Assinaturas eletrônicas podem enganar usuários

Muito se tem comentado a respeito do uso de assinaturas eletrônicas como meio mais seguro de "garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica", conforme o artigo 1º da Medida Provisória 2.200-2, ainda em vigor.

Quanto à validade jurídica — não confundir com eficácia — de um documento eletrônico, muito já foi debatido acerca da real necessidade de se utilizar assinaturas digitais quando o Código Civil (art. 107) diz que "(a) validade da declaração de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir" e o Código de Processo Civil (art. 332) complementa com "todos os meios legais, bem como os moralmente legítimos, ainda que não especificados nesse Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou defesa". Há a interpretação restritiva de que a assinatura digital é requisito para a validade, mas há também a de que ela apenas garante a validade, não sendo necessária para tal efeito, sendo quesito que auxiliaria em sua eficácia.

Apesar das discussões existentes, até este momento não é pacífico se a validade de documento eletrônico depende de forma específica ou não. O mesmo texto da MP 2.200-2 continua no PL 7.316, que está em discussão para a substituição daquela.

A diferença acrescentada é que, pelo PL, art. 5º, "(a)s assinaturas eletrônicas avançadas têm o mesmo valor jurídico e probante das assinaturas manuscritas, na forma do art. 219 da Lei nº 10.406, de 10 de janeiro de 2002 – Código Civil", ou seja, as assinaturas eletrônicas certificadas pela ICP-Brasil serão equivalentes às assinaturas manuscritas. Além disso, garantiriam a autenticidade, a integridade e a validade do mesmo, o que simples assinaturas manuscritas não o fazem.

Mas além das discussões jurídicas, ainda existem algumas questões técnicas que precisam ser melhor trabalhadas. Por exemplo, a definição de que tipos de documentos podem ser assinados e de quais recursos tais documentos podem utilizar.

Isso porque alguns tipos de documentos, os interpretados, ou seja, aqueles que antes de serem exibidos na tela ou impressos no papel passam por algum tratamento pelo software a ele associado, podem ser utilizados para fraudar documentos sem que sua assinatura digital seja invalidada. Demonstramos tal hipótese na palestra "O Sistema ICP-Brasil e a Usabilidade do Certificado Digital no Mundo Jurídico: o uso do sistema nacional de certificação digital na modernização do judiciário", apresentada no 2° Certforum organizado pelo ITI — Instituto Nacional de Tecnologia da Informação, no dia 23 de novembro de 2004.

Fraudes de documentos eletrônicos com assinaturas digitais

Uma das maiores bandeiras dos defensores das assinaturas digitais é sua força frente a tentativas de fraudes. Calcadas em modelos matemáticos complexos, estas impedem que qualquer alteração realizada em um conjunto de zeros e uns (arquivos binários) passe despercebida.

Qualquer documento eletrônico é composto de zeros e uns, seja em *hard disks*, disquetes, memória

RAM, CD-ROMs ou outros semelhantes. O mesmo vale para todos os arquivos que podem ser gravados em computadores, ou seja, sons, vídeos, etc. Assim, uma das vantagens do uso de assinaturas digitais é que outros meios de provas até então não-assináveis são agora passíveis de reconhecimento prévio pelas partes. Uma assinatura digital pode ser colocada em qualquer arquivo composto de zeros e uns, fazendo com que sejam considerados documentos assinados. Se forem certificados pela ICP-Brasil, terão então garantidas a sua autenticidade, a integridade e a validade jurídica.

Ocorre que uma assinatura digital é realizada sobre o conjunto de zeros e uns que estão gravados em algum lugar, e não sobre o resultado que o computador exibe em alguma saída padrão, seja o monitor, seja um impressora ou qualquer outra forma de exibir o conteúdo dos arquivos binários.

A possibilidade de fraude de assinaturas digitais que demonstramos no 2° Certforum reside justamente em realizar as alterações não no documento gravado e assinado, mas na exibição de sua interpretação para o usuário. Isso faria com que as alterações na exibição do documento não invalidassem as assinaturas digitais sobre os mesmos.

Isso é possível em virtualmente qualquer tipo de documento, pois o que se assina é o arquivo binário, que não necessariamente é igual ao que é exibido. Para isso, em tese, é necessário um programa adulterado para fazer com que a exibição seja diferente do que é salvo.

Mas em determinados tipos de documentos, e infelizmente a lista é bem extensa, é possível se utilizar de tal ponto fraco das assinaturas eletrônicas apenas com os próprios recursos dos programas mais comuns, sem que seja necessário alterar o software. Podemos citar como exemplos os documentos produzidos pelo Microsoft Word (.doc), Microsoft Power Point (.ppt), Adobe Acrobat (.pdf), arquivos HTML (.htm), OpenOffice (.sxi, sxw), etc.

O exemplo que utilizamos na demonstração consistia em uma declaração de doação com data futura produzido no Microsoft Word. Se aberto em qualquer computador ou impresso em qualquer impressora, o documento conteria o termo da declaração com uma certa data futura.

O documento foi assinado digitalmente, o que impede que qualquer alteração no seu conjunto correspondente de zeros e uns seja realizada sem invalidar a assinatura.

Entretanto, a parte do documento que exibia a data futura para a doação era um campo especial do documento, que estava programado para sempre exibir o dia atual somado de um. Ou seja, a data para a doação nunca chegaria, pois seria sempre o dia seguinte à data atual do computador.

A data em si não é salva dentro do documento composto por zeros e uns, ela é apenas exibida na tela ou no papel. No documento binário que recebe a assinatura, fica salvo um comando, por exemplo: {mostrar: data atual + 1 dia}. Ou seja, o comando não será alterado, mas o seu resultado sim. Isso permite a exibição de um mesmo documento de diversas formas sem invalidar a assinatura.

Os signatários, se não pedirem para o Word exibir os campos que são variáveis, poderiam ser ludibriados, pensando estarem assinando o documento conforme estão vendo na tela ao passo que o queé salvo com a assinatura é diferente.

Apesar de o exemplo ter sido realizado com uma data, ele poderia conter virtualmente qualquer possibilidade de alteração. Poderia ser o nome do beneficiário, por exemplo, que se alteraria depois de um número definido de dias.

Claro que o uso de tal recurso pode ser facilmente periciado. Mas pode não ser possível recuperar, pela perícia, o valor existente no momento da assinatura.

Um outro exemplo que podemos citar é o da assinatura de um documento em formato HTML contendo a foto de um carro, objeto do contrato de compra e venda. Os documentos HTML não guardam as imagens dentro do próprio arquivo, mas fazem referência a um arquivo externo. A assinatura eletrônica de um documento com esse formato não impediria a troca da figura por outra, ela continuaria válida quando verificada e o carro, objeto do contrato, poderia ser modificado.

Se nossa legislação diz que as assinaturas digitais, quando certificadas pela ICP-Brasil, objetivam “garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica”, como tratar tal hipótese?

Sabemos que, até este momento, não se conhece forma de violar a autenticidade de uma assinatura digital certificada pela ICP-Brasil. Assim, a garantia de integridade, que pode ser violada no nível da interpretação dos documentos eletrônicos, é apenas dos signatários ou da própria cadeia de certificação, que responderia solidariamente?

Se nossa legislação coloca toda a ICP-Brasil na condição de garantir a validade e a integridade de documentos eletrônicos, podemos considerar a hipótese de chamar uma Autoridade Certificadora – AC à lide se acontecer caso semelhante a este?

Invalidação de assinaturas decorrente do uso de meta-dados

Outra falha que pode ocorrer tem ligação com esta que acabamos de citar. Os documentos interpretados, os mesmo que estão sujeitos àquele tipo de fraude, podem conter os chamados meta-dados.

Meta-dados são informações ocultas nos documentos que não precisam estar à mostra para os usuários e que são utilizados para armazenar informações sobre os documentos. Por exemplo, um documento pode armazenar a data de sua última impressão.

Esses meta-dados, apesar de não poderem ser utilizados para fraudar documentos, podem fazer com que documentos legítimos tenham suas assinaturas invalidadas sem que os usuários saibam disso.

Imaginem que um documento celebrado em determinada data é assinado em formato digital e cada parte mantém uma cópia consigo. Após certo período de tempo, cada uma das partes imprimiu algumas vias do documento. Se foi utilizado um editor de textos como o Microsoft Word, por exemplo, e os

documentos não estiverem protegidos contra gravação, as assinaturas digitais não mais confirmarão a integridade do documento, mesmo que os signatários estejam de boa-fé e não tenham pretendido realizar alterações no mesmo.

Nesta hipótese, retornamos mais uma vez ao que diz nossa legislação: as assinaturas digitais certificadas pela ICP-Brasil objetivam “garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica”. Assim, a perda da assinatura retiraria a validade de um documento eletrônico? Este deixaria de ser válido para o mundo jurídico?

Conclusão

Documentos eletrônicos não são iguais a documentos físicos. Sua natureza é distinta e, conseqüentemente, seu tratamento jurídico também o deve ser.

A simples equiparação dos documentos eletrônicos assinados digitalmente, com o uso de chaves certificadas pela ICP-Brasil ou não, aos documentos físicos pode trazer algumas situações complexas. Algumas delas são: a possibilidade de adulteração do documento sem deixar mostras claras ao leigo ou a possibilidade de sua completa invalidação por mera alteração em dados irrelevantes, como os meta-dados.

No primeiro caso, a perícia poderia detectar o uso de meios para a fraude, mas não poderia detectar como o documento foi exibido no momento da assinatura. Na segunda hipótese, a perícia detectaria uma alteração que invalidaria as assinaturas por completo, possibilitando à parte de má-fé alegar a ausência de valor do documento, já que a validade é dada pela assinatura da ICP-Brasil, o que não ocorreria em perícia de documento físico, que poderia detectar a parte adulterada do texto.

Devemos notar, por fim, que tal falha não é das assinaturas digitais e nem do modelo de certificação, seja ICP-Brasil ou qualquer outro, mas sim da forma como alguns documentos podem ser exibidos diferentemente do que são armazenados. Isso também não quer dizer que documentos eletrônicos não sejam seguros, ou até mesmo mais seguros que os documentos físicos. Quer apenas dizer que não são absolutamente perfeitos e que essas questões merecem um debate mais amplo.

Além disso, os usos de documentos eletrônicos trazem inúmeras outras vantagens, como a facilidade de manutenção, baixo custo de guarda e a possibilidade de serem tratados em lotes, o que é um fator de suma importância econômica em sociedades de massa tão complexas como a contemporânea, que produz muito mais documentos do que em qualquer outro momento da história.

Date Created
01/12/2004