Certificação Eletrônica na Legislação Brasileira Atual (The Electronic Certification in the current Brazilian Legislation)

Augusto Tavares Rosa Marcacini

Escrever sobre a certificação eletrônica e sua legislação mostra-se uma tarefa até certo ponto dificultosa, eis que se trata de um tema em franco movimento. As assinaturas digitais e a certificação eletrônica são uma novidade para o mundo e, certamente, ainda há muito o que a ciência jurídica possa desenvolver sobre o tema.

Embora o título aqui proposto envolva a "certificação eletrônica", é necessário dizer que o verdadeiro aspecto central, de onde partir qualquer discussão sobre o tema, é o documento eletrônico. Afinal, o problema prático que se quer ver resolvido é a possibilidade de uso de documentos eletrônicos, em substituição ao tradicional papel.O documento pode ser entendido como um registro de um fato. Em sua modalidade eletrônica, o documento consiste em uma seqüência de bits que, traduzida por determinado programa de computador, seja representativa de um fato.

Como documentos eletrônicos podem ser alterados, sem deixar vestígios físicos, e por não ser possível lançar sobre eles uma assinatura autógrafa, a literatura jurídica que se desenvolveu até meados da década de 90 recusava aceitá-lo como prova documental.

Esses problemas vieram a ser contornados por meio de assinaturas digitais, produzidas por uma variante da criptografia, denominada criptografia assimétrica. É esse o único meio conhecido e demonstrado de atribuir-se ao documento eletrônico duas qualidades essenciais, para que possa ser racionalmente aceito como meio de prova: a autenticidade e a integridade.

Para assinar digitalmente, é pressuposto inicial que o sujeito tenha gerado, primeiramente, um par de chaves, único e exclusivo para si, formado por uma chave privada e uma chave pública. O resultado da codificação de um documento utilizando criptografia assimétrica, tendo uma destas chaves como "senha", só pode ser decifrado com o uso da outra chave do mesmo par.

Desta forma, cifrando o documento com o uso da chave privada, que deve ser mantida em poder exclusivo do titular, o resultado dessa operação é o que chamamos de assinatura digital. A sua conferência é feita com o uso da chave pública, que pode e deve ser livremente distribuída. Se a assinatura digital puder ser decifrada sem erros com o uso da chave pública, isso é sinal que: a) quem gerou a assinatura digital tinha a correspondente

chave privada em seu poder (autenticidade); b) o documento eletrônico não foi alterado depois de lançada a assinatura (integridade).

Neste contexto, o certificado eletrônico é uma forma - não a única, mas talvez a mais prática - de se demonstrar a titularidade da chave pública utilizada para conferir a assinatura. Pode ser entendido, sob o ângulo jurídico, como uma declaração de uma pessoa - o ente certificante - em relação à chave pública de uma outra pessoa, atestando essa titularidade. Tecnicamente falando, o certificado é um arquivo eletrônico, assinado pelo certificante com a sua chave privada, contendo a chave pública e informações pessoais do titular desta chave pública. Do ponto de vista técnico, os certificados eletrônicos não são essenciais para que uma assinatura digital possa ser produzida. Para tanto, basta o par de chaves e um sistema que realize funções criptográficas.

Em nosso país, a primeira proposta de regulamentação legal do uso de documentos eletrônicos e assinaturas digitais partiu da Comissão de Informática da OAB-SP, quando apresentou anteprojeto de lei sobre o tema, que acabou se transformando no PLC nº 1589/99. O projeto previa tanto a certificação pública, pelo Tabelião, quanto as certificações privadas, não havendo obrigatoriedade do certificado emitido por um terceiro como requisito essencial da assinatura ou do documento eletrônico. A não obrigatoriedade do certificado, aliás, é uma tendência observada nas mais modernas legislações que têm surgido ao redor do mundo.

Com a aprovação, no Senado, do Projeto de Lei nº 672/99, este foi remetido à Câmara, onde acabou recebendo uma versão substitutiva, fortemente baseada no PLC nº 1589/99. Aprovado na Comissão Especial, este substitutivo aguarda votação em plenário.

Enquanto tramitavam no Congresso esses projetos de lei, o Poder Executivo Federal entendeu por bem instituir, por meio de mais uma Medida Provisória, uma infra-estrutura nacional de chaves públicas, denominada ICP-Brasil.

A primeira edição da Medida Provisória 2.200, de 28 de junho de 2001, continha vícios gravíssimos, de modo que não hesitamos em denunciar, naquela oportunidade, que tal norma estava muito mais próxima de instituir a espionagem eletrônica do que regular o comércio eletrônico, ou o uso de documentos eletrônicos e assinaturas digitais. Críticas várias foram feitas à época, de modo que, nas versões posteriores, os defeitos mais sensíveis foram retirados, quais sejam, a obrigatoriedade de sujeição à ICP-Brasil, a geração do par de chaves nos computadores das certificadoras e a presença obscura de um órgão dos serviços de inteligência para assessorar o Comitê que define os rumos desta infeliz criação.

Com a emenda constitucional que restringiu o uso de medidas provisórias, a MP 2.200, já na segunda versão, não mais pôde ser reeditada, passando a vigorar por tempo indeterminado, até que o Poder Legislativo a aprecie.
Não obstante reconhecer que, em sua versão atual, a MP nº 2.200 seja muito menos agressiva do que a primeira edição, a proposta padece de vícios originais, que não serão sanados enquanto se pretender levar a cabo a idéia de uma infra-estrutura nacional de chaves públicas, única, multifuncional e encabeçada pela Administração Federal.

O principal inconveniente que pode ser apontado deriva da própria concepção do projeto. Não se tem notícia de uma ICP com tamanhas proporções. Talvez não tenha o Executivo Federal se dado conta dos riscos sociais, econômicos e políticos envolvidos.

Do ponto de vista técnico, acredita-se que o elo mais sensível da utilização maciça de assinaturas digitais seja a defesa das chaves privadas. Se uma chave privada cair em poder de terceira pessoa, esta poderá gerar assinaturas digitais como se fosse o seu verdadeiro titular. Mas não é da defesa das chaves privadas da população em geral que me refiro, quando aponto os riscos desnecessários da ICP-Brasil, mas da própria chave raiz. Não porque este problema seja irrelevante, mas porque, infelizmente, qualquer que seja a concepção, os riscos envolvidos na guarda da própria chave privada por parte dos usuários estarão sempre presentes.

A estrutura única proposta pela MP 2.200 faz com que uma autoridade certificadora que se coloque logo abaixo da autoridade raiz possa emitir certificados para todos os fins, bancário, fiscal, comercial, identificando o titular para a prática de qualquer ato jurídico, de natureza pública ou privada.

Este fato faz com que o valor da chave raiz do Governo Federal, ou de uma AC por ela reconhecida, passe a ser infinito. Conseqüentemente, todo e qualquer esforço e investimento monetário que um criminoso puder realizar para se apossar da chave raiz, ou para fazer com que a chave raiz assine uma chave falsa, será certamente recompensado. Mais do que as chaves do cofre do Tesouro Nacional, a chave raiz da ICP-Brasil - se é que essa estrutura virá a vingar - será o alvo mais valioso do país para toda a sorte de criminosos e fraudadores.

Ao contrário, a existência de múltiplas estruturas distribuiria o risco. Seria muito mais conveniente que a iniciativa privada pudesse criar as suas próprias estruturas e a Administração Pública outras tantas. Ao prever uma estrutura única para o setor público e privado, os mentores da ICP-Brasil pressupõem que as necessidades são as mesmas. Até para o setor público não se justifica a criação de uma só infra-estrutura de chaves públicas. Afinal, a necessidade de segurança a ser implementada na ICP de uma Universidade Federal, para que alunos consultem notas ou peçam revisão e segunda chamada de provas, é muitíssimo menor do que a necessidade de segurança de uma ICP que fosse utilizada pelas Forças Armadas ou pelo Bacen.

O Executivo Federal, porém, ignorando as responsabilidades derivadas da ICP-Brasil, tem insistido em manter esta estrutura paquidérmica, apesar de não conseguir deixar minimamente claro qual o benefício que isso vai redundar para a sociedade, ou para o florescimento do comércio eletrônico. Aliás, sequer ficou clara a razão de o Estado Brasileiro precisar assumir tamanho risco, que amanhã pode ser suportado com o dinheiro público. Seria mais prudente deixar que o setor privado caminhasse por suas próprias pernas e, principalmente, assumisse o seu próprio risco.

Por outro lado, é de se notar que a edição da MP 2.200 praticamente congelou o nascente mercado de certificados eletrônicos, dado que os agentes econômicos, e mesmo as várias estruturas administrativas do Estado, estão com as mãos amarradas aguardando para ver no que a ICP-Brasil vai dar. Ou que rumo vai tomar, após tantas idas e vindas.

Do ponto de vista jurídico, por seu turno, a MP 2.200 também padece de defeitos, que merecem ser analisados de modo mais detido.

O conteúdo normativo da referida MP, em verdade, é bem pequeno. A maior parte dos seus vinte artigos destina-se a regular a estrutura administrativa da ICP-Brasil. Analisarei, adiante, apenas os artigos que regulam diretamente os documentos, assinaturas ou certificados eletrônicos.

O artigo 1º estabelece que "fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras".

Um primeiro e evidente equívoco pode ser notado já neste texto. "Validade jurídica" não é uma qualidade que se atribua a documentos. Validade ou invalidade são atributos dos atos jurídicos, não dos documentos. Documentos podem ser falsos ou verdadeiros, pode-se falar no seu valor probante, mas não há sentido na expressão "validade jurídica de documentos em forma eletrônica". Até porque a validade de um ato jurídico envolve vários requisitos outros, que nenhuma relação mantêm com o documento.

Por outro lado, quando se afirma que a ICP-Brasil foi criada para garantir a autenticidade ou a integridade de documentos eletrônicos, o texto legal está, em verdade, apenas anunciando os objetivos da estrutura que é ali prevista, e não normatizando.

É que autenticidade e integridade são qualidades de um documento, físico ou eletrônico, e se situam no plano dos fatos, não do Direito. No caso do documento eletrônico, o que assegura e permite conferir sua autenticidade e integridade são as operações e sistemas que utilizam criptografia assimétrica. Não é a lei, portanto, que pode afirmar que um documento, físico ou eletrônico, é autêntico e não foi adulterado.

Que fique claro, portanto, que não poderia a MP 2.200 atribuir autenticidade ou integridade a documentos eletrônicos que ainda serão criados. A ICP-Brasil, como qualquer outra estrutura de chaves públicas, é tendente a criar uma rede de confiança que permita demonstrar a titularidade de chaves públicas, não havendo sentido em afirmar-se, na lei, que os documentos daí gerados serão autênticos e materialmente verdadeiros. Nem pode a lei determinar que os sistemas que utilizam criptografia assimétrica para produzir e conferir assinaturas não estejam sujeitos a falhar, fato que a literatura técnica não descarta e a experiência, por vezes, confirma.

Por último, diz o artigo que a ICP-Brasil irá também garantir a "realização de transações eletrônicas seguras". A frase "transações eletrônicas seguras", embora bastante sonora, carece de um significado jurídico claro. Aliás, a expressão soa tão bem que se tornou marca registrada de um produto lançado há alguns anos por conhecida empresa do setor financeiro, como bem tem lembrado o advogado e amigo Marcos da Costa, sempre arrancando sonoros risos da platéia. Já do ponto de vista do Direito, é de se destacar que,

primeiramente, por "transação" provavelmente se quis dizer "contratação", palavra que seria mais apropriada.

Mas, por outro lado, que tipo de segurança se pensa que uma ICP pode conferir à contratação como um todo? Ao "garantir" essa segurança, estaria o Governo se responsabilizando por ela?

Daí em diante, até o artigo 9º, a MP somente trata da estrutura orgânica da ICP-Brasil. No artigo 10º, encontramos:

"Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

"§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1º de janeiro de 1916 - Código Civil.

"§ 2º 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."

O caput do artigo nos dá conta do risco envolvido na ICP-Brasil, de que tratei acima. A ICP-Brasil certifica chaves para todos os fins. No contexto da primeira edição da MP, esta regra era claramente tendente a criar uma obrigatoriedade no uso de chaves certificadas pela ICP-Brasil, sugerindo que somente documentos eletrônicos assinados com essas chaves poderiam ser aceitos no conceito de documento público ou particular.

Em virtude das críticas que foram dirigidas a essa MP, os dois parágrafos foram inseridos na primeira reedição, sendo que o parágrafo segundo, adiante comentado, retirou o caráter obrigatório e monopolístico da ICP-Brasil.

O parágrafo primeiro é texto absolutamente inútil, diante do que já consta do caput. Como, porém, interpretações errôneas têm surgido a seu respeito, vale a pena tecer algumas considerações sobre esta norma.

O dispositivo em questão diz que os documentos eletrônicos assinados com chaves da estrutura da ICP-Brasil "presumem-se verdadeiros em relação aos signatários", na forma do artigo 131 do Código Civil. Este artigo diz que "as declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários". Ora, o artigo referido diz a mesma coisa, para documentos em geral, de modo que o texto constante da Medida Provisória é redundante. Aliás, a mesma regra também se encontra no Código de Processo Civil, em seu artigo 368: "as declarações constantes do documento particular, escrito e assinado, ou somente assinado, presumem-se verdadeiras em relação ao signatário".

Na medida em que o caput do artigo 10 diz que os documentos eletrônicos são equiparados a documentos públicos ou privados, as regras dos artigos 131 do CC e 368 do CPC já lhes seriam automaticamente aplicáveis. O parágrafo, então, nada acrescenta de novo.

Essas regras todas estabelecem a chamada presunção de veracidade do documento, enquanto meio de prova, presunção essa que se limita ao signatário do documento. Noutras palavras, o documento faz prova contra seu autor. Se um sujeito assina um documento, é porque assume como verdadeiro o seu conteúdo. Como essa presunção não é absoluta, admite-se que o signatário impugne a veracidade de um documento, alegando ser ideologicamente falso, isto é, que os seus dizeres são falsos, embora o documento seja materialmente verdadeiro. Entretanto, a presunção de veracidade faz com que o signatário tenha que provar o que alega e, na falta de prova, prevalece o teor do documento.

Todo documento, público ou privado, goza desta presunção de veracidade que, em última análise, deriva do próprio valor probante da prova documental.

Outra coisa, bastante diversa, é a presunção de autenticidade. Autenticidade é a certeza quanto à autoria do documento, ou seja, que o seu signatário é verdadeiramente a pessoa que está ali indicada como tal. A autenticidade, em regra, não se presume, e disso não trata, em absoluto, nem o artigo 131 do Código Civil, nem o artigo 368 da lei processual, nem tão pouco este artigo 10 da MP 2.200. Mesmo nos casos em que a lei confere a algum ato o condão de presumir a autenticidade de um documento (p.ex., no artigo 369, do CPC), esta presunção não é absoluta, mas relativa, significando apenas uma inversão do ônus da prova, de modo que se transfere a quem alega a falsidade da assinatura a tarefa de demonstrar esse fato ao juiz. E, na falta desta prova, prevalece a presunção de autenticidade.

Outra afirmação despropositada relacionada com a questão, e que pulula mundo afora, diz respeito ao conceito de não repúdio. Tornou-se modismo dizer que, utilizando-se assinaturas e certificados digitais, o documento se torna imune à qualquer impugnação posterior. A expressão não repúdio, primeiramente, não tem qualquer significado jurídico. Como assinala Bruce Schneier (in "Secrets and Lies - Digital Security in a Networked World"), o termo era utilizado na literatura acadêmica sobre criptografia para significar tão somente que o algoritmo matemático se mostra inquebrável. Ainda segundo Schneier, foi a indústria de PKI que se apossou da expressão, sugerindo nela o significado jurídico absurdo que lhe tem sido atribuído.

O uso jurídico que se quer dar ao termo não repúdio esbarra no fato de que, para o bem ou para o mal, a verdade ainda não se transformou em uma operação matemática.

Impedir alguém de impugnar a veracidade de uma assinatura em um documento é algo que não encontra guarida no nosso Direito atual, e duvidamos que possa existir em um Estado Democrático de Direito, no qual não se possa suprimir do Poder Judiciário a apreciação e solução dos conflitos.

Pode-se até argumentar que a prova contra a assinatura digital, ou contra o certificado, seja uma prova difícil. Entretanto, isso não significa que o documento eletrônico possa estar

imunizado de toda e qualquer impugnação, ou que o juiz não possa apreciar a sua veracidade de modo livre e racional.

Evidentemente, a MP 2.200, cujas normas sequer atribuem presunção de autenticidade aos documentos gerados pela estrutura ali criada, não pode tornar irrepudiáveis os documentos eletrônicos.

O parágrafo segundo, por seu turno, pode ser considerado a mais sensata disposição contida na Medida Provisória. Adotando a linha das legislações modernas, como já ressaltado acima, reconhece-se que documentos eletrônicos podem servir como meio de prova, independentemente do uso de chaves certificadas pela ICP-Brasil, ou por qualquer terceiro.

A parte final do dispositivo, porém, é um tanto confusa e, na verdade, não importa propriamente em uma restrição ao uso de documentos eletrônicos, como pode parecer à primeira vista.

Um "outro meio de comprovação da autoria e integridade" de documentos eletrônicos, para ser racional, e ser considerado como prova documental, não pode deixar de utilizar criptografia assimétrica e assinaturas digitais assim produzidas, já que essa é a única maneira conhecida a permitir equiparar documentos eletrônicos com as funções exercidas pelo papel. O que se pode interpretar a partir do texto é que o uso de assinaturas digitais se tornou livre e reconhecido pelo ordenamento jurídico, dispensando-se adiante, no texto, o uso de certificados da ICP-Brasil.

A demonstração da autoria deste documento eletrônico envolve a prévia demonstração da titularidade da chave pública utilizada na conferência da assinatura. Essa é uma questão de fato que, como tal, pode ser provada por outros meios, além do certificado, como, por exemplo, o prévio reconhecimento, por escrito, do titular das chaves, de que a chave pública é mesmo sua.

A "pessoa a quem for oposto o documento" é a mesma que o assinou, já que documentos em geral fazem prova contra o signatário. Ora, essa pessoa, primeiramente, gerou um par de chaves para seu uso e, posteriormente, utilizou sua chave privada para assinar digitalmente um documento. Esse ato, por si, caracteriza sua aceitação quanto ao conteúdo do documento. A aceitação do signatário é, pois, inerente ao ato de assinar. Não se confunda, entretanto, com a prova de que foi verdadeiramente ele o signatário, questão relativa à autenticidade do documento e, por pressuposto, da chave pública utilizada na conferência.

O artigo 11, por sua vez, estabelece que "a utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei no 5.172, de 25 de outubro de 1966 - Código Tributário Nacional". O artigo do CTN, por sua vez, dispõe que:

"Art. 100 - São normas complementares das leis, dos tratados e das convenções internacionais e dos decretos:

I - os atos normativos expedidos pelas autoridades administrativas;

II - as decisões dos órgãos singulares ou coletivos de jurisdição administrativa, a que a lei atribua eficácia normativa;

III - as práticas reiteradamente observadas pelas autoridades administrativas;

IV - os convênios que entre si celebrem a União, os Estados, o Distrito Federal e os Municípios.

"Parágrafo único. A observância das normas referidas neste artigo exclui a imposição de penalidades, a cobrança de juros de mora e a atualização do valor monetário da base de cálculo do tributo."

O caminho tortuoso e confuso que foi adotado neste artigo o torna de difícil compreensão. Aparentemente, quer-se dizer que esta Medida Provisória e sua regulamentação podem ser consideradas normas complementares da legislação tributária e, com isso, permitir-se o uso de documentos eletrônicos no campo fiscal. De certo modo, a norma aparenta ser desnecessária, pois se o artigo anterior afirma que documento eletrônico é espécie de documento, seria natural admiti-lo também para a documentação tributária.
Os demais artigos, de 12 a 18, voltam a tratar da estrutura orgânica da ICP-Brasil, e os dois últimos trazem disposições gerais e transitórias, de modo que tudo o que dispõe a MP, sobre documentos eletrônicos, assinaturas e certificados, são os três artigos acima comentados.

Disponível em:< http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=1424 Acesso em.: 10 set. 2007.