A Assinatura Digital e o Processo Judicial Eletrônico: Um Estudo do Impacto da Revogação do Certificado Digital na Validade dos Atos Processuais

Ramses Henrique Martinez
Faculdade de Tecnologia de São Paulo – FATEC-SP – Brasil
ramses@usp.br

Benedito Cristiano Aparecido Petroni
Faculdade de Tecnologia de Jundiaí – FATEC Jundiaí – Brasil
prof.benedito@fatecjd.edu.br

RESUMO – A proposta deste trabalho foi realizar uma pesquisa exploratória na adoção das assinaturas digitais no processo eletrônico, e pretende estudar o impacto da revogação do certificado digital sobre a validade dos documentos eletrônicos, por meio dos quais os atos judiciais são realizados. O Poder Judiciário tem se modificado para aumentar a sua eficiência por meio da implementação de sistemas eletrônicos de processamento de ações judiciais, como o processo eletrônico. O processo envolve a substituição da assinatura eletrônica de documentos em papel pela assinatura digital. Assim, é necessária uma certificação válida de assinaturas digitais, de modo que, mais tarde, não haja rupturas que possam restringir, ou mesmo impedir, a adoção do processo eletrônico.

ABSTRACT – The proposal of this work was to perform an exploratory research in the adoption of digital signatures in electronic proceedings, and intends to study the impact of the repeal of the digital certificate on the validity of electronic documents, through which the judicial acts are performed. The judiciary has moved to increase their efficiency by implementing electronic systems for the processing of lawsuits, such as the electronic process. The lawsuit involves the replacement electronic signature of paper documents into the digital signature. Thus, it is necessary to valid certification of digital signatures, so that, later, there are disruptions that could restrict or even prevent, the adoption of electronic proceedings.

Palavras-Chave: *signature; certified; digital*

1. INTRODUÇÃO

A proposta deste trabalho é realizar uma pesquisa exploratória, no âmbito da adoção da assinatura digital no processo judicial eletrônico, e pretende estudar o impacto da revogação do certificado digital na validade dos documentos eletrônicos, por meio dos quais os atos judiciais são praticados. Segundo Martinez [1] (p. 1), "*a prestação jurisdicional é função do Poder Judiciário (inciso XXXV, do artigo 5º., da Constituição Federal de 1988): por meio de seus magistrados, o Poder Judiciário aplica a lei (normas gerais e abstratas impostas pelo Estado aos particulares) para resolver conflitos de interesse que o cidadão-jurisdicionado leva a seu conhecimento (casos concretos)*". O Poder Judiciário tem caminhado para aumentar sua eficiência, por meio da implementação de sistemas eletrônicos para o processamento de ações judiciais, tais como o processo eletrônico. Nesse aspecto, cabe observar que a

eficiência já foi elevada a princípio constitucional, pela Emenda Constitucional nº. 19, de 04/06/1998, conforme dispõe seu artigo 37.

2. PROBLEMA DE PESQUISA E OBJETIVO

O processo judicial eletrônico envolve a substituição da assinatura de documento em papel pela assinatura digital. Assim, torna-se necessária a certificação válida das assinaturas digitais, para que, posteriormente, não ocorram anomalias que possam restringir, ou até mesmo impedir, a adoção do processo judicial eletrônico. Atualmente, a utilização de métodos e técnicas forenses tem auxiliado o Poder Judiciário na investigação de atos ilícitos envolvendo assinaturas digitais, fornecendo-lhes elementos importantes para a apuração de tais atos. Paralelamente aos métodos e técnicas forenses [2, 3], foi desenvolvido o conceito de certificação digital. Desse modo, a questão-problema desta pesquisa pode ser formulada da seguinte maneira: como a revogação do certificado digital impacta a validade dos documentos eletrônicos, por meio dos quais os atos judiciais são praticados.

3. REVISÃO BIBLIOGRÁFICA

3.1. Assinatura de Documento em Papel

Como ensina Bernal [4], a assinatura de documento em papel tem as seguintes características: "*garantia de autoria – a assinatura é utilizada para validar o autor da assinatura; garantia da irretratabilidade de geração – somente o autor da assinatura pode ter assinado; garantia da integridade – garantida pela ausência de rasuras no documento assinado; permite a verificação da assinatura por um terceiro – um documento assinado pode ser verificado por uma terceira parte, com o objetivo de solucionar eventuais disputas; signatários – podem existir diversos signatários; documento – o documento pode conter várias folhas. Neste caso, é inserida uma rubrica em cada folha*". Quanto ao instante da assinatura, Bernal [4] ensina que "*o instante que consta no documento é o instante acordado pelos signatários*", sendo que "*o instante da assinatura não é 'confiável'*". Diante disso, Bernal [4] levanta a seguinte questão: "*como garantir o instante da assinatura?*". "*Através de uma 'terceira parte' confiável (ex. cartório); 'dá fé' que o instante que consta no documento é o instante no qual o documento foi assinado; 'terceira parte' (cartório) observa a assinatura dos signatários e também assina o documento, atestando o instante da assinatura*" [4]. Desse modo, Bernal [4] conclui que "*existem duas classes de assinatura tradicional: - assinatura sem garantia da data de assinatura (envolve somente os signatários); - assinatura com garantia da data de assinatura (envolve os signatários e uma terceira entidade de confiança)*".

3.2. Documento Eletrônico

De acordo com o ITI [5], conteúdo digital é "*um documento eletrônico sobre o qual se realiza uma assinatura digital*", sendo que documento eletrônico é "*uma seqüência de bits elaborada mediante processamento eletrônico de dados, destinada a reproduzir uma manifestação do pensamento ou um fato*". O documento eletrônico é a representação de um fato concretizado por meio de um computador e armazenado em programa específico, capaz de traduzir uma seqüência da unidade internacional, conhecida como bit.

3.3. Geração Técnica da Assinatura Digital

Segundo Guelfi [6] (p. 66), "*a geração técnica da assinatura ocorre em dois ciclos, seguindo os seguintes passos: 1º. Ciclo. De posse de um arquivo eletrônico, o usuário gera um bloco hash. Para a geração deste bloco é necessária a utilização de um algoritmo criptográfico de função hash como MD2, MD4, MD5, SHA1 entre*

outros. O bloco hash consiste num valor seqüencial de bits com tamanho fixo obtido a partir da mensagem original. Ocorrendo a mudança de um único bit que seja da mensagem original, o valor seqüencial de bits que se obterá será totalmente diverso daquele gerado anteriormente à modificação do arquivo. 2º. Ciclo: A assinatura digital propriamente dita é engendrada, quando o bloco hash originalmente gerado a partir da mensagem é criptografado utilizando-se a chave privada do signatário. Os mais comuns são RSA[1] *(baseado na teoria dos números), DAS (baseado na teoria dos logaritmos discretos) e o ECDSA (baseado na teoria das curvas elípticas). O documento eletrônico assinado digitalmente é formado pelo arquivo eletrônico e a assinatura digital, que juntos ou separadamente seguem o seu caminho para seu destinatário*". A seguir, a Fig. 2 ilustra o funcionamento da geração da identificação de uma assinatura digital. Pode-se observar que na Fig. 2 existe um texto original onde é utilizada a função *hash* contendo as informações e a partir disto é gerada a assinatura digital através de um algoritmo para criptografia, pelo remetente. O formato utilizado para o encapsulamento de documentos eletrônicos e assinaturas digitais PKCS#7/CMS[2] envolve todos os elementos necessários para a verificação da assinatura: bloco de assinatura, o certificado digital, a lista de certificados revogados, o documento eletrônico que foi assinado, carimbo de tempo e contra-assinaturas [6]. Conforme destaca Marcacini [7], a obrigação de armazenamento da chave privada de forma segura consiste num elemento novo na órbita jurídica, tendo em vista que esta hipótese não possui precedentes quanto às assinaturas convencionais, destacando a importância desta medida como sendo aspecto fundamental da segurança das assinaturas digitais. De acordo com Guelfi [6] (p. 42/43), "diante desta responsabilidade do titular de par de chaves em manter a chave privada em total segurança contra ataques externos, algumas técnicas são propostas, como o uso de smart-cards e tokens, que possuem um chip interno à prova de invasão e somente podem ser utilizados através de uma senha ou algum tipo de biometria (por exemplo, impressão digital). Esses dispositivos são capazes de processamento interno e podem receber programas que usam a chave privada protegendo-a contra qualquer tipo de invasão".

3.4. Certificação Digital

Certificação digital é um documento eletrônico que contém o nome, um número público exclusivo denominado chave pública, e muitos outros dados que mostram quem somos para as pessoas e para os sistemas de informação. A chave pública serve para validar uma assinatura realizada em documentos eletrônicos [5]. A utilização de uma assinatura digital tem por finalidade assegurar a autenticidade e a integridade aos documentos eletrônicos. A técnica de assinatura digital é uma forma eficaz de garantir autoria de documentos eletrônicos [5]. "O certificado digital surgiu exclusivamente para completar a lacuna encontrada na tecnologia das assinaturas digitais. O uso da criptografia assimétrica, em si, assegura a integridade dos dados eletrônicos, entretanto, para assegurar força probante documental a esses dados, era preciso assegurar também a autenticidade. Para tanto, surgiu o certificado digital, completando os requisitos exigidos pelas normas legais, para conferir aos dados eletrônicos a garantia documental" [6] (p. 76). De acordo com o ITI [5], "*o certificado digital é um documento eletrônico assinado digitalmente por uma terceira parte confiável, que associa uma entidade (pessoa, processo ou servidor) a uma chave pública*".

[1] Rivest, Shamir e Adleman

[2] CMS – Cryptographic Message Syntax

3.5. Validação legal e técnica de um certificado digital

Como destaca Guelfi [6] (p. 67/68), "*ao receber o arquivo assinado digitalmente, contido ou não no formato PKCS#7/CMS, o destinatário deverá observar os seguintes passos a fim de verificar a autoria e a integridade do arquivo. - De início, o destinatário deverá obter a chave pública do signatário de uma forma confiável. Num contexto de infra-estrutura de Chaves Públicas, (...), essa chave é extraída do certificado digital do signatário. - Realizada referida tarefa, o destinatário promoverá a geração de um bloco hash. Este novo bloco hash gerado é denominado de "hash corrente". Esta geração ocorre somente sobre o arquivo original recebido, excluindo-se a assinatura digital. Para tanto, o destinatário deverá utilizar-se do mesmo algoritmo de hash utilizado pelo signatário quando da geração da assinatura; - Em seguida, o destinatário decifrará a assinatura digital utilizando a chave publica certificada. O resultado obtido corresponderá ao bloco hash gerado pelo signatário quando da produção da assinatura; - Como última ação de verificação realizada pelo destinatário, haverá a comparação entre os blocos hashs anteriormente citados. Ocorrendo a igualdade entre ambos, o destinatário terá a certeza de que a assinatura digital é válida e foi gerada pela chave privada correspondente a chave pública certificada, utilizada por ele na operação de verificação. Como resultado, terá assegurada a autenticidade e integridade da mensagem*". Ainda segundo Guelfi [6] (p. 71), "*ao se analisar a validade legal e técnica de um certificado digital, no momento de verificação da assinatura digital, o destinatário deverá observar algumas regras. A primeira delas diz respeito à finalidade sobre a qual o par de chaves foi gerado. A presente informação pode ser obtida no próprio certificado, na extensão Digital Signature, especificado no campo Key usage do certificado. A segunda regra corresponde à verificação do prazo de validade do certificado, ou seja, verificar se o certificado não esteja revogado. A revogação poderá ocorrer tanto pelo decurso do prazo de validade do certificado, como por expressa vontade de seu proprietário. Por fim, verificar se as normas técnicas referentes à emissão e distribuição de certificados digitais pelas Autoridades Certificadores foram obedecidas*". A seguir, a Fig. 3 ilustra o processo onde é feito a comparação do documento, por meio da leitura da assinatura digital pelo destinatário. É importante ressaltar que a semelhança existente entre a assinatura digital e a assinatura manuscrita reside no fato de conferir a autoria de um documento. Conforme o ITI [5], as assinaturas manuscritas seguem um padrão, sendo semelhantes entre si e possuindo características pessoais e biométricas de cada indivíduo. Ainda sob o mesmo pensamento do ITI [5], a assinatura digital é composta pela representação eletrônica de dados, ou seja, por uma seqüência de bits (0s e 1s), que necessitam de um computador para a sua visualização e conferência, sendo que na assinatura digital é gerada uma assinatura diferente para cada documento, uma vez que está relacionada ao resumo do documento.

3.6. Função *Hash*

De acordo com o ITI [5], função *hash* é "uma transformação matemática que faz o mapeamento de uma seqüência de bits de tamanho arbitrário para uma seqüência de bits de tamanho fixo menor – conhecido como resultado *hash* ou resumo criptográfico – de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado *hash* (resistência à colisão) e que o processo reverso também não seja realizável (dado um resultado *hash*, não é possível recuperar a mensagem que o gerou)". O resultado *hash* é "um valor calculado a partir de um documento eletrônico com a ajuda de uma função *hash*". Segundo Guelfi [6] (p. 101),

“são características de código *hash* viável: a) resistência à primeira inversão, onde dado o bloco de *hash* é computacionalmente improvável a obtenção da mensagem original; b) resistência à segunda inversão, sendo computacionalmente improvável que se encontre uma outra mensagem que utilizando-se da mesma função de *hash* encontra o mesmo bloco; e c) resistência a colisões, sendo improvável que duas mensagens distintas gerem o mesmo resumo”. A criptografia é o resultado retornado por uma função de *hash*, sendo comparado a uma impressão digital, pois cada documento possui um valor único de resumo e até mesmo uma pequena alteração no documento, como a inserção de um espaço em branco, resulta em um resumo completamente diferente, podendo tornar a autenticidade inválida. O NIST [8] “especifica cinco algoritmos de *hash* que podem ser usados para gerar resumos das mensagens. Os resumos são usados para detectar se as mensagens foram alteradas desde que os resumos foram gerados”. Conforme Guelfi [6] (p. 102), a mesma equipe chinesa liderada por Xiaoyun e Hongbo [9], “responsável pela primeira quebra do MD5, desenvolveu novas técnicas capazes de encontrar colisões na função de *hash* SHA-1. (...) Sua resistência foi reduzida de 2^{80} para ^{253}. Com isso conseguiram reduzir o tempo de quebra do SHA-1 pela força bruta em 2000 vezes”. Segundo Guelfi [6] (pp. 55/56), “quando usamos a expressão, assinatura digital, para designar o elemento aposto aos documentos eletrônicos, subentendemos equivocadamente que este elemento assegura sua autoria. Em verdade, a verificação da autoria neste processo utiliza a chave pública do signatário. Vejamos, uma vez assegurado juridicamente o vínculo entre a chave pública e o signatário, por meio de um documento denominado certificado digital, o resultado positivo no processo de verificação de inalterabilidade do documento eletrônico com o uso desta chave pública certificada garante a autoria do documento eletrônico ao proprietário do certificado. Ocorrendo repúdio sobre a autoria de uma assinatura manuscrita, o exame grafotécnico é o meio empregado para o direito a fim de dirimi-la. Nos documentos eletrônicos, a impossibilidade de realização de exames grafotécnicos não inviabiliza sua utilidade pelo ordenamento jurídico brasileiro, uma vez que o exame grafotécnico poderá ser substituído por exames sobre a validade ou invalidade do certificado digital”.

3.7. ICP-Brasil

“A ICP-Brasil, conjunto de regras e procedimentos técnicos, é responsável pela atividade de certificação digital no Brasil. Possui como órgão administrativo a Autoridade Certificadora Raiz – AC-Raiz – que hoje é incorporada por uma Autarquia Federal (o ITI), considerada Pessoa Jurídica de Direito Público interno, e a emissão do certificado digital para o usuário final ocorre por meio de prévia habilitação conferida pelo ITI às Pessoas Jurídicas de Direito Público ou Privado – denominadas de Autoridades Certificadoras Subseqüentes (AC Sub) – e as Pessoas Jurídicas de Direito Público ou Privado denominadas de Autoridades de Registro – AR” [6] (p. 76). Guelfi [6] (p. 78) destaca que “os certificados digitais são de quatro tipos: A1; A2; A3; e A4, de acordo com o grau crescente de segurança disponibilizado. O certificado digital para assinatura tem por objetivo principal vincular o proprietário/signatário à chave pública assegurando a autenticidade aos documentos eletrônicos assinados digitalmente a partir da correspondente chave privada. A certificação digital, nesta órbita, é uma atividade ligada à força probante dos documentos eletrônicos. Para Guelfi [6] (p. 78), “(...) o objetivo imediato dos certificados digitais de aplicação em assinaturas (...) (a) vinculação do signatário à chave pública utilizada para conferir a assinatura digital (b) conferindo autenticidade aos documentos eletrônicos assinados

digitalmente. De acordo com Guelfi [6] (p. 80), “(...) o conceito de certificado digital de assinatura digital corresponde a um documento eletrônico assinado digitalmente por agente competente, que desempenha uma função de possibilitar asseverar a autoria de outros documentos eletrônicos assinados digitalmente por meio da vinculação entre o proprietário do certificado e sua respectiva chave pública (utilizada para conferir a regularidade da assinatura digital), identificando e individualizando este mesmo proprietário diante dos seus pares no mundo eletrônico. De acordo com o ITI [5], “para validar uma assinatura digital ICP-Brasil, realizada sobre um documento eletrônico (...), é necessário assegurar-se que: a) o estado criptográfico da assinatura digital seja válido, o que envolve: i. autenticação e/ou autoria: pela decifração da assinatura digital gerada sobre o conteúdo digital utilizando a chave criptográfica assimétrica pública contida no certificado digital do signatário; ii. integridade: por comparação de resultados *hash*, mostrando que o conteúdo digital não foi alterado desde que sua assinatura digital foi criada pelo signatário. b) o certificado digital correspondente à chave privada utilizada para geração da assinatura seja válido, o que envolve a verificação de: i. observância aos requisitos definidos (...); ii. validade da assinatura digital da entidade que emitiu o certificado do signatário”. O parágrafo único, do artigo 154, da Lei nº. 5.869, de 11/01/1973 (Código de Processo Civil), dispõe que: “os tribunais, no âmbito da respectiva jurisdição, poderão disciplinar a prática e a comunicação oficial dos atos processuais por meios eletrônicos, atendidos os requisitos de autenticidade, integridade, validade jurídica e interoperabilidade da Infra-Estrutura de Chaves Públicas Brasileira – ICP – Brasil” (incluído pela Lei nº. 11.280, de 16/02/2006). O parágrafo segundo, do referido artigo, dispõe que: “todos os atos e termos do processo podem ser produzidos, transmitidos, armazenados e assinados por meio eletrônico, na forma da lei” (incluído pela Lei n. 11.419, de 19/12/2006). Segundo Guelfi [6] (p. 95), “(...) o Poder Judiciário, através da contratação de uma Autoridade Certificadora Subseqüente, emite um certificado para cada um de seus membros, a fim de exercer suas funções nos atos eletrônicos. Vale ressaltar que o exercício do poder de conferir autenticidade é feito pelo Poder Judiciário através de uma Autoridade Certificadora Subseqüente e não diretamente pela Autoridade Certificadora Subseqüente. Entretanto, esta redução não representa atualmente um perigo em potencial, a ponto de ser afastado o uso do SHA-1, mas demonstra que o SHA-1 é vulnerável, tendo seu tempo de vida útil reduzido. Guelfi [6] (p. 104) adverte que, “com a natural evolução científica, a segurança técnica oferecida pelos algoritmos criptográficos de função *hash* não é duradoura, aniquilando assim a idéia de perpétua confiança dos documentos eletrônicos assinados digitalmente”. Segundo Guelfi [6] (p. 106), “ao estudarmos os aspectos dos problemas enfrentados pelos algoritmos criptográficos de função *hash* na geração das assinaturas digitais verificamos que não há segurança técnica perpétua. Esta condição desencadeia uma relação de limite de tempo para a força probante dos documentos eletrônicos. Todavia, este período não condiz com o período de vida útil do documento, uma vez que, (...) os documentos são criados para assegurar valor perpétuo às informações nele contidas”.

4. METODOLOGIA

Segundo Yin [10] (p. 8), “*o estudo de caso é preferido para examinar eventos contemporâneos, mas quando os comportamentos relevantes não podem ser manipulados*”. Por sua vez, de acordo com Tachizawa [11], os estudos de múltiplos casos podem ser adotados quando a pesquisa envolve a comparação entre as

organizações selecionadas, objeto da análise de dados desta pesquisa. Assim, a metodologia utilizada nesta pesquisa baseia-se no modelo proposto por Tachizawa [11] e no modelo metodológico de estudos de múltiplos casos proposto por Yin [10], o que permitiu estudar um fenômeno contemporâneo, como é o caso do impacto da revogação do certificado digital na validade dos documentos eletrônicos, por meio dos quais os atos judiciais são praticados, considerando a adoção da assinatura digital no processo judicial eletrônico [11, 12, 10]. Embora a generalização dos resultados não possa ser realizada devido à natureza da amostra não ser probabilística, o modelo da pesquisa permitiu obter resultados que têm validade no contexto da amostra selecionada e que podem ser comparados com pesquisas anteriores sobre o tema. Com base no que foi discutido anteriormente e para obter os dados para este estudo, foi selecionada uma amostra de caráter intencional – por julgamento ou não-probabilística – por ser possível identificar elementos definidos da população [13], formada pelo Tribunal de Justiça de São Paulo (TJSP), órgão do Poder Judiciário (artigo 92, da Constituição Federal de 1988). Considerando os objetivos da presente pesquisa, a forma de coleta de dados adotada foi a de consultas a bancos de dados, documentação e pesquisas disponíveis [13]. A partir das consultas realizadas, foi estudado o impacto da revogação do certificado digital na validade dos documentos eletrônicos, por meio dos quais os atos judiciais são praticados, considerando a adoção da assinatura digital no processo judicial eletrônico. No tribunal estudado, a pesquisa examinou a implementação do processo eletrônico. O plano de pesquisa deste trabalho começa com o levantamento do processo de assinatura digital e, em seguida, trata, especificamente, do processo de certificado digital. Na seqüência, mapeia os problemas relacionados àqueles processos e, finalmente, analisa os impactos da revogação do certificado digital na perpetuidade dos documentos eletrônicos.

5. ANÁLISE DOS RESULTADOS.

Com base nas consultas realizadas pelos pesquisadores, foram analisados os impactos da revogação do certificado digital na validade dos documentos eletrônicos, por meio dos quais os atos judiciais são praticados, considerando a adoção da assinatura digital no processo judicial eletrônico. Nos juizados especiais cíveis, a petição inicial e os documentos que a acompanham são inseridos no sistema de processo judicial eletrônico de quatro formas: petição em papel – digitalização; petição digital (arquivo eletrônico assinado digitalmente pela parte ou advogado) – cópia para o sistema; petição narrativa: o escrivão digita diretamente no sistema; via Internet – entrada direta no sistema. A partir desse ponto é autuado um processo virtual que somente é impresso caso seja necessário o envio para a turma recursal. As demais peças processuais e respectivos documentos seguem as duas primeiras formas. De acordo com Arruda [15], citado por Freitas e Loebens [16], "*a principal vantagem do processo virtual não reside na digitalização de documentos exógenos, como petições ou provas, mas sim na manutenção dos documentos endógenos, como o termo de audiência, o acordo ou a sentença (...) Obtém-se uma solução de baixo custo, de rápida implantação e aceitação*". A sentença é gerada digitalmente e assinada com um certificado emitido dentro da estrutura da ICP-Brasil. Proferida a decisão, que é registrada no sistema, a sentença é assinada digitalmente na própria audiência. No momento da publicação, qualquer interessado tem acesso imediato, via Internet, ao inteiro teor da sentença. O sistema tem tido plena aceitação por parte de magistrados, servidores, advogados e partes. Todavia, uma das diferenças entre a assinatura em papel e a assinatura digital reside no fato de que o certificado

digital pode ser revogado [16]. A revogação do certificado digital pode ocorrer por conta do usuário, quando “a chave é comprometida” ou “alguma informação do certificado é alterada”, ou por conta de alteração no processo de assinatura [16]. Bernal [16] aponta que, em função da revogação do certificado digital, seu uso é permitido até o instante de sua revogação (período de uso válido do certificado), independentemente do período de validade do certificado.

Desse modo, se a data da assinatura encontra-se dentro do período de uso permitido, a assinatura é considerada válida. Se a data da assinatura encontra-se dentro do período de validade do certificado, mas fora do período de uso permitido, a assinatura é considerada inválida. Entretanto, Bernal [16] apresenta o seguinte problema (Fig. 4): um usuário (magistrado, servidor, advogado ou mesmo uma das partes) pode ser forçado a entregar o *smartcard* e a informar a senha de proteção.

Ainda que, de imediato, esse usuário solicite a revogação do certificado, um atacante poderia assinar um documento informando um instante de assinatura anterior à data de revogação.

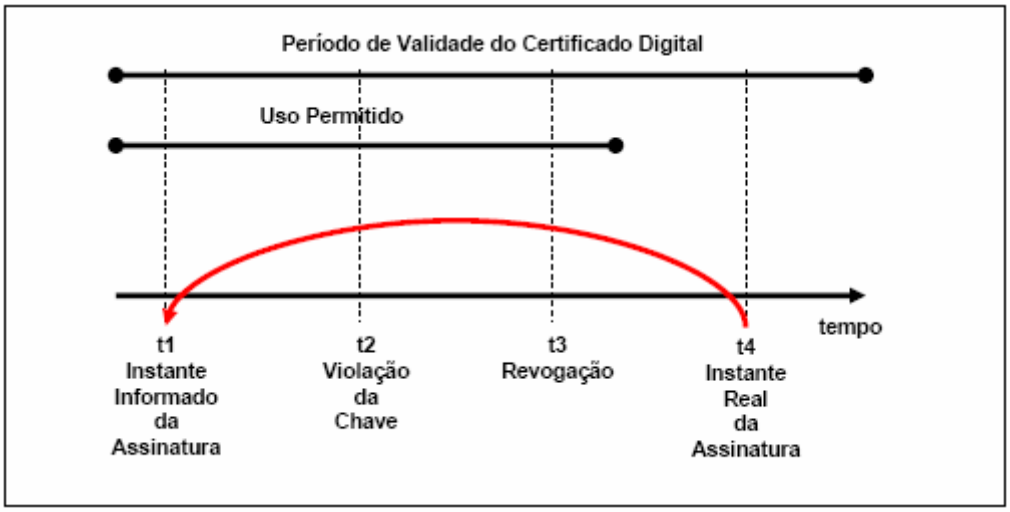

Figura 1: Exemplo de problema.
Fonte: BERNAL [16].

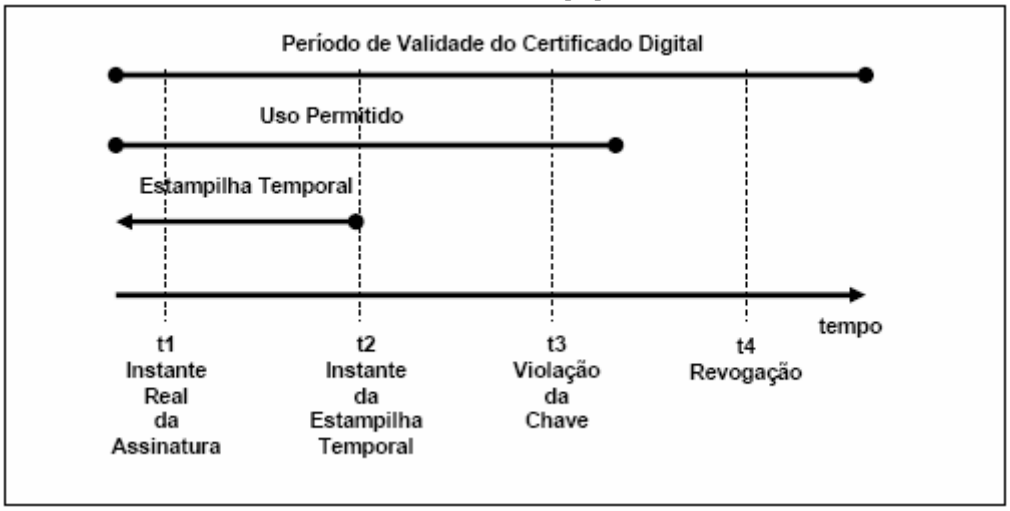

Figura 2: Exemplo de assinatura válida.
Fonte: BERNAL [16].

Para que isso não ocorra, torna-se necessária a “*existência de alguma informação garantindo que a assinatura foi realizada antes da data da revogação*” [16]. A solução apontada por Bernal [16] é a estampilha temporal (Time Stamp Token). Como se pode verificar na Fig. 5, o objetivo da Time Stamp Token é “provar

que a assinatura realmente existiu antes de um determinado momento" [16]. A estampilha temporal contém o *hash* da assinatura do usuário, a data e a assinatura destas informações por um terceiro confiável. A estampilha temporal é acrescentada ao documento assinado como um atributo não assinado (Fig. 6).

Outro problema que se aponta é a perpetuidade dos documentos eletrônicos, por meio dos quais os atos judiciais são praticados (Fig. 7). Nesse aspecto, cabe lembrar que, "de acordo com as recentes pesquisas apresentadas, cientistas chineses afirmam que a força do SHA-1 foi inicialmente fragilizada" ´[6] (p. 103).

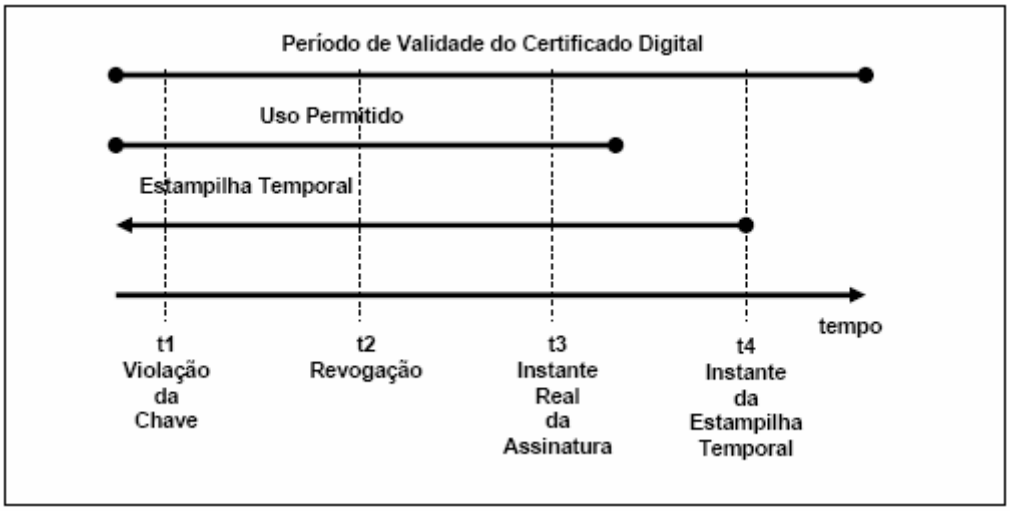

Figura 3: Exemplo de assinatura inválida.
Fonte: BERNAL [16].

6. CONCLUSÃO

Como se pode verificar na literatura recente, um dos problemas que se apresentam em relação à adoção dos certificados digitais envolve a validade do certificado, no momento da assinatura digital. Os métodos e técnicas forenses permitem investigar a ocorrência de eventual ato ilícito praticado por meio da assinatura digital de documentos eletrônicos, quando o certificado digital já se encontra revogado. Considerando a dependência cada vez maior dos tribunais dos sistemas de informação, a garantia da autenticidade, integridade e confiabilidade dos documentos eletrônicos por meio dos quais os atos judiciais são praticados é relevante para a adoção do processo judicial eletrônico no tribunal estudado, contribuindo para a celeridade e efetividade na entrega da prestação jurisdicional e para a eficiência das atividades administrativas. A pesquisa exploratória procurou analisar os impactos da revogação dos certificados digitais na validade dos documentos eletrônicos, por meio dos quais os atos judiciais são praticados, considerando a adoção de assinatura digital no processo judicial eletrônico. O objetivo dessa pesquisa foi atingido durante seu desenvolvimento, com base nas consultas realizadas.

7. REFERÊNCIAS BIBLIOGRÁFICAS

[1] MARTINEZ, Ramses Henrique. A gestão de conhecimento e a informatização do processo judicial: um estudo do impacto dos fatores contextuais do poder judiciário brasileiro na aprendizagem e seus reflexos nos processos de inovação, 2009.

[2] MARTINEZ, Ramses Henrique. Ciência forense aplicada à tecnologia da informação: adoção de técnicas forenses pelos ciclos de vida de desenvolvimento de sistemas de informação, 2009.

[3] KENT, Karen; CHEVALIER, Suzanne; GRANCE, Tim; DANG, Hung. *Guide to integrating forensic techniques into incident response:* recommendations of the National Institute of Standards and Technology. Special Publication 800-86. Gaithersburg, MD: NIST, 2006.
[4] BERNAL, Volnys Borges. *Assinatura de documentos em papel*. 2009. Material de aula. EPUSP/Escola Politécnica da Universidade de São Paulo – Laboratório de Sistemas Integráveis, São Paulo.
[5] ITI. Instituto Nacional de Tecnologia da Informação. Padrões e algoritmos criptográficos da ICP-Brasil. DOC ICP-01.01. Versão 2.0. Disponível em http://www.iti.gov.br/twiki/bin/view/Certificacao/DocIcp. Acesso em 03 set. 2009.
[6] GUELFI, Airton Roberto. *Análise de elementos jurídico-tecnológicos que compõem a assinatura digital certificada digitalmente pela infra-estrutura de chaves públicas do Brasil – ICP-Brasil*. 2007. 135p. Dissertação (Mestrado) – EPUSP/Escola Politécnica da Universidade de São Paulo, São Paulo.
[7] MARCACINI, Augusto Tavares Rosa. Certificação eletrônica, sem mitos e sem mistérios. *Revista do Advogado*, São Paulo, n. 69, p. 111, Maio 2003.
[8] NIST. Nacional Institute of Standard and Technology. Information Technology Laboratory. *FIPS PUB 180-3*. Federal Information Processing Standards Publication. Secure *Hash* Standard (SHS). Gaithersburg, October 2008. Disponível em http://csrc.nist.gov/publications/PubsFIPS.html. Acesso em 03 set. 2009.
[9] XIAOYUN, Wang. HONGBO, Yu. How to break MD5 and other *hash* functions. Shandong University, Jinan 250100, China, *apud* GUELFI, Airton Roberto. *Análise de elementos jurídico-tecnológicos que compõem a assinatura digital certificada digitalmente pela infra-estrutura de chaves públicas do Brasil – ICP-Brasil*. 2007. 135p. Dissertação (Mestrado) – EPUSP/Escola Politécnica da Universidade de São Paulo, São Paulo.
[10] YIN, Robert K. *Case study research:* design and methods. 2ª. Ed. Thousand Oaks: Sage Publications, Inc., 1994.
[11] TACHIZAWA, T. *Metodologia da pesquisa aplicada à administração*: a internet como instrumento de pesquisa. Rio de Janeiro: Pontal, 2002.
[12] LAVILLE, Christian, DIONNE Jean. *A construção do saber*: manual de metodologia da pesquisa em ciências humanas. Porto Alegre: Artes Médicas Sul, 1999.
[13] LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Metodologia Cientifica*. 3ª. Ed. São Paulo: Atlas, 2000.
[14] ARRUDA, Eduardo Henrique Pereira de. Acórdãos eletrônicos. Palestra proferida no Seminário de Direito & Tecnologia da Informação, em agosto de 2004. Caxias do Sul, RS. *Anais*. Caxias do Sul, RS: 2004, *apud* FREITAS, Vinicius Pimentel de; LOEBENS, João Carlos. Contratos eletrônicos e o comércio internacional – uma proposta. Ponencia VIII Seminário Internacional de la Federación Internacional de antiguos alumnos del I.N.A.P. de Espana, em agosto de 2004. Toledo. Anais. Toledo: 2004
[15] FREITAS, Vinicius Pimentel de; LOEBENS, João Carlos. Contratos eletrônicos e o comércio internacional – uma proposta. Ponencia VIII Seminário Internacional de la Federación Internacional de antiguos alumnos del I.N.A.P. de España. Toledo, agosto de 2004.
[16] BERNAL, Volnys Borges. *Assinatura eletrônica de documentos*. 2009. Material de aula. EPUSP/Escola Politécnica da Universidade de São Paulo – Laboratório de Sistemas Integráveis, São Paulo.