A PETIÇÃO ELETRÔNICA: CO-ASSINATURA DIGITAL E A IMPORTÂNCIA DE REQUISITOS TEMPORAIS

Mário Furlaneto Neto[1]
Fábio Dacêncio Pereira [2]
Leandro Yukio Mano Alves [3]
Bianca Nascimento[4]

Resumo

Os sistemas e-DOC, e-STJ e Pet v2, em uso nos tribunais superiores não permitem a co-assinatura digital na petição eletrônica. Neste contexto, os tribunais superiores, nomeadamente o STJ, vêm proferindo decisões que visam enfrentar a lacuna do

[1] Delegado de Polícia. Doutor em Ciência da Informação pela UNESP. Professor da graduação e Mestrado em Direito do Centro Universitário Eurípides de Marília (UNIVEM) e Coordenador do Núcleo de Estudos e Pesquisas em Direito e Internet (NEPI). E-mail: mariofur@univem.edu.br.

[2] Doutor em Engenharia Elétrica pela Escola Politécnica da USP. Professor e coordenador adjunto do bacharelado em Ciência da Computação do UNIVEM. Líder do grupo de pesquisa em sistemas computacionais aplicados (SCA/COMPSI) e coordenador do Núcleo de Apoio à Extensão do UNIVEM (NAPEx). E-mail: prof.fabiopereira@gmail.com.

[3] Graduando em Ciência da Computação do Centro Universitário Eurípides de Marília (UNIVEM) e membro do grupo de pesquisa em sistemas computacionais aplicados (SCA/COMPSI). E-mail: leandroyukiomano@gmail.com.

[4] Graduanda em Direito do Centro Universitário Eurípides de Marília (UNIVEM) e membro do Núcleo de Estudos e Pesquisas em Direito e Internet (NEPI). E-mail: biancahnascimento@hotmail.com.

sistema, o que contraria o critério do não-repúdio. Assim, por meio de uma revisão bibliográfica, legislativa e jurisprudencial, propõe-se um estudo de caso com o software assinador digital ICP-Brasil, bem como o carimbador de tempo enquanto ferramenta indispensável para minimizar fraude no emprego da certificação digital.
Palavras-chave
Assinatura digital; carimbo de tempo; petição eletrônica; co-assinatura digital.

Abstract

The e-DOC, e-STJ e Pet v2 systems in use in the higher courts do not allow the co-signature petition in digital electronics. In this context, the higher courts, including the Supreme Court, delivering orders to come face gap system, which contradicts the criterion of non-repudiation. Thus, through a literature review, legislative and judicial, it proposes a case study with software signer digital ICP-Brazil, as well as time stamping indispensable tool to minimize fraud in the use of digital certification.
Keywords
Digital signature, time stamp; electronic petition; co-signature.

1 Introdução

Hodiernamente, com os avanços tecnológicos e a disseminação da Internet, o fluxo das comunicações eletrônicas passou a ser realidade em vários setores sociais, tais como comércio, sistema financeiro e governo eletrônico viabilizando, inclusive, a implementação do e-processo.
A Emenda Constitucional nº 45, de 08 de dezembro de 2004, ao estabelecer a redação do inciso LXXVIII, do artigo 5º, da CF

(BRASIL, 2013), estipulou a razoável duração do processo, com os recursos inerentes, enquanto princípio fundamental da pessoa humana. Nesta seara, o e-processo torna-se ferramenta indispensável para a concretização do princípio em tela, ao promover maior celeridade na tramitação dos atos processuais.

A Lei nº 11.419, de 19 de dezembro de 2006 (BRASIL, 2013a), regulamentou os parâmetros e critérios para a efetiva informatização do processo, possibilitando a viabilização do ato processual em formato eletrônico.

Enquanto meio eletrônico tem-se "qualquer forma de armazenamento ou tráfego de documentos e arquivos", ao passo que a tramitação eletrônica se "caracteriza por toda forma de comunicação à distância com a utilização de redes de comunicação, preferencialmente a rede mundial de computadores" (BRASIL, 2013a).

Assim como, no meio tradicional, as petições e decisões são assinadas por seus autores ou prolatores, a Lei de Informatização do Processo estipulou ser a assinatura eletrônica forma de identificação inequívoca do signatário, composta pela assinatura digital baseada em certificado digital emitido pela autoridade certificadora credenciada, nos termos da lei, complementada pelo cadastro do usuário junto ao Poder Judiciário exigindo, para tanto, identificação presencial do interessado perante o tribunal respectivo (BRASIL, 2013a). O objetivo de se exigir a identificação presencial perante o tribunal respectivo foi o de assegurar o sigilo, a identificação e a autenticidade de suas comunicações.

A lei em comento estabeleceu, ainda, que os sistemas a serem desenvolvidos pelos órgãos do Poder Judiciário deverão usar, preferencialmente, programas com código aberto, acessíveis ininterruptamente por meio da rede mundial de computadores, priorizando-se a sua padronização (BRASIL, 2013a).

A padronização dos sistemas dos diversos tribunais facilita o acesso, minimiza o tempo de conexão, indispensável para que o site funcione adequadamente mas, acima de tudo, maximiza a

publicidade do processo ao permitir o acesso de pessoas que não sejam parte do feito.

Os sistemas desenvolvidos pelos tribunais como, por exemplo, o e-DOC5 em uso pelos TRTs e TST, bem como o e-STJ e o Pet v2, em uso no STF, consideram os critérios estabelecidos pela Lei de Informatização do Processo conferindo validade jurídica ao documento eletrônico assinado e certificado digitalmente com base no sistema da ICP-Brasil.

A segunda versão do sistema e-DOC6, regulamentado pelo Instrução Normativa nº 30 do TST, permite o acesso pelas partes, advogados e peritos por meio de conta única vinculada ao CPF. Os documentos devem ser enviados em formato Portable Document Format (PDF) e o documento principal e anexos devem ser encaminhados em um único lote, com tamanho máximo de 2 megabytes. A nova versão permite a utilização de qualquer certificado digital do sistema ICP-Brasil, inclusive das cadeias de confiança V2 e V3, porém, roda apenas na plataforma Windows 7 ou XP, exige a instalação do Java na versão 6 ou superior, bem como demanda que o navegador seja Internet Explorer versa 8 ou superior, ou ainda o Google Chrome 15. Assim, o equipamento a ser utilizado pelo sujeito processual terá que atender aos requisitos mínimos admitidos pelo sistema, sob pena de não estabelecer a interconectividade.

De acordo com a Resolução STJ nº 1/2010, o acesso ao sistema e-STJ7 pode ser feito por usuários internos, cujo contexto se inserem os Ministros e serventuários do STJ devidamente autorizados, bem como por usuários externos, assim definidos os membros do Ministério Público Federal que atuam no STJ e os

---

5 Em 26 de fevereiro de 2013 foi oficialmente lançado o sistema de Processo Judicial Eletrônico da Justiça do Trabalho (PJe JT). O sistema funcionará em caráter experimental por 30 a 60 dias junto à 6ª Turma do TST e gabinetes e ela vinculadas e será implementado gradativamente em todo o judiciário trabalhista (PJE JT, 2013).

6 Informação disponível em: <http://www.tst.jus.br/web/guest/peticionamento-eletronico>. Acesso em: 26 fev. 2013.

7 Informação disponível em:<http://www.stj.jus.br/portal_stj/publicacao/engine.wsp?tmp.area=983>. Acesso em: 26 fev. 2013.

procuradores e representantes das partes que comprovam capacidade postulatória.

Assim como no sistema e-DOC v2, as petições devem ser enviadas em formato PDF, sendo que no sítio do STJ faz-se referência à extensão máxima de 5 megabytes por arquivo a ser anexado por petição, possibilitando-se que cada petição tenha no máximo cem anexos, o que totaliza uma petição com extensão de 100 megabytes.

Em termos de conectividade, o e-DOC v2 exige que o sistema operacional do usuário seja Windows NT ou superior, foi desenvolvido para ser utilizado em navegador Internet Explorer 6.0 ou superior e o Firefox 1.5 ou superior e demanda a instalação do Java na versão 1.5.0_08 ou superior.

Para a efetivação do peticionamento eletrônico, tanto no sistema e-DOC V2 quanto no sistema e-STJ, além da instalação de programa conversor de PDF, exige-se um programa responsável pela administração da certificação digital.

Enquanto requisitos de acesso, o sistema Pet v28, em uso no STF, exige que o usuário disponha de certificado de categoria A3, registrado em nome de pessoa física e vinculado à cadeia certificadora da ICP-Brasil, além de o equipamento informático ser dotado de sistema operacional Windows (XP, Vista ou Seven) ou OSX, com navegador Internet Explorer (versões 7, 8 e 9), Google Chrome ou Mozila Firefox 5. Para a conectividade ser estabelecida, exige-se que o equipamento informático seja dotado do Java 1.6, na versão 15 ou superior, e a instalação de programas gerador e leitor de PDF, bem como de assinador digital, além dos certificados da cadeia de certificação específicos do certificado utilizado.

Referido sistema somente admite que a petição e arquivos anexados ostentem no máximo 10 megabytes de extensão.

A análise dos requisitos de interoperabilidade dos sistemas revela exigências diferentes de níveis de certificados digitais, bem como

---

8 Informação disponível em:<http://www.stf.jus.br/portal/cms/verTexto.asp?servico=processoPeticao Eletronica>. Acesso em: 26 fev. 2013.

de sistemas operacionais, sendo que o Pet v2 é o único que permite acesso por meio do OSX.

Todos os sistemas de peticionamento eletrônico alhures aduzidos possibilitam que apenas uma pessoa assine digitalmente o documento. Como resolver a questão, diante da necessidade de uma petição eletrônica exigir a assinatura de mais de uma parte? Ademais, é possível haver fraude mediante a utilização de um certificado digital revogado para assinar uma petição eletrônica dentro dos sistemas de peticionamento eletrônico acima mencionados?

Diante da realidade da tecnologia da informação fornecer suporte para que os atos realizados no meio tradicional possam, também, ser realizados no meio ambiente eletrônico, tem-se por objetivo enfrentar a questão de como os tribunais superiores, nomeadamente o STJ, vêm se posicionando diante da hipótese de assinatura digital divergente daquele que efetivamente assinou a petição digitalizada, mormente em face dos critérios da garantia de confiabilidade, identificação, integridade e o não repúdio (DEVEGILI, 2001), assim como apontar eventual falha dos sistemas por conta da não adoção de uma autoridade certificadora de tempo, indispensável para verificar, em tempo real, a validade do certificado digital.

Assim, por meio de uma revisão bibliográfica, legislativa e jurisprudencial, buscar-se-á analisar o sistema de Infra-Estrutura de Chaves Públicas (ICP-Brasil), como alicerce para discutir criticamente os julgados dos tribunais superiores, em especial o STJ, e verificar se, efetivamente, a tecnologia da informação é capaz de resolver a questão da co-assinatura digital da petição eletrônica e a validade do certificado digital em tempo real.

Como estudo de caso apresenta-se um software que permite a co-assinatura digital seguindo o padrão estabelecido pela ICP-Brasil e destaca-se ainda a importância do requisito temporal para garantir o não repudio de transações realizadas nesse âmbito.

2 Estrutura da ICP-Brasil e critérios de validade jurídica do documento eletrônico

Preocupada com a questão da autenticidade e veracidade do documento eletrônico, a *United Nations Commission on International Trade Law* (UNCITRAL) sedimentou, no ano de 2001, o *Model Law on Eletronic Signatures* enquanto uma diretriz a ser seguida para a regulamentação de atos jurídicos, nomeadamente àqueles voltados às transações comerciais *on line*. Adotou o critério da neutralidade quanto às regras técnicas para estabelecer firmas eletrônicas, aprovando qualquer método ou técnica comprovadamente eficaz e segura (GUIMARÃES, NASCIMENTO e FURLANETO NETO, 2005).

Nesta época, vigorava no Brasil o Decreto nº 3.587, de 5 de setembro de 2000 (BRASIL, 2013b), que instituiu normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal (ICP-Gov) e estipulou a necessidade de uso da criptografia assimétrica para relacionar um certificado digital a um indivíduo ou a uma entidade enquanto ferramenta para garantir segurança na tramitação de documentos entre os órgãos do governo. O objetivo era viabilizar a oferta de serviços de sigilo, validade, autenticidade e integridade de dados, irrevogabilidade e irretratabilidade das transações eletrônicas e das aplicações de suporte que utilizam certificados digitais.

O referido decreto serviu de alicerce para instituição da Medida Provisória nº 2.200-2, de 24 de agosto de 2001 (BRASIL, 2013c), que estabeleceu o sistema de Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), com o objetivo de garantir autenticidade, integridade e validade jurídica de documentos eletrônicos. Ampliou-se, assim, o alcance e aplicação da certificação digital, agora não mais restrita ao âmbito da Administração Pública Federal. De acordo com Custódio (2001), a ICP-Brasil compreende um conjunto de técnicas, práticas e procedimentos com o objetivo de fornecer suporte à implementação e à operação de um sistema de certificação.

A Medida Provisória nº 2.200-2/2001 (BRASIL, 2013c) transformou o Instituto Nacional de Tecnologia da Informação (ITI) em autarquia federal e o vinculou ao Ministério da Ciência e Tecnologia, com a função de Autoridade Certificadora Raiz (AC-Raiz). O ITI passou a ser a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, tendo como função credenciar e fiscalizar as entidades integrantes da ICP-Brasil.

Diferentemente do sistema americano, pontuado pela autonomia das autoridades certificadoras, a ICP-Brasil possui uma estrutura hierárquica. Afora a AC-Raiz, a estrutura é composta pelas Autoridades Certificadoras (AC), entidades credenciadas a emitir certificados digitais vinculando pares criptográficos ao respectivo titular, com a incumbência de emitir, expedir, distribuir, revogar e gerenciar certificados, publicar listas de certificados revogados e outras informações pertinentes, além de manter registro de suas operações, bem como as Autoridades de Registro (AR), operacionalmente vinculadas a uma AC, com competência para identificar e cadastrar usuários presenciais, encaminhar solicitações de certificados às ACs e manter registros das operações eletrônicas

Quaisquer entidades públicas e as pessoas jurídicas de direito privado poderão ser credenciadas como AC e AR. Proíbe-se, no entanto, a AC certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, aprovados pelo Comitê Gestor da ICP-Brasil.

Os certificados podem ser destinados para assinaturas, cujo objetivo é confirmar a identidade em uma operação eletrônica, ou assinaturas e sigilo em diferentes níveis, que delimitam a segurança atribuída ao certificado e servem para cifrar documentos, base de dados e outras informações eletrônicas (FREITAS e LOEBENS, 2004).

O Decreto nº 3.996, de 31 de outubro de 2001 (BRASIL, 2013d), revogou expressamente o Decreto nº 3.587, de 5 de setembro de 2000 (BRASIL, 2013b), e passou a estipular que os serviços de

certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil. Modificado pelo Decreto nº 4.414, de 7 de outubro de 2002 (BRASIL, 2013e), estabeleceu que as aplicações e demais programas utilizados no âmbito da Administração Pública Federal direta e indireta que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitido por qualquer AC integrante da ICP-Brasil.

Assim, o sistema da ICP-Brasil emprega a criptografia assimétrica, composta por um par de chaves públicas e privadas. A chave privada, destinada para cifrar o documento e a pública para decifrar.

Para o documento servir como prova, há necessidade de que o pensamento humano esteja materializado em um suporte, em cujo contexto se insere o eletrônico, e que a manifestação do pensamento humano sirva para comprovar algo. Dentro deste contexto, a identificação da autoria do documento é um dos requisitos para conferir força probante ao documento. No âmbito eletrônico, Volpi (2001, p. 36) salienta que:

> Para a prevenção deste tipo de situação, surgiu a certificação digital. Seu funcionamento pode ser comparado a de um serviço notarial efetuado pelo tabelião. Fundamenta-se na existência de uma autoridade certificadora, responsável pela emissão do certificado digital, que possui registrado, em sua base de informações, a chave pública usada para decifrar a mensagem - criptoanálise do emissor do documento. Por meio de mecanismos próprios, a autoridade certificadora pode identificar como original o documento do emissor e, a partir desta comprovação, certificar, com uma assinatura digital própria, a autenticidade do documento eletrônico.

O documento eletrônico, com sua assinatura digital e seu respectivo certificado digital, é empregado por apresentar segurança ao poder judiciário, devido ao seu alto grau de complexidade, nomeadamente em relação à criptografia assimétrica, garantindo assim a autoria e integridade do documento. A assinatura digital é o mecanismo de autenticação que permite ao criador de uma mensagem anexar um código que atue como uma assinatura (STALLINGS, 2008). Esse tipo de assinatura possui o mesmo valor de uma assinatura manuscrita, portanto somente as assinaturas digitais realizadas com certificados emitidos por autoridades credenciadas na ICP-Brasil tem validade jurídica reconhecida.

Apesar do tratamento análogo com a assinatura manuscrita, a assinatura digital é elaborada e validada por sistemas computacionais em que se utilizam técnicas matemáticas e algoritmos criptográficos, e sua integração com outras soluções tecnológicas, como o certificado digital, permite não só a garantia de autenticidade, mas a integridade e o não repúdio sobre um documento digital.

Para a garantia da eficácia da assinatura digital e de sua certificação, dois aspectos merecem ser observados: a segurança das informações que individualizam cada indivíduo e a segurança da chave privada de cada certificado. Embora ambos os elementos sejam essenciais para a segurança da assinatura digital, o sujeito passivo se distingue da obrigação da segurança das informações.

Quanto à segurança das informações individuais, a responsabilidade compete ao Poder Público, através da ICP-Brasil, mas a segurança da guarda da chave privada compete exclusivamente ao proprietário do certificado digital. Essa distinção é importante, pois aponta o possível responsável pela reparação de danos causados a outrem provenientes de fraudes na utilização do certificado digital emitido pela ICP-Brasil. Ressalta-se que o documento eletrônico é passível de fraude assim como o documento tradicional. No entanto, o que se pretende com a

assinatura digital é minimizar a possibilidade de fraude e identificá-la quando ocorrer, o que se traduz em maior segurança jurídica.
Segundo Devegili (2001), o emprego da criptografia no sistema da ICP-Brasil, possibilita obter:

a) confiabilidade: a mensagem cifrada transmitida entre as partes não pode ser obtida por terceiros estranhos à relação;
b) identificação: possibilita a identidade dos autores do documento;
c) integridade: garante a originalidade da mensagem e permite a detecção de alterações;
d) Não-repúdio: caracteriza-se pela impossibilidade do remetente da mensagem negar o seu envio, quando do recebimento pelo destinatário.
Ocorre que, atualmente, os sistemas de peticionamento eletrônico permitem apenas a uma pessoa assiná-lo. Necessário enfrentar como os tribunais superiores, nomeadamente o STJ, vem se manifestando diante da questão da assinatura digital na petição eletrônica.

3 A validade da assinatura digital na visão dos tribunais superiores

Na prática forense, invariavelmente, as petições elaboradas no suporte papel são assinadas por mais de um advogado. A questão que se impõe se concentra na possibilidade da petição eletrônica ser assinada, concomitantemente ou em momentos diferentes, por mais de uma pessoa como, por exemplo, na proposição de homologação de acordo elaborado pelas partes. Neste aspecto, os sistemas e-DOC, e-STJ e Pet v2 não atendem às necessidades hodiernas, ao permitirem que o documento eletrônico seja assinado digitalmente apenas por uma única pessoa. Assim, no exemplo citado, um advogado assina digitalmente a petição eletrônica, enquanto o outro se dirige pessoalmente ao cartório da

respectiva Vara para assiná-la presencialmente. Tal situação contraria a finalidade dos sistemas.

Questões pertinentes à assinatura digital já foram objeto de discussão junto aos tribunais superiores. Recentemente, o Ministro Luiz Fux, da 1ª Turma do STF, proferiu decisão em sede de embargos de declaração em agravo regimental no RE 470885/RS, em que frisou ser a "assinatura digital equivalente à manuscrita, por isso que o equívoco no sentido de que a petição do agravo regimental restada apócrifa quando dela constava assinatura eletrônica deve ser corrigido" (BRASIL, 2012).

Por outro lado, o Ministro Og Fernandes, da 6º Turma do STJ, ao prolatar decisão em Embargos de Declaração em face de decisão proferida em sede de Agravo Regimental no Resp. 597304/RS, onde se enfrentou, dentre de outros temas, a ausência de identidade entre os advogados indicados na petição e o titular da assinatura digital, salientou que, na "instância especial, não há oportunidade para aplicação das diligências previstas nos arts. 13 e 37 do CPC, conforme a Súmula 115/STJ, que assim se orienta: "Na instância especial é inexistente recurso interposto por advogado sem procuração nos autos" (BRASIL, 2013h). No mesmo sentido já havia sido a decisão proferida nos autos do AREsp 21761 / SP (BRASIL, 2013i), consoante segue:

> Processo: AgRg no AREsp 21761/SP. AGRAVO REGIMENTAL NO AGRAVO EM RECURSO ESPECIAL 2011/0106649-7. Relator: Ministro Ricardo Villas Bôas Cueva. Órgão julgador: Terceira Turma. Data do julgamento: 27/11/2012. Data da publicação/Fonte: Dje 06/12/2012. Ementa:1. **Não havendo identidade entre o titular do certificado digital utilizado para assinar o documento e o nome do advogado indicado como subscritor da petição, deve a peça ser tida como inexistente, haja vista o descumprimento do disposto nos arts. 1º, § 2º, inciso III, e 18 da Lei nº 11.419/2006 e nos arts. 18, § 1º, e 21, inciso I, da Resolução STJ nº 1, de 10 de fevereiro de 2010.** 2. Agravo

> regimental não conhecido. Acórdão: Vistos e relatados estes autos, em que são partes as acima indicadas, decide a Terceira Turma, por unanimidade, não conhecer do agravo regimental, nos termos do voto do(a) Sr(a) Ministro(a) Relator(a). Os Srs. Ministros Nancy Andrighi, Sidnei Beneti e Paulo de Tarso Sanseverino (Presidente) votaram com o Sr. Ministro Relator. (grifo nosso)

Em decisão proferida nos autos dos Embargos de Declaração no Agravo Regimental no Agravo 1234470/SP (BRASIL, 2013j), o Ministro Paulo de Tarso Sanseverino, da 3ª Turma do STJ, assim se pronunciou:

> O acesso ao serviço de recebimento de petições eletrônicas depende da utilização, pelo credenciado, da sua identidade digital, pessoal e de uso exclusivo (Resolução n. 01/2010 da Presidência do STJ). Desnecessidade, no entanto, do advogado que assina digitalmente a petição eletrônica nela fazer grafar o seu nome, bastando que possua procuração judicial para atuar no feito.

Por sua vez, contrariando a tese de que a identidade digital é pessoal e de uso exclusivo, a 2ª Turma do STJ considerou válida a assinatura digital de advogado de pessoa jurídica de direito público, não titular do certificado digital, consoante segue:

> PROCESSO AgRg no REsp 1303294/ES. AGRAVO REGIMENTAL NO RECURSO ESPECIAL 2012/0007424-5. Relator Ministro HUMBERTO MARTINS (1130). Órgão Julgador: T2 – Segunda Turma. Data do julgamento: 29/05/2012. Dje 01/06/2012. RMDCPC vol. 48, p. 104. Ementa: PROCESSUAL CIVIL. AGRAVO REGIMENTAL. PETIÇÃO ENVIADA ELETRONICAMENTE. IDENTIDADE DO SUBSCRITOR DA PETIÇÃO NÃO CORRESPONDENTE COM O TITULAR DO

CERTIFICADO DIGITAL. ADVOGADO PÚBLICO. REPRESENTAÇÃO EX LEGE. POSSIBILIDADE. SERVIDOR PÚBLICO MUNICIPAL. LEI LOCAL. SÚMULA 280/STF. 1. Nos termos do que dispõem os arts. 1º, § 2º, III, "a" e "b"; e 2º, caput, da Lei n. 11.419, de 2006, a assinatura eletrônica destina-se à identificação inequívoca do signatário do documento digital, ou seja, aquele devidamente credenciado como usuário autorizado para envio de petições em geral, mediante o uso de meios eletrônicos. 2. **É possível o conhecimento de petição eletrônica encaminhada por advogado representante *ex lege* de pessoa jurídica de direito público ou no caso de advogado privado, cujo nome conste da procuração ou de instrumento de substabelecimento, ainda que haja divergência entre o advogado que consta como subscritor da peça processual e aquele que a encaminhou a peça por meio eletrônico.** 3. O dispositivo da legislação federal supostamente violado não foi debatido na instância ordinária, de forma a possibilitar o conhecimento do apelo nobre. Registre-se que o mero fato de o Tribunal de origem ter feito referência ao dispositivo supostamente violado não significa que houve o debate apto a viabilizar o conhecimento do recurso especial. O prequestionamento somente estará caracterizado quando o tribunal manifestar-se expressamente sobre a incidência ou não ao caso concreto de determinado dispositivo legal, expondo as razões pelas quais a aludida norma deve ou não ser aplicada à questão que lhe foi posta, o que não ocorreu no caso vertente, incidindo, portanto a Súmula 282 do STF. Agravo regimental improvido. Acórdão: Vistos, relatados e discutidos os autos em que são partes as acima indicadas, acordam os Ministros da Segunda Turma do Superior Tribunal de Justiça: "A Turma, por unanimidade, negou provimento ao agravo regimental, nos termos do voto do Sr. Ministro-Relator, sem destaque e em bloco." Os Srs. Ministros Herman Benjamin (Presidente), Mauro

> Campbell Marques, Cesar Asfor Rocha e Castro Meira votaram com o Sr. Ministro Relator. (BRASIL, 2013g) (grifo nosso)

Ao admitir que o advogado público possa fazer uso da assinatura digital de outrem para fins de peticionamento eletrônico, o STJ relativiza o critério do não-repúdio apontado por Devegili (2001) e afeta toda a lógica de segurança do sistema da ICP-Brasil, já que o par de chaves deve ser pessoal e intransferível. Isto, logicamente, vai possibilitar que o titular da chave possa fornecê-la à outrem para fins de uso, o que, poderá gerar abusos e ausência de segurança jurídica.

A solução pode estar na adoção de um sistema de co-assinatura digital, a ser enfrentada a seguir.

4 Processo de co-assinatura digital

O processo de geração das assinaturas digitais no ICP-Brasil prevê três contextos distintos: assinaturas simples (quando uma única assinatura é gerada sobre o documento eletrônico), contra-assinaturas e co-assinaturas.

A geração de contra-assinaturas digitais ocorre quando uma ou mais assinaturas digitais são realizadas sobre uma seqüência de *bytes*, que representa uma assinatura digital já existente, ou seja, a assinatura de uma assinatura digital.

A geração de co-assinaturas digitais ocorre quando duas ou mais assinaturas digitais são geradas de forma independente pelos signatários utilizando conteúdos digitais idênticos. Cada co-assinatura ou contra-assinaturas geradas podem conter atributos próprios, assinados e não assinados.

Este procedimento é realizado acrescentando informações do novo assinante à estrutura do arquivo digital. Trata-se de um processo aceitável e homologado, pois não compromete a segurança tanto do documento em si como de outras assinaturas digitais contidas no documento. No entanto, resguarda a Instrução Normativa ITI Nº 9 DE 05/07/2012 que contra-assinaturas não

devem ser empregadas após a aposição de qualquer carimbo do tempo de arquivamento devido à interferência no processo de validação.

Existem três cenários propostos para realização da co-assinatura: a) co-assinatura digital síncrona; b) co-assinatura digital assíncrona e; co-assinatura digital em conjunto, possibilitando a assinatura de documentos eletrônicos por indivíduos distintos.

O modelo de co-assinatura digital síncrona estabelece uma política de ordem para a geração da assinatura do documento eletrônico, necessário em situações em que o documento somente pode ser assinado por um indivíduo após a verificação da assinatura anterior. Neste processo uma das partes realiza a assinatura digital do documento eletrônico, disponibilizando posteriormente o mesmo documento para que a próxima parte acrescente sua assinatura digital, verificando se a assinatura da parte anterior consta no documento.

No processo de co-assinatura digital assíncrona é preciso que todas as partes assinem o documento, desconsiderando a ordem de realização. Para tal processo pode-se adotar duas políticas: a) o documento original é assinado por uma das partes e disponibilizado para que qualquer outra realize a assinatura digital do mesmo, possibilitando que pessoas em localidades diferentes possam assinar o documento; b) o documento original é disponibilizado a todas as partes que após gerarem suas assinaturas disponibilizam este arquivo para que uma das partes faça a união de todas as assinaturas em um único documento eletrônico.

Por sua vez, no modelo de co-assinatura em conjunto é necessário que todas as partes estejam reunidas em um mesmo lugar e utilizar o mesmo microcomputador, cada um, munido do seu certificado digital para realizar a assinatura em conjunto. Apesar de o sistema ser mais simples e limitado, trata-se de um dos modelos mais usuais, aplicável na hipótese de uma petição ser assinada digitalmente por dois ou mais advogados em um mesmo escritório, situação cada vez mais comum em face das sociedades criadas para a formação de escritórios de advocacia.

Qualquer um dos modelos de co-assinaturas apresentados podem ser usados no âmbito jurídico, pois possibilita que a peça inicial da ação seja assinada digitalmente por dois advogados, assim como viabiliza a materialização de acordos firmados entre partes, independente de estarem fisicamente presentes no mesmo ambiente.

5 Modelo de software que permite co-assinaturas em documentos digitais

O Laboratório de Sistemas Integráveis Tecnológico - São Paulo/SP (LSI-TEC) juntamente com o Laboratório de Pesquisa em Computação e Sistemas de Informação (COMPSI/UNIVEM) desenvolveram o Assinador Digital ICP-Brasil que permite a realização da co-assinatura digital de documentos eletrônicos e a verificação das assinaturas e respectivos certificados presentes em um documento assinado digitalmente.
Para tanto, o *software* foi dividido em cinco módulos, que juntos compõem os serviços de assinatura que atendem aos requisitos da ICP-Brasil (DOC ICP-BRASIL, 2013), conforme demonstra a tabela 2.

Tabela 2- Descrição dos módulos do *software*, Assinador Digital ICP-Brasil, que permite a realização da co-assinatura digital de documentos eletrônicos e a verificação das assinaturas e respectivos certificados presentes em um documento assinado digitalmente.

Módulo	Descrição
Assinador	Responsável pelas operações criptográficas relacionadas à assinatura digital no padrão ICP-Brasil e geração do documento eletrônico assinado no formato CMS

Verificador	Realiza a verificação da cadeia de certificados utilizada na geração do documento assinado, lista de certificados revogados (LCR), validade sequencial e temporal das informações durante o processo de assinatura
Validador	Responsável pela análise/autenticação da assinatura digital de um documento assinado no padrão ICP-Brasil
Configurador	Responsável pelas configurações das opções e parâmetros utilizados pelo aplicativo Assinador Digital
Carimbador	Solicita carimbo de tempo a Autoridade Certificadora de Tempo(ACT) e verifica se atende ao padrão ICP-Brasil exigido

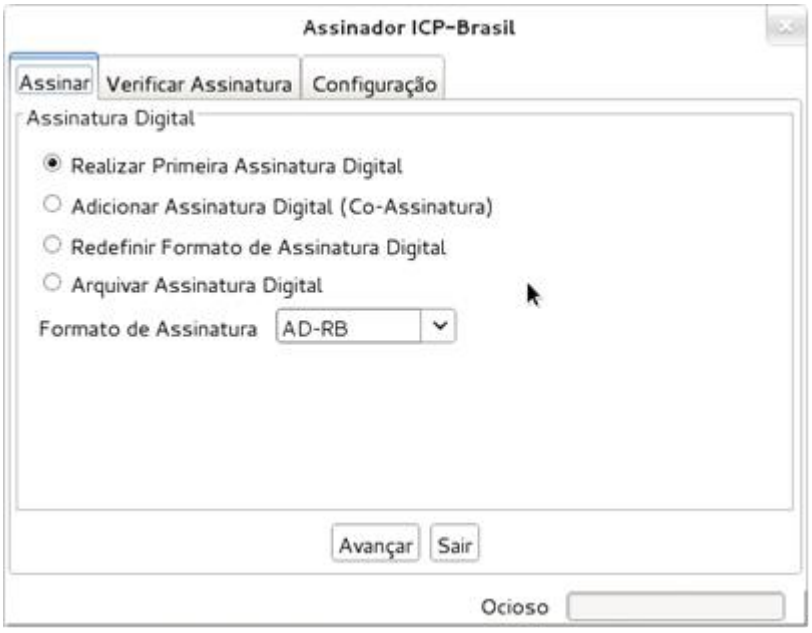

Figura 1- Demonstração da interface principal do Assinador ICP-Brasil.

O *software,* criado na linguagem de programação Java, utiliza bibliotecas criptográficas e *Application Programming Interface* (API) de desenvolvimento *Bouncy Castle* (2012). A *Bouncy Castle* consiste de uma coleção de bibliotecas de código aberto, usadas em processos criptográficos, sendo periodicamente atualizada e revisada por seus mantenedores.
Na figura 1 pode-se visualizar uma das janelas do *software* Assinador ICP-Brasil. Destaca-se a funcionalidade "Adicionar Assinatura Digital (Co-assinatura)" seguindo as normas estabelecidas pela ICP-Brasil.
O programa permite a realização da co-assinatura digital síncrona, assíncrona e em conjunto, de forma que quaisquer um dos processos de co-assinaturas propostos podem ser utilizados no âmbito jurídico, independentemente de as partes signitárias estarem ou não fisicamente presentes em um mesmo ambiente.

6 Importância de requisitos temporais

Em algumas transações de documentos eletrônicos assinados digitalmente, torna-se necessária a inclusão de informações sobre a data/hora em que o processo foi realizado. Neste contexto surgiu a importância de agregar o fator tempo aos documentos eletrônicos assinados.
As referências temporais são pontos chave nas operações relacionadas à assinatura digital. Existem três referências temporais: a) aquelas relacionadas ao instante da assinatura; b) aquelas relacionadas ao intervalo de validade do certificado digital e; c) aquelas relacionadas ao intervalo de validade de uso do certificado digital.

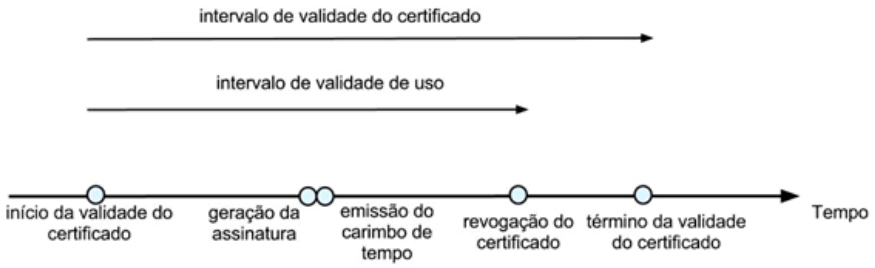

Figura 2- Referências temporais dos processos de assinaturas.
Fonte: DOC ICP-BRASIL, 2013.

Para tanto, alguns intervalos de tempo devem ser respeitados para o processo de validação da assinatura digital: a) o instante da realização do processo de assinatura digital necessita estar no período válido do certificado digital; b) a assinatura digital deverá ser realizada antes de uma possível data de revogação do certificado digital e; c) o instante de início de validação do certificado necessita ser menor do que o instante do término da validação do certificado, como ilustrado na figura 2.
Algumas referências temporais devem ser emitidas por fontes seguras como: a) início e término da validade do certificado digital (Autoridades Certificadoras); b) instante de revogação do certificado digital do signatário (Autoridades Certificadoras) e; c) instante de emissão do carimbo de tempo (Autoridades Certificadoras de Tempo)
Garantindo as fontes seguras de tempo citadas anteriormente, o instante da formalização da assinatura pode ser gerado por uma fonte não confiável como, por exemplo, a data/horário do microcomputador onde foi gerada a assinatura do documento eletrônico.
Diante deste contexto surgiu o conceito de carimbo de tempo, que é a forma segura e confiável de agregar e registrar a data e hora em transações de documentos eletrônicos, em especial os assinados

digitalmente, obtendo prova que tal documento assinado existia na data incluída no carimbo de tempo.

Em 19 de novembro de 2008, a ICP-Brasil aprovou as normas para implementação de Autoridades de Carimbo de Tempo (ACT), que permite determinar o horário da assinatura digital. O Carimbo de Tempo é uma assinatura digital de um terceiro confiável que garante que um documento existia em determinada data, desta forma é possível assinar documentos digitalmente anexando data e hora específica, garantida pelo Observatório Nacional, que é responsável pelo fornecimento da hora legal no Brasil, que possui infra-estrutura de segurança obedecendo aos mais altos padrões mundiais.

Apesar da utilização de carimbos de tempo ser facultativa no âmbito da ICP-Brasil, as referências temporais são elementos obrigatórios na geração de alguns formatos de assinaturas digitais. Somente a política de assinatura básica não faz uso de carimbos de tempo.

No dia 28 de janeiro de 2013 foi publicado no Diário Oficial da União o credenciamento da Caixa Econômica Federal (CEF) como a primeira Autoridade de Carimbo de Tempo da ICP-Brasil. Segundo Renato Martini (CAIXA, 2013), diretor-presidente do ITI, com o credenciamento da ACT CAIXA a AC-Raiz passa a operar suas instalações enquanto raiz do tempo da ICP-Brasil, tratando de mais um atributo de confiança em prol a adoção de documentos e processos eletrônicos. Inicialmente a ACT CAIXA somente emitiram carimbos de tempo aos processos de assinaturas digitais referentes às áreas de negócio internas da CEF que necessitam da comprovação temporal.

O uso de carimbo de tempo é uma realidade desde maio de 2007 no judiciário. O Supremo Tribunal Federal (STF) recebe e a tramita processos de forma totalmente eletrônica. Para atestar a data e o horário em que os processos chegam ao sistema, o Tribunal utiliza uma solução de carimbo do tempo O sistema de petição eletrônica, com certificação digital ICP-Brasil do STF, é utilizado inclusive para as petições iniciais (as que darão início a

uma ação judicial) e para todos os tipos de classes processuais e, também, os processos de suporte ainda em papel. Nessas petições são utilizados o carimbo do tempo para aferir com exatidão o horário desta transação eletrônica.

7 Conclusão

A análise dos sistemas e-DOC, e-STJ e Pet v2 permitiu concluir que estas ferramentas não possibilitam, no cenário atual, a co-assinatura da petição eletrônica.

Por conta disso, os tribunais superiores, nomeadamente o STJ, vêm proferindo decisões que visam disciplinar esta lacuna, admitindo que a assinatura eletrônica pode ser divergente do titular do certificado digital. No entanto, esta decisão contraria o critério do não-repúdio.

O estudo da infra-estrutura da ICP-Brasil revelou que não há objeção à adoção de *software* de especialidade que permita a co-assinatura digital, desde que obedeça os padrões e critérios de validade jurídica do documento eletrônico por ela estabelecidos.

Assim, a co-assinatura é uma funcionalidade prevista pela ICP-Brasil, tecnologicamente factível e em condições de ser implementada com segurança jurídica, com potencialidade de mitigar as dificuldades relacionadas à autenticidade da assinatura na petição eletrônica.

Em algumas operações eletrônicas assinadas digitalmente, especificamente na área jurídica, o uso de carimbo de tempo é uma forma confiável de agregar e registrar a data e o horário das transações de documentos eletrônicos. Como a lista de certificados digitais revogados não é atualizada em tempo real, a não adoção do carimbo de tempo possibilita que uma pessoa, eventualmente, assine digitalmente um documento eletrônico com um certificado vencido, o que pode gerar fraude.

A adoção da certificação do carimbo de tempo, portanto, permite obter prova que tal documento assinado existia, assim como o certificado digital nele empregado, na data incluída no carimbo de

tempo, maximizando a segurança jurídica no processo de certificação digital e tramitação da petição eletrônica.

Referências

BRASIL. Constituição da República Federativa do Brasil. Promulgado em 05 out. 1988. Disponível em: <http://www.senado.gov.br>. Acesso em 28 fev. 2013.

_____. Lei 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial; altera a lei 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Disponível em: <http://www.senado.gov.br>. Acesso em: 28 fev. 2013a.

_____. Decreto nº 3.587, de 5 de setembro de 2000. Estabelece norams para a infra-estrutura de chaves públicas do Poder Executivo Federal – ICP-Gov. E dá outras providências. Disponível em: <http://www.senado.gov.br/legislacao/>. Acesso em: 26 fev. 2013b.

_____. Media Provisória 2.200/2, de 24 de outubro de 2011. Institui a infra-estrutura de chaves públicas brasileira – ICP-Brasil, transforma o instituto nacional de tecnologia da informação em autarquia, e dá outras providências. Disponível em: <http://www.senado.gov.br/legislacao/>. Acesso em: 26 fev. 2013c.

_____. Decreto nº 3.996, de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da administração pública federal. Disponível em: <http://www.senado.gov.br>. Acesso em: 28 fev. 2013d.

_____. Decreto nº 4.414, de 7 de outubro de 2002. Altera o Decreto 3.996, de 31 de outubro de 2001, que dispõe sobre a prestação de serviços de certificação digital no âmbito da administração pública federal. Disponível em: <http://www.senado.gov.br>. Acesso em: 28 fev. 2013e.

_____. Supremo Tribunal Federal. Embargos de declaração no Agravo Regimental no Recurso Extraordinário 470885/RS. Relator: Luiz Fux. Brasília, 09 de dezembro de 2011. Disponível em: <http://www.stj.jus.br>. Acesso em: 28 fev. 2013f.

_____. Superior Tribunal de Justiça. Agravo Regimental no Recurso Extraordinário 1303294/ES. Relator: Humberto Martins. Brasília, 29 de maio de 2012. Disponível em: <http://www.stj.jus.br>. Acesso em: 28 fev. 2013g.

_____. Superior Tribunal de Justiça. Agravo Regimental no Recurso Especial 597304/RS. Relator: Og Fernandes. Brasília, 27 de setembro de 2011. Disponível em: <http://www.stj.jus.br>. Acesso em: 28 fev. 2013h.

_____. Superior Tribunal de Justiça. Agravo Regimental no Agravo em Recurso Especial 21761/SP. Relator: Ricardo Villas Bôas Cueva. Brasília, 79 de novembro de 2012. Disponível em: <http://www.stj.jus.br>. Acesso em: 28 fev. 2013i.

_____. Superior Tribunal de Justiça. Embargos de Declaração no Agravo Regimental nos Embargos de Declaração no Agravo Regimental no Agravo de Instrumento 1234470/SP. Relator: Paulo de Tarso Sanseverino. Brasília, 10 de abril de 2012. Disponível em: <http://www.stj.jus.br>. Acesso em: 28 fev. 2013j.

BOUNCY CASTLE API. The legion of the Bouncy Castle. 2012. Disponível em: <http:// bouncycastle.org>. Acesso em 15 dez. 2012.

CAIXA: primeira Autoridade Certitificadora do Tempo da ICP-Brasil. Disponível em:<http://www.iti.gov.br/noticias/boletim-digital/4171-boletim-digital-273>. Acesso em: 01 mar. 2013.

CUSTÓDIO, Ricardo Felipe. Análise crítica da ICP-Brasil: resposta a consulta pública. Florianópolis: Laboratório de Segurança da Computação/UFSC, 2001. 18p.

DEVEGILI, Augusto Jun. Farnel: uma proposta de protocolo criptográfico para votação digital. Dissertação (Mestrado em Ciência da Computação)-Faculdade de Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2001. Disponível em: <http://www.labsec.ufsc.br>. Acesso em: 20 dez. 2012.

DOC ICP-Brasil. Resoluções da ICP-Brasil em vigor. Disponível em: <http://www.iti.gov.br/legislacao>. Acesso em: 25 fev. 2013.

FREITAS, Vinicius Pimentel; LOEBENS, João Carlos. Contratos eletrônicos e o comércio internacional: uma proposta. 2004. Disponível em: <http://www.inap.map.es>. Acesso em: 30 nov. 2012.

GUIMARÃES, José Augusto Chaves; NASCIMENTO, Lúcia Maria Barbosa; FURLANETO NETO, Mário. Aspectos jurídicos e diplomáticos dos documentos eletrônicos. São Paulo: Associação de Arquivistas de São Paulo, 2005. 74p.

ICP-BRASIL, Instituto Nacional de Tecnologia da Informação (ITI). Estrutura da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Disponível em: < http://www.iti.gov.br/icp-brasil> 14 mar. 2013.

PJE-JT será instalado hoje no TST. Disponível em <http://www.tst.jus.br>. Acesso em 26 fev. 2013.

STALLINGS, Willian. Criptografia e segurança de redes. São Paulo: Pearson, 2008. 492p.

VOLPI, Marlon Marcelo. Assinatura digital - aspectos técnicos, práticos e legais. Rio de Janeiro: Axcel Books, 2001. 121p.