

PROCESSO JUDICIAL ELETRÔNICO: ANÁLISE DA
LEI N.º 11.419/2006 SOB A ÓTICA ARQUIVÍSTICA

*ELECTRONIC LAWSUIT: ANALYSIS OF THE LAW N° 11.419/2006
UNDER THE ARCHIVAL VIEW*

MATEUS DE MOURA RODRIGUES¹ E DANIEL FLORES²

Recebido em: 27/06/2013
Aprovado em: 26/09/2014

RESUMO

O presente artigo apresenta uma abordagem do Processo Judicial Eletrônico, modalidade processual que tem como premissa a desburocratização e agilidade no trâmite, trazendo uma nova perspectiva para os usuários e profissionais envolvidos. O advento da Lei n.º 11.419/2006 teve a finalidade de padronizar a implementação do processo eletrônico em todo o Brasil. Porém, sabe-se que todo trâmite de informação reflete diretamente no fazer arquivístico e, neste caso específico, envolve mudanças de paradigma. Assim sendo, este estudo teve como objetivo analisar as práticas processuais que ocorrem por meio eletrônico em conformidade com a legislação, verificando os preceitos arquivísticos envolvidos e o paralelo entre o processo tradicional e eletrônico, bem como realizando uma análise da Lei n.º 11.419/2006 sob a ótica arquivística. Para tanto, procedeu-se a uma revisão da literatura que abrange a temática, fazendo-se um apanhado de todos os tópicos pertinentes ao assunto. Os resultados obtidos mostraram que as práticas processuais por meio eletrônico são uma realidade no cenário jurídico e que a Lei n.º 11.419/2006 tem o papel de conduzir essa nova prática unindo-se à teoria arquivística para superar os problemas que ainda existem e buscando a efetiva gestão da informação.

Palavras-chave: Arquivologia; Processo eletrônico; Documento digital; Documentos jurídicos.

ABSTRACT

This paper presents an approach to the electronic lawsuit, procedural method that is premised to agility in the processing, bringing a new perspective for users and professionals. The enactment of Law 11.419/2006 was important to standardize the implementation of the electronic legal proceedings in Brazil. However, it's known that all processing of information directly reflected in the archives and in this particular case, involves paradigm changes. So, this study aimed to analyze the electronic legal proceedings in accordance with the law, checking the archival principles involved, the comparison between the traditional lawsuit and electronic lawsuit, and analysis of the Law 11.419/2006 under the archival view. Was performed a literature review around the topic, taking an overview of all relevant subjects and, checking the collected data, the results showed that the electronic legal proceeding is a reality in the legal scenario and the Law 11.419/2006 and archival science must to lead this new practice together, overcoming all problems that still exist and seeking effective information management.

Keywords: Archives; Electronic Lawsuit; Digital Document; Juridical Documents.

¹ Professor do curso de Arquivologia da Universidade Federal de Rio Grande (FURG), Brasil. E-mail: mateusmrodrigues@gmail.com.

² Professor do curso de Arquivologia da Universidade Federal de Santa Maria (UFSM), Brasil. E-mail: dffloresbr@gmail.com.

1 Introdução

O Processo Judicial Eletrônico é uma realidade irreversível. Tendo como intuito reduzir a morosidade do Poder Judiciário e promover agilidade no trâmite, essa modalidade cria uma nova perspectiva aos usuários acerca de sua segurança, simplicidade de uso e desburocratização. O tempo de espera, consequência de trabalhos manuais, como distribuição, autuação, juntadas de petições, cadastros e conclusões, tem a séria necessidade de minimização atendida com o advento da Lei n.º 11.419/2006.

Essa Lei, precedida por outras tantas que já visavam desburocratizar os serviços do Poder Judiciário, tem como objetivo implementar o Processo Judicial Eletrônico em todas as instâncias da Justiça em nível nacional. Após sua promulgação, cada tribunal passou a ter autonomia para padronizar e regulamentar suas funcionalidades e sistemáticas para a elaboração de normas de organização. Como consequência, uma grande variedade de práticas processuais por meio eletrônico surgiram em cada tribunal do Brasil. Esse novo cenário trouxe novas perspectivas, que estão intimamente ligadas ao fazer arquivístico, pois envolve inúmeras mudanças de paradigma.

Assim, sabe-se que as práticas processuais por meio eletrônico impulsionam o estudo aprofundado acerca da adoção de políticas arquivísticas e modelos de requisitos que nasceram da necessidade de adequação da gestão às novas tecnologias da informação. Nesse sentido, o presente estudo teve como objetivo apresentar as características dessa nova modalidade de práticas processuais, ao mesmo tempo em que investiga as suas principais prerrogativas no que diz respeito ao trâmite da informação em meio digital, verificando seus atributos no que concerne à harmonia ou colisão com os preceitos arquivísticos.

Para isso, foram abordados os preceitos jurídicos relativos ao processo judicial em si, estabelecendo-se,

também, um paralelo com o processo eletrônico, possibilitando a visualização das semelhanças e diferenças entre ambos. Esta pesquisa se baseou na teoria arquivística, focada nos conceitos de documento em suporte físico e em meio digital, bem como na visão jurídica sobre este, nas fundamentações teóricas que tangem o fazer profissional do arquivista e na legislação vigente.

2 Referencial teórico

Neste capítulo, são abordados os preceitos teóricos que fundamentam o estudo. Inicia-se pela análise do conceito de documento sob as óticas arquivística e jurídica. Após, discute-se a problemática da legitimidade do documento digital, bem como a Arquivologia e as Tecnologias da Informação. Por fim, trata-se da legislação e da segurança da informação em meio digital e do processo judicial tradicional e eletrônico.

2.1 O documento na visão arquivística e jurídica

O profissional arquivista trabalha com a gestão da informação, independente do suporte em que esta se apresenta. Nesse contexto, faz-se necessário apresentar algumas definições importantes, como o conceito de documento arquivístico.

Segundo o Glossário da Câmara Técnica de Documentos Eletrônicos, documento arquivístico é todo aquele “elaborado ou recebido no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência” (CONARQ, 2010, p. 12). Já o Dicionário Brasileiro de Terminologia Arquivística conceitua o documento como uma “unidade de registro de informações, qualquer que seja o suporte ou formato” (ARQUIVO NACIONAL, 2005, p. 73).

O documento, quando não está em seu suporte tradicional – o papel –, tem sido apresentado na literatura ar-

quivística internacional, de modo muito comum, como documento eletrônico ou documento digital. Nota-se nesse cenário que ambas as terminologias, muitas vezes, são utilizadas sem que haja distinção entre elas, ou seja, como sinônimos. Como exemplo, pode-se citar Marques (2008), que, no decorrer de sua obra, trata acerca do documento digital, usando como sinônimos documento eletrônico, documento informático ou, ainda, *ciberdocumento*. Porém, sabe-se que essa é uma visão equivocada.

De acordo com o Glossário da Câmara Técnica de Documentos Eletrônicos, documento digital é a “informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional” (CONARQ, 2010, p. 13). Já o documento eletrônico consiste na “informação registrada, codificada em forma analógica ou em dígitos binários, acessível e interpretável por meio de um equipamento eletrônico” (CONARQ, 2010, p. 13).

Assim, percebe-se que não se trata de sinônimos, pois, como define o Dicionário Brasileiro de Terminologia Arquivística, documento eletrônico pode ser conceituado, também, como um “gênero integrado por documentos em meio eletrônico, ou somente acessível por equipamentos eletrônicos, como cartões perfurados, disquetes e documentos digitais” (ARQUIVO NACIONAL, 2005, p. 75).

Partindo-se da aparência física do documento, é necessário transmutá-la para o aspecto virtual, ou seja, considerar a informação desagregada de um suporte físico, pois, como enfatiza Marques (2008), o documento digital é totalmente desvinculado do meio em que foi originalmente armazenado. O autor também entende o documento digital como uma fonte de dados ou informações gravadas em um suporte computacional, que assume a forma de uma sequência de *bits*, podendo essa mesma sequência ser transferida para outro tipo de mídia, mantendo sua integralidade,

ou seja, sem nenhuma perda. A partir daí, explicita-se a ideia de que o documento digital é constituído apenas da informação em si, podendo ela migrar de suporte sem sofrer alterações.

Na visão do Direito, Guimarães (2005, p. 20) destaca que a representação por escrito de um fato jurídico, ou manifestação de vontade juridicamente considerada, são elementos primordiais para a caracterização do documento jurídico. O documento é de cunho probatório, tendo em vista que se propõe a manifestar a verdade. Desse modo, Guimarães (2005, p. 20) destaca que prova é o elemento determinado para alcançar essa verdade, que, por sua vez, vale-se de métodos variáveis de acordo com seu objetivo.

A partir dessa visão, observa-se que não é imposto um suporte determinado para sua apreciação, podendo ser considerada como documento a informação fixada a qualquer suporte, sendo preciso, apenas, verificar a idoneidade do conteúdo. O registro do fato, tanto em meio eletrônico quanto em suporte físico, demonstra a verossimilhança entre o documento tradicional e o documento digital.

2.2 A problemática do documento digital para questões de legitimidade

Os documentos digitais atualmente estão no cerne das preocupações e discussões acerca das atividades de gestão arquivística. O Processo Judicial Eletrônico ilustra de maneira enfática esse cenário pela posição de destaque que vem tomando desde o seu advento.

Porém, existem especificidades do documento digital que preocupam a comunidade arquivística, como as questões de suscetível comprometimento da autenticidade e fidedignidade por acessos indevidos e alterações. A Diplomática, que, segundo Bellotto (2008), é uma das vertentes das ciências documentárias, tem por objetivo legitimar os documentos, submetendo-os a uma sistematização imposta pelo Direito.

De acordo com Santos (2005, p. 39), a Diplomática tem como objeto de estudo a estrutura formal dos documentos, mediante a análise de seus elementos externos (físicos) e internos (conteúdo), independente da forma documental. Duranti (1995 apud Santos, 2005, p. 40) destaca alguns dos caracteres extrínsecos e intrínsecos dos documentos tradicionais, que transmutados para o âmbito digital, caracterizam-se por:

- Extrínsecos (aparência externa) – suporte, mídia; escrita, que pode ser identificada como o *software* utilizado para produção e recuperação da informação; linguagem, representada pelo código; signos especiais e selos, que, no documento tradicional, são elementos externos de grande relevância, mas, no âmbito digital, não são usados; anotações, que podem ser incluídas no documento no momento de sua produção (autenticações de firmas ou conteúdo de cópias) e no momento de sua tramitação (despachos, marcas de controle ou locuções como “urgente”), ou anotações feitas pelo serviço de arquivo (número de registro, data de recepção ou código de localização);
- Intrínsecos (modo de apresentação do conteúdo) – protocolo, que contém o contexto administrativo da ação; texto, que contém a ação e as suas considerações; escatocolo, que indica a responsabilidade em relação ao ato documental.

Santos (2005, p. 41) ressalta que, em princípio, a mudança de paradigma do documento físico para o meio digital não acarreta problemas, pois é possível identificar os elementos intrínsecos e extrínsecos na composição dos documentos digitais. Porém, os selos, neste caso, passam a ser um elemento intrín-

seco, tendo em vista que a validação é feita por meio de técnicas informáticas, como a criptografia. As anotações, da mesma forma, passariam a ser um elemento intrínseco.

Nesse sentido, os elementos contidos nos documentos digitais são os mesmos vistos em documentos tradicionais, diferenciando-se, apenas, na forma de apresentação (nos documentos digitais os elementos aparecem armazenados na forma de metadados), como explica Rondinelli (2005, p. 59). Para a autora, como foi definido pela Tecnologia da Informação, metadados nada mais são do que informações necessárias para dar significado aos dados armazenados em um sistema de computador.

Percebe-se, então, que, de acordo com os objetivos da Diplomática, como enfatiza Rodrigues (2008), os documentos diplomáticos são de natureza jurídica, pois remetem ao poder de prova que deve acompanhar o documento, independentemente de seu suporte.

2.3 A Arquivologia e as Tecnologias da Informação

Tendo-se a tecnologia a favor da gestão documental, pode-se afirmar que a estreita relação do fazer arquivístico com a Informática ocorreu de maneira notória, pois esta é tida como uma ferramenta de uso imprescindível em todos os segmentos do trabalho, auxiliando em tarefas de organização, pesquisa e difusão de qualquer tipo de informação. Tomando-se o uso de recursos tecnológicos em meio às ciências da informação, surgiu o conceito de Tecnologia da Informação (TI), que, para Alecrim (2004), pode ser definido como um conjunto de todas as atividades e soluções providas por recursos de computação. Sua aplicabilidade engloba o Gerenciamento Eletrônico de Documentos (GED), isto é, um conjunto de tecnologias que possibilitam o armazenamento, a localização e a recuperação de informações fixadas em documentos eletrônicos.

Levando-se em conta todos os preceitos arquivísticos, a Câmara Técnica de Documentos Eletrônicos do Conselho Nacional de Arquivos (CONARQ) elaborou o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil), visando estabelecer requisitos mínimos para um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD). Nesse sentido, a *United Nations Educational, Scientific and Cultural Organization* (UNESCO), juntamente com o CONARQ, no ano de 2004, publicou a Carta para a Preservação do Patrimônio Arquivístico Digital, alertando para a possibilidade do desaparecimento do legado digital e sugerindo uma série de estratégias e políticas a fim de garantir a preservação e o acesso em longo prazo dos documentos digitais.

No que diz respeito à fidedignidade da informação, desenvolveram-se três formas de proteção com um grau de complexidade elevado: a criptografia, que consiste em um modo de escrever mensagens que possam ser compreendidas apenas por quem o autor autoriza por meio de chaves públicas ou privadas; a assinatura digital, que é um conjunto de procedimentos matemáticos que permite a comprovação da autoria de um conjunto de dados; e o certificado digital, obtido por meio de uma Autoridade Certificadora (AC) mediante verificação da identidade de um usuário e associação de uma chave a este. A Ordem dos Advogados do Brasil (OAB), por exemplo, é autorizada a atuar como autoridade certificadora, podendo fornecer certificação digital aos advogados de todo o Brasil para que estes atuem em tribunais, fóruns e varas que já possuem processos judiciais eletrônicos.

2.4 O documento digital, a legislação e a segurança da informação

No que diz respeito à legislação, o Governo Federal instituiu, por meio da Medida Provisória n.º 2.200, de 28

de junho de 2001, a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Esta assumiu a incumbência de providenciar a validação jurídica do comércio eletrônico no país, garantindo autenticidade, integridade, eficácia e validade jurídica dos documentos e dos certificados digitais.

A Medida Provisória n.º 2.200/2001 definiu o Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e Tecnologia como a Autoridade Certificadora Raiz, responsável por emitir uma chave pública para cada pessoa ou empresa que deseje possuir um certificado digital, o que torna a pessoa (física ou jurídica) apta a usar a assinatura digital em documentos digitais, dando-lhes validade jurídica. A Medida Provisória também considera os documentos eletrônicos tratados por ela como legais, desde que tenham sido produzidos com a utilização do processo de certificação disponibilizado pela ICP-Brasil.

A Lei n.º 11.419/2006, que dispõe sobre os processos judiciais eletrônicos, instituiu que documentos digitalizados produzidos pelos órgãos da Justiça, pelo Ministério Público, pelas procuradorias, pelas autoridades policiais, pelas repartições públicas e por advogados públicos e privados têm a mesma força probante dos originais. O prazo de preservação dos originais desses documentos digitalizados deve ser até o trânsito em julgado da sentença ou, quando admitida, até o final do prazo para a interposição de ação rescisória.

No âmbito da Arquivologia, o Conselho Nacional de Arquivos (CONARQ) trouxe resoluções que dizem respeito aos documentos digitais, como, por exemplo:

- Resolução n.º 20, de 16 de julho de 2004, que dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e das entidades integrantes do Sistema Nacional de Arquivos (SINAR);

- Resolução n.º 24, de 3 de agosto de 2006, que estabelece diretrizes para a transferência e o recolhimento de documentos arquivísticos digitais para instituições arquivísticas públicas;

- Resolução n.º 25, de 27 de abril de 2007, que dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil) pelos órgãos e pelas entidades integrantes do SINAR.

Além do CONARQ, outras entidades também apresentaram resoluções referentes ao trâmite de documentação em meio digital. Alguns exemplos são:

- Resolução n.º 1.020, de 2005, do Conselho Federal de Contabilidade, que dispõe sobre a escrituração contábil em forma eletrônica;

- Resolução n.º 1.821, do Conselho Regional de Medicina, que dispõe sobre a digitalização e o descarte de prontuários médicos;

- Resolução n.º 1.639, do Conselho Federal de Medicina, de 10 de julho de 2002, que dispõe da aprovação das “Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manutenção do Prontuário Médico”, possibilitando a elaboração e o arquivamento do prontuário em meio eletrônico.

A Lei n.º 9.296/1996, que trata do sigilo das transmissões de dados, proíbe a qualquer pessoa ou entidade a interceptação de mensagens digitais ou telefônicas, bem como quaisquer comunicações entre dois computadores por meios telefônicos, telemáticos ou digitais. A adulteração e a quebra de sigilo são as principais preocupações dos produtores de documentos digitais. Então, segundo Ferrère (1998 apud GUIMARÃES, 2005, p. 32), o que se busca são meios que “ofereçam uma margem de segurança razoável, adequada para beneficiar a presunção de autenticidade e veracidade”.

De acordo com Marques (2008, p. 152), a primeira maneira pensada para proporcionar segurança aos documentos digitais foi a assinatura digitalizada, que consiste em inserir no documento a ima-

gem digitalizada que reproduz a assinatura de próprio punho do autor do documento. Gandini (2001 apud MARQUES, 2008, p. 152-153) enfatiza que, por se tratar de uma imagem que pode ser utilizada inúmeras vezes, a assinatura digitalizada não pode ser considerada como forma de validar o documento, pois consiste em uma sequência de *bits* invariável, fragilizando a segurança da informação.

Marques (2008, p. 153-154) aponta também outros tipos de firmas, como, por exemplo:

- Firmas biométricas, que consistem no reconhecimento de dados do ser humano por meio de suas características físicas, como a íris, a impressão digital, o timbre de voz, o escaneamento da retina e o cálculo geométrico da face;

- Senhas, que são uma sequência de *bits* definida pelo usuário ou fornecida pelo sistema com o qual ele possui vínculo, possibilitando praticar determinados atos, mas sem oferecer a certeza de que a pessoa que está realizando a operação é realmente o dono ou alguém indevidamente apossado da senha;

- Esteganografia, que consiste em transformar um documento legível em ilegível, agregando a ele, quando decifrado, uma marca visível ao leitor, que saberia não se tratar do documento correto no caso da inexistência da marca.

Tais métodos ilustrados podem proporcionar uma maior segurança, mas ainda assim a tecnologia desenvolveu outras formas mais difíceis de serem violadas. É o caso da criptografia, da assinatura digital e do certificado digital.

O processo de criptografia dos documentos digitais tem por base um padrão denominado chave. Quando se utiliza a mesma chave para cifrar e decifrar uma mensagem, tem-se a chamada criptografia simétrica ou de chave privada, utilizada em redes fechadas (intranet) ou computadores isolados, em que o destinatário possua a mesma chave utilizada pelo remetente.

Como bem se percebe, essa característica relativa a esse tipo de criptografia implica um problema relacionado ao manejo, ao uso da chave, porque, uma vez havendo dúvida quanto à honestidade e integridade de um dos receptores da chave, o sistema, obviamente, se tornará inseguro, motivando uma imediata substituição da chave que, por seu turno, deverá ser remetida aos receptores confiáveis (MARQUES, 2008, p. 160).

Quando ocorre o uso de duas chaves distintas, uma para cifrar e outra para decifrar a mensagem, tem-se a criptografia assimétrica ou de chave pública. O referido par de chaves possui vínculo matemático entre si. Uma delas – a chave privada – fica exclusivamente em poder do proprietário do sistema, enquanto a outra – chave pública – fica disponível a todos aqueles com quem se deseja manter uma comunicação segura. Qualquer uma delas terá o poder de cifrar uma mensagem, que somente a outra poderá decifrar e vice-versa. Santos (2008) enfatiza que as chaves podem ser usadas para quatro ações: assinatura digital, identificação da assinatura digital, cifragem e decifragem.

A assinatura digital é um conjunto de procedimentos matemáticos realizados com a utilização de técnicas de criptografia, o que permite, de forma única, a comprovação da autoria de um conjunto de dados, ou seja, a assinatura digital é utilizada para garantir a integridade da informação contida no documento digital. De acordo com Alecrim (2009), a assinatura digital funciona com um conceito conhecido como função *hashing*. Essa função analisa todo o documento e, com base em um complexo algoritmo matemático, gera um valor de tamanho fixo para o arquivo. Esse valor, conhecido como “valor *hash*”, é calculado com base nos caracteres do documento. Na troca de informações, se o documento contiver qualquer alteração, haverá alteração no “valor *hash*” e o documento será considerado inválido.

Em outras palavras, baseado no número de *bits* do documento, a chave pública gera um número *hash*, que, comparado ao gerado pela chave privada, verifica a assinatura gerada. Para comprovar uma assinatura digital, é necessário calcular o resumo criptográfico do documento e decifrar a assinatura com a chave pública do remetente. Se forem iguais, a assinatura está correta, o que significa que foi gerada pela chave privada corresponde à chave pública utilizada na verificação e que o documento está íntegro. Caso sejam diferentes, a assinatura está incorreta, o que significa que pode ter havido alterações no documento.

A assinatura digital é tratada por Atheniense (2010, p. 110-111) como “assinatura eletrônica”. O autor faz menção a duas modalidades de assinatura, diferenciando-as da seguinte maneira:

a) Assinatura eletrônica com certificação digital – É o método de identificação na transmissão eletrônica com o emprego da certificação digital, que é uma tecnologia que se vale dos recursos da criptografia para garantir a integridade e autoria dos dados transmitidos por meio eletrônico e apresenta dois padrões básicos de funcionamento:

- criptografia por chave privada: o emissor e o receptor da mensagem possuem a mesma chave, que serve simultaneamente para codificá-la e decodificá-la;

- criptografia com chave pública: baseia-se em um sistema criptográfico assimétrico que utiliza uma “chave pública” e uma “chave privada”, sendo que a primeira descodifica as mensagens encriptadas com a segunda.

[...]

b) Assinatura eletrônica sem certificação digital – Essa espécie de assinatura eletrônica não possui a mesma credibilidade, justamente em razão da ausência das características tecnológicas mencionadas do Certificado Digital. Várias vezes, a identificação se faz por meio de uma identificação

peçoal (*login*) e uma senha. Os dados assinados eletronicamente com esse recurso trafegam na rede sem criptografia e, por esse motivo, podem ser interceptados e alterados sem deixar vestígio de qualquer adulteração. (ATHENIENSE, 2010, p. 110-111).

Assim, pode-se afirmar que a assinatura digital é uma ferramenta que atesta integridade e a autoria do documento digital.

Já o certificado digital contém a chave pública do usuário e os dados necessários para informar sua identidade. Esse certificado pode ser distribuído na *internet*. Com isso, uma pessoa ou instituição que queira comprovar a assinatura digital de um documento pode obter o certificado digital correspondente. É importante ressaltar que certificados digitais não são usados apenas em conjuntos com assinaturas digitais e que a transmissão de certificados digitais deve ser feita por meio de uma conexão segura, como as que usam o protocolo *Secure Socket Layer* (SSL), que é próprio para o envio de informações criptografadas. O certificado digital cumpre a função de associar uma pessoa ou entidade a uma chave pública. A esse respeito, Rocha (2011) enfatiza o fato de que a certificação digital é um documento válido para qualquer ato da vida civil, isto é, de posse do certificado digital e senha, pode-se realizar quaisquer tipos de negócios jurídicos.

Quanto aos tipos de certificado que a ICP-Brasil oferece aos seus usuários finais, Atheniense (2010, p. 116) diferencia oito, sendo quatro relacionados à assinatura digital (A1, A2, A3 e A4) e quatro relacionados ao sigilo (S1, S2, S3 e S4). O autor explica que, dos referidos tipos de certificados, os dos tipos A1 e S1 são associados a um grau menor de rigorosidade, enquanto os dos tipos A4 e S4 são do mais alto grau de rigorosidade. Assim:

Certificados dos tipos A1, A2, A3 e A4 são utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações. Certificados de tipos S1, S2, S3 e S4 são utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo (ATHENIENSE, 2010, p. 117).

Atheniense (2010, p. 118) menciona, ainda, que, no dia 5 de setembro de 2008, foi publicado no Diário Oficial da União que a Ordem dos Advogados do Brasil (OAB) estava autorizada a atuar como autoridade certificadora, podendo fornecer certificação digital aos advogados de todo o Brasil para que estes atuem em tribunais, fóruns e varas que já possuem processos judiciais eletrônicos. Em relação a esse certificado, o mesmo é do tipo A3, o que significa que se trata de uma certificação digital de alto padrão de segurança e confiabilidade.

2.5 O processo judicial tradicional e eletrônico

O processo é o meio de ligação do Poder Judiciário com a sociedade. Nesse sentido, Cintra (2003, p. 41) aborda sua instrumentalidade, discorrendo sobre todos os obstáculos ao livre acesso à Justiça e sobre o dever de cumprir todas as exigências formais sob pena de invalidade dos atos.

As inovações tecnológicas precisam ser absorvidas no âmbito processual, e a integridade sistêmica do Direito deve ser preservada. Para isso, as balizas para tal renovação e avanço do procedimento judicial têm sido expressas na Lei n.º 11.419/2006. Essa Lei estabelece diretrizes a todas as instâncias do país para a informatização do processo e tem vistas à redução de despesas, à minimização do tempo de trâmite e à eliminação do papel como meio físico.

Quanto à Lei em questão, Athe-

niense é enfático ao afirmar que a obrigatoriedade da utilização da tecnologia no Poder Judiciário é uma questão de tempo:

Ainda que, *a priori*, tal dispositivo legal estabeleça caráter meramente autorizativo quanto ao uso do processo eletrônico pelos tribunais, entendemos que este é um caminho que, em poucos anos, se tornará obrigatório, não somente pela necessidade de evolução tecnológica do judiciário, mas, principalmente, pelo agravamento de sua incapacidade de absorver a crescente demanda pela prestação jurisdicional, que acarreta excessiva e danosa morosidade na resolução dos litígios judiciais. (ATHENIENSE, 2010, p. 25).

Nesse sentido, com a Lei n.º 11.419/2006 servindo como base para uma nova perspectiva de processo judicial, cabe aos órgãos competentes do Poder Judiciário desenvolver sistemas e soluções informáticas que venham ao encontro dos fundamentos arquivísticos e promovam uma grande mudança cultural, de modo a minimizar os impactos e consolidar de maneira positiva a implementação dessa nova tecnologia, que é uma ferramenta a serviço do instrumento processual. Portanto, sua incorporação deve ser feita resguardando-se os princípios do processo e os seus objetivos.

Para tanto, a Resolução n.º 91, de 29 de setembro de 2009, do Conselho Nacional de Justiça (CNJ), instituiu o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (MoReq-Jus), que dispõe sobre o desenvolvimento e a manutenção de sistemas informatizados para as atividades judiciais e administrativas no âmbito do Poder Judiciário. A elaboração desse modelo foi consequência da necessidade de se estabelecerem requisitos que garantissem a confiabilidade, a autenticidade e a acessibilidade aos documentos geridos pelos sistemas informatizados do Poder Judiciário.

Assim, percebe-se que todos os avanços técnicos nas áreas gerais de tratamento da informação, atuais ou futuros (geração, armazenamento e transmissão/comunicação), já são uma realidade agregada ao Poder Judiciário, mas sem ensejar violações aos seculares princípios do processo e aos objetivos para os quais foi estabelecido o mecanismo processual.

3 Método

A presente pesquisa visa abordar a nova realidade do Processo Judicial Eletrônico sob a perspectiva dos seus princípios, incorporando a visão do profissional arquivista no que diz respeito às suas particularidades frente ao processo judicial tradicional em meio físico.

De acordo com o que Silva e Menezes (2005) postulam em sua obra, este estudo é de natureza aplicada, pois visa gerar conhecimentos para aplicação prática, envolvendo verdades e interesses locais. Também se caracteriza pela abordagem qualitativa, não utilizando dados estatísticos como base de análise. No que diz respeito aos seus objetivos, a pesquisa é exploratória e tem o intuito de explicitar um determinado problema, abordando o universo do mesmo. Do ponto de vista dos procedimentos técnicos, pode ser considerada como uma pesquisa bibliográfica, visto que faz uso de publicações técnicas na área da Arquivologia e do Direito e de literaturas que abordem a temática proposta.

A obtenção dos resultados ocorreu mediante o uso de fichamentos como instrumento de coleta de dados. Esse processo auxiliou, também, na análise das publicações consultadas, possibilitando a aproximação desejada entre a teoria e a prática. Após a compilação, análise e compreensão dos dados coletados, foi possível chegar aos resultados que serão apurados e discutidos no capítulo seguinte.

4 Apresentação e discussão dos resultados

Neste capítulo, são expostos os resultados da pesquisa, de modo a contemplar e discutir as práticas processuais em meio eletrônico e analisar a Lei n.º 11.419/2006 sob a ótica arquivística.

4.1 As práticas processuais por meio eletrônico

No novo modelo de processo, a petição inicial pode ser rapidamente ajuizada por via eletrônica, juntamente com todos os documentos necessários digitalizados, de modo que, ao ingressar no sistema, é automaticamente distribuída, sendo-lhe atribuída uma identificação numérica. Desse modo, a petição já estará disponível para ser imediatamente analisada pelos assessores do juiz, podendo estes sugerir o modelo padrão de despacho que, ao ser acordado pelo magistrado, será assinado digitalmente. Nota-se, nesta fase, que a peça processual não passa por nenhum protocolo e, consequentemente, não existe a necessidade de submeter-se ao trato humano. A esse respeito, Clementino (2009, p. 88) enfatiza que até essa etapa todos os atos processuais podem ser concretizados em apenas um dia, o que, no processo tradicional, seria impossível.

Madalena (2007), ao vislumbrar um procedimento simulado de uma ação de mandado de segurança, contemplando todos os recursos possíveis, apontou as múltiplas tarefas que um sistema informatizado pode realizar automaticamente e com a mínima interferência humana, graças à riqueza de ferramentas disponíveis para o desenvolvimento de sistemas que automatizam o processo judicial. Assim, percebe-se que é possível, nessa modalidade, ter o tempo de trâmite minimizado no processo como um todo, além de diminuir o acúmulo que aguarda a efetivação de cada um dos atos processuais.

4.2 Análise da Lei n.º 11.419/2006

Já no artigo 1º, a Lei n.º 11.419/2006 trata dos documentos que compõem o processo eletrônico e de sua transmissão, escolhendo a *internet* como via preferencial para a remessa de documentos por meio dos respectivos *websites* de cada órgão judiciário. A escolha dessa via de transmissão trouxe à tona algumas preocupações acerca da segurança e confiabilidade das informações que tramitam. Ressalta-se, no entanto, que essa Lei faz indispensável uma infraestrutura de segurança que dê o devido suporte a todos os requisitos de integridade dos documentos remetidos ao processo eletrônico.

A manifestação nos atos processuais pressupõe que deve haver veracidade em relação ao signatário. Assim, torna-se indispensável o uso da assinatura digital para identificação inequívoca do signatário. Nesse sentido, quesitos referentes à fidedignidade dos documentos que tramitam eletronicamente também estão presentes no texto da Lei n.º 11.419/2006, como é destacado por Rossi ao discorrer sobre o artigo 11:

[...] o art. 11 predispõe que “os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia de origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais”. Estes dispositivos são complementados por uma série de outros, que regulam a transmissão de peças processuais, a comunicação de atos processuais (procedimentos de citação e intimação), a digitalização e conservação de documentos e outros aspectos da tramitação do processo eletrônico. A Lei 11.419/2006, portanto, adota como linha de princípio a validade de todas as atividades necessárias à implantação de um processo totalmente eletrônico. Todas as leis precedentes a ela tiveram algum tipo de valia, mas se limitaram a tentar informatizar fases, atos ou aspectos específicos do

trâmite processual. Doravante, todo e qualquer ato processual realizado por meio eletrônico recebe a presunção legal de validade se realizado exclusivamente por esse meio (ROSSI, 2009, p. 17).

Sabe-se que, ao se tratar de documento eletrônico, este terá seu valor probante somente a partir de certificação digital. Logo, ao fazer uso de um meio eletrônico para o envio de documentos, deve-se contar com um sistema que permita a verificação de sua fidedignidade.

Diante disso, Rocha (2011) discorre sobre o uso da assinatura digital e da certificação digital, afirmando que ambas estão interligadas. De ordem prática, o autor menciona como exemplo o caso do uso desses instrumentos nas práticas processuais por meio eletrônico em face de discussões e decisões judiciais que negam a validade de documentos recebidos no processo eletrônico que não contenham a assinatura do advogado digitalizada. Porém, o autor também frisa que existe uma diversidade de decisões acerca da validade e aceitação, que depende do tribunal ao qual está sendo remetido o documento em questão. Nesse sentido, pode-se observar uma das deficiências do processo eletrônico, que é a falta de uniformidade dos procedimentos em nível territorial e de uma padronização acerca da aceitação de determinados métodos de validação dos documentos no Processo Judicial Eletrônico.

No que concerne aos documentos digitalizados, ao analisar o artigo 11 da Lei n.º 11.419/2006, Atheniense (2010, p. 219) alerta para a questão da preservação dos originais produzidos em suporte físico que foram digitalizados e transmitidos eletronicamente a um determinado processo, afirmando que esses originais devem ser “preservados pelos detentores até o trânsito em julgado da sentença ou até o prazo final para a interposição da ação rescisória,

quando esta for cabível”. Ora, preservar o original em meio físico é uma precaução contra fatores de risco apresentados pelo meio eletrônico. Um desses fatores e talvez o mais preocupante de todos, é a obsolescência, ou seja, o contexto tecnológico que torna vulnerável todo e qualquer material digital. Esse fator gera uma total dependência que deve ser pensada ao realizar-se o descarte dos originais em suporte físico depois de passado o prazo previsto pela Lei.

Cabe à instituição pensar em soluções que agreguem procedimentos de preservação aos documentos digitais e garantam acesso a estes em qualquer tempo. Nesses casos, algumas das soluções mais plausíveis consistem no uso de formatos abertos e no contínuo refrescamento de suportes de armazenamento, além de outras estratégias de preservação digital que possam ser implementadas a tais documentos. Segundo Santos (2005, p. 64), tal solução visa manter o material digital compatível com tecnologias da época.

Em relação aos sistemas de tráfego de documentos para o processo eletrônico, Rossi explicita que:

O art. 8º [...] traz regra destinada a materializar, na prática, a possibilidade autorizada pela Lei da formação de um processo completamente digitalizado, sem qualquer peça ou ato registrado em suporte físico, como o papel, ao estabelecer que “os órgãos do Poder Judiciário poderão desenvolver sistemas eletrônicos de processamento de ações judiciais por meio de autos total ou parcialmente digitais, utilizando, preferencialmente, a rede mundial de computadores e acesso por meio de redes internas e externas” (ROSSI, 2009, p. 17).

Sobre a uniformização das ferramentas de transmissão empregadas no processo eletrônico, a autora também menciona que muito já foi alcançado na unidade da legislação processual no Brasil. Apesar disso, a padronização

ainda não é uma realidade, mas uma necessidade. Isso fica evidenciado uma vez que, embora o artigo 3º da Lei n.º 11.419/2006 preveja a possibilidade da criação de um cadastro único para credenciamento dos usuários, o que se nota é que cada tribunal opta por desenvolver seu próprio sistema para a tramitação de atos processuais.

Rocha (2011) critica esse cenário, enfatizando o quão preocupante é o fato de não haver padronização das ferramentas do processo eletrônico:

Não temos padronização nem para enviar os arquivos para o judiciário. Cada Estado quer de um jeito. Cada Estado tem um tamanho diferente. Só nisto já temos um problema de padronização e gestão. Além disto, temos regulamentos que definem pontos diferentes (como a assinatura digital) de maneira totalmente diversa no país todo (ROCHA, 2011).

O artigo 14 da mesma Lei determina os requisitos tecnológicos para o desenvolvimento de sistemas para uso dos órgãos do Poder Judiciário. Conforme análise de Atheniense (2010, p. 232-233), esses requisitos devem priorizar a padronização e o acesso, tendo como diretrizes o uso de código aberto, o acesso ininterrupto nos *websites* em que estarão armazenadas as práticas processuais eletrônicas e a obrigatoriedade de os sistemas serem desenvolvidos com a capacidade de identificar os casos de ocorrência de prevenção, litispendência e coisa julgada. Nota-se que a obrigatoriedade do uso de código aberto se remete à livre escolha de cada órgão do Poder Judiciário quanto aos seus sistemas, haja vista que eles possam fazer intercâmbio de informações.

Conforme analisa Atheniense (2010, p. 146), o artigo 3º dessa Lei faz menção ao recibo de documentos e à emissão de protocolo eletrônico, que deve conter pelo menos o nome do órgão judicial para o qual a peça foi distribuída, o nome do órgão receptor, o

número do processo, o número do protocolo de transmissão, o nome das partes envolvidas, a data e hora do recebimento e a identificação do usuário que realizou a transmissão. Essa fase do trâmite garante assegurar que o documento foi transferido com êxito, bem como dar respaldo ao emissor e ao receptor por meio das informações contidas no protocolo de recebimento. Além disso, as identificações do recibo das peças processuais minimizam ou, até mesmo, anulam as probabilidades de extravio do documento.

O armazenamento dos autos processuais parcial ou totalmente eletrônicos é responsabilidade exclusiva do Poder Judiciário. Atheniense (2010, p. 226-227) enfatiza que existem três situações na realidade atual: a dos processos físicos acumulados no decorrer dos anos, a dos processos totalmente digitais e a dos processos híbridos. Estes últimos são frutos das ações que, originalmente, foram atuadas em papel, mas que podem ser convertidas para o formato digital. Neste grupo, estão também os processos que foram atuados eletronicamente, mas que podem ser convertidos para meio físico, caso haja a necessidade de remessa a algum outro órgão do Poder Judiciário que ainda não esteja operando o processo eletrônico.

Nesse ínterim, percebe-se que a Lei n.º 11.419/2006 não obriga a uma rotina específica para o armazenamento, ficando a cargo do respectivo órgão do Poder Judiciário a regulamentação das práticas adotadas. Pode-se recorrer à digitalização ou ao armazenamento total ou parcialmente digital. Essa Lei não fixa sequer um prazo para que seja colocada em prática a digitalização, tendo em vista a variabilidade das infraestruturas orçamentárias de que os tribunais brasileiros dispõem, o que fará com que a efetivação em âmbito nacional do processo eletrônico se dê de maneira gradual.

5 Considerações finais

Diante do exposto no presente estudo, percebe-se que o Processo Judicial Eletrônico é uma realidade irreversível no cenário jurídico brasileiro. Essa nova modalidade está possibilitando o descongestionamento do Poder Judiciário e permitindo uma revisão do modelo de processo tradicional, já obsoleto. O novo modelo de processo desempenhará papel-chave na sociedade, com o encurtamento da distância e diminuição do tempo entre as etapas do processo e a eliminação da possibilidade de extravio ou falta de pessoal para fazer as juntadas de documentos nos autos.

Nesse sentido, pode-se verificar que a Lei n.º 11.419/2006 veio para suprir e eliminar a deficiência processual brasileira, tendo em vista a aptidão das vias eletrônicas para a tramitação de documentos jurídicos e observando determinados critérios que vão ao encontro da teoria arquivística, como a fidedignidade dos documentos, o uso de certificação digital, a preservação dos originais em suporte físico dentro do prazo em que a legislação estipula que o digitalizado passará a ter validade e o protocolo de recebimento dotado das informações pertinentes ao recebedor e ao destino do documento digital.

O advento da Lei n.º 11.419/2006 trouxe, assim, a mudança da mentalidade, a reformulação e a renovação consciente com a distribuição da Justiça, pois, como cita Abrão (2009), não há mais espaço, em muitos estados da federação, para arquivos, gastos e demoras no desarquivamento. Também é notável a preocupação do Poder Judiciário em adotar um modelo de requisitos para o desenvolvimento e a implantação de sistemas informatizados de gestão, o que representa um indicativo de que o uso do documento eletrônico é uma realidade na Justiça brasileira em todas as instâncias.

Contudo, alguns problemas ainda existem e merecem atenção, como a indefinição de padrões para o envio

de arquivos para o processo eletrônico, tendo cada tribunal as suas particularidades em relação às ferramentas usadas na tramitação dos documentos. Por fim, percebe-se que, com a tramitação por vias digitais e o armazenamento em memória eletrônica, o documento em papel passa a ser um mero acessório, e as transformações da tecnologia moderna ganham espaço.

Referências

1. ALECRIM, E. **O que é tecnologia da informação (TI)?** Disponível em: <<http://www.infowester.com/ti.php>>. Acesso em: 19 jun. 2010.
2. ARQUIVO NACIONAL (BRASIL). **Dicionário brasileiro de terminologia arquivística**. Rio de Janeiro: Arquivo Nacional, 2005.
3. ATHENIENSE, A. **Comentários à Lei 11.419/06 e as práticas processuais por meio eletrônico nos tribunais brasileiros**. Curitiba: Juruá, 2010.
4. BELLOTTO, H. L. **Diplomática e tipologia documental em arquivos**. 2. ed. Brasília: Briquet de Lemos, 2008.
5. BRASIL. **Lei n. 11.419 de 19 de dezembro de 2006**. Dispõe sobre a informatização do processo judicial; altera a Lei n. 5.869, de 11 de janeiro de 1973 - Código de Processo Civil; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/11419.htm>. Acesso em: 30 set. 2010.
6. CLEMENTINO, E. B. **Processo judicial eletrônico**. 1. ed. Curitiba: Juruá, 2009.
7. CINTRA, A. C. A.; GRINOVER A. P.; DINAMARCO, C. R. **Teoria geral do processo**. 19. ed. São Paulo: Malheiros Editores, 2003.
8. CONSELHO NACIONAL DE ARQUIVOS (BRASIL). **Glossário**. Câmara Técnica de Documentos Eletrôni-

- cos. Rio de Janeiro: Arquivo Nacional, 2010. Disponível em: <http://www.documentoseletronicos.arquivonacional.gov.br/media/publicacoes/glossario/2010glossario_v5.1.pdf>. Acesso em: 17 set. 2010.
9. CONSELHO NACIONAL DE ARQUIVOS (BRASIL). **e-ARQ Brasil: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos.** Câmara Técnica de Documentos Eletrônicos. Rio de Janeiro: Arquivo Nacional, 2011. Disponível em: <<http://www.siga.arquivonacional.gov.br/Media/earqbrasil.pdf>>. Acesso em: 19 abr. 2011.
10. CONSELHO NACIONAL DE JUSTIÇA (BRASIL). **MoReq-Jus: Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário Brasileiro.** Brasília: CNJ, 2009. Disponível em: <http://www.cnj.jus.br/images/stories/docs_cnj/resolucao/manualmoreq.pdf>. Acesso em: 29 jun. 2011.
11. GUIMARÃES, J. A. C.; NASCIMENTO, L. M. B.; NETO, M. F. **Aspectos jurídicos e diplomáticos dos documentos eletrônicos.** São Paulo: Associação de Arquivistas de São Paulo, 2005.
12. MADALENA, P. Processo judicial virtual: automação máxima. **Jus Navigandi**, a. 12, n. 1597, nov. 2007. Disponível em: <<http://jus.com.br/revista/texto/10656>>. Acesso em: 21 set. 2011.
13. MARQUES, A. T. G. L. **A prova documental na internet: validade e eficácia do documento eletrônico.** 1. ed. Curitiba: Juruá, 2008.
14. ROCHA, G. **Assinatura digital.** Disponível em: <<http://gestao.adv.br/index.php/segunda-do-processo-eletronico-assinatura-digital>>. Acesso em: 18 jul. 2011.
15. ROCHA, G. **Certificação digital.** Disponível em: <<http://gestao.adv.br/index.php/segunda-do-processo-eletronico-certificacao-digital>>. Acesso em: 18 jul. 2011.
16. ROCHA, G. **Uma reflexão sobre processo eletrônico.** Disponível em: <<http://gestao.adv.br/index.php/uma-reflexao-sobre-processo-eletronico>>. Acesso em: 19 jul. 2011.
17. RODRIGUES, A. C. **Diplomática contemporânea como fundamento metodológico da identificação da tipologia documental em arquivos.** 2008. 258 f. Tese (Doutorado em História Social) - Universidade de São Paulo, 2008.
18. ROSSI, A. G. **Processo eletrônico na Justiça Federal Brasileira: enfoque na preservação.** 2009. 72 f. Monografia (Especialização em Gestão em Arquivos) – Universidade Federal de Santa Maria, 2009.
19. SANTOS, V. B. Curso de gestão de documentos digitais. In: CURSO PROMOVIDO PELA UFSM E AARGS, 2008, Santa Maria. **Apostila.** Santa Maria, 2008.
20. SANTOS, V. B. **Gestão de documentos eletrônicos: uma visão arquivística.** 2. ed. Brasília: ABARQ, 2005.
21. SILVA, E. L.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação.** Florianópolis, 2005. Disponível em: <http://tccbiblio.paginas.ufsc.br/files/2010/09/024_Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes1.pdf>. Acesso em 27 ago. 2011.