AUTENTICIDADE DO DOCUMENTO ARQUIVÍSTICO DIGITAL: desafio tecnológico ou de observância de princípios arquivísticos?

Lenora de Beaurepaire da Silva Schwaitzer[1]

RESUMO: Artigo que reflete quanto à adoção do certificado digital tipo A3 como garantia da integridade dos documentos arquivísticos digitais pela Justiça Federal nos moldes previstos pelo MoReq-Jus e quanto à obrigatoriedade de sua manutenção para a produção desses documentos em sistemas informatizados de gestão arquivística de documentos que observam normas de gestão documental. O trabalho é composto de três partes: a primeira, esclarece o contexto para a adoção da criptografia assimétrica para assegurar a integridade dos documentos, a segunda destaca a importância da diplomática e da tipologia documental para garantir a autenticidade dos documentos e a última parte apresenta conclusão no sentido de que documentos produzidos em um sistema informatizado desenvolvido de acordo com o modelo de requisitos para gestão arquivística de documentos e que observe os princípios de gestão documental dispensam o uso de certificado digital para garantir sua autenticidade.

Palavras-chave: Assinatura digital. Diplomática e tipologia documental. Autenticidade e integridade. SIGAD.

AUTHENTICITY OF THE DIGITAL ARCHIVAL DOCUMENT: technological challenge or of observance of archival principles

ABSTRACT: Paper that reflects on the adoption of the digital signature certificate Class 3 to ensure the integrity of Federal Justice's digital records in the manner foreseen by MoReq-Jus and regarding the obligation of its maintenance in an electronic management systems that follow record management standards. The paper is composed of three parts: the first clarifies the context for the adoption of asymmetric cryptography to ensure the integrity of records, the second emphasizes the importance of Diplomatics and Typological Analysis to ensure the authenticity of records and the last part is concluded in the sense that records generated in a electronic management system developed according to the model requirements for the management of electronic records and that follow principles of electronic record management, do not require the adoption of a digital signature certificate to ensure its authenticity.

KEYWORDS: Authenticity and integrity. Digital signature certificate. Diplomatics and Typological Analysis. EDRM.

[1] Doutora em História, Política e Bens Culturais pelo CPDOC/FGV, é graduada em Direito, Arquivologia, Biblioteconomia e Documentação e é graduanda em Sistemas de Informação, todos pela UFF. É especialista em Políticas Informacionais e Organização do Conhecimento pela UFRJ em parceria com o Arquivo Nacional, especialista em Gestão Pública pela FIJ, mestre em Bens Culturais pelo CPFOC/FGV e mestre em Justiça Administrativa pela UFF. É Analista Judiciário e ocupa o cargo de Assessora de Documentação, Informação e Memória do Tribunal Regional Federal da 2ª Região. E-mail: lenoras@id.uff.br ou lenora@trf2.jus.br

1 INTRODUÇÃO

O presente artigo objetiva enfrentar uma questão que vem sendo objeto de preocupações da Justiça Federal da 2ª Região, que engloba os Estados do Rio de Janeiro e Espírito Santo, no que pertine à produção de documentos arquivísticos em sistemas informatizados: a obrigatoriedade do uso de certificado digital para assegurar a autenticidade desses documentos.

É inconteste afirmar que o uso crescente de tecnologias para a produção de documentos arquivísticos vem obrigando pesquisadores e profissionais de arquivo a voltarem suas reflexões quanto à permanência dos princípios da teoria arquivística quando se discute produção e preservação dos documentos arquivísticos digitais e quanto à gestão de documentos em codificação binária. Entretanto, a adoção maciça de ferramentas tecnológicas pelos órgãos do Poder Judiciário e, em particular, pela Justiça Federal, faz com que questões como a que está aqui apresentada suscite questionamentos e preocupações ainda mais pungentes.

Convém lembrar que, em setembro de 2000, o Ministério da Ciência e Tecnologia publicou o Livro Verde marcando, não apenas o término do milênio, mas o início de uma nova era: o da Sociedade da Informação, que privilegia o conhecimento e que usa a tecnologia em prol de benefícios para a coletividade. Nesta publicação, Takahashi (2000) aponta as principais mudanças operadas no curto período após o advento da internet, surgida em 1993 e prevê a adoção da tecnologia em diversas áreas, inclusive no âmbito governamental. Segundo o autor, o uso de tecnologias da informação iria gerar "uma administração pública mais transparente, eficaz e voltada para a prestação de informações e serviços à população" (TAKAHASHI, 2000, p. 8). Em seu prognóstico, a tecnologia seria útil para:

> Emissão de documentos, prestação de informações ligadas aos serviços públicos, acompanhamento das ações de governo e condução dos negócios públicos, acesso aos governantes e representantes eleitos são exemplos das possibilidades do uso das tecnologias de informação e comunicação pela máquina administrativa pública. A tecnologia pode ainda ser largamente aplicada para aperfeiçoar a própria gestão do governo – coordenação, planejamento, execução e controle de ações, contabilidade pública etc. – e suas transações comerciais com o setor privado (TAKAHASHI, 2000, p. 8).

Como primeiro ato para implementação do governo eletrônico, em junho de 2001, foi editada a Medida Provisória Nº 2.200, instituindo a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Além disso, a Medida Provisória dispunha sobre a validade jurídica dos documentos assinados eletronicamente com uso de certificados emitidos dentro da ICP-

Brasil e reconhecia a possibilidade de uso de outro meio de comprovação da autoria e integridade de documentos digitais, contanto houvesse o aceite das partes ou da pessoa a quem o documento fosse destinado.

Mas as iniciativas para o uso de novas tecnologias para a gestão mais transparente e eficaz de suas atividades não se limitava às ações do Executivo Federal. Com efeito, o Judiciário, e particularmente, a Justiça Federal já promovia estudos voltados para a padronização das ações de Tecnologia da Informação e Comunicação – TIC, e para a renovação de seus sistemas processuais e, no ano de 2001, já debatia acerca dos desafios envolvendo a produção, a segurança e a preservação dos documentos àquela época denominados eletrônicos, conforme o Fórum sobre Arquivos e Documentos Eletrônicos, realizado em junho daquele ano no CCJF, em parceria com o Centro de Estudos Judiciários e com o Conselho da Justiça Federal. Logo a seguir, foi editada a Lei no 10.259, de 12 de julho de 2001, que criou os Juizados Especiais Cíveis e Criminais da Justiça Federal, facultou o peticionamento eletrônico e a intimação por meio digital, que impulsionou uma nova fase para a Justiça Federal.

Em julho de 2003, o Juizado Federal de Londrina produz o primeiro processo completamente eletrônico e, no ano seguinte, é instalado o primeiro juizado eletrônico na cidade de São Gonçalo, no Rio de Janeiro. E é também neste mesmo ano que o Conselho da Justiça Federal cria, por meio da Resolução nº 397, de 18 de outubro, a autoridade certificadora do sistema Justiça Federal – AC-JUS, e estabelece diretrizes para o uso da certificação digital, no âmbito do Conselho da Justiça Federal e da Justiça Federal de 1º e 2º graus, por reconhecer que a mesma seria capaz de garantir a autenticidade, a integridade e a validade jurídica de documentos produzidos em forma eletrônica.

Importante ressaltar que é dentro deste contexto que a Justiça Federal da 2ª Região cria seu processo judicial eletrônico e elabora estudos para o desenvolvimento de um sistema para produção de documentos administrativos, o SIGA-Ex, que foi implantado em 2007, tanto nas Seções Judiciárias do Rio de Janeiro e do Espírito Santo, quanto no próprio TRF2.

Com o advento da Emenda Constitucional nº 45, de 30 de dezembro de 2004, que acrescentou o inciso LXXXVIII ao artigo 5º da Constituição Federal e que assegurou, no âmbito judicial e administrativo, a razoável duração do processo e os meios que viessem a assegurar a celeridade de sua tramitação, que se verificou um grande impulso em direção à regulamentação do processo judicial eletrônico, que iria ser iniciado, a nível legislativo, através da Lei nº 11280, de 16 de fevereiro de 2006, que acrescentou ao parágrafo primeiro do artigo 154 do Código de Processo Civil previsão no sentido de que:

> Os tribunais, no âmbito da respectiva jurisdição, poderão disciplinar a prática e a comunicação oficial dos atos processuais por meios eletrônicos, atendidos os requisitos de autenticidade, integridade, validade jurídica e interoperabilidade da infraestrutura de Chaves Públicas Brasileiras - ICP-Brasil. (BRASIL, 2006a, p. 1).

Posteriormente, a Lei nº 11419, de 19 de dezembro de 2006, conhecida como a Lei do Processo Eletrônico dispôs sobre a informatização do processo judicial e alterou normas do Código de Processo Civil em vigor à época. Através deste normativo, foram estabelecidas duas formas para a assinatura eletrônica como meio de identificação inequívoca do signatário:

> 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 (BRASIL, 2006b, p. 1).

A alternativa prevista pelo art. 1º, §2º, inciso III, da Lei do Processo Eletrônico ensejou a flexibilização do uso de certificado digital nas distintas Cortes Judiciais e observou-se paulatina discrepância de critérios, inclusive no âmbito da Justiça Federal, que passaram a estabelecer normas próprias para elaboração de assinatura nos feitos judiciais e nos atos e expedientes administrativos. Visando estabelecer normas básicas para o desenvolvimento de sistemas informatizados de gestão de processos e documentos da Justiça Federal, o CJF iniciou, em abril de 2007, o desenvolvimento do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos da Justiça Federal – MoReq-Jus, inspirado no modelo europeu, mas adaptado à realidade do Judiciário, que foi submetido à consulta pública em novembro do mesmo ano e instituído através da Resolução nº 7, de 7 de abril de 2008.

Posteriormente, o Moreq-Jus é adotado pelo Conselho Nacional de Justiça, através da Resolução nº 91, de 29 de setembro de 2009 e serve como diretriz para o desenvolvimento de novas funcionalidades e para as modificações efetuadas no módulo de gestão documental do SIGA. Os requisitos de segurança relacionados à assinatura digital elencados entre as referências RSE 6.5.1 a RSE 6.5.7, e em particular a previsão de uso obrigatório do padrão ICP-Brasil sempre que houvesse necessidade de emprego de assinatura digital (RSE 6.5.2) enseja que, no âmbito da Justiça Federal da 2ª Região, a Corregedoria-Regional regulamente, através do Provimento nº 58, de 16 de junho de 2009, quanto à utilização de assinatura e registro eletrônicos de sentenças, decisões interlocutórias, despachos, atas de audiências, alvarás de soltura, ofícios, mandados e cartas precatórias, em autos físicos.

Ademais, a observância da Resolução nº 7/2008, do CJF, embasa a Resolução nº 18, de 16 de maio de 2011, que estabelece normas gerais de Gestão Documental da Justiça

Federal da 2ª Região, prevê o uso obrigatório do SIGA para elaboração de atos e expedientes administrativos, e a aquisição de certificado digital para todos os servidores, além de reconhecer o valor dos documentos transcritos para suporte digital mediante certificação por assinatura digital emitida por autoridade certificadora credenciada.

Decorridos quase quinze anos desde a implantação de seu processo eletrônico e a formação de um quadro especializado em gestão documental, a Justiça Federal da 2ª Região estuda a possibilidade de substituir o uso do certificado digital tipo A3 para a assinatura mediante *login* e senha e este artigo consubstancia as razões apresentadas em parecer técnico favorável a tal pretensão. O trabalho está dividido em três partes distintas: a primeira, contextualiza o momento em que há a opção pelo uso de certificado digital para a produção de documentos nos sistemas processuais, judicial e administrativo, e discorre quanto ao Modelo de Requisitos aprovado pelo Conselho da Justiça Federal para desenvolvimento de sistemas informatizados de gestão arquivística de documentos, assim como esclarece os motivos pelos quais o certificado digital foi elencado como requisito de segurança obrigatório para o documento digital produzido pela Justiça Federal de 1º e 2º grau e para o Conselho da Justiça Federal. Na segunda parte, a ênfase está no conceito de documento de arquivo e suas características e na importância da diplomática e da tipologia documental para identificar a autenticidade dos documentos. Na última parte, tomando como base os argumentos apresentados reconhece-se que documentos produzidos em um sistema informatizado desenvolvido de acordo com o modelo de requisitos para gestão arquivística de documentos e que observe os princípios de gestão documental dispensam o uso de certificado digital para garantir sua autenticidade.

2 MOREQ-JUS: requisitos para produção de documentos digitais confiáveis, autênticos e acessíveis ao longo do tempo

O Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos da Justiça Federal – MoReq-Jus, de que trata a retromencionada Resolução nº 7, de 2008, do CJF é fruto de uma iniciativa conjunta da Comissão Técnica Interdisciplinar para Gestão de Documentos da Justiça Federal – CT-GeD – e do Comitê Gestor do Sistema de Tecnologia da Informação e Comunicação da Justiça Federal – SIJUS. Ao apresentar o trabalho, o CJF (2007) enfatiza a inspiração em dois outros documentos voltados para a definição de requisitos para o desenvolvimento de sistemas informatizados de gestão arquivística de documentos: o e-ARQ Brasil, elaborado pela Câmara Técnica de Documentos

Eletrônicos – CTDE – criada pelo Conselho Nacional de Arquivos – CONARQ – e o MoReq, desenvolvido pelo Instituto dos Arquivos Nacionais/Torre do Tombo de Portugal.

Tal modelo tem os objetivos de fornecer especificações técnicas e funcionais para orientar a aquisição, detalhamento e o desenvolvimento de sistemas de gestão de processos e documentos no âmbito da Justiça Federal, assim como o de estabelecer critérios para certificação do grau de aderência ao modelo assegurar uma padronização na gestão desses documentos no âmbito da Justiça Federal. Em sua apresentação esclarece-se que:

> Uma das medidas já em curso é a adoção da infra-estrutura de chaves públicas da ICP-Brasil, que garante a aceitação do processo eletrônico por terceiros. Em complementaridade à adoção da certificação digital, outras medidas precisam ser implementadas para garantir a segurança e a preservação de longo prazo e, dessa forma, assegurar o direito à informação, albergado na Constituição Federal (CF) de 1988 (CJF, 2007, p. 8).

Dentre estas medidas complementares, está a definição de padrões de metadados, de controles de autenticidade e integridade de mídias e de normas e procedimentos que assegurem a acessibilidade, a autenticidade e a integridade dos processos eletrônicos dos Juizados Especiais Federais, das varas de execução fiscal e de outros documentos em formato digital.

No normativo, estabelece-se a obrigatoriedade da sua utilização para o desenvolvimento de novos sistemas informatizados que suportam as atividades judiciárias e as administrativas no âmbito do Conselho e da Justiça Federal. Reconhece-se que a conjugação de diversos fatores, como o gerenciamento dos sistemas informatizados pela área de tecnologia, a não participação de profissionais da área de arquivo em todas as fases de gestão dos documentos ali gerados e a falta de funcionalidades de gestão arquivística nos sistemas processuais, de forma a evitar perda ou adulteração de documentos justificam a criação e a observância do modelo criado a fim de que se possa manter a autenticidade, a confiabilidade e o acesso dos documentos digitais. Diz que, sem a gestão arquivística:

> Os requisitos de assinatura digital são necessários para as instituições que recebem documentos digitais assinados e onde são necessárias verificações de integridade e autenticidade. Nesses casos, o não-repúdio é garantido pela MP 2.200-2, de 2001, utilizando certificados digitais emitidos no âmbito da ICP-Brasil (CJF, 2008, p. 64).

No modelo, afirma-se que os sistemas informatizados da Justiça Federal de uma forma geral devem obedecer a diversas funcionalidades, dentre elas:

- Organização dos documentos (plano de classificação)

    - Para o MoReq-Jus, os documentos institucionais da Justiça Federal eram os processos judiciais e administrativos, que deveriam ser classificados por meio da Tabela Única de Classe - TUC e da Tabela Única de Assuntos – TUA, quando fossem processos judiciais ou pelo Plano de Classificação e Tabela de Temporalidade da Documentação Administrativa da Justiça Federal – PCTT. De acordo com o modelo, os sistemas informatizados deveriam ser capazes de configurar e administrar planos de classificação e tabelas, associar metadados relacionados à classificação e reclassificação dos documentos, além de controlar abertura e encerramento de volumes de processos, inclusão e desentranhamento de novos documentos, apensação, desapensação, desmembramento e consulta de processos.
- Captura
    - Previa-se dentre as ações incluídas nesta funcionalidade o protocolo, a autuação, a classificação, a indexação, a atribuição de restrição de acesso e o arquivamento. Além disso, estabeleciam-se requisitos para a captura de documentos em lote e de mensagens geradas em sistemas de comunicação eletrônica (e-mail);
- Armazenamento
    - A funcionalidade incluía requisitos para assegurar um armazenamento criterioso desde o momento da criação dos documentos, visando garantir sua preservação de longo prazo. Além disso, contemplava requisitos visando sua proteção contra o acesso não autorizado e perdas por destruição, furto ou sinistro, a escalabilidade no armazenamento, de modo a permitir a expansão ilimitada dos dispositivos de armazenamento;
- Preservação
    - Neste item incluiu-se aspectos físicos, lógicos e genéricos capazes de manter os documentos acessíveis e utilizáveis por todo o tempo que se fizer necessário, com vistas a garantir sua longevidade, funcionalidade e disponibilidade;
- Segurança
    - Estabeleceram-se controles de acesso e procedimentos de segurança voltados para a garantia da confidencialidade, da integridade e da disponibilidade dos documentos. Dentre eles, estavam a utilização de controles técnicos e programáticos, diferenciando tipos de documentos, perfis de usuários, as características a serem observadas para o acesso aos dados, a manutenção de trilhas de auditoria e de rotinas de cópias de segurança, além da observância de exigências e procedimentos relativos à infraestrutura das instalações. É nesta funcionalidade que o uso de certificado digital foi incluído como um requisito obrigatório para os sistemas informatizados da Justiça Federal. Para fins de armazenamento de dados e a recuperação de informações sigilosas foi autorizado o uso de criptografia simétrica, que se vale da mesma chave tanto para criptografar quanto para decriptografar arquivos.
    -

3 CERTIFICADO DIGITAL: estratégia de segurança da informação

Conforme já ressaltado no MoReq-Jus, a segurança é uma das funcionalidades essenciais para a produção de documentos confiáveis, autênticos e acessíveis. Com efeito, a adoção de práticas voltadas para assegurar que os ativos[2] (neles incluídos sistemas e ambientes) que produzem, transmitem, disseminam, armazenam ou descartem as informações estejam protegidos contra a violação da privacidade e do sigilo de dados e informações (quebra de confidencialidade), contra questionamentos relacionados à confiabilidade do dado ou da informação (comprometimento de integridade) e contra a indisponibilidade de seu acesso é essencial para a confiabilidade, autenticidade e acessibilidade dos documentos produzidos em um sistema informatizado. Isto porque é necessário reconhecer que, ao mesmo

[2] Segundo a norma ABNT/ISO 55.000:2014, um ativo é "um item, algo ou entidade que tem valor real ou potencial para uma organização" (ABNT, 2014)

tempo em que o uso de novas tecnologias auxilia na disseminação da informação, também aumenta o risco de alteração, subtração e até mesmo de destruição das informações. A fim de minimizá-lo, é preciso estabelecer políticas, elaborar estratégias e instituir processos voltados para garantir a confidencialidade, integridade e disponibilidade dos ativos, mantendo sempre como diretriz a finalidade do organismo ou entidade.

Como base para a segurança da informação, há um arcabouço normativo abrangente que auxilia na sua implementação. No caso do Judiciário nacional, a Resolução nº 90, de 29 de setembro de 2009, revogada pela Resolução nº 211, de 15 de dezembro de 2015, ambas do CNJ reconhece a segurança da informação como uma das atividades estratégicas dos serviços de tecnologia de informação dos órgãos do Judiciário, e orienta para que os mesmos estabeleçam e implantem políticas de segurança da informação (art. 13), assim como para que a observem na contratação ou desenvolvimento de sistemas (art. 6º).

3.1 CERTIFICADO DIGITAL

A instituição de Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, composta por uma autoridade gestora de políticas e por uma cadeia de autoridades certificadoras nelas incluídas a Autoridade Certificadora Raiz - AC Raiz, as Autoridades Certificadoras - AC e as Autoridades de Registro - AR, por meio da Medida Provisória nº 2200-2, de 24 de agosto de 2001, se propõe a garantir a autenticidade, a integridade e a validade jurídica de documentos produzidos em codificação binária e a realização de transações eletrônicas seguras.

Incumbe às Autoridades Certificadoras, que funcionam como um cartório digital, a emissão de certificados digitais vinculando pares de chaves criptográficas assimétricas que devem ser geradas pelo próprio titular do certificado e que serão utilizadas para a assinatura digital através do uso de criptografia matemática. Além disso, o uso de certificação digital assegura o não repúdio, já que é feito uso de algoritmos que requerem duas chaves, uma para o processo de cifrar e outra para decifrar o *hash* que está anexado ao documento juntamente com o certificado digital do signatário do documento.

Existem basicamente duas séries de certificados digitais que podem ser obtidas: Série A e S. Segundo Resende (2009, p. 119), a primeira está voltada para "a confirmação de identidade na Web, em e-mail, em redes privadas virtuais (VPN) e em documentos eletrônicos com verificação da integridade de suas informações" e a segunda, Série S, é utilizada para a "codificação de documentos, de bases de dados, de mensagens e de outras informações eletrônicas sigilosas". Elas diferem, além do objetivo de uso – que pode ser para assinatura digital ou para garantia de sigilo – , pelo nível de segurança e pela sua validade.

Ambas as séries possuem dois níveis distintos de certificado digital: Nível 1 e níveis 2 a 4. De uma forma bem simplificada, pode-se afirmar que as diferenças básicas entre esses níveis são a geração e o armazenamento das chaves criptográficas (arquivo digital, *token* ou cartão) e o prazo de validade dos mesmos. O primeiro certificado, nível 1, possui validade fixa de um ano e é um arquivo digital que é gerado e armazenado no computador do usuário. Já os demais certificados digitais e, em particular o A3, utilizado para confirmação de identidade do subscritor de um documento pela Justiça Federal, possui validade de um a três anos e "as chaves privadas e as informações que se referem ao seu certificado ficam armazenadas em um *hardware* criptográfico, ou seja, um *smart card* (um cartão inteligente) ou cartão de memória (*token USB* ou *pen drive*)" (RESENDE, 2009, p. 119).

Segundo o CJF (2008), um arquivo assinado digitalmente geralmente é composto do documento original, do resumo criptográfico do arquivo – *hash* – que foi submetido a uma encriptação por meio da chave privada do signatário e de seu certificado. Para identificar a integridade do documento, o receptor desempacota e verifica a validade do certificado e da cadeia de certificação. Uma vez validado o certificado, extrai-se a chave pública do signatário, aplicando-a à assinatura para decifrar se a mesma corresponde à chave privada utilizada para sua assinatura e só com o reconhecimento da autoria da assinatura é que se obtém o *hash* do documento, que é comparado com o *hash* do documento assinado.

Em decorrência do detalhado e extenso processo criptográfico que utiliza chaves assimétricas, da não participação de profissionais da área de arquivo em todas as fases de gestão dos documentos gerados nos sistemas informatizados e da falta de funcionalidades de gestão arquivística nesses sistemas, de forma a evitar perda ou adulteração de documentos, o uso de certificados digitais vem sendo apontado como estratégia para assegurar a integridade e o não repúdio dos documentos digitais e é utilizado nos últimos anos pela Justiça Federal da 2ª Região tanto no sistema processual judicial quanto no sistema administrativo de gestão de documentos, o SIGA-Doc.

Sem que haja a pretensão de menosprezar o valor do certificado digital em conformidade com o estabelecido pela Medida Provisória 2200-2, de 2001, é importante ressaltar que o mesmo não é o único recurso capaz de assegurar a integridade de um documento digital, embora se deva reconhecer que o maior mérito pelo seu uso é o de assegurar o não repúdio aos atos por ele chancelados, já que os procedimentos elencados no diploma legal se equivalem à autenticação por autenticidade procedida em cartório.

4 AUTENTICIDADE: normas processuais civis

Ao discorrer sobre arquivos permanentes, Bellotto (2006) ressalta que a redação de atos formais jurídicos e administrativos acarreta o surgimento de organizações burocrático-governamentais, a construção das bases do direito público e o crescimento e especialização de chancelarias, secretarias e de tabeliães responsáveis pela produção, registro e garantia da autenticidade de um documento, a partir da observância de padrões – denominados fórmulas diplomáticas – e de procedimentos preestabelecidos.

De outra parte, Rodrigues [20--?] esclarece que, segundo as normas legais brasileiras, incumbe ao tabelião de notas ou notário o reconhecimento de firma, que tem o condão de atribuir e conferir credibilidade e autenticidade às assinaturas apostas em documentos. Segundo o autor, na modalidade de reconhecimento de firma por autenticidade, o interessado é identificado e sua assinatura é lançada no documento na presença do notário ou de seu preposto e o ato é descrito em livro próprio no qual são lavrados os termos de comparecimento das partes com a inclusão da qualificação da parte, do ato de apresentação do documento original, da indicação do local, da data e da natureza do ato e com a coleta de amostra da assinatura em ficha-padrão que ficará custodiada no cartório. Segundo o art. 369 do Código de Processo Civil – CPC, de que trata a Lei nº 5869, de 11 de janeiro de 1973, o reconhecimento do tabelião de que o documento foi assinado em sua presença assegurava a sua autenticidade.

Relevante destacar a ampliação das possibilidades de autenticidade de documentos promovida pela Lei do Processo Eletrônico ao estabelecer em seu art. 11, § 1º que:

> Os extratos digitais e os documentos digitalizados e juntados aos autos pelos órgãos da Justiça e seus auxiliares, pelo Ministério Público e seus auxiliares, pelas procuradorias, pelas autoridades policiais, pelas repartições públicas em geral e por advogados públicos e privados têm a mesma força probante dos originais, ressalvada a alegação motivada e fundamentada de adulteração antes ou durante o processo de digitalização (BRASIL, 2006b, p. 1).

Com a entrada em vigor do novo CPC, a autenticidade de um documento, de acordo com o seu art. 411, passou a poder ser assegurada de três formas: por meio do reconhecimento da firma do signatário pelo tabelião, por outro meio legal de certificação e quando não houver impugnação da parte contra quem foi produzido o documento.

Pode-se afirmar, portanto, que na realidade atual, além das hipóteses de reconhecimento de firma realizado pelo tabelião e pelo uso de seu equivalente digital, que é a

assinatura por meio de certificado digital, a autenticação do documento pode ocorrer pela sua aceitação pela parte capaz de impugná-lo, ou seja, a autenticidade de um documento decorre não apenas de um ato chancelado por autoridade competente – seja ela um tabelião notarial ou certificado digital –, mas também resulta da presunção de autenticidade conferida pela parte oposta, que assegura força probante a um documento.

E é o estudo da observância de procedimentos para produção, registro e atesto da autenticidade de um documento para assegurar a fidedignidade de determinados documentos medievais que enseja o surgimento da **diplomática**, como ciência documentária.

5 AUTENTICIDADE: objeto de estudo da diplomática e da tipologia documental

Conforme ressaltado por Bellotto (2006), a diplomática surge com a denominada **guerra diplomática,** travada no século XVII entre jesuítas e beneditinos, e teve o intuito de distinguir documentos falsos daqueles que efetivamente asseguravam privilégios, bens e propriedades eclesiásticas. A diplomática é fruto do estudo do beneditino Jean Mabillon, que resultou no clássico *De Re Diplomatica libri VI*, publicado em 1681, no qual se apresentava os diferentes tipos de escrita medieval e de manuscritos para afastar questionamentos do jesuíta Daniel de Papenbroeck quanto à autenticidade de documentos da ordem beneditina.

Segundo a autora, um "documento público é, invariavelmente, em sua essência, a junção do *actio* (fato, ato documentado) e *conscriptio* (sua transferência para um suporte semântica e juridicamente credível)" (BELLOTTO, 2006, p. 48) e cada tipo de documento segue uma fórmula diplomática específica que observa a classificação dos atos administrativos e que confere significado jurídico ao conteúdo. Diz que:

> Documentos diplomáticos são aqueles de natureza estritamente jurídica que refletem, no ato escrito, as relações políticas, legais, sociais e administrativas entre o Estado e os cidadãos. Abrangem, portanto, quase a totalidade dos chamados documento de arquivo, já que deles são excluídas as denominadas "fontes narrativas" – inscrições, anais, crônicas, ensaios, comentários, memórias. Trata-se de documentos cujos elementos semânticos são submetidos a formas preestabelecidas. (BELLOTTO, 2006, p. 51-52).

Bellotto (2006) esclarece ainda que, enquanto a diplomática está voltada para a estrutura formal do documento, que deve observar uma identidade de construção para registro de um determinado fato, a tipologia documental, que incorpora todo o corpo teórico e metodológico da diplomática, observa também a base teórica arquivística e a lógica orgânica,

ou seja, os procedimentos observados dentro de um conjunto documental que disponha ou que cumpra uma mesma função para verificar sua autenticidade. A autora leciona que:

> Desde sua gênese, o documento, considerando-se aqui sobretudo o documento público e, mais, o diplomático, é reconhecível por sua proveniência, categoria, espécie e tipo. A gênese documental está no 'algo a determinar, a provar, a cumprir', dentro de determinado setor de determinado órgão público ou organização privada. (BELLOTTO, 2006, p. 57).

Para Bellotto (2008), o objeto e objetivos da diplomática e da tipologia documental devem ser fundidos para que se possa estudar a estrutura, a forma, a gênese e a tradição dos documentos de arquivo e seja possível classificar as espécies documentais e, a partir de sua análise, comprovar a autenticidade de um documento de arquivo.

6 DOCUMENTO DE ARQUIVO: conceito

O glossário da Câmara Técnica de Documentos Eletrônicos do Arquivo Nacional – CTDE (CONSELHO NACIONAL DE ARQUIVOS, 2010, p. 12), afirma que o **documento arquivístico** é aquele "produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência". Schellenberg (2006), por seu turno, entende que o termo documento de arquivo, tradução do termo **record**, refere-se a:

> Todos os livros, papéis, fotografias, ou outros materiais documentais, independentemente de sua apresentação física ou características, expedidos ou recebidos por qualquer entidade pública ou privada no exercício de seus encargos legais ou em função das suas atividades e preservados ou depositados para preservação por aquela entidade ou seus legítimos sucessores como prova de suas funções, sua política, decisões, métodos, operações ou outras atividades, ou em virtude do valor informativo dos dados neles contidos. (SCHELLENBERG, 2006, p. 41).

Conclui que tais documentos para serem considerados arquivos "devem ter sido produzidos ou acumulados na consecução de um determinado objetivo e possuir valor para fins outros que não aqueles para os quais foram produzidos ou acumulados". (SCHELLENBERG, 2006, p. 41)

Duranti (1994, p. 50) sustenta que os arquivos, ao longo da história, "têm representado, alternada e cumulativamente, os arsenais da administração, do direito, da história, da cultura e da informação" e que os documentos de arquivo "são as provas

primordiais para as suposições e conclusões relativas a essas atividades e às situações que elas contribuíram para criar, eliminar, manter ou modificar" (DURANTI, 1994, p. 50).

Diz que essa propriedade dos documentos de arquivo resulta da "relação especial entre os documentos e a atividade da qual eles resultam, relação essa que é plenamente explorada no nível teórico pela diplomática e no nível prático por numerosas leis nacionais". (DURANTI, 1994, p. 50-51).

7 CLASSIFICAÇÃO DOS DOCUMENTOS DE ARQUIVO

Bellotto (2006, p. 48) destaca que a diplomática acata a classificação estabelecida pelo direito administrativo que "são estipuladas pelas gradações da representatividade jurídica dos conteúdos dos documentos que nelas se enquadram" e ressalta que, conforme Manuel Vázquez, os documentos podem ser classificados em três grandes categorias: dispositivos, testemunhais e informativos. Na primeira categoria enquadram-se os documentos normativos, os de ajuste e os de correspondência. Enquadra-se em documentos normativos aqueles que são exarados em momento anterior aos atos e fatos nele implicados, os documentos pactuais se caracterizam como o acorde de vontade entre duas ou mais partes e os documentos de correspondência normalmente são aqueles que derivam de um ato administrativo e que determinam sua execução em um âmbito mais restrito de jurisdição.

Os documentos testemunhais acontecem após o cumprimento de um ato dispositivo, ou derivam de sua não observância ou se referem a observações sujeitas a relatórios. Eles podem ser de assentamento, quando registram oficialmente fatos ou ocorrências ou de comprovação que são sempre derivados dos documentos de assentamento para a finalidade de comprová-los. Já os documentos informativos tem o intuito de esclarecer questões contidas em outros documentos e auxiliam ou fundamento uma resolução.

Por seu turno, Meirelles (2011) leciona que, embora não haja uniformidade quanto à classificação dos atos administrativos, os mesmos podem ser agrupados a partir da análise de seus destinatários, em atos gerais e individuais. Avaliando o alcance dos atos administrativos, os mesmos podem ser divididos em atos internos e externos. Se observar seu objeto, em atos de império, de gestão e de expediente e considerando o seu regramento, em atos vinculados e discricionários.

Os atos gerais, normativos ou regulamentares são expedidos sem destinatários determinados e possui finalidade normativa com alcance abrangente a todos os que se encontrem na mesma situação de fato abrangida por seus preceitos. Constituem-se em "atos

de comando abstrato e impessoal, semelhantes aos da lei, e, por isso mesmo, revogável a qualquer tempo pela administração, mas inatacáveis por via judicial, a não ser pelo questionamento da constitucionalidade" (MEIRELLES, 2011, p. 174). Já os atos individuais ou especiais são dirigidos a destinatários certos e criam situação jurídica particular, gerando direitos subjetivos para os destinatários e encargos administrativos pessoais. Por conta disso, são suscetíveis de anulação pela própria administração ou pelas vias judiciais quando ilegais ou com lesão ao patrimônio público. Quando qualquer um desses atos possuem efeitos externos, dependem de publicação em veículo oficial para que entre em vigor e produza efeitos jurídicos.

Um ato administrativo é classificado como interno quando os efeitos circunscrevem-se às repartições administrativas e visa a operatividade caseira. Eles podem ser gerais ou especiais, normativos, ordinatórios, punitivos ou de outras espécies demandadas pelas exigências do serviço público. Tais atos, quando limitados ao ambiente interno, não dependem de publicação oficial para sua vigência, bastando a cientificação direta aos destinatários ou a divulgação regulamentar da repartição. Entretanto, se houver incidência sobre os administrados, é necessária a sua divulgação. Quando produzidos em seus estritos limites, não costumam direitos aos destinatários e, por conta disso, podem ser revogados ou modificados a qualquer tempo, mas se ofenderem direitos individuais ou o patrimônio público, estão sujeitos ao controle do Poder Judiciário (MEIRELLES, 2011, p. 175).

Os atos administrativos de efeitos externos normalmente provêem direitos, obrigações, negócios ou conduta perante a Administração ou estabelecem "providências administrativas que, embora não atingindo diretamente o administrado, devam produzir efeitos fora da repartição que as adotou" (MEIRELLES, 2011, p. 176). Por isto, estão sujeitos à publicidade para sua validade.

Os atos de império ou de autoridade são "aqueles que a Administração pratica usando sua supremacia sobre o administrado ou servidor e lhes impõe obrigatório atendimento" (MEIRELLES, 2011, p. 176). Já os atos de gestão são aqueles que não exigem a coerção sobre os interessados, mas se tornam vinculantes, mas que geram direitos subjetivos. Por conta de seu objeto, esses atos estão sujeitos à publicidade. Os atos de expediente são aqueles realizados para dar andamento aos processos, preparando-os para a decisão da autoridade competente e, por conta de seu objeto, não possuem forma padronizada, caráter decisório ou vinculante nem estão sujeitos a questionamento.

Os atos vinculados ou regrados são aqueles para os quais a lei estabelece requisitos e condições de sua realização que devem ser observados pela Administração, que está obrigada

a motivá-los a fim de evidenciar a sua conformação com as exigência e requisitos legais que pressupõem a sua existência e validade. Por seu turno, os atos discricionários são aqueles que a legislação facultou à Administração liberdade de escolha de seu conteúdo, de seu destinatário, de sua conveniência, de sua oportunidade e do modo de sua realização.

Deve-se lembrar, também, que os atos administrativos nascem com a presunção de legitimidade, independentemente da norma legal que a estabeleça. Demais disso, conforme enfatizado por Meirelles (2011, p. 168),

> [...] a presunção de legitimidade e veracidade dos atos administrativos responde a exigência de celeridade e segurança das atividades do Poder Público, que não poderiam ficar na dependência da solução de impugnação dos administrados, quanto à legitimidade de seus atos, para só após dar-lhes execução, Já a presunção de veracidade, inerente à de legitimidade, refere-se aos fatos alegados e afirmados pela Administração para a prática do ato, os quais são tidos e havidos como verdadeiros até prova em contrário. A presunção também ocorre com os atestados, certidões, informações, atos registrais e declarações da Administração, que, por isso, gozam de fé pública (MEIRELLES, 2011, p. 168-169).

Uma das consequências da presunção de legitimidade e veracidade dos atos administrativos é a transferência do ônus da prova de invalidade do ato administrativo para quem o invoca a fim de demonstrar sua nulidade em decorrência de vício formal, ideológico ou de motivo. Com isso, uma vez completado o "procedimento formativo, o ato adquire existência legal, tornando-se eficaz e vinculativo para a Administração que o expediu, porque traduz a manifestação de vontade administrativa em forma regular" (MEIRELLES, 2011, p. 169).

Entretanto, a partir da produção crescente de documentos digitais tal presunção não foi mantida ante a admissão de sua fragilidade e volatilidade e do fracasso dos desenvolvedores dos sistemas em observar normas de gestão documental. Com isso, a assinatura com certificado digital Tipo A3 passa a ser a estratégia adotada para assegurar a integridade dos documentos digitais. Para o CJF (2007) não estava claro que a diplomática, criada para validar documentos medievais, a tipologia documental, desenvolvida para avaliação de documentos físicos e os princípios arquivísticos continuavam a ser as mais completas e abrangentes ferramentas para a validação de documentos arquivísticos e buscou-se na assinatura digital solução para enfrentar o desafio enfrentado.

8 AUTENTICIDADE: característica de documentos de arquivo

Conforme ressaltado por Bellotto (2006), a autenticidade de um documento vem sendo objeto de estudo sistematizado desde a criação da diplomática e foi intensificado com a análise da tipologia documental, que agrega as premissas da diplomática com a observância da lógica orgânica de um conjunto documental com vistas a identificar um documento de arquivo independente do suporte em que foi produzido.

Por outro lado, Luciana Duranti (1994, p. 50) afirma que a dependência de *hardware* e *software* para manifestação dos documentos digitais e a dificuldade dos profissionais de tecnologia da informação em compreenderem a natureza e finalidade dos documentos é preciso buscar no cerne dos princípios teóricos arquivísticos as garantias de autenticidade dos documentos que servem como prova de ação.

8.1 Autenticidade: uma das características do documento de arquivo

Segundo Duranti (1994), os documentos de arquivo possuem dois pressupostos fundamentais, quais sejam, eles atestam ações e transações e sua veracidade depende das circunstâncias de sua criação e preservação. Leciona ainda que os documentos arquivísticos possuem algumas características específicas, dentre elas, a imparcialidade, a naturalidade, o inter-relacionamento, a unicidade e a autenticidade.

A imparcialidade permite reconhecer que os documentos arquivísticos são "inerentemente verdadeiros" e que as razões pelas quais eles foram produzidos e as circunstâncias de sua criação garantem que não foram redigidos para a posteridade, trazendo consigo uma "promessa de fidelidade aos fatos e ações que manifestam e para cuja realização contribuem" (DURANTI, 1994, p. 51). A naturalidade diz respeito "à maneira como os documentos se acumulam no curso das transações de acordo com as necessidades da matéria em pauta" (DURANTI, 1994, p. 52).

O inter-relacionamento permite reconhecer que "os documentos estabelecem relações no decorrer do andamento das transações e de acordo com suas necessidades", podendo-se concluir que os mesmos "são interdependentes no que toca a seu significado e sua capacidade comprobatória" (DURANTI, 1994, p. 52). Já a unicidade assegura que cada documento "assume um lugar único na estrutura documental do grupo ao qual pertence e no universo documental" (DURANTI, 1994, p. 52).

Finalmente, a autenticidade, tema central deste tópico, está "vinculada ao **continuum** da criação, manutenção e custodia" (DURANTI, 1994, p. 51). Para o projeto InterPARES 2 (2018), a autenticidade se traduz na "credibilidade de um documento de arquivo como tal, isto é, a qualidade de um documento de arquivo que é aquilo que se propõe a ser e que está livre de adulteração ou corrupção"[3] (tradução nossa).

Duranti (2005, p. 11) enfatiza que há uma importante distinção entre autenticidade e autenticação. Diz que, enquanto a autenticidade é uma propriedade do documento que o acompanha enquanto ele existir, a autenticação é um meio de provar que o documento é o que parece ser num determinado momento, podendo ser definida como uma declaração de autenticidade resultante tanto da inserção como do acréscimo ao documento de um elemento ou de uma afirmação. Por conta disto, a definição de autenticidade para a Arquivística Contemporânea passa a ser dividida em dois componentes:

- Identidade – refere-se aos atributos de um documento que o caracterizam como único e o distinguem dos outros documentos
- Integridade – é a completude e o poder de prova de um documento e pode ser demonstrada pela evidência encontrada na aparência do documento, nos metadados a ele relacionados ou em um ou mais de seus contextos.

De acordo com Duranti (2005), para avaliar a autenticidade de um documento digital é preciso estabelecer sua identidade e demonstrar sua integridade, por meio do reconhecimento da presença de certas condições ou requisitos de autenticidade, durante o processo de avaliação do documento e que tal processo de avaliação requer a compreensão de conceitos, como os de documento arquivístico e de autenticidade, além de princípios arquivísticos capazes de garantir sua identidade e integridade, protegendo-o de futuras mudanças tecnológicas, além de produzir regras que determinem a responsabilidade e os meios de sua autenticação em similaridade com os procedimentos estabelecidos para o documento em papel.

Considerando todos os argumentos até aqui apresentados pode-se afirmar que a assinatura de um documento digital com o uso de certificado garante apenas uma parte da autenticidade, ou seja, a integridade do documento, não sendo estratégia capaz de assegurar a confiabilidade, a autenticidade e a acessibilidade do documento arquivístico digital.

[3] "The trustworthiness of a record as a record; i.e., the quality of a record that is what it purports to be and that is free from tampering or corruption".

9 IMPORTÂNCIA DE UM SIGAD COM NORMAS DE GESTÃO DOCUMENTAL

Conforme já mencionado anteriormente, os modelos de requisitos de gestão arquivística de documento elencam requisitos obrigatórios e desejáveis para desenvolvimento de sistemas informatizados que venham a produzir, tramitar, armazenar e proceder à destinação final dos documentos ali produzidos. Ao longo dos anos, vem sendo concebidos diversos modelos com o intuito de assegurar que a alteração semântica, de suporte e de procedimentos resultantes da adoção de ferramentas tecnológicas não inviabilize a gestão dos documentos e que garanta sua confiabilidade, autenticidade e acessibilidade pelo tempo necessário para sua retenção.

O SIGA-Doc, módulo de gestão de documentos do Sistema Informatizado de Gestão Administrativa da Justiça Federal da 2ª Região e que já foi apresentado no V Congresso Nacional de Arquivologia. Na ocasião, esclareceu-se que o sistema é um software livre e de código aberto que foi projetado e implantado por servidores públicos federais, o que garante um completo controle sobre o sistema e a total independência de terceiros. Enfatizou-se que o sistema pode ser utilizado por qualquer órgão interessado, uma vez que foi concebido para ser um sistema nacional de gestão de documentos e pode ser facilmente adaptado a qualquer sistema de RH e às necessidades específicas de cada órgão.

É certo ainda que, embora tendo sido desenvolvido em época anterior ao MoReq-Jus, vem sofrendo desde 2014 melhorias tanto para aumentar sua aderência aos modelos de requisitos como e-Arq e MoReq-Jus, como foi o caso da incorporação do módulo de gestão de identidade, que gerencia a autenticação e controle de acesso de usuários e suas senhas, além de armazenar informações históricas e produzir diversos relatórios relevantes. Ultimamente, as modificações são resultado de especificações apresentadas por profissionais da área de gestão documental, visando à inserção de princípios e de procedimentos típicos da área. Com isso, cada vez mais se aumenta sua aderência ao modelo aprovado pela Justiça Federal, que atualmente gira em torno de 90%. Frise-se que, atualmente, o SIGA-Doc possui mecanismos e metadados que asseguram tanto a proveniência quanto a organicidade dos documentos nele produzidos, permitindo que a autenticidade de um documento ali produzido possa ser averiguada não apenas pela estrutura de dados que compõem cada unidade documental como também a partir do registro da relação orgânica de um conjunto documental. Isso faz com que se possam verificar os atributos que tornam um documento de arquivo único e os elementos que comprovam que o mesmo foi produzido dentro de um contexto que o legitima. Através de estratégias tecnológicas e procedimentais, é possível assegurar a unicidade e o inter-

relacionamento entre unidades e conjuntos documentais. Considerando que o sistema é utilizado para o registro diário das atividades desenvolvidas, tem-se que a naturalidade e a imparcialidade dos documentos estão naturalmente asseguradas.

Pode-se afirmar, igualmente, que os metadados que evidenciam a relação orgânica do conjunto documental acrescidos dos metadados descritivos e administrativos a ele vinculados atuam como registros incontestes tanto da sua identidade quando da sua integridade já são sozinhos capazes de assegurar a autenticidade dos documentos, independente de constituírem atos dispositivos, testemunhais ou informativos.

Além disso, o sistema possui funcionalidades que permitem o encaminhamento dos documentos dispositivos para publicação em veículo oficial – seja o e-DJF2R ou o Boletim Eletrônico – a fim de dar publicidade sobre os mesmos, com inserção de metadados comprobatório do ato. Em alguns casos específicos, os atos normativos e os de ajuste firmados com um dos órgãos da Justiça Federal da 2ª Região podem ainda ser encaminhados para o Diário Oficial da União, para dar cumprimento a normas legais específicas.

10 CONSIDERAÇÕES

O presente trabalho visa justificar as razões pela qual a assinatura digital com uso de certificado do Tipo A3 pode ser dispensada em um sistema informatizado de gestão de documentos que atenda grande parte dos requisitos do modelo concebido pelo CJF (2007), como é o SIGA-Doc. No artigo, busca-se evidenciar que a obrigatoriedade do requisito de segurança reflete tanto a falta de gestão documental nos sistemas quanto o desconhecimento dos desenvolvedores quanto às características dos documentos de arquivos. Esclarece-se que tanto os controles estabelecidos pelo módulo de gestão de identidade, quanto a inclusão de diversas outras funcionalidades com foco na aderência ao MoReq-Jus asseguram a produção de documentos mais confiáveis, autênticos e acessíveis. Demais disso, a inserção de metadados que asseguram a proveniência, a organicidade, a unicidade, a integridade e a cumulatividade conforme parâmetros estabelecidos por arquivistas tornam dispensável o uso de estratégia tecnológica voltada para garantia da integridade dos documentos.

No mais, tem-se que a publicação de documentos normativos e de ajustes em veículo digital eletrônico nos moldes estabelecidos em preceitos legais leva a uma conclusão de que, ainda que o uso de certificado digital constitua um requisito de segurança previsto no MoReq-Jus, a assinatura com uso de certificado digital constitui um requisito obrigatório que pode ser

flexibilizado para se adequar às conveniências econômicas e procedimentais de cada administração.

REFERÊNCIAS

ABNT, N. NBR ISO 55000 : 2014. **Gestão de ativos:** visão geral, princípios e terminologia. São Paulo: ABNT, 2014.

ARQUIVÍSTICA, DICIONÁRIO BRASILEIRO DE TERMINOLOGIA. Rio de Janeiro: Arquivo Nacional, 2005. 232p.; 30cm. Publicações Técnicas, n. 51.

BELLOTTO, Heloísa Liberalli. **Arquivos permanentes**: tratamento documental. 4. ed. Rio de Janeiro: Editora FGV, 2006.

BELLOTTO, Heloísa Liberalli. **Diplomática e tipologia documental em arquivos**. Brasília: Briquet de Lemos, 2008.

BRASIL. **Lei nº 8.159, de 8 de janeiro de 1991**. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L8159.htm >. Acesso em: 25 out. 2013

_____. **Lei nº 11.280, de 16 de fevereiro de 2006**. Altera os arts. 112, 114, 154, 219, 253, 305, 322, 338, 489 e 555 da Lei nº 5.869, de 11 de janeiro de 1973 - Código de Processo Civil, relativos à incompetência relativa, meios eletrônicos, prescrição, distribuição por dependência, exceção de incompetência, revelia, carta precatória e rogatória, ação rescisória e vista dos autos; e revoga o art. 194 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil. 2006a. Disponível em: <http://www2.camara.leg.br/legin/fed/lei/2006/lei-11280-16-fevereiro-2006-541113-publicacaooriginal-43397-pl.html > Acesso em: 10 jun. 2018.

_____. **Lei nº 11.419, de 19 de dezembro de 2006**. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. 2006b. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm > Acesso em: 10 jun. 2018.

CONSELHO DA JUSTIÇA FEDERAL. Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos da Justiça Federal - MoReq-Jus. Brasília: CJF, 2007

CONSELHO NACIONAL DE ARQUIVOS. Câmara Técnica de Documentos Eletrônicos. **Glossário**. Rio de Janeiro: Arquivo Nacional, 2010. Disponível em: < http://www.documentoseletronicos.arquivonacional.gov.br/media/publicacoes/glossario/2010glossario_v5.1.pdf >. Acesso em: 12 out. 2013.

DURANTI, Luciana. Registros documentais contemporâneos como provas de ação. **Revista Estudos Históricos**, v. 7, n. 13, p. 49-64, 1994.

_____. Rumo a uma teoria arquivística de preservação digital: as descobertas conceituais do projeto InterPARES. **Revista Arquivo & Administração**, Rio de

Janeiro, v. 4, n. 5, p. 5-18, jan./jun. 2005.

INTERPARES 2 PROJECT. **Glossary**. Disponível em: < http://www.interpares.org/ip2/display_file.cfm?doc=ip2_glossary.pdf&CFID=16563396&CFTOKEN=90961120 >. Acesso em: 29 jun. 2018.

MEIRELLES, Hely Lopes. **Direito Administrativo Brasileiro**. São Paulo: Malheiros Editores, 2011

RESENDE, Dilma A. Certificação Digital. **Revista Jurídica UNIGRAN.** Dourados, MS, v. 11, n. 22, 2009.

RODRIGUES, Felipe Leonardo. O reconhecimento de firma, letra, chancela e da autenticação de cópias. **Colégio Notarial do Brasil – Conselho Federal** [20--?] Disponível em: < http://www.notariado.org.br/index.php?pG=X19leGliZV9ub3RpY2lhcw==&in=MzM4NQ==&filtro=9&Data= > Acesso em: 1 jun. 2018

SCHELLENBERG, Theodore Roosevelt. **Arquivos modernos**: princípios e técnicas. 6. ed. Rio de Janeiro: Editora FGV, 2006.

TAKAHASHI, Tadao. **Sociedade da informação no Brasil**: livro verde. Ministério da Ciência e Tecnologia (MCT), 2000.