CERTIFICADO DIGITAL

Angelo Boreggio Neto*
Gustavo Nahasan**

INTRODUÇÃO

Os computadores estão sendo utilizados com freqüente crescimento, devido à praticidade e rapidez que esses equipamentos têm proporcionado aos usuários, que com alguns minutos podem acessar informações em diversas regiões do mundo

A interligação de computadores, via internet, tem proporcionado grandes mudanças nas formas de comércio, ocasionando a dispensabilidade dos documentos físicos e trazendo um novo meio de prova, a ser estudada e amparada pelo direito processual. Mesmo a assinatura deste, até então levada a efeito pela rubrica de próprio punho dos contratantes, vem sendo substituída pela denominada assinatura digital.

Conceituaremos a assinatura digital, que é um meio de certificação digital, que propicia a validade jurídica do documento eletrônico, abordando a importância do Direito regular a validade jurídica dos meios eletrônicos, visto que já se constituem em uma realidade no dia-a-dia daqueles que se utilizam da internet, nas suas transações, seja por intermédio de uma releitura de suas regras, seja por meio da edição de novas normas que permitam lidar satisfatoriamente com esta nova realidade. Também será demonstrado como a utilização do documento eletrônico como um meio de prova pode ser tão seguro e eficiente quanto os meios manuais de assinatura.

HISTÓRICO

O certificado digital teve início nos Estados Unidos da América, em 1993, quando o governo anunciou uma nova iniciativa criptográfica com vistas

* Advogado, mestrando em Direito pela PUC/SP, especialista em Processo Tributário pela PUC/SP, superintendente do Procon/MT, professor da Unic.

** Advogado, especialista em Direito Tributário pela Esud.

a proporcionar um alto nível e segurança nas comunicações: projeto Clipper.

Esse foi o primeiro passo para se atribuir valor probatório aos documentos eletrônicos.

O Estado de Utah foi o primeiro a produzir uma lei sobre a certificação digital, o "Digital Signature Act Utah", em 1995, e modificado em 1996[1], baseando-se em um "Criptosistema Assimétrico" definido como um algoritmo que proporciona um par de chaves seguro.

Após o Estado de Utah, a maioria dos estados norte-americanos fizeram sua legislação sobre a certificação digital, trazendo assim uma grande controvérsia a respeito do assunto.

Nessa mesma época a Alemanha já avançava nas pesquisas para a criação de uma assinatura digital que conseguisse manter a integridade do documento, podendo valer como boa opção nas transações comerciais.

Desta feita, os EUA e a Alemanha lideraram as discussões sobre esse assunto na ONU, em 1996, no Plenário da Comissão das Nações Unidas para o Direito Mercantil, em Nova York.

Dessa reunião surgiu a LEI MODELO (Resolução Geral da Assembléia 51/162, de 16 de dezembro de 1996)[2], sobre o comércio eletrônico, que eram diretrizes básicas para que todos os países adotassem o mesmo sistema de certificação digital.

Esse modelo adotado criou uma regra matriz, que permitia que empresas diferentes fizessem um mesmo tipo de certificação digital. Ainda estabelece que os registros eletrônicos, para que recebam o mesmo nível de reconhecimento legal, devem satisfazer, no mínimo, o exato grau de segurança que os documentos em papel oferecem, o que deve ser alcançado por uma série de recursos técnicos.

Em síntese, podemos dizer que essa lei, modelo para todos os países, estabelece uma série de requisitos que permitem que um documento digital tenha função equivalente ao documento escrito, assinado e original.

Já em 1997, a Alemanha foi o primeiro país a editar uma lei específica sobre o tema. A *Signaturgesetz*, que introduziu as condições estruturais para a adoção das assinaturas eletrônicas. Já sob a égide desta lei, no seu parágrafo

1 EUA, UTAH. Digital Signature Act Utah. Disponível em http://www.utah.com/snowmobile/laws.htm. Acesso em 23/04/2004.

2 A UNCITRAL *(United Nations Commission on International Trade Law)* consiste em uma comissão especial da ONU (Organização das Nações Unidas), que trata da legislação comercial internacional. Disponível em: http://www.unicrio.org.br/leis?h.htm

quarto, alínea 1, o legislador alemão previa a obrigatoriedade de os prestadores de serviços de certificação digital obterem uma licença perante o órgão público competente para que pudessem iniciar as suas atividades.

A França é um dos países que mais têm avançado em termos de legislação em matérias envolvendo a informática. A reforma do Código Civil da França (Lei n 2000-230, de 2000)[3], sobre a adaptação do direito de prova às novas tecnologias da informação e relativa à firma eletrônica, introduziu importantes modificações no Capítulo Da prova das obrigações e do pagamento.

Atribuiu, assim, força probatória ao documento eletrônico nas mesmas circunstâncias que o escrito em suporte de papel, desde que observe três condições fundamentais: identificação do autor do documento; o processo de geração do documento deve garantir sua integridade; o processo de conservação do documento deve garantir sua integridade.

Já no México, os certificados emitidos na rede de certificação digital, em convênio com a Associação Nacional de Notariado Mexicano, veiculam uma pessoa determinada a um par de chaves necessárias para dar segurança e fidelidade ao uso de firmas eletrônicas em comunidades amplas e de grande escala. Esta é a solução encontrada para o problema da integridade, autenticidade e a recusa da origem do documento, tornando-o legalmente válido.

No Brasil, tramitam dois projetos de lei: PL-7316/2002 e PL-1589/1999, ambos ainda emperrados no Congresso Nacional. Portanto, o governo federal editou a MP 2.200/2001, para introduzir o país no comércio eletrônico.

Em 27 de julho de 2001, o presidente da República reeditou a MP 2.200 com algumas alterações, numa tentativa de "corrigir" os abusos apontados pela OAB/SP. Dentre outras mudanças, admitiu mais um representante da iniciativa privada no Comitê Gestor da ICP-Brasil.

Essa MP, além de esclarecer que a privacidade da pessoa certificada estará garantida, estipulou que ninguém será obrigado a obter certificados, pois a validade jurídica é um atributo ligado a qualquer meio de prova, seja eletrônico ou não, desde que obtido por meio lícito. Ainda previu que haverá presunção de veracidade dos documentos digitais, com a possibilidade de utilização de meios comprobatórios diversos para se demonstrar a sua autoria e integridade.

A partir de então foi criada a ICP BRASIL, que será estudada em capítulo posterior.

3 FRANÇA. Lei n. 2000-230. Disponível em: http://www.europa.eu.int/search/srq?.vts: acesso em 25 abril 2004.

CONCEITO

Não podemos conceituar certificado digital sem antes trazer uma introdução sobre o documento digital, que pode ser denominado como documento eletrônico, documento informático ou documento não físico, sendo todos produzidos por meio do uso do computador.

Dessa maneira, o certificado digital nada mais é do que a confirmação que determinados dados não foram modificados, em documentos digitais, por qualquer sistema de computador.

O certificado digital se baseia em um aglomerado de sistemas que o tornam seguro. Uma dessas formas de segurança se dá pelas assinaturas digitais, que é um meio eletrônico de tornar os documentos digitais seguros.

Essas assinaturas encontram sua validade nas chaves, que podem ser públicas ou privadas. A primeira é o órgão regulador das certificações digitais e a segunda é a empresa ou órgão autorizado a emitir esses certificados.

DOCUMENTO DIGITAL

O documento digital é como uma representação da realidade, podendo apresentar-se em forma textual, gráfica, sonora ou outra admitida pela técnica, tendo como base qualquer suporte que possa garantir sua certeza e imutabilidade, e que possa ser atribuído a um sujeito determinado.

Um documento eletrônico não pode ser assinado no modo tradicional, maneira pela qual o autor se identifica. Por isso, costuma-se atribuir aos documentos eletrônicos as características da volatilidade, alterabilidade e fácil falsificação.

Apesar da impossibilidade de os documentos digitais terem a mesma forma que um documento tradicional, determinados mecanismos informáticos podem trazer aos documentos digitais as três funções fundamentais dos documentos tradicionais, que são a função identificativa, a declarativa e a probatória, bem como os seus três requisitos básicos, quais sejam, a integridade, a autenticidade e a tempestividade.

No âmbito jurídico, o maior obstáculo em aceitar um documento, petição ou certidão, enviados via internet ou até mesmo via fax, é a verificação da assinatura, ou seja, quanto à segurança na identificação do autor.

CERTIFICADO E ASSINATURA DIGITAL

A certificação digital é um método de identificação de partes em meio eletrônico que está sendo utilizado em inúmeros países (Estados Unidos, Itália, França, Alemanha, etc.) como tecnologia padrão para a circulação de documentos neste meio.

Essa certificação é obtida pela assinatura digital, que são os elementos necessários para que o certificado digital tenha validade, é ela que garante a segurança e veracidade dos documentos digitais.

Essas assinaturas são feitas com a utilização de técnicas de criptografia, que consistem numa mistura de dados ininteligíveis, tornando necessário o uso de duas chaves, a pública ou a privada, para que eles possam se tornar legíveis. É como se fosse um cofre forte que somente para quem tem o seu segredo é acessível.

Assim, ele em nada se assemelha à assinatura com a qual estamos acostumados, pois na verdade a assinatura eletrônica é um emaranhado de números que somente poderá ser codificado por quem possua a chave privada e sua decodificação deverá ser feita por meio de uma chave pública.

As assinaturas digitais surgem justamente para sanar uma imperfeição ínsita das comunicações veiculadas no meio digital, qual seja, a de não se ter certeza da identidade da pessoa com a qual se está falando. Enquanto no mundo físico, no mais das vezes, travamos contato presencial com a pessoa com quem contrataremos ou entabularemos algum tipo de comunicação, no mundo virtual essa já não é a regra.

CHAVES PÚBLICAS

Uma infra-estrutura de chaves públicas (ICP) poderia ser conceituada como um sistema que tem por finalidade precípua, mas não exclusiva, atribuir certificados digitais (e conseqüentemente assinaturas digitais) a um universo de usuários.

Em realidade, além de fornecerem esses documentos eletrônicos às pessoas naturais, aos órgãos e às entidades públicas e privadas, os entes que compõem uma ICP - terceiros autorizados – desempenham a tarefa de gerenciar o ciclo de vida dos certificados, uma vez que a qualquer momento pode haver necessidade de revogar e emitir novos certificados, como no caso de comprometimento da chave privada de determinado titular de um certificado digital.

Portanto, uma infra-estrutura de chaves públicas tem o mesmo princí-

pio de qualquer outra instalação estrutural posta à disposição da sociedade, o de prover um serviço que pode ser obtido por qualquer interessado.

Atualmente no Brasil existe, advindo da Medida Provisória 2.200-2, o ICP-Brasil (infra-estrutura de chaves públicas – Brasil), que está sendo implantado pelo Comitê Gestor, que é uma espécie de conselho deliberativo com a atribuição principal de coordenar o início e o funcionamento da ICP-Brasil, bem com definir as normas técnicas a serem observadas neste âmbito.

Essas diretrizes são editadas mediante resoluções, e, previamente, todas as matérias a serem apreciadas serão analisadas pela Comissão Técnica Executiva (COTEC) que assiste e dá suporte técnico ao órgão deliberativo.

ENTIDADES CERTIFICADORAS

A Autoridade, ou Entidade de Certificação, deve reunir os técnicos e experiência necessária, de forma que se ofereça confiança, confiabilidade e segurança.

As funções de uma autoridade de certificação devem ser, entre outras, as seguintes: geração e registro de chaves; identificação de petições de certificados; emissão de certificado; armazenamento na AC (autoridade certificadora pública) de sua chave privada; manter as chaves vigentes e revogá-las.

Vale observar que o credenciamento perante o ICP-Brasil não é obrigatório para que as Autoridades Certificadoras possam emitir certificados digitais. O teor do disposto no parágrafo segundo do art. 10 da Medida Provisória:

> O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.[4]

Portanto, as partes de um contrato, por exemplo, podem escolher a utilização de certificados digitais emitidos por entidades não credenciadas na ICP-Brasil. Essa diretriz adotada pela Medida Provisória, qual seja, a de não condicionar o início do funcionamento das Autoridades Certificadoras à

4 BRASIL. Disponível em http://www.presidencia.gov.br. Acesso em 12 fevereiro 2004.

prévia autorização do poder público, é a mesma prevista na Diretiva Européia 1999/93, que dispõe sobre o quadro legal comunitário para as assinaturas eletrônicas.

Para essas entidades certificadoras, entretanto, deverá ser previsto o caso de desaparecimento do organismo certificador com a criação de um registro geral de certificação tanto nacional, como internacional.

VALOR PROBATÓRIO DO CERTIFICADO DIGITAL

Um documento eletrônico não pode ser assinado no modo tradicional, pelo qual o autor se identifica. Dessa maneira, é impossível que ele tenha a mesma forma que um documento tradicional, mas nada impede que determinados mecanismos informáticos possam trazer aos documentos digitais as três funções fundamentais dos documentos tradicionais, que são as funções identificativa, declaratória e a probatória.

Entende-se por integridade a estimativa que se faz se um documento foi ou não modificado após sua concepção. Será verificada a existência ou não de contrafação (rasuras, cancelamentos, escritos inseridos posteriormente, etc). Portanto, a integridade diz respeito ao conteúdo, às informações inseridas no documento.

A autenticidade é a verificação de sua proveniência subjetiva, determinando-se com certeza quem é seu autor. No documento em papel, o que demonstra a autoria geralmente é a assinatura. Naqueles documentos que não se costuma assinar, serão feitas análises grafológicas, no caso dos documentos digitais deverá ser analisado o certificado emitido digitalmente.

Quanto à tempestividade, é ela que garante a confiabilidade probatória do documento analisado. Será conferida pela verificação das formas de impressão, do tipo de tinta, os quais deverão estar compatíveis com a tecnologia disponível quando da feitura do documento.

Num primeiro plano analisa-se se o documento digital possui integridade, evitando, assim, que hajam adulterações não detectáveis. Posteriormente, deve ser um documento autêntico; isso significa que devem necessariamente estar presentes mecanismos aptos a identificar seu autor e sua proveniência, para que, dessa forma, garanta o seu não repúdio.

Por último, a data atribuída aos documentos eletrônicos é de suma importância, pois é assim que saberemos se há tempestividade, possibilitando sobremaneira a almejada segurança.

PRINCÍPIOS

Os documentos eletrônicos também devem obedecer a uma série de princípios inerentes às suas características, de maneira a torná-los válidos no âmbito jurídico. Entre estes princípios podemos destacar os seguintes:

- Princípio da Autenticação: onde as assinaturas digitais serão de fundamental importância, pois é com a utilização deste tipo de autenticação que as partes serão identificadas nos documentos eletrônicos;
- Princípio da Irrejeitabilidade: o documento eletrônico não perderá sua validade, sendo vedada a alegação de invalidade jurídica do documento eletrônico quando este cumprir com todos os requisitos de validade;
- Princípio da Conservação ou Arquivamento: documentos eletrônicos que convalidam determinada situação jurídica devem ficar armazenados em meio eletrônico, e no caso do Brasil, as entidades de Certificação é que deverão fazê-lo;
- Princípio da Privacidade: para ter validade deve o documento eletrônico ser confeccionado em ambiente seguro, por isso a necessidade de entidades de certificação. Vale observar que este princípio não descaracteriza a publicidade dos atos jurídicos, portanto, a privacidade aqui encontrada diz respeito à não interferência de terceiros na elaboração de um documento eletrônico.

As entidades de certificação são responsáveis pela privacidade dos documentos, além de conservarem e emitirem a autenticação. Elas funcionam de modo muito parecido com os cartórios, que emitem certidões com fé pública, portanto, as entidades de certificação são as responsáveis pela autenticidade e privacidade dos documentos elaborados de forma eletrônica.

IDENTIFICAÇÃO DAS PARTES EM MEIO ELETRÔNICO

São adotadas algumas cautelas de cunho jurídico no intuito de realizar uma identificação prévia das partes, utilizando-se, para tanto, de presunções inerentes aos registros públicos.

Conforme consagrado internacionalmente, as chaves de identificação são concedidas por Autoridades Certificadoras. As autoridades certificadoras, em regra, são empresas privadas encarregadas de averiguar a identidade de pessoas para fins de emissão de uma espécie de identidade eletrônica, no

intuito de possibilitar a realização de operações identificadas nas redes de computadores.

Elas disponibilizam aos usuários as chaves privadas, e cada um destes terá a sua. Esta chave é utilizada todas as vezes que um usuário necessitar de um certificado digital.

Assim, é criado o documento e assinado digitalmente pelos usuários interessados, cada um emite um certificado digital, utilizando suas chaves privadas. Após esta certificação, é elaborada pela entidade certificadora uma Chave Pública, que fica armazenada na Autoridade Raiz e torna aquele documento inalterável unilateralmente.

VALIDADE JURÍDICA DO DOCUMENTO DIGITAL

A validade do documento eletrônico em si não deve ser questionada. Uma vez que o contrato verbal é admitido como válido desde 1916, o contrato realizado em meio eletrônico por maior razão deverá ser considerado como válido, afinal quem pode o mais pode o menos.

O Código Civil de 2002 também não trouxe especificamente a validade do documento eletrônico, entretanto, isso não obsta sua validade, pois o documento eletrônico é considerado documento válido, ou seja, pode ser apresentado como meio de prova.

Alguns autores não consideram o documento eletrônico como um documento válido, porque ele não se reveste da forma tradicional de elaboração de documentos.

Entretanto, essa não nos parece a solução mais acertada, pois não considerar o documento eletrônico como documento válido é a mesma coisa que afirmar que não existe documento eletrônico.

Infelizmente, algumas pessoas ainda mantêm um certo receio quanto à utilização de documentos eletrônicos, pela sua grande volatilidade. É por essa razão que foi criada a certificação digital, para dar segurança aos documentos.

Portanto, o grande problema com que nos deparamos se relaciona à eficácia do documento eletrônico, mais especificamente a eficácia probatória.

A validade e eficácia dos documentos eletrônicos como meio de prova em muito diferem dos documentos comuns, isso porque eles apresentam uma série de peculiaridades de cunho técnico-informático, que lhe são próprias.

Em sede de direito comparado, a saída encontrada foi a elaboração de normas específicas sobre o tema que atendessem àquelas peculiaridades.

Assim sendo, em nossa legislação, por faltarem normas específicas aplicáveis ao caso, os documentos eletrônicos podem ser admitidos como meio de prova com fundamento no art. 332, do CPC, que determina que "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 defesa".

Porém, não há como se negar que o documento digital ainda causa um abalo na certeza quanto à integridade de seu conteúdo e quanto à sua autoria, o que gera uma fragilidade diante de uma fundamentada impugnação.

Com relação à validade dos documentos eletrônicos, temos algumas situações que devem ser consideradas:

A primeira é quanto à obrigatoriedade, pelo artigo 366 do Código de Processo Civil, de que a prova dos fatos jurídicos seja feita obrigatoriamente por documentos. Partindo dessa premissa, restará ao julgador a decisão de qualificar ou não o documento digital como um documento validamente inserido nas regras processuais para que, assim, se possa utilizá-lo como meio de prova de um fato jurídico, dentro do processo.

Quando a lei exige, para o negócio jurídico, determinada forma, não suportada pelos meios eletrônicos, há aí fortes empecilhos legais para que o documento digital seja considerado como prova do negócio firmado.

Mas, em outras negociações que admitem a forma livre, a comunicação da proposta e da aceitação entre contraentes capazes e legítimos, por documentos digitais, é plenamente adequável às normas brasileiras, não restando qualquer óbice para que tais documentos sejam utilizados com tal finalidade.

Devido à falta de legislação, o governo brasileiro editou a Medida Provisória 2.200/01 para garantir a segurança e a confiabilidade dos documentos emitidos via computador. Essa medida foi modificada devido às grandes críticas que sofreu, e foi reeditada com o número 2.200-2.

Essa MP introduziu a certificação digital em nosso país, tornando assim o documento eletrônico seguro e eficaz para a realização de qualquer tipo de negociação.

A MEDIDA PROVISÓRIA 2.200-2

Esta medida institui a infra-estrutura de chaves públicas brasileiras, o ICP-Brasil, com isso, passam a ser regulamentados, pelo menos inicialmente,

os certificados digitais em nosso ordenamento jurídico.

Com apenas vinte artigos, a medida provisória visa traçar as diretrizes da assinatura eletrônica brasileira, estabelecendo os órgãos reguladores, as autoridades certificadoras e principalmente trazendo a garantia de que os documentos eletrônicos se fixem como meio probatório absoluto.

No tocante à composição das chaves públicas brasileiras, temos que a ICP-Brasil é composta por um órgão gestor de políticas, por uma autoridade raiz e por uma rede de autoridades certificadoras.

O comitê gestor dessa ICP está vinculado à Casa Civil, tendo sua composição regulada pelo artigo 3º da medida provisória.

Este órgão gestor tem a finalidade de adotar as medidas necessárias para coordenar a implantação e o funcionamento da ICP-Brasil, estabelecendo o critério e as normas técnicas para o credenciamento das autoridades certificadoras, da autoridade raiz e dos demais prestadores desse serviço.

A primeira medida tomada pelo ITI foi tratar da interoperabilidade, que nada mais é que um elemento necessário para qualquer infra-estrutura e pode ser definida como a capacidade que possuem os aparelhos ou equipamentos que dela fazem parte de se comunicarem entre si, independentemente de sua procedência, ou do seu fabricante, ou seja, em um sistema de telefonia celular, por exemplo, a interoperabilidade permite que dois indivíduos que tenham aparelhos diversos e linhas telefônicas de operadoras diversas possam conversar sem problemas.

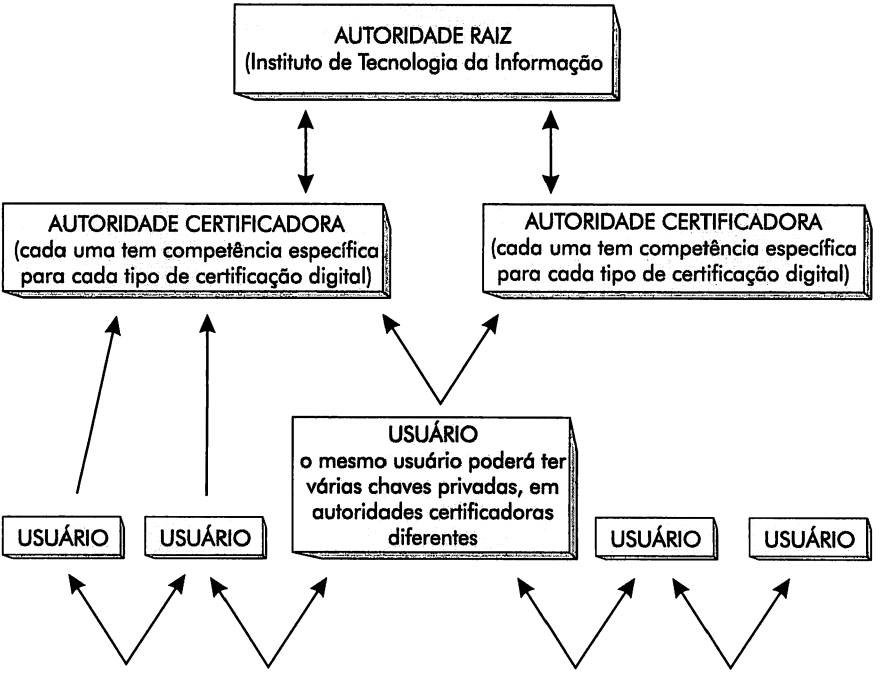
As regras operacionais na prática de certificação efetuadas pelas autoridades certificadoras e autoridade raiz também são regulamentadas pelo comitê gestor, que além dessas funções também é o responsável por avaliar as ICPs internacionais, podendo ainda negociar e aprovar acordos de certificação.

Qualquer órgão público ou particular poderá fazer parte da rede de certificação digital brasileira, não sendo exclusividade de órgãos públicos.

A autoridade raiz é o principal ente da certificação brasileira, incumbida de executar as políticas de certificados, normas operacionais e técnicas, tendo o papel de fiscalizadora das autoridades certificadoras, podendo emitir, expedir, distribuir, revogar e gerenciar a lista de certificados emitidos pelas AC.

O parágrafo único do artigo 5º desta medida provisória estabelece a posição da autoridade raiz (AR) em relação à autoridade certificadora (AC), colocando-as em escala hierárquica, uma vez que a autoridade raiz está no topo da hierarquia e as autoridades certificadoras estão subordinadas às regras

criadas pelo comitê gestor e aplicadas pela AR.



De acordo com o artigo 13 da MP 2.200-2, a autoridade raiz, ou principal autoridade certificadora brasileira, é o ITI – Instituto de Tecnologia da Informação, passando este a ser uma autarquia federal, portanto, a certificação digital brasileira será coordenada por um órgão público.

Essa coordenação pública foi muito criticada pela doutrina, uma vez que estaria atrapalhando a livre estipulação comercial, porém, esta mesma medida não obriga ninguém a utilizar a ICP-Brasil como meio de certificação, podendo assim utilizar-se de outros meios de certificação (artigo 10, §2°).

Para exercer suas funções com maior agilidade, o artigo 16 desta medida autoriza o ITI a contratar terceiros, podendo ainda requisitar servidores de outros órgãos, incluindo militares. Neste último caso, os servidores poderão ser requisitados para exercer cargos na diretoria do instituto e manterão os direitos e vantagens que têm no respectivo órgão de origem.

Já as autoridades certificadoras poderão ser qualquer entidade que esteja credenciada ao ITI, para que possa emitir certificados digitais, vinculando pares de chaves criptográficas ao titular, assim, o documento digital recebe a chamada "autenticidade".

Essas autoridades não poderão certificar documento fora de sua competência, ou seja, não poderão validar determinado documento que seja de competência de outra autoridade certificadora, porém, poderão, fazer autentificação com entidades da mesma competência.

Essa medida provisória foi criada para dar veracidade e segurança aos documentos digitais, propiciando assim uma maior agilidade nos atos praticados pelo computador, portanto, o artigo 10° é o dispositivo legal que dá a validade jurídica aos documentos produzidos digitalmente.

Vale ressaltar que também está expresso nessa medida que o certificado digital emitido por autoridade certificadora não credenciada ao ICP-Brasil poderá ser utilizado como meio de comprovação da autoria e integridade de documentos digitais.

Quanto à utilização do documento certificado digitalmente como meio probatório para fins tributários, a medida provisória coloca, além dos requisitos normais dos documentos eletrônicos, ainda, a necessidade de se respeitar o disposto no artigo 100 da Lei 5172 .

CONSIDERAÇÕES FINAIS

A falta de regulamentação e atribuição de validade jurídica aos documentos digitais representavam empecilhos ao desenvolvimento do comércio eletrônico.

As limitações que os documentos tradicionais, apostos em papel, nos apresentam quanto à rapidez e agilidade na circulação das informações, são gigantescas. Desta forma, a doutrina e a jurisprudência tendem para uma maior flexibilização, visando adaptar aos conceitos de documento a qualidade de dados digitais, não relacionados à materialização.

Apesar de alguns autores não admitirem a validade do documento digital, por não possuir a forma escrita, conforme exigida em lei, o posicionamento mais acertado seria no sentido da validade, visto que contratos de várias espécies podem ser realizados e, da mesma forma, considerados válidos, quando celebrados até mesmo por telefone ou de forma oral.

Para tal fim, a informática nos apresenta uma maneira inovadora de assinar, que é a assinatura digital, visando aumentar a confiança de seus usuários, garantindo, assim, que os requisitos inerentes a eles sejam verificados.

Com a assinatura digital, seu usuário tem certeza de que o documento não será modificado, sem deixar vestígios e também o destinatário poderá

confiar que a mensagem é mesmo de seu autor e que foi enviada exatamente na hora indicada.

A cada mensagem a assinatura será diferente, pois ela utiliza o conteúdo do texto e sua chave privada, formando o que chamamos de certificação de mensagem.

Conseqüentemente, cada documento terá uma assinatura diferente, pois seus conteúdos são diferentes, não tendo em hipótese alguma intenção de torná-la ilegível.

Uma vez que cada chave privada terá direito de modificar o documento conforme sua vontade, assim que ele for finalizado e certificado digitalmente por intermédio de cada chave privada (cada usuário tem a sua), será criada uma chave pública, que é imodificável unilateralmente.

Essa chave pública não será modificada, a não ser por vontade das partes, de comum acordo. O documento original será mantido, e cada modificação será feita e registrada como um novo documento que está apenso ao primeiro documento.

A normatização da questão indubitavelmente traz segurança nas relações negociais, possibilitando uma maior demanda nos negócios virtuais, gerando uma maior celeridade para os vários setores, além de provocar a captação de novos investimentos para o país.

Para proporcionar aos documentos digitais validade jurídica, devem ser criadas autoridades certificadoras, que emitem os pares de chaves. Essas autoridades têm responsabilidade quanto aos dados que confirmam, como também quanto à identificação e autenticação que fazem, ao intermediar relações entre as pessoas. Com a Medida Provisória nº 2.200-2 de 2001, a matéria referente às Autoridades Certificadoras foi regulamentada.

Com essa regulamentação, foi criado a ICP BRASIL, que tem como objetivo regulamentar e fiscalizar os certificados digitais emitidos dentro de nosso território.

Essa ICP – BRASIL é representada pelo ITI – Instituto de Tecnologia da Informação. Uma autarquia federal que tem o objetivo de regulamentar, fiscalizar e autorizar as entidades certificadoras. Cada entidade certificadora terá sua competência para determinada função, não podendo uma ultrapassar a competência da outra.

Essa regulamentação trouxe um grande avanço em nosso sistema de comércio, proporcionando às nossas empresas mais agilidade e segurança nas negociações internacionais, bem como nacionais (devido ao tamanho do país).

BIBLIOGRAFIA

BASSO, Maristela. A inclusão legal na economia digital. *Jus Navigandi*, Teresina, a. 6, n. 58, ago. 2002. Disponível em: <http://www1.jus.com.br/>. Acesso em: 14 mar. 2004.

BRASIL, Angel Bittencourt. *Assinatura Digital não é Assinatura Formal.* Disponível em: <http://www.ciberlex.adv.br> Acesso em: 11 mar. 2004.

BRASIL. Lei nº. 5.69, 11.1.1973. Código de Processo Civil, artigo 332.

BRASIL. Medida Provisória nº. 2.200-2. Disponível em: <http://www.presidencia.gov.br>. Acesso em 12 fevereiro 2004.

DINIZ, Davi Monteiro. *Documentos eletrônicos, assinaturas digitais.* São Paulo: LTr, 1999. p. 39.

MATTIUZO JÚNIOR, Alcides. *A Aplicação das Regras Gerais do Código Civil aos Contratos Eletrônicos.* Disponível em: <http:// www.mmo.adv.br>. Acesso em 26/05/2004.