

A ASSINATURA DE ATOS PROCESSUAIS PRATICADOS EM MEIO ELETRÔNICO

Rodrigo Melo do Nascimento*

RESUMO

Com o advento do processo eletrônico, surgiu a necessidade da assinatura segura de atos processuais praticados eletronicamente. Para a garantia da integridade e da autenticidade dos atos processuais, a assinatura eletrônica deve ser realizada mediante a adoção de certificado digital vinculado à ICP-Brasil, sendo certo que outras modalidades de assinatura, como aquelas com *login* e senha, não oferecem a necessária segurança para a prática desses atos. No presente artigo, aborda-se a assinatura de atos processuais praticados em meio eletrônico em seus aspectos jurídico e técnico, com especial ênfase à certificação digital, sem a qual o ato processual reputa-se inexistente.

Palavras-chave: Atos processuais. Assinatura eletrônica. Certificado digital. ICP-Brasil. Princípio da instrumentalidade das formas.

1 INTRODUÇÃO

Nos últimos anos, tem-se assistido à extraordinária expansão da tecnologia em todas as áreas do conhecimento humano. Nesse contexto, no que se refere ao Direito, assume especial relevo o advento de sistemas de processo eletrônico, em substituição aos processos físicos tradicionais, cujo meio de suporte é o papel.

O que se tem vivenciado hodiernamente compara-se, *mutatis mutandis*, à transição, ocorrida no início do século XX, concernente à implantação, na Justiça brasileira, da máquina datilográfica. Alguns juristas, conforme relato de 1926 (BRANDÃO, 2013), chegaram a questionar a validade jurídica de ato processual praticado com o uso da máquina de escrever, tendo em vista eventual quebra da fé pública advinda do abandono da tradicional escrita a bico de pena.

À semelhança do que ocorre em processos físicos, no decorrer dos processos em meio eletrônico, são praticados inúmeros atos processuais, que devem ser assinados pelos agentes legalmente competentes para sua prática, com a diferença de que a assinatura não ocorre de forma manuscrita, como nos processos físicos, mas sim eletronicamente.

Segundo Mourão *et al* (2009, p. 30), o espaço da tradicional assinatura manuscrita tem sido cada vez mais ocupado pela assinatura eletrônica, no âmbito de iniciativas visando à substituição de documentos em papel por documentos confeccionados, arquivados e enviados eletronicamente.

Nesse diapasão, faz-se necessário perquirir a(s) forma(s) pela(s) qual(is) pode(m) se dar a assinatura de atos processuais em meio eletrônico, de forma a

* Advogado. Assessor da Assessoria de Segurança da Informação (ASSIG) do Tribunal de Contas da União (TCU). Auditor Federal de Controle Externo do TCU. Especialista em Direito Processual Civil. Bacharel em Direito pela UnB.

garantir um adequado nível de segurança na prática desses atos.

O objetivo deste artigo é, por meio de pesquisa doutrinária e jurisprudencial, abordar a moderna temática da assinatura eletrônica de atos processuais, com o objetivo de apontar como deve ocorrer tal assinatura à luz do ordenamento jurídico ora em vigor.

2 INTEGRIDADE E AUTENTICIDADE DOS ATOS PROCESSUAIS

Os atos processuais são atos jurídicos que exprimem manifestações de vontade ou de conhecimento, praticados pelos diversos sujeitos processuais, por meio dos quais se forma, se desenvolve e se extingue o processo. Classificam-se de acordo com o sujeito de que emanam ou que os pratica em: atos do juiz, atos das partes e atos dos auxiliares da justiça (GRECO, 2011, p. 234).

Importa registrar que a prática de atos processuais assinados digitalmente em processo total ou parcialmente eletrônico¹ encontra-se prevista no § 2º do art. 169 do Código de Processo Civil (CPC), sendo ainda dignos de menção o § 2º do art. 154 e o parágrafo único do art. 556 do CPC. Já a assinatura eletrônica dos atos do juiz tem previsão específica no parágrafo único do art. 164 do CPC.

Os atos processuais em geral comumente consubstanciam-se em documentos, cujo meio de suporte pode ser físico (documentos em papel) ou eletrônico, afigurando-se fundamental - para que se garanta a necessária segurança jurídica envolvida na prática desses atos - que tais documentos tenham sua integridade e autenticidade preservadas.

Mas o que vêm a ser a integridade e a autenticidade segundo a ciência da segurança da informação?

A integridade pode ser definida como o princípio da segurança da informação que “garante a não-violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital.”

Já a autenticidade é o atributo inerente à segurança da informação que assegura a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria (TCU, 2008).

Os meios para a preservação da integridade e da autenticidade são bem conhecidos para os documentos em papel. Assim, para a garantia da integridade, está há muito consolidada a praxe da rubrica de todas as páginas de um documento (à exceção da última) por seu subscritor, com o que se dificulta eventual troca de uma folha por outra de conteúdo distinto. Já a autenticidade é preservada pela assinatura de próprio punho (normalmente na última página do documento), que permite se atribua a autoria de um documento a seu subscritor, o qual não poderá, posteriormente, refutar a autoria desse documento,

¹ Atualmente, há vários sistemas de processo eletrônico ainda em operação nos diversos órgãos do Poder Judiciário. Segundo levantamento feito pela Seccional da OAB/PR em 2011, o Brasil possui quase cem tribunais e cerca de 45 sistemas diferentes de processo virtual (BRANDÃO, 2013). A título exemplificativo, existem o e-STF, o e-STJ e o e-DOC (este no âmbito do TST), os quais exigem - para garantia da autenticidade e da integridade dos documentos - o uso de certificado digital.

ressalvada a hipótese de falsificação da assinatura.² À impossibilidade de o autor da declaração de vontade assinada obter sucesso em eventual tentativa de negar sua vinculação ao teor do documento dá-se o nome de garantia de não-repúdio (MENKE, 2005, p. 52).

Com a extraordinária expansão dos meios tecnológicos à disposição do homem, a tradicional tecnologia representada pelo papel (PECK PINHEIRO, 2010, p. 204) vem sendo gradualmente substituída por novas tecnologias, baseadas na eletrônica³, ou seja, os meios de suporte das informações em geral - e dos atos processuais em particular - vêm se transmutando do físico para o digital (MOURÃO *et al*, 2009, p. 30), afigurando-se necessário garantir a integridade e a autenticidade dos atos processuais praticados eletronicamente.⁴

Tal necessidade faz-se ainda mais patente quando se considera o advento do Processo Judicial Eletrônico (PJe), um *software* elaborado pelo Conselho Nacional de Justiça (CNJ) em progressiva implantação nos órgãos do Poder Judiciário. O PJe permite a prática de atos processuais em meio eletrônico por magistrados, servidores e demais participantes da relação jurídica processual, independentemente do órgão jurisdicional em que o processo tramite (CNJ, 2010, p. 5), sendo dotado do atributo da ubiquidade, já que possibilita o amplo e integral acesso simultâneo por qualquer usuário e em diferentes locais (BRANDÃO, 2013).

No âmbito do PJe, a ferramenta tecnológica adotada para a garantia da integridade e da autenticidade dos atos processuais é o certificado digital tipo A3 (CNJ, 2010, p. 19 e 22). De fato, a certificação digital afigura-se a melhor solução para a assinatura de peças processuais, conforme abordado no tópico a seguir.

3 A ASSINATURA COM CERTIFICADO DIGITAL

Segundo Peck Pinheiro (2010, p. 216), a assinatura com certificado digital é mais segura que aquela de próprio punho, pois é verificada em tempo real por intermédio de uma complexa função matemática de criptografia assimétrica (envolvendo um par de chaves), enquanto a assinatura manual não é verificada imediatamente e muitas vezes não é sequer conferida, como ocorre com cheques e cartões de crédito.

Mas o que vem a ser o certificado digital?

O certificado digital é uma espécie de carteira de identidade no meio eletrônico que possibilita a identificação segura do autor de um documento ou transação em

² Para minimizar o risco de falsificação e se obter maior segurança jurídica no que tange à autenticidade e ao não-repúdio, costumeiramente se exige o reconhecimento de firma em cartório após a assinatura de documentos em papel, a exemplo do que ocorre com a Autorização para Transferência de Propriedade de Veículo (ATPV), documento informalmente denominado "DUT Recibo".

³ Nesse contexto, a assinatura vem perdendo suas características de estilo pessoal, criado por impulsos cerebrais que são transferidos manualmente para o papel, em prol de uma técnica matemática realizada sobre o documento eletrônico assinado, denominada criptografia assimétrica (VALÉRIO E CAMPOS, 2011, p. 203), que é a base da certificação digital.

⁴ Nos termos do art. 11 da Lei n. 11.419/2006, os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário são considerados originais para todos os efeitos legais.

rede de computadores. É um arquivo eletrônico, validado por uma terceira parte confiável (autoridade certificadora), que identifica uma pessoa física ou jurídica na rede (TCU, 2010).

Segundo Menke (2005, p. 49), o certificado digital consiste em uma estrutura de dados sob a forma eletrônica, assinada digitalmente por uma terceira parte confiável que associa o nome e atributos de uma pessoa a uma chave pública. Trata-se de serviço semelhante à expedição de carteiras de identidade em que o futuro titular do certificado é identificado pelo terceiro de confiança mediante sua presença física e a apresentação dos documentos necessários.

Normalmente, o certificado digital é armazenado em um *token*⁵, que é conectado a uma entrada USB do computador, permitindo ao titular do certificado assinar documentos eletrônicos por meio do uso de uma senha pessoal e intransferível. Tal assinatura digital⁶ é validada por uma autoridade certificadora, com vistas a garantir a autenticidade e a integridade dos documentos.

Para a melhor compreensão da dinâmica envolvida na certificação digital, é necessário analisar o arcabouço jurídico que fundamenta sua utilização.

3.1 Fundamentos jurídicos

O Direito Processual Civil não poderia ficar alheio à intensiva informatização que tem impactado as relações sociais de nossos tempos⁷, tendo-se em conta inclusive a busca pela eficiência na prestação jurisdicional (MOURÃO *et al*, 2009, p. 35). Nesse sentido, para fazer frente à necessidade de informatização do processo judicial, foi editada a Lei n. 11.419, de 19 de dezembro de 2006, que - a par de alterar dispositivos do CPC de 1973, idealizado em uma época na qual os atos processuais eram formalizados por meio de documentos físicos - trouxe importantes previsões acerca da assinatura digital.

A assinatura eletrônica é definida pelo art. 1º, § 2º, III, da Lei n. 11.419/2006 nos seguintes termos, *verbis* (grifos nossos):

Art. 1º [...]

§ 2º Para o disposto nesta Lei, considera-se:

[...]

III - assinatura eletrônica as seguintes formas de identificação inequívoca do signatário:

⁵ O *token* é um dispositivo criptográfico semelhante a um *pen drive*. O certificado digital também pode ser armazenado em outras mídias, a exemplo de *chip* inserido em versões mais recentes da carteira profissional de advogado, que pode então ser acoplada a uma leitora para assinar documentos eletrônicos.

⁶ Assinatura digital não é sinônimo de assinatura digitalizada. Aquela é feita com certificado digital, garantindo a autenticidade e a integridade do documento assinado por meio de uma operação matemática realizada sobre este. Esta é mera reprodução da imagem da assinatura de próprio punho gerada por um equipamento do tipo *scanner*. Tal imagem pode ser facilmente copiada e inserida em outro documento, razão pela qual não garante nem autoria nem preservação de conteúdo.

⁷ Peck Pinheiro (2006, p. 09), diante das mudanças sociais trazidas pela tecnologia, afirma que o Direito que não está baseado na realidade é um Direito obsoleto, que não preserva mais sustentabilidade nem aptidão a gerar eficácia jurídica.

- a) assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica;
- b) mediante cadastro de usuário no Poder Judiciário, conforme disciplinado pelos órgãos respectivos.

A forma de assinatura eletrônica prevista na retrotranscrita alínea “b” será objeto de discussão no próximo item deste artigo. Já a exigência de lei específica contida na alínea “a” é suprida pela Medida Provisória n. 2.200-2, de 24 de agosto de 2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), cujo objetivo é “[...] garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica [...] que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras” (art. 1º da MP n. 2.200-2/2001).^{8 9}

Em apertada síntese, nos termos da mencionada MP, a ICP-Brasil é estruturada na forma de uma cadeia hierarquizada¹⁰ composta por uma Autoridade Certificadora Raiz (AC Raiz), por Autoridades Certificadoras (AC) e por Autoridades de Registro (AR), na forma a seguir sistematizada:

- a) AC Raiz: situa-se no topo da hierarquia da ICP-Brasil. Tal papel é desempenhado pelo Instituto Nacional de Tecnologia da Informação (ITI), autarquia vinculada à Casa Civil da Presidência da República, a qual compete emitir certificados digitais para as AC, de nível imediatamente subsequente ao seu, sendo-lhe vedado emitir certificados diretamente a usuários finais. É a “âncora de confiança” do sistema (Menke, 2005, p. 102);
- b) AC: entidades credenciadas pela AC Raiz a emitir certificados digitais aos respectivos titulares;
- c) AR: entidades operacionalmente vinculadas a determinada AC, às quais compete identificar e cadastrar presencialmente os usuários finais, com vistas à emissão de certificados digitais a tais pessoas pelas AC.¹¹

Uma vez que determinada pessoa tenha recebido certificado digital no âmbito

⁸ A MP n. 2.200-2, de 24 de agosto de 2001, encontra-se em pleno vigor por força do disposto no art. 2º da Emenda Constitucional n. 32, de 11 de setembro de 2001, segundo o qual “As medidas provisórias editadas em data anterior à da publicação desta emenda continuam em vigor até que medida provisória ulterior as revogue explicitamente ou até deliberação definitiva do Congresso Nacional.”

⁹ Castro (2011, p. 26), por exemplo, afirma que a lei específica a que se refere o art. 1º, § 2º, III, da Lei n. 11.419/2006 é atualmente a MP n. 2.200-2.

¹⁰ Segundo Menke (2005, p. 58), o modelo hierárquico de infraestrutura de chaves públicas configura-se na forma de uma árvore invertida, no topo da qual se situa uma entidade na qual todos os que estão abaixo devem confiar. A confiança se dissemina de cima para baixo: a entidade no ápice da hierarquia emite um certificado para uma autoridade certificadora de segundo nível e esta emite um certificado para o usuário final.

¹¹ O procedimento envolvido na identificação presencial do interessado é o “calcanhar de Aquiles” da certificação digital, podendo gerar inúmeros casos de danos e de indenizações, caso não sejam tomadas as devidas cautelas de que tratam o art. 7º da MP n. 2.200-2 e demais normas da ICP-Brasil. O contato presencial entre o consumidor e o fornecedor do certificado por intermédio da AR pode servir como momento adequado para o cumprimento do dever de informação, nos termos do art. 6º, III, e art. 8º do CDC (MENKE, 2005, p. 118 e 122/123).

da ICP-Brasil, estará apta a assinar digitalmente documentos eletrônicos, mediante o uso de senha pessoal e intransferível (código PIN), cadastrada após a emissão do certificado.¹²

Sem prejuízo da assinatura digital (baseada em certificado digital), nos termos do art. 1º, § 2º, III, "a", da Lei n. 11.419/2006, o art. 2º da mesma lei prevê a necessidade de credenciamento prévio do titular do certificado no Poder Judiciário, conforme disciplinado pelos órgãos respectivos, estabelecendo, em seu § 1º, a necessidade de procedimento no qual esteja assegurada a adequada identificação presencial do interessado. Considerando que já houve a identificação presencial do usuário perante as AR por ocasião da própria emissão do certificado, o disposto no art. 2º, § 1º, da Lei n. 11.419/2006 é adequadamente atendido mediante o preenchimento de formulário eletrônico no Portal do Tribunal na Internet, por ocasião do primeiro acesso ao respectivo sistema. Nos formulários eletrônicos do STF, do STJ e do TST, por exemplo, o advogado deve fornecer dados complementares não contidos no certificado, a exemplo de endereço, telefone, *e-mail* e número de inscrição profissional na OAB.¹³

Nesse particular, Atheniense (2009) externa pertinente preocupação acerca do fato de que a maioria dos tribunais brasileiros não consulta obrigatoriamente o cadastro nacional de advogados mantido pela OAB para aferir se determinado titular de certificado digital encontra-se no regular exercício da advocacia para a prática de atos processuais, apesar do que preceitua o art. 1º da Lei n. 8.906, de 04 de julho de 1994 (Estatuto da OAB). Referido autor sugere que, para efeito da prática de atos processuais em meio eletrônico, somente deva ser admitido certificado digital emitido pela Autoridade Certificadora da Ordem dos Advogados do Brasil (AC-OAB).¹⁴

Conquanto louvável a preocupação externada pelo autor, o PJe - ao exigir o credenciamento do titular de certificado digital mediante o preenchimento de formulário eletrônico, com esteio no art. 2º da Lei n. 11.419/2006 - apresenta funcionalidade que realiza obrigatoriamente validação junto ao cadastro nacional da OAB a partir do CPF do titular do certificado (CSJT, 2012a), ou seja, o sistema não permite o credenciamento de pessoas que não estejam no regular exercício da advocacia, independentemente de o certificado ter sido emitido ou não pela AC-OAB.

Tal entendimento encontra-se em sintonia com o objetivo da interoperabilidade¹⁵, que constitui apanágio de qualquer infraestrutura em geral - e

¹² O certificado digital também pode ser utilizado para a realização de operações na *Internet* com significativo ganho em termos de segurança, a exemplo de transações bancárias e do acesso ao e-CAC (Centro Virtual de Atendimento ao Contribuinte da Receita Federal). O Portal e-CAC - que disponibiliza ao contribuinte diversos serviços protegidos por sigilo fiscal - pode ser utilizado com código de acesso ou com certificado digital, mas alguns serviços estão disponíveis apenas para usuários que estiverem fazendo uso de certificado digital (RECEITA FEDERAL, 2013).

¹³ Dados similares são solicitados no PJe, à exceção do número de inscrição profissional na OAB, que é preenchido automaticamente pelo sistema.

¹⁴ Um dos requisitos para a obtenção de um Certificado Digital OAB é estar regularmente inscrito na Ordem dos Advogados do Brasil (AC-OAB, 2010).

¹⁵ Para mais detalhes acerca do tema, recomenda-se a leitura da obra "Panorama da Interoperabilidade no Brasil", editada pelo Ministério do Planejamento, Orçamento e Gestão (2010).

da ICP-Brasil em particular - e pode ser definida como a “capacidade que possuem os aparelhos ou equipamentos que dela fazem parte de comunicarem-se entre si, independentemente de sua procedência ou do seu fabricante” (MENKE, 2005, p. 59). Nesse sentido, a permissão de que quaisquer AC no âmbito da ICP-Brasil emitam certificados digitais para advogados é privilegiar a interoperabilidade de tal infraestrutura de chaves públicas.¹⁶

O mesmo não se diga da permissibilidade contida no § 2º do art. 10 da MP n. 2.200-2/2001, segundo o qual nada impede 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.

Apesar da índole inegavelmente democrática do dispositivo, em prol da liberdade e da autonomia privada, no sentido de permitir a existência de outros meios de comprovação de autoria e integridade, a interoperabilidade do sistema pode restar comprometida, caso não se garanta uma confiança na utilização do serviço antes e depois de efetuada a transação eletrônica. Assim, a assinatura deve ser passível de verificação por um lapso temporal significativo após o momento em que o documento foi assinado, o que implica a necessidade de que as autoridades certificadoras armazenem, por extenso interregno, as chaves públicas dos titulares de certificados digitais já expirados (MENKE, 2005, p. 127/130). A existência desse nível de confiança fora do âmbito da ICP-Brasil é bastante questionável.¹⁷

Nesse sentido, há um maior grau de segurança jurídica na prática de atos processuais mediante a utilização de processo de certificação disponibilizado pela ICP-Brasil, tendo em vista o disposto no § 1º do art. 10 da MP n. 2.200-2/2001, segundo o qual documentos eletrônicos assinados com certificado digital presumem-se verdadeiros em relação aos signatários. Em outras palavras, estes terão extrema dificuldade para recusar a autoria de documentos assinados com certificado digital vinculado à ICP-Brasil, ou seja, haverá uma sólida garantia de não-repúdio.¹⁸ O referido dispositivo reporta-se inclusive ao art. 131 do revogado Código Civil de 1916, reproduzido pelo art.

¹⁶ Por óbvio, isso não impede que a AC-OAB - em um regime concorrencial com outras ACs e em homenagem à condição de representante exclusiva dos advogados ostentada pela Ordem, nos termos da Lei n. 8.906/94 - ofereça condições mais vantajosas e estimule a aquisição de certificados digitais por causídicos, considerando que a cultura da certificação digital ainda não se disseminou entre os advogados. Prova disso é que, segundo pesquisa realizada há três anos, apenas 6% dos advogados no Estado de São Paulo possuíam certificado digital (PECK PINHEIRO E HAIKAL, 2012, p. 60).

¹⁷ Segundo Menke (2005, p. 127/128), além da interoperabilidade operacional, formal, técnica ou objetiva - referente à capacidade de os aparelhos ou equipamentos comunicarem-se entre si, independentemente de sua procedência ou do seu fabricante -, há a interoperabilidade substancial, jurídica ou subjetiva, a qual invoca um fundo principiológico comum atinente à confiança na utilização do serviço tanto pelos signatários do documento quanto pelas *relying parties*, não só no “aqui e agora”, como também “para trás e para frente”.

¹⁸ Conforme mencionado alhures, a garantia de não-repúdio dificulta que o subscritor de certo documento refute ser ele o seu autor. Trata-se de presunção relativa ou *juris tantum*, que admite prova em contrário. Segundo Peck Pinheiro e Haikal (2012, p. 59), tendo em vista o não-repúdio, o certificado digital com base na ICP-Brasil proporciona a inversão do ônus da prova em desfavor da pessoa que assinou o documento.

219 do Código Civil ora em vigor¹⁹, indicando que a assinatura com certificado digital no âmbito da ICP-Brasil se equipara à tradicional assinatura manuscrita, lançada de próprio punho. Trata-se da chamada equivalência funcional (MENKE, 2005, p. 140/141).²⁰

Em razão da maior segurança jurídica proporcionada pela certificação digital no âmbito da ICP-Brasil, o art. 3º da Lei n. 12.682, de 09 de julho de 2012, ao tratar do processo de digitalização, preconiza a adoção de certificado digital vinculado à ICP-Brasil, com vistas à manutenção da integridade e da autenticidade dos documentos eletrônicos fruto da digitalização, entendida - nos termos do art. 1º da Lei n. 12.682/2012 - como a conversão da fiel imagem de um documento em papel para o código digital.

A assinatura com certificado digital vinculado à ICP-Brasil, a par de ser a modalidade de assinatura eletrônica dotada de maior grau de segurança jurídica, também é a modalidade mais segura do ponto de vista técnico, conforme abordado a seguir.

3.2 Aspectos técnicos

Não é por acaso que os sistemas de processo eletrônico²¹ do STF, do STJ e do TST - denominados, respectivamente, e-STF, e-STJ e e-DOC -, bem como o PJe²², exigem o uso de certificado digital pelos advogados como requisito para o peticionamento eletrônico (ATHENIENSE, 2010, p. 12). Trata-se da modalidade de assinatura eletrônica mais segura do ponto de vista técnico.

Referidos sistemas são objeto de regulamentação²³ pelos citados Tribunais Superiores com base no parágrafo único do art. 154 do CPC, que estabelece, *verbis* (grifo nosso):

Art. 154 [...]

Parágrafo único. 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 Infraestrutura de Chaves Públicas Brasileira - ICP - Brasil. (Incluído pela Lei n. 11.280, de 2006)

Para o pleno atendimento dos requisitos acima grifados, não se pode conceber a prática de atos processuais em meio eletrônico sem o uso de certificado

¹⁹ "Art. 219 do CC. As declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários."

²⁰ Borges (2003 *apud* MENKE, 2005, p. 142) amplia o conceito, equiparando não só a assinatura digital à assinatura manuscrita, mas também os documentos eletrônicos aos documentos em papel.

²¹ A criação de sistemas de processo eletrônico pelos órgãos do Poder Judiciário encontra guarida no art. 8º da Lei n. 11.419/2006.

²² Como mencionado anteriormente, o PJe é um sistema desenvolvido pelo CNJ que se encontra em progressiva implantação com vistas à utilização uniforme do processo eletrônico nos diversos órgãos do Poder Judiciário, por intermédio de um único sistema.

²³ O e-STF, o e-STJ e o e-DOC são objeto de regulamentação, respectivamente, pelas: Resolução-STF n. 427, de 20 de abril de 2010; Resolução-STJ n. 14, de 28 de junho de 2013, e Instrução Normativa-TST n. 30, de 13 de setembro de 2007.

digital vinculado à ICP-Brasil (ALMEIDA FILHO, 2011, p. 269).

A título ilustrativo, veja-se o caso da Justiça do Trabalho. Por intermédio da Instrução Normativa n. 30, de 13 de setembro de 2007, o TST regulamentou a Lei n. 11.419/2006 no âmbito da Justiça do Trabalho, estabelecendo a prática de atos processuais em meio eletrônico por intermédio do Sistema Integrado de Protocolização e Fluxo de Documentos Eletrônicos (e-DOC).

Referida Instrução Normativa n. 30/2007 estabelece, em seu art. 4º, duas modalidades de assinatura eletrônica²⁴, *verbis* (grifos nossos):

Art. 4º [...]

I - assinatura digital, baseada em certificado digital emitido pela ICP - Brasil, com uso de cartão e senha;

II - assinatura cadastrada, obtida perante o Tribunal Superior do Trabalho ou Tribunais Regionais do Trabalho, com fornecimento de *login* e senha.

Cabe destacar que a aludida IN n. 30/2007 revogou a IN n. 28, de 02 de junho de 2005, a qual estabelecia que o acesso ao e-DOC dependia exclusivamente da utilização, pelo usuário, de certificado digital perante qualquer Autoridade Certificadora credenciada pela ICP-Brasil.

Impende registrar ainda que, no interregno entre a IN n. 28/2005 e a IN n. 30/2007, foi editada a Lei n. 11.419/2006, cujo art. 2º, § 1º, estabelece duas formas de assinatura eletrônica, razão pela qual a IN n. 30/2007 seguiu a mesma linha da lei ao regulamentá-la.

Conquanto louvável a alteração empreendida pela IN n. 30/2007 - a qual, de certa forma, ampliou o acesso à justiça ao permitir o uso da “assinatura cadastrada”, com *login* e senha, como alternativa à “assinatura digital”, com certificado -, o uso de certificado digital não foi dispensado pelo CNJ no âmbito do PJe, conforme já mencionado alhures.²⁵

Tampouco o Conselho Superior da Justiça do Trabalho (CSJT), criado pela Emenda Constitucional n. 45, de 30 de dezembro de 2004, dispensou o uso de certificado digital para as assinaturas empreendidas no âmbito do Processo Judicial Eletrônico na Justiça do Trabalho (PJe-JT).²⁶ Nesse sentido, o art. 5º da Resolução n. 94/CSJT, de 23 de março de 2012, estabelece expressamente que, para

²⁴ Segundo Menke (2005, p. 42), sob a denominação “assinatura eletrônica”, incluem-se vários métodos de comprovação de autoria empregados no meio virtual. Já a “assinatura digital” refere-se exclusivamente ao procedimento de autenticação baseado na criptografia assimétrica - que é aquela baseada em um par de duas chaves: uma pública e outra privada -, que constitui o fundamento da certificação digital.

²⁵ Atheniense (2009), ao comentar a IN n. 30/2009 à época de sua edição, já entendia que a assinatura com *login* e senha teria prazo de validade bem limitado, haja vista a futura adoção em massa da certificação digital, a não mais justificar a modalidade de assinatura cadastrada, que apresenta uma série de vulnerabilidades.

²⁶ O PJe-JT deriva de acordo de cooperação técnica firmado entre o CNJ, o TST e o CSJT, com vistas à elaboração de um sistema único de tramitação eletrônica de processos judiciais. Decorre ainda de acordo de cooperação técnica firmado entre o TST, o CSJT e os 24 TRTs (CSJT, 2012b). Portanto, o PJe-JT é uma ramificação do PJe no âmbito da Justiça Especializada trabalhista. Nos termos da Resolução n. 94/CSJT/2012, os atos processuais no âmbito da Justiça do Trabalho são praticados exclusivamente por intermédio do PJe-JT.

acesso ao PJe-JT, é obrigatória a utilização de assinatura digital, assim entendida aquela baseada em certificado digital padrão ICP-Brasil. Tal exigência manteve-se inalterada por ocasião da edição da Resolução n. 120/CSJT, de 21 de fevereiro de 2013²⁷, e da Resolução n. 128/CSJT, de 30 de agosto de 2013, que alteraram a citada Resolução/CSJT n. 94/2012.

O CSJT (2012a) assim justifica a exigência de assinatura com certificado digital, *verbis* (grifos nossos):

A opção pela certificação digital partiu do Conselho Nacional de Justiça e segue uma tendência mundial em segurança da informação. Além de identificar com precisão pessoas físicas e jurídicas, garante confiabilidade, privacidade, integridade e inviolabilidade em mensagens e diversos tipos de transações realizadas na *internet* - como o envio de uma petição, por exemplo.

A partir da experiência vivenciada pelo Judiciário trabalhista, cabe indagar os aspectos técnicos de segurança da informação que teriam motivado o CSJT a editar ato normativo passando a exigir a assinatura com certificado digital no âmbito da Justiça do Trabalho, considerando a prévia existência de IN do TST que flexibilizava a assinatura eletrônica ao permitir a “assinatura cadastrada” mediante o uso de *login* e senha.²⁸

Nesse sentido, sistematizam-se comparativamente, nos subitens a seguir, aspectos de segurança da informação envolvidos na assinatura com certificado digital padrão ICP-Brasil (assinatura digital) *versus* assinatura com *login* e senha (assinatura cadastrada).

3.2.1 Integridade e autenticidade

A assinatura digital garante integridade e autenticidade. Já a assinatura cadastrada garante apenas integridade, mas não autenticidade.

A assinatura com certificado digital padrão ICP-Brasil tem como base a criptografia assimétrica, que envolve a utilização de um par de chaves (chave pública e chave privada). A chave privada de um certificado digital tipo A3 fica armazenada exclusivamente em um dispositivo criptográfico (ex: *token*) e é usada para a aposição da assinatura digital propriamente dita em um documento eletrônico (a chave privada é usada por meio de um código PIN digitado pelo titular do certificado); a chave pública está disponível na AC para que qualquer pessoa, por meio de *softwares* específicos, possa conferir a validade da assinatura. Em

²⁷ A Resolução n. 120/CSJT, de 21 de fevereiro de 2013, detalhou vários aspectos do PJe-JT e consolidou o sistema no âmbito da Justiça do Trabalho, objetivando evitar a multiplicidade de sistemas de tramitação processual e o desperdício de recursos públicos no desenvolvimento de soluções de TI incompatíveis entre si. Esse objetivo advém de recomendação do Tribunal de Contas da União (TCU) emanada no âmbito do Acórdão n. 1094/2012 (Segunda Câmara).

²⁸ Não há que se olvidar, porém, da motivação contida no próprio excerto acima transcrito, qual seja, a opção pela certificação digital por parte do CNJ no âmbito do PJe, o que também levou o CSJT a exigir a assinatura com certificado digital no âmbito do PJe-JT, por uma questão de compatibilidade entre soluções de TI.

outros termos, a AC é um terceiro confiável que atesta a validade da assinatura no âmbito da ICP-Brasil.

Se o documento eletrônico que materializa o ato processual, por qualquer razão, for adulterado, ou seja, ainda que um único caractere seja mudado, suprimido ou acrescentado, a assinatura digital se perde.²⁹ Nesse sentido, a assinatura digital garante a integridade de conteúdo da peça processual. Além disso, como a chave privada está armazenada exclusivamente em dispositivo criptográfico de propriedade do titular do certificado e só este conhece o código PIN para usar a chave e assinar o documento, a autenticidade está garantida.

Por outro lado, na assinatura com *login* e senha, a chave precisa ser compartilhada com um terceiro ou armazenada em um servidor de arquivos para que seja viável a conferência posterior da assinatura, ou seja, tal chave não fica sob o exclusivo domínio do subscritor do documento.

Se o documento eletrônico for alterado, será possível detectar a adulteração, portanto a integridade está garantida. Já a autenticidade fica comprometida em função do potencial conhecimento da chave por terceiros, o que impede se atribua inequivocamente a autoria do documento à pessoa que supostamente o assinou.

3.2.2 Fatores de autenticação

A assinatura digital utiliza dois fatores de autenticação (dispositivo criptográfico e código PIN). Já a assinatura cadastrada utiliza um único fator de autenticação (senha).

Para a aposição de assinatura digital, são necessários cumulativamente a posse de dispositivo criptográfico (ex: *token*; carteira profissional da OAB) - contendo a chave privada do titular do certificado - e o conhecimento de código PIN. Esse código é pessoal, sendo exigido para o próprio uso do certificado digital por ocasião da assinatura.

Todavia, para a assinatura cadastrada, é necessário apenas o conhecimento da senha de quem assina o documento, não existindo dispositivo criptográfico que a proteja contra acesso indevido.

3.2.3 Risco de acesso indevido

Na assinatura digital, o código PIN é digitado em *software* instalado no próprio computador do usuário e de forma protegida, ou seja, o código não trafega na *Internet*, razão pela qual o risco de sua interceptação por terceiros é bem menor. Ainda que o código PIN fosse acessado hipoteticamente por um *hacker*, este não conseguiria assinar um documento eletrônico no lugar do titular do certificado, pois seria necessária a posse do dispositivo criptográfico (*token*) para a realização da assinatura digital. Segundo Atheniense (2009), é inegável que, com o uso da certificação digital, a possibilidade de fraudes é bem menor que com o uso de

²⁹ Os atuais programas de criptografia são capazes de cifrar um documento eletrônico e marcá-lo com uma assinatura digital, de tal forma que, se houver qualquer alteração no documento, a chave pública não mais o abrirá, acusando-se assim a falsificação (RAMOS, 2011, p. 22).

senhas. Para Brandão (2013), o acesso mediante certificado digital evita que sistemas “espiões” capturem dados do usuário e possibilitem a prática fraudulenta de atos nos processos.

Por outro lado, na assinatura cadastrada, a senha é digitada no próprio *site*, ou seja, trafega pela *Internet* até o servidor que hospeda o *site* para fins de validação. Em função do tráfego da senha e de o ambiente para sua digitação não estar necessariamente protegido, o risco de interceptação por terceiros é bem maior. Sendo assim, *hackers* poderiam em tese acessar indevidamente a senha e assinar documentos eletrônicos no lugar de seu titular. Para Atheniense (2009), essa modalidade de assinatura apresenta vulnerabilidades, ou seja, não garante ao assinante que as informações transmitidas tenham chegado ao destinatário final sem qualquer tipo de interceptação indevida e/ou alteração na sequência binária dos dados (ATHENIENSE, 2009). Na mesma esteira, Oliveira (2012, p. 449) entende que a utilização de senhas não ostenta a mesma segurança proporcionada pela certificação digital.

3.2.4 Validação da assinatura

A assinatura digital é validada por um terceiro legalmente autorizado no âmbito da ICP-Brasil. Já a assinatura cadastrada é validada pelo próprio órgão que gerencia o sistema de processo eletrônico.

Por meio do uso de *softwares* específicos, a assinatura digital - realizada por meio da chave privada do titular do certificado - pode ser validada por intermédio de sua chave pública, fornecida pela AC que emitiu o respectivo certificado. A AC é um terceiro confiável e legalmente autorizado a gerenciar certificados digitais, para fins de validação futura da assinatura de documentos eletrônicos.

De outro lado, a assinatura cadastrada somente pode ser validada pelo próprio órgão que gerencia o sistema de processo eletrônico. Mediante a posse da senha utilizada pelo usuário, o órgão pode realizar a conferência de determinada assinatura e disponibilizar o resultado dessa verificação em um ambiente específico.

4 ASSINATURA DIGITAL E INSTRUMENTALIDADE DAS FORMAS

Questão assaz importante diz respeito aos eventuais limites para a aplicação do princípio da instrumentalidade das formas aos procedimentos envolvidos na assinatura de atos processuais com certificado digital (assinatura digital).

O princípio da instrumentalidade das formas encontra guarida nos arts. 154, 244 e 249 do CPC. Para a discussão que ora se propõe, transcreve-se a seguir o referido art. 154, *verbis*:

Art. 154. Os atos e termos processuais não dependem de forma determinada senão quando a lei expressamente a exigir, reputando-se válidos os que, realizados de outro modo, lhe preenchem a finalidade essencial.

Acerca do tema, Almeida Filho (2011, p. 271) distingue o ato processual - espécie de ato jurídico praticado em razão de uma relação processual, gerando efeitos no processo, a exemplo da sentença, que é ato processual exclusivo do juiz -

do ato jurídico puro. Exemplo daquele seria a sentença que reconhece a paternidade após a regular tramitação do processo; exemplo deste seria o reconhecimento de paternidade realizada em cartório na presença de um notário.

Segundo o autor, o ato processual produz efeitos endoprocessuais, devendo ser revestido de autenticidade, integridade e segurança (art. 154, parágrafo único, do CPC), o que só pode ser alcançado mediante a adoção de certificado digital vinculado à ICP-Brasil. Já o ato jurídico puro pode ser inserido no processo por meio de certificado digital, hipótese na qual as declarações contidas no documento eletrônico presumir-se-ão verdadeiras em relação aos signatários, ou mediante a utilização de outro meio de comprovação da autoria e integridade, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento (§§ 1º e 2º do art. 10 da MP n. 2.200-2/2001).

Destarte, sendo a petição inicial e os recursos em geral exemplos de atos processuais, devem necessariamente ser assinados pelo advogado com seu certificado digital. Já eventuais documentos eletrônicos juntados ao processo como meio de prova, a exemplo de contratos eletrônicos, não necessitariam a rigor, para sua validade jurídica, da assinatura com certificado digital, muito embora a adoção deste pelos contraentes seja extremamente recomendada, para que o teor desses documentos conte com a presunção de veracidade prevista no § 1º do art. 10 da MP n. 2.200-2/2001.

E não há de se invocar o parágrafo único do art. 164 do CPC, segundo o qual “A assinatura dos juízes, em todos os graus de jurisdição, pode ser feita eletronicamente, na forma da lei.” (grifo nosso), para se entender que a assinatura digital de atos processuais pelos juízes seja facultativa. Na verdade, uma interpretação teleológica e sistemática do dispositivo conduz à necessária conclusão de que a faculdade indicada pelo verbo “poder” diz respeito à possibilidade de se praticar o ato judicial por meio eletrônico, enquanto alternativa à prática pelos meios tradicionais, por intermédio do papel. Uma vez eleito³⁰ o meio eletrônico para a prática do ato processual, este há de ser assinado com certificado digital, sem o qual não se pode conceber a autenticidade do ato, ou seja, um ato processual assinado com *login* e senha - que não é assinatura digital³¹, mas sim modalidade de assinatura eletrônica - não se reveste de autenticidade, razão pela qual não se teria verdadeiramente um ato praticado, mas sim a inexistência do ato processual (ALMEIDA FILHO, 2011, p. 272).

É exatamente dessa forma que entendem os Tribunais Superiores. O TST, ao apreciar caso no qual o recurso não se encontrava assinado com certificado digital, entendeu que recurso com mera “assinatura digitalizada” equivale a recurso apócrifo, razão pela qual o considerou inexistente, nos termos da OJ n. 120 da

³⁰ Para garantir o acesso à justiça, é de bom alvitre que os sistemas de processo eletrônico inicialmente apenas facultem o uso do meio eletrônico para a prática de atos processuais, permanecendo possível a adoção do meio físico tradicional por um lapso temporal razoável. Estratégia similar foi adotada pela Receita Federal para a recepção das declarações de imposto de renda via *Internet*, as quais permaneceram podendo ser feitas por intermédio de formulários em papel durante vários anos, concomitantemente à possibilidade da transmissão eletrônica. Hoje, a Receita recebe declarações exclusivamente por meio eletrônico.

³¹ A assinatura digital é aquela praticada com certificado digital vinculado à ICP-Brasil.

SBDI-I.³² Confira-se a decisão a seguir ementada, *verbis* (grifo nosso):

AGRAVO DE INSTRUMENTO EM RECURSO DE REVISTA. NÃO CONHECIMENTO DO RECURSO ORDINÁRIO. AUSÊNCIA DE ASSINATURA ORIGINAL. APELO INEXISTENTE. EXEGESE DA ORIENTAÇÃO JURISPRUDENCIAL 120 DA SBDI-I DO TST. Hipótese em que o recurso ordinário não foi conhecido, por se encontrar subscrito com mera assinatura digitalizada, o que equivale a encontrar-se apócrifo. Com efeito, constata-se que não houve a aposição de assinatura original nos termos da Orientação Jurisprudencial 120 da SBDI-I do TST, somente se admitindo a validade da petição em que o advogado tenha apostado originalmente sua assinatura, ou na hipótese de assinatura eletrônica, a qual não se verificou nos autos. Precedentes do STF. Agravo de instrumento não provido.

(TST, 7ª Turma, AIRR 135900-27.2009.5.10.0004, Relatora: Min. Delaíde Miranda Arantes, Data de Julgamento: 20.03.2013, DEJT 26.03.2013.)

Poder-se-ia eventualmente argumentar que a decisão teria privilegiado a forma em detrimento da finalidade do ato processual e, conseqüentemente, não teria observado o princípio da instrumentalidade das formas, mas tal argumento não se sustenta, pois a “assinatura digitalizada” é mera imagem correspondente à cópia da assinatura de próprio punho, sendo, portanto, passível de inserção em documento eletrônico por qualquer pessoa, ou seja, não garante a autenticidade do ato.

Nesse sentido, o STF entende que a exigência de certificado digital não é mero formalismo processual, mas sim exigência razoável para impedir a prática de atos cuja responsabilização não seria possível, conforme a ementa de julgado a seguir transcrita (grifos nossos):

EMENTA: Ato processual: recurso: chancela eletrônica: exigência de regulamentação do seu uso para resguardo da segurança jurídica. 1. Assente o entendimento do Supremo Tribunal de que apenas a petição em que o advogado tenha firmado originalmente sua assinatura tem validade reconhecida. Precedentes. 2. No caso dos autos, não se trata de certificado digital ou versão impressa de documento digital protegido por certificado digital; trata-se de mera chancela eletrônica sem qualquer regulamentação e cuja originalidade não é possível afirmar sem o auxílio de perícia técnica. 3. A necessidade de regulamentação para a utilização da assinatura digitalizada não é mero formalismo processual, mas exigência razoável que visa impedir a prática de atos cuja responsabilização não seria possível.

(STF, Primeira Turma, AI 564765, Relator: Min. Sepúlveda Pertence, Data do Julgamento: 14.02.2006, DJ 17.03.2006.)

Na mesma esteira, o STJ tem inúmeros julgados apontando para a inexistência de recurso desprovido de assinatura com certificado digital cujo titular seja advogado com poderes nos autos para representar a parte recorrente. A título exemplificativo, no julgado abaixo, proferido recentemente pela Corte Especial do

³² Orientação Jurisprudencial (OJ) n. 120, da Subseção I da Seção Especializada em Dissídios Individuais (SBDI-I) do TST (grifo nosso):

RECURSO. ASSINATURA DA PETIÇÃO OU DAS RAZÕES RECURSAIS. VALIDADE. O recurso sem assinatura será tido por inexistente. Será considerado válido o apelo assinado, ao menos, na petição de apresentação ou nas razões recursais.

STJ, o advogado indicado no corpo da petição como autor do documento não havia assinado o ato processual com seu próprio certificado digital, razão pela qual o recurso foi considerado inexistente. Eis a ementa (grifos nossos):

EMBARGOS DE DECLARAÇÃO. RECURSO EXTRAORDINÁRIO LIMINARMENTE INDEFERIDO. PETIÇÃO ELETRÔNICA. FALTA DE IDENTIDADE ENTRE O SUBSCRITOR DA PETIÇÃO E O TITULAR DO CERTIFICADO DIGITAL. RECURSO INTERPOSTO POR ADVOGADO SEM PROCURAÇÃO NOS AUTOS. INAPLICABILIDADE DO ART. 13 DO CPC NA VIA EXTRAORDINÁRIA. EMBARGOS DE DECLARAÇÃO NÃO CONHECIDOS.

I. Não havendo identidade entre o titular do certificado e do advogado indicado como autor da petição, deve a peça ser tida como inexistente.

II. Eventual falha na representação processual não pode ser suprida posteriormente, porquanto inaplicável na instância especial o disposto no artigo 13 do Código de Processo Civil.

III. Embargos de declaração não conhecidos.

(STJ, Corte Especial, EDcl no AgRg no ARE no RE no AgRg nos EDcl no AREsp 32879/SP, Relatora: Min. Eliana Calmon, Data do Julgamento: 20.02.2013, DJe 28.02.2013.)

Corroborando tal entendimento, o STJ considerou inexistente recurso interposto por advogado que não detinha procuração nos autos, nos termos da Súmula n. 115 da mesma Corte.³³ Segundo o STJ, a identificação de quem peticiona nos autos é a proveniente do certificado digital, independentemente do nome do causídico que apareça no corpo da peça processual. Se o advogado titular do certificado digital não detiver poderes para atuar em nome da parte recorrente, o recurso é tido por inexistente, conforme a decisão a seguir ementada (grifos nossos):

PROCESSUAL CIVIL. PETIÇÃO ELETRÔNICA. IRREGULARIDADE NO USO DO CERTIFICADO DIGITAL. AUSÊNCIA DE PROCURAÇÃO NOS AUTOS. RECURSO INEXISTENTE. SÚMULA 115 DO STJ.

1. Nos termos da jurisprudência do STJ, a identificação de quem peticiona nos autos é a proveniente do certificado digital, independentemente da assinatura que aparece na visualização do arquivo eletrônico. Precedentes: AgRg no AREsp 145.381/BA, Rel. Min. Mauro Campbell Marques, Segunda Turma, julgado em 19.06.2012, DJe 07.06.2012; AgRg no REsp 1304123/AM, Rel. Min. Humberto Martins, Segunda Turma, julgado em 22.05.2012, DJe 29.05.2012.

2. Hipótese em que o advogado titular do certificado digital utilizado para assinar a transmissão eletrônica do agravo regimental não possui instrumento de procuração nos autos. Recurso inexistente. Incidência da Súmula 115 do STJ. Agravo regimental não conhecido.

(STJ, 2ª Turma, AgRg no AREsp 202417/RJ, Relator: Min. Humberto Martins, Data do Julgamento: 28.08.2012, DJe 03.09.2012.)

Resta, porém, um espaço - ainda que restrito - para a aplicação do princípio da instrumentalidade das formas. Se tal princípio não tem o condão de dispensar o uso de certificado digital por advogado com procuração nos autos, admite-se recurso no qual conste o nome de causídico diverso daquele que efetivamente

³³ Súmula n. 115 do STJ: "Na instância especial é inexistente recurso interposto por advogado sem procuração nos autos." Não há, portanto, espaço para a aplicação do art. 13 do CPC em instância especial.

assinou digitalmente a peça processual, contanto que o titular do certificado digital detenha poderes para atuar nos autos. Isso se dá porque, conforme a retrotranscrita decisão, o que realmente importa para fins de identificação de quem peticiona nos autos é o certificado digital, e não o nome que aparece na visualização do documento. Nesse sentido, veja-se o julgado a seguir (grifo nosso):

PROCESSUAL CIVIL. AGRAVO REGIMENTAL NO RECURSO ESPECIAL. INTEMPESTIVIDADE. PETIÇÃO ELETRÔNICA. CERTIFICAÇÃO DIGITAL. ASSINATURA. IRREGULARIDADE.

1. Conforme o entendimento desta Corte, não havendo identidade entre o titular do certificado digital usado para assinar o documento e o nome do advogado indicado como autor da petição, deve esta ser tida como inexistente.

2. Possibilidade de superação da irregularidade, quando o advogado que assine digitalmente conste da procuração constante dos autos eletrônicos, o que não ocorre na espécie.

3. AGRAVO NÃO CONHECIDO.

(STJ, 3ª Turma, AgRg no REsp 1154727/PR, Relator: Min. Paulo de Tarso Sanseverino, Data do Julgamento: 04.09.2012, DJe 11.09.2012.)

Portanto, diante da não-adoção de certificado digital ou de sua utilização por pessoa sem poderes para praticar o ato processual em questão, a firme jurisprudência dos Tribunais Superiores é pela inexistência do ato. Importante asseverar que a não-utilização de certificado digital para a assinatura do documento por pessoa competente para a prática do ato processual não implica vício de validade que possa eventualmente ser superado diante da ausência de prejuízo às partes, mas sim falta de requisito para a própria existência do ato.

5 CONCLUSÃO

Por todo o exposto, pode-se concluir que:

- a) Para um adequado nível de segurança na prática de atos processuais em sistemas de processo eletrônico, há que se garantir a integridade e a autenticidade desses atos;
- b) a assinatura digital, com certificado vinculado à ICP-Brasil, garante a segurança na prática de atos processuais eletrônicos, o que não ocorre em outras modalidades de assinatura eletrônica, como aquela mediante a utilização de *login* e senha;
- c) a ausência de certificado digital pertencente a pessoa com poderes para a prática do ato processual leva, inexoravelmente, à sua inexistência, conforme firme jurisprudência dos Tribunais Superiores;
- d) o princípio da instrumentalidade das formas não pode ser aplicado para dispensar a assinatura com certificado digital por agente competente para a prática do ato processual, mas se admite seja superada irregularidade consistente na indicação equivocada do agente responsável pelo ato, desde que o titular do certificado digital usado para assinar o documento tenha poderes ou seja competente para praticar o ato processual.

Portanto, andou bem a Justiça do Trabalho ao exigir em regulamento - editado

com base no parágrafo único do art. 154 do CPC c/c o art. 18 da Lei n. 11.419/2006 - a certificação digital para a prática de atos processuais em meio eletrônico no PJe-JT.

A exigência de certificado digital para a prática de atos processuais guarda inclusive sintonia com a exemplar posição de vanguarda que a Justiça do Trabalho tem assumido no âmbito do Poder Judiciário no que tange à adoção do PJe, haja vista sua implantação no TST e em todos os TRTs, bem como em inúmeras Varas Trabalhistas.

Ressalte-se que, no decorrer de todo este artigo, tratou-se da prática de atos processuais em meio eletrônico, que difere da mera consulta aos autos processuais. Assim, considerando ser prerrogativa do advogado “[...] examinar [...] autos de processos findos ou em andamento, mesmo sem procuração, quando não estejam sujeitos a sigilo” (inciso XIII do art. 7º do Estatuto da OAB), afigura-se coerente a recente deliberação do CSJT no sentido de liberar o acesso para visualização de autos no âmbito do PJe mediante *login* e senha, em atendimento à solicitação da OAB (CSJT, 2013).

Sem prejuízo da visualização de autos por advogados mediante *login* e senha, mesmo sem procuração, a prática de atos processuais no âmbito do PJe deve se dar por meio de certificado digital - cujo titular deve ter procuração para atuar nos autos - sob pena de ofensa à autenticidade e consequente inexistência do ato processual.

Foi exatamente nesse sentido que caminhou a recente Resolução CSJT n. 128, de 30 de agosto de 2013, que alterou a Resolução CSJT n. 94/2012 com vistas a permitir a utilização de *login* e senha exclusivamente para a visualização de autos, exceto nas hipóteses de sigilo ou segredo de justiça. Para a assinatura de atos processuais no PJe, a citada Resolução manteve como obrigatória a utilização do certificado digital.

ABSTRACT

From the institution of the electronic process of law, arose the need of secure signature of processual acts electronically practiced. To assure the integrity and authenticity of processual acts, the electronic signature must be carried out by the adoption of a digital certificate linked to ICP-Brasil, and it's unquestionable that other signature modalities, such as those with login and password, don't offer the necessary security for the practice of these acts. In the present article, it's discussed the signature of processual acts practiced by electronic means both in its juridical and technical matters, with special emphasis to the digital certification, without which the processual act is regarded inexistent.

Keywords: *Processual acts. Electronic signature. Digital certificate. ICP-Brasil. Principle of form instrumentality.*

REFERÊNCIAS

- ALMEIDA FILHO, José Carlos de Araújo. A teoria geral dos atos processuais praticados por meios eletrônicos, a partir de um novo CPC. *Revista de Informação*

- Legislativa*. Brasília, n. 190, p. 267-278, 2011.
- ATHENIENSE, Alexandre Rodrigues. *Comentários a Instrução Normativa n. 30/2007 do TST*. 2009. Disponível em: <<http://conteudojuridico.com.br/?artigos&ver=2.24603>>. Acesso em: 12 maio 2013.
 - _____. Os avanços e entraves do processo eletrônico no judiciário brasileiro em 2010. *Seleções Jurídicas*. São Paulo, p. 11-15, jan. 2011.
 - AUTORIDADE CERTIFICADORA DA ORDEM DOS ADVOGADOS DO BRASIL. *Certificado digital OAB: vantagens que todo advogado precisa conhecer*. 2010. Disponível em: <<http://www.acoab.com.br/projetos/acoab/site/pdf/folder-acoab-A5.pdf>>. Acesso em: 12 maio 2013.
 - BRANDÃO, Cláudio. Processo judicial eletrônico - uma silenciosa revolução na Justiça do Trabalho. *Revista LTr*. São Paulo, v. 77, n. 01, 2013.
 - CASTRO, Aldemario Araújo. O triunfo da convergência digital e as cautelas necessárias. *Revista Jurídica Consulex*. Brasília, v. 15, n. 338, p. 25-26, fev. 2011.
 - CONSELHO NACIONAL DE JUSTIÇA. *PJe - Processo judicial eletrônico*. 2010. Disponível em: <http://www.cnj.jus.br/images/dti/processo_judicial_eletronico_pje/processo_judicial_eletronico_grafica2.df>. Acesso em: 12 maio 2013.
 - CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO. *Certificação digital*. 2012a. Disponível em: <<http://www.csjt.jus.br/certificacao-digital>>. Acesso em: 12 maio 2013.
 - _____. *Histórico do Processo Judicial Eletrônico da Justiça do Trabalho (PJe-JT)*. 2012b. Disponível em: <<http://www.csjt.jus.br/historico>>. Acesso em: 12 maio 2013.
 - _____. *CSJT aprova importantes alterações no PJe-JT*. 2013. Disponível em: <http://www.csjt.jus.br/pje-jt/-/asset_publisher/B7fk/content/csjt-aprova-importantes-alteracoes-no-pje-jt?redirect=%2Fpje-jt>. Acesso em: 13 set. 2013.
 - _____. Institui o sistema processo judicial eletrônico da Justiça do Trabalho - PJe-JT como sistema de processamento de informações e prática de atos processuais e estabelece os parâmetros para sua implementação e funcionamento. *Resolução n. 94/CSJT, de 23 de março de 2012*. Diário Eletrônico da Justiça do Trabalho de 26.03.2012.
 - _____. Altera a Resolução CSJT n. 94, de 23 de março de 2012, que institui o Sistema Processo Judicial Eletrônico da Justiça do Trabalho - PJe-JT como sistema de processamento de informações e prática de atos processuais e estabelece os parâmetros para sua implementação e funcionamento. *Resolução n. 120/CSJT, de 21 de fevereiro de 2013*. Diário Eletrônico da Justiça do Trabalho de 22.02.2013.
 - _____. Altera a Resolução n. 94, de 23 de março de 2012, que institui o Sistema Processo Judicial Eletrônico da Justiça do Trabalho - PJe-JT como sistema de processamento de informações e prática de atos processuais e estabelece os parâmetros para sua implementação e funcionamento. *Resolução/CSJT n. 128, de 30 de agosto de 2013*. Diário Eletrônico da Justiça do Trabalho de 05.09.2013.
 - GRECO, Leonardo. *Instituições de processo civil*. V. 1. 3. ed. Rio de Janeiro: Forense, 2011.
 - MENKE, Fabiano. *Assinatura eletrônica no direito brasileiro*. São Paulo: Editora Revista dos Tribunais. 2005.

- MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. *Panorama da interoperabilidade no Brasil*. Brasília: MP/SLTI, 2010.
- MOURÃO, Licurgo; ELIAS, Gustavo Terra; FERREIRA, Diogo Ribeiro. A imprescindibilidade da assinatura eletrônica, da assinatura mecânica e da certificação digital para a administração pública brasileira. *Revista do Tribunal de Contas do Estado de Minas Gerais*. Belo Horizonte, v. 73, n. 4, p. 29-43, 2009.
- OLIVEIRA, Cristiano de. O “processo eletrônico” sob a ótica da instrumentalidade técnica e do acesso qualitativo da atividade jurisdicional. *Revista de Processo*. São Paulo, v. 207, p. 435-456, 2012.
- PECK PINHEIRO, Patrícia. A questão da prova legal na sociedade digital. *Revista do Tribunal Regional Federal da 3ª Região*. São Paulo, n. 78, p. 9-30, 2006.
- _____. *Direito digital*. 4. ed. São Paulo: Saraiva, 2010.
- PECK PINHEIRO, Patrícia; HAIKAL, Victor Auilo. O judiciário e o fisco digitais: o que muda e o que deve mudar? In: PECK PINHEIRO, Patrícia *et al.* *Direito digital aplicado*. São Paulo: Intelligence, 2012, p. 57-65.
- RAMOS, Mônica Gomes. O valor probatório do documento eletrônico. 2011. 81 f. Monografia (Graduação) - Curso de Direito, Universidade de Brasília, Brasília, 2011.
- RECEITA FEDERAL. Portal e-CAC (Centro Virtual de Atendimento ao Contribuinte). Disponível em: <<http://www.receita.fazenda.gov.br/atendvirtual/defaultatendcertdigital.htm>>. Acesso em: 01 maio 2013.
- SUPREMO TRIBUNAL FEDERAL. Regulamenta o processo eletrônico no âmbito do Supremo Tribunal Federal e dá outras providências. *Resolução n. 427, de 20 de abril de 2010*. Diário da Justiça Eletrônico do Supremo Tribunal Federal de 26.04.2010.
- SUPERIOR TRIBUNAL DE JUSTIÇA. Regulamenta o processo judicial eletrônico no âmbito do Superior Tribunal de Justiça. *Resolução n. 14, de 28 de junho de 2013*. Diário da Justiça Eletrônico do Superior Tribunal de Justiça de 03.07.2013.
- TRIBUNAL DE CONTAS DA UNIÃO - TCU. Dispõe sobre a Política Corporativa de Segurança da Informação do Tribunal de Contas da União (PCSI/TCU). *Resolução -TCU n. 217, de 15 de outubro de 2008*. Diário Oficial da União de 17.10.2008.
- _____. Certificado digital. 2010. *Folder*.
- TRIBUNAL SUPERIOR DO TRABALHO. Dispõe sobre o Sistema Integrado de Protocolização e Fluxo de Documentos Eletrônicos da Justiça do Trabalho (e-DOC). *Instrução Normativa n. 28, de 02 de junho de 2005*. Diário da Justiça de 07.06.2005.
- _____. Regulamenta, no âmbito da Justiça do Trabalho, a Lei n. 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial. *Instrução Normativa n. 30, de 13 de setembro de 2007*. Diário da Justiça de 18.09.2007.
- VALÉRIO, Marcos Aurélio Gumieri; CAMPOS, José Fernando dos Santos. Títulos de crédito eletrônico. A tecnologia a serviço do direito cambial. *Revista de Informação Legislativa*. Brasília, n. 189, p. 189-209, 2011.

AGRADECIMENTO

O autor deste artigo agradece a Luisa Helena Santos Franco, Auditora Federal de Controle Externo lotada na Assessoria de Segurança da Informação do TCU, pela inestimável contribuição para a construção deste trabalho, a partir de seu vasto conhecimento e experiência em segurança da informação, particularmente no que se refere aos aspectos técnicos da certificação digital.