o documento eletrônico e a assinatura deste mesmo documento a uma série de *bits*, qualquer alteração do documento cifrado e assinado, por mais simples que seja, voluntária ou involuntariamente, torna impossível sua decifragem por parte do destinatário da mensagem, o que demonstraria a ocorrência de eventual alteração do documento, ou até mesmo a falsificação do documento eletrônico (GICO JÚNIOR, 2000, p. 348).

A chave utilizada pelo destinatário para decifrar a mensagem (assimétrica - pública ou privada) não conseguirá abrir o documento eletrônico, acusando sua alteração ou falsificação.

Eis, portanto, o método eficiente que garante de forma amplamente confiável a autenticidade do documento eletrônico, o que torna sua utilização indiscutivelmente segura e precisa, insuscetível de violação.

Nesse aspecto, pode-se dizer que o documento eletrônico possui uma grande força probante em juízo, não absoluta ainda, a bem da verdade, como veremos adiante, mas muito eficaz.

Portanto, é inquestionável sua admissibilidade como meio de prova para efeitos processuais, equiparando-se ao documento assinado autograficamente, como bem aduz o Código Civil Francês em seu art. 1.316-3: "O escrito sobre suporte eletrônico tem a mesma força probante do escrito sobre o suporte papel".

3.3 Assinatura criptográfica

A criptografia, meio pelo qual através de métodos matemáticos se transformam mensagens inteligíveis em ininteligíveis, com o uso de códigos ou cifras, vem sendo utilizada há muitos anos, inclusive nas guerras, sendo objeto de controle por diversos países, devido a seu poderio em manter extremamente seguras as mensagens enviadas e recebidas, respectivamente, pelo emissor e destinatário.

Atualmente, sua utilização tornou-se aguda em decorrência da prática cotidiana e corriqueira dos contratos celebrados na *web*, tendo por finalidade garantir a privacidade e segurança do conteúdo das cláusulas insertas no documento eletrônico, de modo a atribuir eficácia probatória ao documento.

Em tempo oportuno, no mesmo diapasão, conforme veiculado na agência de notícias do Superior Tribunal de Justiça, o eminente Ministro Ruy Rosado de Aguiar traçou breves notas acerca do assunto:

> O consumidor deve ter conhecimento de que existe um sistema moderno, já adotado em outros países, denominado criptografia. Só com ele é possível controlar a autenticidade e a veracidade das informações contidas nas cláusulas do documento eletrônico, em função de impugnação da outra parte. Sem o uso da assinatura criptográfica, não se obtém documento eletrônico com força probante em juízo.

Para que um texto, mensagem, som, imagem, arquivo possa ser criptografado, é necessário que haja um *software* de criptografia, sendo o mais presente o PGP (*Pretty Good Privacy*), ligado a algum algoritmo, compreendido como sendo uma seqüência de complexos métodos matemáticos utilizados para cifrar ou codificar a mensagem que se deseja tornar ininteligível, sendo os mais conhecidos o IDEA (*International Data Encryption Algorithm*) e o RSA (*Rivest, Shamir and Adleman*).

A partir daí, o processo de criptografia se desenvolve de duas formas:

A criptografia simétrica, também conhecida como "criptografia da chave privada", é aquela em que entre remetente e destinatário é utilizada apenas uma única chave (código) para que a mensagem possa ser criptografada e decriptada.

Nesse sistema, o remetente cifra a mensagem a ser enviada com a sua chave, e o destinatário, ao recebê-la, a decifra com a mesma chave utilizada pelo remetente. Verifica-se, assim, que o destinatário deve possuir a chave usada pelo remetente, ou ter total conhecimento do algoritmo utilizado para cifrar a mensagem enviada, caso contrário não conseguirá de forma alguma decifrar a mensagem recebida (SOARES DE QUEIRÓZ, 2000, p. 391).

A criptografia assimétrica, também conhecida como "criptografia da chave pública", consiste em um sistema diverso e muito mais avançado do que a criptografia simétrica.

Nesse sistema, são utilizadas duas chaves, uma privada e uma pública. Em princípio, o remetente cifra a mensagem com a sua chave privada, de uso exclusivo seu, sendo esta decifrada com a chave pública do destinatário ou de quaisquer outras pessoas que a tenham por conveniência de comunicabilidade com o remetente.

Ressalte-se que pode também ocorrer o inverso, ou seja, de a mensagem ser cifrada pela chave pública e ter de ser decifrada pela chave privada. Nunca a mesma chave, seja a privada ou a pública, poderá cifrar e ao mesmo turno decifrar a mensagem.

A chave pública, sendo distribuída a certo número de pessoas, significa que várias outras pessoas e não somente o destinatário poderão ter acesso à mensagem, interceptando-a e decriptando-a, tendo, assim, ciência do conteúdo da mensagem que se deseja manter sob pleno sigilo, o que desnatura o propósito do instituto da criptoanálise.

Com o escopo de evitar que tal constrangimento ocorra, há um método infalível, garantidor da privacidade da comunicação, visando a compatibilizar o uso da chave privada e pública.

Dessarte, deve o remetente cifrar a mensagem com o uso da chave pública do destinatário, enviando-a, contudo, por meio da sua chave privada. Ao receber a mensagem, deve o destinatário decifrá-la utilizando a chave pública do remetente e, para ter acesso à mensagem já inteligível, bastará utilizar sua chave privada (SOARES DE QUEIRÓZ, 2000, p. 392).

Temos, pois, satisfeitos todos os requisitos de validade do documento eletrônico.

Quanto à autenticidade do documento, dúvidas não pairam, pois com o uso da criptografia assimétrica é possível identificar, com absoluta certeza, remetente e destinatário da mensagem. Em se tratando da integridade do documento, com a assinatura digital, qualquer alteração do documento será evidenciada e não poderá ser decifrada pelo destinatário, o qual com sua chave não conseguirá abrir o documento.

Por fim, em relação à confidencialidade do conteúdo do documento, terceiros não terão acesso algum, inclusive se utilizado o método supra, no que tange ao uso da chave pública do destinatário para cifrar a mensagem e a chave pública do remetente para decifrar a mesma mensagem.

3.4 Autenticação e certificação digital

Pelas razões apresentadas em relação à utilização das chaves como fator de garantia de autenticidade do documento eletrônico, deparamos com certo problema.

Quem garantirá que determinada chave pertence a determinada pessoa, ou seja, como garantir que certa chave utilizada para gerar a assinatura digital do documento eletrônico é realmente do emissor - remetente da mensagem eletrônica?

Veja-se que é de primordial importância fazer menção a tal questão, pelo fato de os contratos eletrônicos serem efetivados em escala cada vez maior, e, como tal, necessário ao seu êxito que o sistema utilizado a provar a avença seja plenamente confiável.

Ademais, a prática de tais contratos é considerada realizada entre um número indeterminado de pessoas e entre ausentes, vale dizer, na grande maioria das vezes, não é realizada entre pessoas conhecidas, das quais não se tem ciência ao certo com quem se está estabelecendo o contrato, o que, inevitavelmente, acaba por criar uma incômoda sensação de insegurança e desconfiança.

Desse modo, instituiu-se a autenticação digital, em que a identificação do proprietário das chaves é analisada e comprovada por um terceiro agente, ao qual, restando indiscutivelmente evidenciado que a propriedade da chave pública é de quem realmente se diz ser e, sendo assim, fora emitida a mensagem por esta pessoa, expedirá um certificado digital conferindo validade ao ato.

Função secundária dessa entidade certificadora, decorrente da autenticação e certificação, é de publicar a chave pública em diretórios seguros, de forma a permitir sua livre consulta por qualquer pessoa que tenha interesse.

Do contrário, consoante anota Regis Magalhães Soares de Queiroz (2000):

> Um elemento mal intencionado poderia gerar uma chave pública e distribuí-la para terceiros como se fosse pertencente a uma outra pessoa. Feito isso, ele poderá emitir documentos assinados com a chave privada correspondente e quem vier a recebê-los, quando decodificá-lo com a falsa chave pública distribuída pelo fraudador, será levado a acreditar na autenticidade da origem daquela mensagem.

Temos, assim, que a autenticação do documento eletrônico é comprovada por um certificado, emitido por uma autoridade certificadora que atua como um verdadeiro "cartório eletrônico".

Dada sua importância, citaremos, consoante a Diretiva Européia 1999/93/CE, o que vem a ser um certificado e quais os seus requisitos de validade.

O art. 2º.9 define simplesmente certificado, enquanto o item 10 define certificado qualificado. Vejamos, respectivamente:

> 'Certificado', um atestado eletrônico que liga os dados de verificação de assinatura a uma pessoa e confirma a identidade dessa pessoa.
>
> 'Certificado qualificado', um certificado aos requisitos constantes do anexo I e é fornecido por um prestador de serviços de certificação que cumpre os requisitos constantes do anexo II.

Vejamos o anexo I, que dispõe acerca dos requisitos aplicáveis aos certificados qualificados:

Um certificado qualificado deve conter:
Uma indicação de que o certificado é emitido como certificado qualificado;

a) A identificação do prestador de serviços de certificação e o país em que está estabelecido;
b) O nome do signatário ou um pseudônimo, que deve ser identificado como tal;
c) Uma cláusula para a inclusão, se relevante, de um atributo específico do signatário, segundo os objetivos visados com a emissão do certificado;
d) Os dados de verificação de assinaturas correspondentes aos dados de criação de assinaturas que estejam sob o controle do signatário;
e) Identificação da data de início e de fim do prazo de validade do certificado;
f) O código de identidade do certificado;
g) A assinatura electrônica avançada do prestador de serviços de certificação que o emite;
h) As restrições ao âmbito de utilização do certificado, se for o caso; e
i) As restrições ao valor das transações nas quais o certificado pode ser utilizado, se for o caso.

O art. 2º.11 define a figura do prestador de serviços de certificado, que vem a ser a própria autoridade certificadora digital, tratando-se, portanto, "de uma entidade ou uma pessoa singular ou colectiva que emite certificados ou presta outros serviços relacionados com assinaturas eletrônicas".

Registre-se que tais "cartórios eletrônicos", prestadores de serviços de certificação, devem ser realizados por empresas especializadas, e não somente, e, sobretudo, pelo órgão público, como pretendeu o Projeto de Lei nº 1.589/1999.

Essa foi a mesma tendência posicionada pela União Européia, dispondo em sua nota 10 e nota 13 que, "para estimular a oferta de serviços de certificação à escala comunitária através de redes abertas, os prestadores de serviços de certificação devem poder fazê-lo sem necessidade de autorização prévia..." e, "a presente directiva não impede a criação de sistemas de controle baseados no sector privado...".

4 Considerações finais

Tendo em vista que os contratos eletrônicos se tornaram hodiernamente uma constante e duradoura prática de criar, modificar e extinguir direitos, como elevada expressão dos negócios jurídicos, provenientes da evolução social e da transmudação de costumes, inegável reconhecer-se em juízo, como prova, o documento eletrônico, que se distingue da própria avença.

O simples fato de o documento não estar materializado em uma cártula, como tradicionalmente se deu, e sim em uma série de *bits*, não pode e não deve ser levado a efeito a ponto de repeli-lo como meio idôneo e moralmente legítimo de prova que é, sob pena de estarmos arraigados e tolhidos ao conservadorismo.

Por mais, conforme demonstrado, nenhum impedimento legal há para sua aceitação, ao revés, o próprio ordenamento jurídico pátrio, infraconstitucional e constitucional, prescreve-o como meio de prova idôneo a conferir validade e eficácia ao contrato pactuado.

O Direito, compreendido como freqüente mecanismo regulador de fatos sociais, não se vê, de maneira alguma, de mãos atadas para enfrentar tal desafio, progressivamente acrescentado pela tecnologia, que certamente não parará por aí, sempre se renovando frente às necessidades humanas.

Dessarte, há que interpretá-lo com sensibilidade e espírito aberto, pena de apequená-lo em vista de sua promíscua aplicação imprimida por seus operadores e aplicadores.

5 Referências bibliográficas

CHIOVENDA, Giuseppe. *Instituições de direito processual civil*. v. III, São Paulo: Acadêmica-Saraiva & Cia., 1945.

CARNELUTTI, Francesco. *La prova civile.* Seconda edizione. Roma: Edizione Dell'ateneo, 1947.

GARCIA JÚNIOR, Armando Alvarez. *Contratos via internet*. São Paulo: Aduaneiras, 2001.

GICO JÚNIOR, Ivo Teixeira. A assinatura eletrônica. *Repertório IOB de Jurisprudência*, nº 16/2000, 2ª quinzena de agosto de 2000.

SOARES DE QUEIRÓZ, Regis Magalhães. Assinatura digital e o tabelião virtual. *In* DE LUCCA, Newton e SIMÃO FILHO, Adalberto (coord.) *Direito & internet* – aspectos jurídicos relevantes, São Paulo: Edipro, 2000.