A PROVA DOCUMENTAL E AS NOVAS TECNOLOGIAS

ROSÂNE MARLY SILVEIRA ASSMANN*

RESUMO: Com a evolução da internet e a possibilidade de registro dos fatos em diversas mídias, faz-se necessário analisar o modo de produção e os requisitos de um documento eletrônico para servir como meio de prova e a necessária confiabilidade de sítios (*sites*) na internet. Analisa-se, também, quanto a perícia para a verificação de integridade da prova produzida em meio eletrônico, destacando a necessidade de um setor de perícias para documentos que se encontram em diversos suportes.

PALAVRAS-CHAVE: Documento Eletrônico; Requisitos; Provas por Meio Eletrônico; Perícia.

1 INTRODUÇÃO

Ao trazer as provas para o processo, a parte busca demonstrar e convencer, o juiz, de que tem razão quanto as suas alegações. O Código de Processo Civil, em seu artigo 332, admite "todos os meios legais, bem como os moralmente legítimos" para que a parte possa "provar a verdade dos fatos, em que se funda a ação ou a defesa". Igualmente, o artigo 369 do novo CPC (Lei nº 13.105/15) admite todos os meios legais, bem como os moralmente legítimos, ainda que não especificados no Código.

Antônio Terêncio G. L. Marques em sua obra *A Prova documental na Internet – Validade e Eficácia do Documento Eletrônico* (2005, p. 18) "visa a demonstrar a licitude do **documento eletrônico** ou **ciberdocumento** em ser meio hábil para a obtenção de provas ou para robustecer determinada pretensão em face da nova esfera jurídica: **Direito da Internet**".

O presente estudo, por sua vez, tem por fim analisar o modo de produção e os requisitos de um documento eletrônico para servir como meio de prova.

* Juíza Titular da 2ª Vara do Trabalho de Santa Cruz do Sul – RS; Especialista em Direito Processual, Profissionalizante pela Escola Superior de Advocacia/RS e UFSC; Especialista em Direito Processual Civil pela UNISC.

Visa, ainda, trazer subsídios para a verificação de integridade da prova produzida em meio eletrônico.

Ressalto que, embora os termos técnicos possam parecer áridos, há necessidade de compreendê-los para que se possa verificar o preenchimento dos requisitos do documento eletrônico que as partes pretendam utilizar como prova.

Inicialmente, necessário um breve retrospecto sobre o surgimento do computador e da internet.

2 INFORMÁTICA E INTERNET

A revolução nas comunicações começa com o surgimento do computador, que era, inicialmente, um equipamento de grande porte.

Consoante André Lemos (2004, p. 104-5), "o primeiro microcomputador, o Altair, nasceu em Albuquerque, na Terra do Encantamento, no Novo México, em 1975. [...] Em 1977, aparecem simultaneamente a cultura punk na Inglaterra e o Apple II na garagem dos Steves (Jobs e Wozniak). Em 1981, o primeiro PC (personal computer) nasce de um modelo da IBM". Afirma, igualmente, que o Apple Macintosh surgiu em 1984, "criado em uma garagem e pretendendo ser interativo, convival e democrático" ao contrário do modelo da IBM, "um empreendimento gigantesco, centralizado e ligado à pesquisa militar".

Criados os computadores, necessário se fazia uni-los para possibilitar a comunicação entre eles. André Lemos afirma ainda que (2004, p.117) "A idéia de unir computadores em rede é desenvolvida por Bob Taylor, diretor em 1966 do DARPA, Departamento de Projetos de Pesquisa Avançadas da Agência de Defesa Americana".

Posteriormente, referido autor, em nota (2004, p. 265) esclarece que:

> Os pioneiros da internet são Vincent Cerf, Charlie Herzfeld, chefe do escritório executivo do DARPA; Larry Roberts, que abre caminho para o processamento de dados em rede no Lincoln Laboratory do MIT; Wes Clark que criou o processador de mensagens; Roger Scantlebury, inglês, que também trabalhou nas redes de computadores; Bob Kahn, teórico das redes; Dave Walden (o programador), Severo Ornstein, gênio do hardware e que criou mais tarde o CPSR – Computer Profissionals for Social Responsability e Ben Barker (designer de hardware).

Leonardo Netto Parentoni, por sua vez (2007, p. 27-8) salienta que a origem histórica da rede é controvertida, existindo duas correntes:

1) a que defende sua origem militar, na ARPAnet, no final da década de 60, início da década de 70;

2) a que pugna pela origem, acadêmica da internet, Universidade da Califórnia em Los Angeles – UCLA e no Instituto de Tecnologia de Massachusetts – MIT.

Conforme Marcelo Xavier de Freitas Crespo (2011, p. 30-1) a *Advanced Research Projects Administration* (Administração de Projetos e Pesquisas

Avançadas) era de uso exclusivo das Forças Armadas norte-americanas com o propósito de prover um contínuo funcionamento, mesmo em caso de calamidade como um ataque nuclear. Destaca que foi a implementação do TCP/IP (Protocolo de Controle de Transferência/Protocolo de Internet) que efetivamente possibilitou o surgimento da Internet.

Leonardo Netto Parentoni refere, ainda (2007, p. 29), que o Brasil ingressou na rede mundial de computadores somente em 1988, por iniciativa da comunidade acadêmica, sendo posteriormente coordenada pelo Ministério da Ciência e Tecnologia.

Na página do Instituto Nacional de Tecnologia da Informação (www.iti.gov.br), no item legislação, consta o Glossário ICP-Brasil, onde é possível consultar termos técnicos.

André Lemos informa (2004, p. 118) que:

> [...] A internet, como uma rede de redes, é formada por LANs (Local Area Network ou Redes Locais), MNs (Metropolitan Area Network ou Redes Metropolitanas) e WAN (World Area Network ou Redes Mundiais. [..] O idioma de computadores na rede internet é o protocolo TCP/IP (Transmission Control Protocol/Internet Protocol), desenvolvido nos anos 70 no Darpa e usado pela primeira vez em 1983 na Arpanet.

Cumpre destacar que, já em 1999, Pierre Lévy (1999, p. 167) afirmou que "O ciberespaço, interconexão dos computadores do planeta, tende a tornar-se a principal infra-estrutura de produção, transação e gerenciamento econômicos".

No artigo 6º da Lei nº 12.965/14 (marco civil da Internet) consta: "Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural".

Assim, criados os computadores e a internet, resta verificar a forma em que as informações circulam na rede.

3 DIGITALIZANDO AS INFORMAÇÕES

As informações já existentes no mundo físico podem ser inseridas no mundo virtual mediante digitalização.

Pierre Lévy (1999, p. 50) afirma que:

> Digitalizar uma informação consiste em traduzi-la em números. [...] Uma imagem pode ser traduzida em pontos ou pixels ('picture elements') [...]. Um som também pode ser digitalizado se for feita uma amostragem, ou seja, se forem tiradas medidas em intervalos regulares (mais de 60 mil vezes por segundo a fim de capturar as altas frequências).
>
> [...]
>
> As imagens e os sons também podem ser digitalizados, não apenas ponto a ponto ou amostra por amostra mas também de forma mais

> econômica, a partir de descrições das estruturas globais das mensagens iconográficas ou sonoras. Para tanto, usamos sobretudo funções senoidais para o som e funções que geram figuras geométricas para as imagens.
>
> Em geral, não importa qual é o tipo de informação ou de mensagem: se pode ser explicitada ou medida, pode ser traduzida digitalmente.

Ressalta, ainda, (1999, p. 51) que todos os números podem ser expressos em linguagem binária, sob a forma de 0 e 1 e que os números binários podem ser representados por uma grande variedade de dispositivos de dois estados (aberto ou fechado, plano ou furado, negativo ou positivo etc). Contrapõe que as informações codificadas digitalmente podem ser transmitidas e copiadas quase indefinidamente 'sem perda de informação', já que a mensagem original pode ser quase reconstituída integralmente (porque utiliza apenas dois valores nitidamente diferenciados), enquanto que a analógica, por ser representada por uma 'sequência contínua de valores', se degrada irremediavelmente a cada nova cópia ou transmissão.

Destaca também que (1999, p. 51-2):

> Mesmo se falamos muitas vezes de 'imaterial' ou de 'virtual' em relação ao digital, é preciso insistir no fato de que os processamentos em questão são sempre operações físicas elementares sobre os representantes físicos dos 0 e 1: apagamento, substituição, separação, ordenação, desvio para determinado endereço de gravação ou canal de transmissão.
>
> Após terem sido tratadas, as informações codificadas em binário vão ser traduzidas (automaticamente) no sentido inverso, e irão manifestar-se como textos legíveis, imagens visíveis, sons audíveis, sensações tácteis ou proprioceptivas, ou ainda em ações de um robô ou outro mecanismo.

Ressalta, por fim, (1999, p. 53) que é "porque as informações estão codificadas como números que podemos manipulá-las com tamanha facilidade: os números estão sujeitos a cálculos, e computadores calculam rápido".

Ou seja, de certa forma podemos dizer que tudo se transforma em números, que são rapidamente reconhecidos e manipulados pelo computador.

Assim, ainda que não se goste de números, passa-se a viver intensamente dependentes deles.

4 DOCUMENTO E DOCUMENTO ELETRÔNICO

A informação digitalizada sempre tem um documento original no meio físico, enquanto que há informações que **são geradas e circulam no meio virtual**.

Com a inclusão do parágrafo único ao artigo 154[1] do CPC pela Lei nº 11.280/06, a realização de atos processuais por meios eletrônicos trouxe à

[1] Art. 154. Os atos e termos processuais não dependem de forma determinada senão quando a lei expressamente a exigir, reputando-se válidos os que, realizados de outro modo, lhe preencham a finalidade essencial.
Parágrafo único. Os tribunais, no âmbito da respectiva jurisdição, poderão disciplinar a prática e a

tona a utilização do documento eletrônico. Nesse sentido também o artigo 193 do novo CPC.[2]

Assevera Marinoni (2000, p. 19) que "Documento é toda coisa capaz de representar um fato" e que (p. 17) "Prova documental é, somente, aquela através da qual se tem a representação imediata do fato a ser reconstruído".

Ensina ainda que (2000, p. 20):

> Os documentos compõem-se de dois elementos: Haverá sempre um conteúdo e um suporte. O primeiro equivale ao aspecto semiótico do documento, à idéia que pretende transmitir. Revela, portanto, o próprio fato que se pretende representar através do documento. Já o suporte constitui o elemento físico do documento, a sua expressão exterior, manifestação concreta e sensível; é, enfim, o elemento material, no qual se imprime a idéia transmitida.

Leonardo Netto Parentoni (2007, p. 33) suscita a questão do suporte material: "A questão é a seguinte: os arquivos de computador podem ser considerados documento em sentido técnico-jurídico?".

Discorre (2007, p. 33-4) que os arquivos de computador necessitam de um equipamento tecnológico e de um *software* para serem lidos, porém frisa que a prova documental é sempre uma prova material, pois deve estar gravada em um bem corpóreo e pondera que esse suporte material não precisa ser, necessariamente, o papel, admitindo-se também a mídia digital, caso em que se terá um documento eletrônico.

Conforme Carlos Affonso Pereira de Souza (p. 114): "Dessa forma, a mensagem eletrônica constitui um documento válido no ordenamento jurídico nacional, uma vez que ela opera como representação material de uma declaração, fornecendo-lhe o suporte no qual a sua existência permanece registrada e passível de posterior consulta".

Os documentos, portanto, podem ter como suporte o meio papel, o papel fotográfico, o CD, o DVD etc. A utilização de tais mídias possibilita o armazenamento e o trânsito das informações de forma mais rápida que os documentos em meio papel, porém, deve possibilitar também a verificação da integridade e autenticidade do documento.

Antônio Marques (2006, p. 126-7) afirma que o documento físico está atrelado de modo indissociável ao meio físico. Quanto ao documento eletrônico, ressalta que:

---

comunicação oficial dos atos processuais por meios eletrônicos, atendidos os requisitos de autenticidade, integridade, validade jurídica e interoperabilidade da Infra-Estrutura de Chaves Públicas Brasileira - ICP - Brasil. (Incluído pela Lei nº 11.280, de 2006)

§ 2º Todos os atos e termos do processo podem ser produzidos, transmitidos, armazenados e assinados por meio eletrônico, na forma da lei. (Incluído pela Lei nº 11.419, de 2006).

[2] Art. 193 (novo CPC). Os atos processuais podem ser total ou parcialmente digitais, de forma a permitir que sejam produzidos, comunicados, armazenados e validados por meio eletrônico, na forma da lei.

> No concernente ao documento eletrônico, uma vez que não se prende ao meio físico em que está gravado, possuindo autonomia em relação a ele, nada mais representa que uma sequência de bits que, traduzida por meio de um determinado programa de computador, seja representativo de um fato.
>
> Desta forma, percebe-se que os documentos eletrônicos possuem os mesmos elementos que um documento escrito em suporte de papel, contendo, entretanto, os seguintes aspectos: a) constam em suporte material (disquete, circuitos, chips de memória, redes); b) contêm uma mensagem, em que está escrita em linguagem convencional de dígitos binários ou bits, entidades magnéticas que os sentidos humanos não podem perceber diretamente; c) estão escritos em um idioma ou código determinado; e d) podem ser atribuídos a uma pessoa determinada com a qualidade de autor, mediante uma assinatura digital ou chave eletrônica.

Consoante o glossário do Instituto Nacional de Tecnologia da Informação, documento é a "Unidade de registro de informações, qualquer que seja o suporte". Já o documento digital é a "Unidade de registro de informações, codificada por meio de dígitos binários". E o documento eletrônico é a "Unidade de registro de informações, acessível por meio de um equipamento eletrônico" (BRASIL. Instituto Nacional de Tecnologia da Informação, 2010).

Assim, verificadas as características próprias do documento eletrônico, há também requisitos para a sua validade.

4.1 Requisitos do documento eletrônico

Antônio Marques (2006, p. 132-3) ressalta os requisitos de "autenticidade, integridade e perenidade do conteúdo" para que o documento eletrônico possa ser considerado legítimo, sob o prisma jurídico.

4.1.1 *Integridade*

No que tange à integridade ou veracidade, Antônio Marques (2006, p. 135) destaca que:

> [...] para servir de suporte probatório, o documento eletrônico não pode ser passível de alteração, ou seja, não pode ser modificado após sua concepção, quando é transmitido do emissor para o receptor, nem tão pouco, quando armazenado; e se for alterado, que seja identificável com métodos e técnicas apropriadas.

E cita o exame pericial e a inspeção judicial, inclusive para rastrear a emissão, recepção e a respectiva data.

4.1.2 *Perenidade*

Já quanto à perenidade, Antônio Marques destaca que (2006, p. 137):

> [...] Quando se assina um documento eletrônico – que será através da chave privada – é possível conferir a assinatura digital, mediante o uso da chave pública. E, além disso, ao realizar a assinatura, o programa

> criptográfico utilizará fórmulas matemáticas altamente sofisticadas, vinculando a assinatura digital ao documento assinado, de tal maneira que a assinatura digital seja somente válida para aquele documento.
>
> Assim, qualquer alteração na seqüência de bits, que forma o documento eletrônico invalida a assinatura.

4.1.3 *Autenticidade*

No artigo 411 do novo CPC consta:

> Art. 411. Considera-se autêntico o documento quando:
>
> I - o tabelião reconhecer a firma do signatário;
>
> II - a autoria estiver identificada por qualquer outro meio legal de certificação, inclusive eletrônico, nos termos da lei;
>
> III - não houver impugnação da parte contra quem foi produzido o documento.

Antônio Marques (2006, p. 133-4) afirma que a autenticidade implica a autoria identificável pela assinatura digital, que constitui um sinal identificável, único e exclusivo de uma determinada pessoa.

Marcacini (citado por Antonio Marques- p. 134) compara que:

> Se a assinatura tradicional é única e exclusiva porque corresponde à escrita manual do signatário, comandada pelos impulsos nervosos vindos do cérebro, a assinatura eletrônica obtém esta característica uma vez assegurada a ***exclusivitá del mezzo tecnico***. Ou seja, somente o sujeito que estiver de posse da chave privada tem condições técnicas de gerar uma assinatura como aquela.

Esclarece Leonardo Netto Parentoni (2007, p. 133) que:

> [...] Assinatura eletrônica é qualquer mecanismo utilizado para identificar um sujeito em meio eletrônico. Exemplo são as senhas bancárias. Por outro lado, assinatura digital é técnica mais complexa que permite auferir, com precisão, a autenticidade e integridade de um documento.

O PIN (*Personal Identification Number* ou Número de Identificação Pessoal); o *Password* (palavra de aprovação) e *Passphrase* (frase de passagem ou aprovação) são senhas utilizadas para produzir a assinatura digital.

Há, também, outras modalidades de assinatura, conforme referido por Alexandre Atheniense (2010, p. 127-8):

> * Assinatura autógrafa: É aquela baseada na inscrição grafotécnica, pelo autor, no documento, do seu próprio nome, completo ou abreviado, ou de qualquer outro sinal que o identifique. [...]

> * Assinatura digitalizada: A assinatura digitalizada é um arquivo de imagem gerado com base na digitalização de uma imagem contendo a assinatura grafotécnica aposta em um papel primeiramente, ao contrário das assinaturas com e sem certificação digital que são geradas originariamente no meio eletrônico. [...]
>
> * Chave biométrica: a chave biométrica é uma forma de identificação a que se procede mediante verificação de determinada parte do corpo que denota seus elementos personalíssimos que o distinguem dos demais.

4.1.4 *Interoperabilidade*

No parágrafo único do artigo 154 do CPC também consta a exigência de interoperabilidade da Infraestrutura de Chaves Públicas Brasileiras – ICP – Brasil. Igualmente, os artigos 194 e 196 do novo CPC repetem essa exigência[3].

Leonardo Netto Parentoni afirma que:

> [...] interoperabilidade é a capacidade de um sistema de se comunicar com outro, de modo harmônico. Para tanto, é necessário que ambos sejam compatíveis e obedeçam a um conjunto mínimo de normas e especificações técnicas (2007, p. 159).
>
> [...] Há duas espécies de interoperabilidade: a objetiva e a subjetiva. Aquela se relaciona à utilização de um padrão operacional mínimo que permita compatibilizar os meios materiais e imateriais que compõem a infra-estrutura, como softwares, hardwares, cabos, tipos de voltagem etc. Diz-se objetiva por referir-se aos equipamentos utilizados no procedimento e não aos sujeitos que dele participam.
>
> Por outro lado, a interoperabilidade subjetiva é um conjunto de princípios e regras que incide sobre os sujeitos que, de um modo ou de outro, se relacionam com essa infra-estrutura, como os órgãos de fiscalização e execução, os usuários etc (2007, p. 160).
>
> [...] Especificamente em relação à ICP-Brasil: Infra-Estrutura de Chaves Públicas Brasileira, interoperabilidade se traduz na adoção de um padrão mínimo que assegure a compatibilidade entre as chaves fornecidas pelos órgãos que integram o sistema, bem como entre os diversos softwares e hardwares utilizados no procedimento" (2007, p.163).

[3] Art. 194 (novo CPC). Os sistemas de automação processual respeitarão a publicidade dos atos, o acesso e a participação das partes e de seus procuradores, inclusive nas audiências e sessões de julgamento, observadas as garantias da disponibilidade, independência da plataforma computacional, acessibilidade e interoperabilidade dos sistemas, serviços, dados e informações que o Poder Judiciário administre no exercício de suas funções.
[...]
Art. 196 (novo CPC). Compete ao Conselho Nacional de Justiça e, supletivamente, aos tribunais, regulamentar a prática e a comunicação oficial de atos processuais por meio eletrônico e velar pela compatibilidade dos sistemas, disciplinando a incorporação progressiva de novos avanços tecnológicos e editando, para esse fim, os atos que forem necessários, respeitadas as normas fundamentais deste Código.

4.2 Criptografia e certificação digital

Alexandre Atheniense (2010, p. 114) afirma que:

> A utilização da assinatura digital com a certificação digital providencia a prova inegável de que uma mensagem veio do emissor. Para verificar esse requisito, uma assinatura digital deve ter as seguintes propriedades:
>
> * autenticidade: o receptor deve poder confirmar que a assinatura foi feita pelo emissor;
>
> * integridade: qualquer alteração da mensagem faz com que a assinatura não corresponda mais ao documento;
>
> * não repúdio ou irretratabilidade: o emissor não pode negar a autenticidade da mensagem.
>
> A criptografia que garante a segurança do certificado digital é o estudo dos princípios e das técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de maneira que possa ser conhecida apenas por seu destinatário, detentor da 'chave pública', o que torna difícil de ser lida por alguém não autorizado. Assim, sendo, só o receptor da mensagem pode ler a informação com facilidade.

Antônio Marques (2006, p. 162) afirma que "nos Estados Unidos, o sistema criptográfico é considerado matéria de defesa nacional e faz parte do *United States Munitions List*, na categoria XIII – Equipamento Auxiliar submetendo-se às restrições do *Arms Export Control Act*".

Informa, ainda, Antônio Marques que (2006, p.160-1):

> O padrão criptográfico utilizado para cifrar ou decifrar mensagens é conhecido como **chave**.
>
> Quando a mesma chave é utilizada para cifrar e para decifrar a mensagem, temos a denominada criptografia **simétrica** ou de **chave privada**, normalmente utilizada em redes fechadas ou computadores isolados.
>
> [...] Quando são utilizadas duas chaves distintas todavia matematicamente vinculadas entre si, uma para cifrar mensagem, e outra para decifrá-la, temos aqui a **criptografia assimétrica** ou de **chave pública**, destinadas à utilização em redes abertas como a internet. Aqui, as chaves são totalmente independentes entre si, porém, uma chave completa a outra.

Ressalta, ainda (2006, p. 166), que a assinatura digital "não é um método de criptografia assimétrica, mas sim, uma técnica destinada a garantir e a proporcionar maior segurança, confiabilidade do conteúdo das mensagens na infovia, ou seja, é uma marca, um traço característico, o qual viabiliza a identificação da autoria do documento eletrônico".

Conforme Leonardo Netto Parentoni (2007, p. 67-8), a Medida Provisória nº 2.200-2, de 24.08.2001, introduziu no Brasil "a base legal necessária para conferir plena validade jurídica ao documento eletrônico" ao criar "um sistema de certificação digital dos documentos eletrônicos denominado *Infra-estrutura*

de Chaves Públicas Brasileira - ICP-Brasil. Esse sistema é composto de um órgão de cúpula, denominado de Autoridade Gestora e por três grupos de órgãos subordinados: a Autoridade Certificadora RAIZ (AC-Raiz), as Autoridades Certificadoras (AC) e as Autoridades de Registro (AR)".

Nos termos do Instituto Nacional de Tecnologia da Informação:

> A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI, além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

Salienta Leonardo Netto Parentoni (2007, p. 70) que:

> [...] a certificação particular é mais restrita, pois gera presunção inter partes de validade do documento eletrônico, ao passo que na certificação pública tal presunção opera erga omnes. Assim, por exemplo, um e-mail submetido à certificação pública terá sua autenticidade e integridade oponíveis a qualquer pessoa, ao passo que o mesmo e-mail, se certificado por entidade não credenciada pela ICP-Brasil, terá essas características asseguradas entre emissor e destinatário, podendo um terceiro questionar a validade do documento.

Ressalta (2007, p. 72) "que a Lei 11.419, de 19.12.2006, tornou *obrigatória* a adoção de assinatura digital nos atos processuais praticados por meio eletrônico".

Destaca, ainda, Leonardo Netto Parentoni (2007, p. 140-1) que "a assinatura digital gerada nos moldes da ICP-Brasil (Medida Provisória 2.200-2/01) equivale à assinatura manuscrita para todos os fins" e que "faz prova plena da autoria e integridade de um documento eletrônico". Destaca que, ao contrário (2007, p. 141), a 'assinatura' digitalizada é apenas cópia que pode ser extraída por qualquer um, sendo imprestável para comprovar a autoria e integridade da peça.

Consoante o Instituto Nacional de Tecnologia da Informação, assinatura digital constitui o:

> Código anexado ou logicamente associado a uma mensagem eletrônica que permite de forma única e exclusiva a comprovação da autoria de um determinado conjunto de dados (um arquivo, um e-mail ou uma transação).
>
> A assinatura digital comprova que a pessoa criou ou concorda com um documento assinado digitalmente, como a assinatura de próprio punho comprova a autoria de um documento escrito. A verificação da origem do dado é feita com a chave pública do remetente (BRASIL. Instituto Nacional de Tecnologia da Informação, 2010).

Além dos requisitos propriamente ditos acima mencionados, acrescentamos, ainda, o requisito da confiabilidade no conteúdo quanto às informações presentes na internet.

4.3 Uso da internet e sítios (*sites*) confiáveis

Havendo abundantes informações na internet sobre todos os assuntos, há necessidade que também se possa confiar no conteúdo dessas informações.

Por exemplo, para esclarecer questões em perícia médica, os sítios na internet devem ser de origem médica ou de pesquisa, não podendo ser sítios de programas de TV ou de revistas em geral. Na área científica, o sítio www.scielo.br (A *Scientific Electronic Library Online* - SciELO é uma biblioteca eletrônica que abrange uma coleção selecionada de periódicos científicos brasileiros) ou o Pubmed (http://www.ncbi.nlm.nih.gov/pubmed/ ou www.pubmed.com) são alguns dos confiáveis. Também, o sítio http://lilacs.bvsalud.org/, do Centro Latino-Americano e do Caribe de Informação em Ciências da Saúde, é um abrangente índice da literatura científica e técnica da América Latina e Caribe.

Igualmente, os sítios de fabricantes de produtos químicos manuseados pelo trabalhador ou do fabricante da máquina em que houve um acidente, por exemplo, podem auxiliar a parte como prova e o juiz na decisão.

5 PROVAS POR MEIO ELETRÔNICO: VALIDADE

Explicitados os requisitos do documento eletrônico, passa-se a analisar a possibilidade de utilização como prova em processo judicial.

Antônio Marques (2006, p. 49) afirma que "Através da possibilidade de as partes participarem no convencimento do juiz é que a decisão judicial torna-se legítima".

Carlos Affonso Pereira de Souza (p. 114-5) destaca que:

> O Código Civil adotou o princípio da liberdade de forma para a manifestação da vontade, no que concerne aos negócios jurídicos, conforme dispõe o art. 107, determinando que ela 'não dependerá de forma especial, senão quando a lei expressamente o exigir'.
>
> [...]
>
> O Código Civil, no art. 212 consagra a liberdade de forma na produção de provas, excepcionando apenas os negócios para os quais se exige forma especial[4].

Consoante Alexandre Atheniense (2010, p. 216):

> A prova no processo judicial é extremamente importante, uma vez que contribui, diretamente, para a formação do convencimento do julgador sobre a lide. [...] As provas obtidas por meio eletrônico diferem das demais,

[4] Art. 212. Salvo o negócio a que se impõe forma especial, o fato jurídico pode ser provado mediante: I - confissão; II - documento; III - testemunha; IV - presunção; V - perícia.

> apenas quanto à forma de armazenamento, já que, acompanhando o avanço da tecnologia da informação, o armazenamento das informações passou do papel para os bits, substituindo a grafia tradicional e o uso do papel pelos impulsos eletrônicos.

A utilização do documento eletrônico como meio de prova pode ocorrer observando-se as disposições dos artigos 170 e 332[5] do CPC e 195, 369[6] e 210 do novo CPC.

Igualmente, os artigos 439, 440 e 441 do novo CPC dispõem acerca do documento eletrônico:

> Art. 439. A utilização de documentos eletrônicos no processo convencional dependerá de sua conversão à forma impressa e da verificação de sua autenticidade, na forma da lei.
>
> Art. 440. O juiz apreciará o valor probante do documento eletrônico não convertido, assegurado às partes o acesso ao seu teor.
>
> Art. 441. Serão admitidos documentos eletrônicos produzidos e conservados com a observância da legislação específica.

Vimos, portanto, os requisitos do documento eletrônico para possibilitar a sua utilização como meio de prova.

Antônio Marques compara a prova documental física com a prova mediante documento eletrônico (2006, p. 133-8). Ressalta que, no documento tradicional, a assinatura lançada no suporte material e, no eletrônico, a assinatura digital, têm a função de autenticação, autoria identificável. Assevera possível que o magistrado, de ofício ou a requerimento da parte (2006, p. 136):

> acesse a rede de informações e determine que o provedor ou a autoridade certificadora, libere, de seus registros cadastrais informações específicas, relativas à análise judicial feita, sem invadir a esfera jurídica de terceiros, evidentemente, para provar se o documento eletrônico averiguado nele foi originado de uma determinada pessoa e o nome dessa mesma pessoa, para localizá-la e se chegar a sua autoria com um certo grau de certeza.

---

[5] Art. 170. É lícito o uso da taquigrafia, da estenotipia, ou de outro método idôneo, em qualquer juízo ou tribunal. (Redação dada pela Lei nº 8.952, de 13.12.1994)
Art. 332. Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa.

[6] Art. 195 (novo CPC). O registro de ato processual eletrônico deverá ser feito em padrões abertos, que atenderão aos requisitos de autenticidade, integridade, temporalidade, não repúdio, conservação e, nos casos que tramitem em segredo de justiça, confidencialidade, observada a infraestrutura de chaves públicas unificada nacionalmente, nos termos da lei.
Art. 369 (novo CPC). As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz.
Art. 210 (novo CPC). É lícito o uso da taquigrafia, da estenotipia ou de outro método idôneo em qualquer juízo ou tribunal.

Ressalta, ainda (2006, p. 141), que conforme o artigo 389, II, do CPC[7] (art. 429 do novo CPC[8]), quem alegar a apropriação e uso ilícito da chave privada deverá comprovar esse fato. Assevera que "o ônus da prova recai sobre o autor que produziu o documento digital" e cita Marcacini (Augusto Tavares Rosa Marcacini): "*compete à parte que produz o documento eletrônico provar a autenticidade da chave pública que afirma ser do suposto signatário, e com a qual iremos conferir a assinatura digital*".

É necessário, ainda, que quem assina o documento eletrônico não possa negar que o assinou. O artigo 195 do novo CPC estabelece a exigência de não repúdio.

O Instituto Nacional de Tecnologia da Informação estabelece que:

> Não-repúdio: garantia que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica, não poderá posteriormente negar sua autoria, visto que somente aquela chave privada poderia ter gerado aquela assinatura digital. Deste modo, a menos de um uso indevido do certificado digital, fato que não exime de responsabilidade, o autor não pode negar a autoria da transação.
>
> Transações digitais estão sujeitas a fraude, quando sistemas de computador são acessados indevidamente ou infectados por cavalos-de-tróia ou vírus. Assim, os participantes podem, potencialmente, alegar fraude para repudiar uma transação (BRASIL. Instituto Nacional de Tecnologia da Informação, 2010).

O documento eletrônico assinado mediante certificação digital tem asseguradas a integridade, a perenidade e a autenticidade.

Mas e no caso de o documento eletrônico sem assinatura?

Leonardo Netto Parentoni, (2007, p. 138), ao indagar se é possível considerar válido um documento eletrônico *sem assinatura* esclarece que:

> Inicialmente, poder-se-ia cogitar da aplicação do art. 371, III, do Código de Processo Civil, que trata dos documentos que comumente não se costuma assinar. Neste caso, há presunção relativa de que é autor a pessoa que mandou compor o documento. Exemplo são os e-mails. Ainda que não assinados, presume-se que tenham sido escritos pelo titular da conta. Ademais, o art. 154 do Código determina que os termos e atos processuais não dependem de forma especial, salvo quando a lei o exigir[9].

[7] Art. 389. Incumbe o ônus da prova quando:
I - se tratar de falsidade de documento, à parte que a argüir;
II - se tratar de contestação de assinatura, à parte que produziu o documento.
[8] Art. 429 (novo CPC). Incumbe o ônus da prova quando:
I - se tratar de falsidade de documento ou de preenchimento abusivo, à parte que a arguir;
II - se tratar de impugnação da autenticidade, à parte que produziu o documento.
[9] Art. 371. Reputa-se autor do documento particular:
I - aquele que o fez e o assinou;
II - aquele, por conta de quem foi feito, estando assinado;

No novo CPC, a remissão corresponderá ao artigo 410, III.

Alexandre Atheniense, por sua vez afirma que (2010, p. 217): "Os documentos assinados digitalmente podem ser considerados como prova inequívoca e têm valor probante *erga omnes*. Mas, ainda que o documento eletrônico não tenha sido assinado, é possível verificar a autenticidade e integridade mediante a devida perícia técnica".

A Lei nº 11.419/06 estabelece a possibilidade de arguição de falsidade (art. 11, § 2º).

Se arguida a falsidade, há necessidade de verificar as conexões estabelecidas no computador.

Os artigos 13 e 15 da Lei nº 12.965/14 preveem:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
>
> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

A credibilidade da prova por meio digital está intrinsicamente relacionada à possibilidade de verificar o preenchimento dos requisitos mencionados. Joel Ribeiro Fernandes, na Introdução de sua obra "Perícias em Áudios e Imagens Forenses" (2013) expõe que:

> Os avanços tecnológicos do processamento digital de sinais sonoros e de imagens aumentaram de maneira vertiginosa as condições para gravar e possibilitar uma documentação permanente dos mais variados eventos. Vivenciamos uma fase na qual a tecnologia permite que quase tudo seja gravado e possa, posteriormente, ser utilizado em inúmeras finalidades.
>
> [...]
>
> **Devemos sempre ouvir e olhar com atenção o que nos é apresentado no mundo digital, pois muito do que pode parecer não o é, e muito fácil é concluir errado, iluminado por uma induzida percepção.** (Grifei.)

III - aquele que, mandando compô-lo, não o firmou, porque, conforme a experiência comum, não se costuma assinar, como livros comerciais e assentos domésticos.

Art. 372. Compete à parte, contra quem foi produzido documento particular, alegar no prazo estabelecido no art. 390, se lhe admite ou não a autenticidade da assinatura e a veracidade do contexto; presumindo-se, com o silêncio, que o tem por verdadeiro.

Parágrafo único. Cessa, todavia, a eficácia da admissão expressa ou tácita, se o documento houver sido obtido por erro, dolo ou coação.

No artigo 225 do Código Civil consta: “As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão.”

Igualmente, o artigo 383, caput, do Código de Processo Civil:

> Art. 383. Qualquer reprodução mecânica, como a fotográfica, cinematográfica, fonográfica ou de outra espécie, faz prova dos fatos ou das coisas representadas, se aquele contra quem foi produzida lhe admitir a conformidade.
>
> Parágrafo único. Impugnada a autenticidade da reprodução mecânica, o juiz ordenará a realização de exame pericial.

No novo CPC, disposições semelhantes se encontram nos artigos 422 e 425 e parágrafos:

> Art. 422. Qualquer reprodução mecânica, como a fotográfica, a cinematográfica, a fonográfica ou de outra espécie, tem aptidão para fazer prova dos fatos ou das coisas representadas, se a sua conformidade com o documento original não for impugnada por aquele contra quem foi produzida.
>
> § 1º As fotografias digitais e as extraídas da rede mundial de computadores fazem prova das imagens que reproduzem, devendo, se impugnadas, ser apresentada a respectiva autenticação eletrônica ou, não sendo possível, realizada perícia.
>
> § 2º Se se tratar de fotografia publicada em jornal ou revista, será exigido um exemplar original do periódico, caso impugnada a veracidade pela outra parte.
>
> § 3º Aplica-se o disposto neste artigo à forma impressa de mensagem eletrônica.
>
> [...]
>
> Art. 425. Fazem a mesma prova que os originais:
>
> I - as certidões textuais de qualquer peça dos autos, do protocolo das audiências ou de outro livro a cargo do escrivão ou do chefe de secretaria, se extraídas por ele ou sob sua vigilância e por ele subscritas;
>
> II - os traslados e as certidões extraídas por oficial público de instrumentos ou documentos lançados em suas notas;
>
> III - as reproduções dos documentos públicos, desde que autenticadas por oficial público ou conferidas em cartório com os respectivos originais;
>
> IV - as cópias reprográficas de peças do próprio processo judicial declaradas autênticas pelo advogado, sob sua responsabilidade pessoal, se não lhes for impugnada a autenticidade;
>
> V - os extratos digitais de bancos de dados públicos e privados, desde que atestado pelo seu emitente, sob as penas da lei, que as informações conferem com o que consta na origem;

> VI - as reproduções digitalizadas de qualquer documento público ou particular, quando juntadas aos autos pelos órgãos da justiça e seus auxiliares, pelo Ministério Público e seus auxiliares, pela Defensoria Pública e seus auxiliares, pelas procuradorias, pelas repartições públicas em geral e por advogados, ressalvada a alegação motivada e fundamentada de adulteração.
>
> § 1º Os originais dos documentos digitalizados mencionados no inciso VI deverão ser preservados pelo seu detentor até o final do prazo para propositura de ação rescisória.
>
> § 2º Tratando-se de cópia digital de título executivo extrajudicial ou de documento relevante à instrução do processo, o juiz poderá determinar seu depósito em cartório ou secretaria.

O parágrafo único do artigo 434 do novo CPC estabelece que a exposição de reprodução cinematográfica ou fonográfica será efetuada em audiência, com a intimação prévia das partes.

O exame pericial verificará o documento mediante meios e programas para constatar se houve ou não alterações.

5.1 Perícia para verificar a integridade do documento

Dependendo do suporte em que se encontra o documento, há diversos meios para a verificação da integridade do documento. A seguir, alguns suportes e os meios habitualmente utilizados.

5.1.1 *Fotografia*

O método mais simples consiste em ampliar a fotografia. Se há falsificação, há diferença no número de pixels (*pictures elements*) que se constata quando se expõe ao aumento.

Joel Ribeiro Fernandes informa que "a qualidade da imagem depende do número de pixels existentes na mesma" (2013, p. 145) e sugere a análise da recompressão, a análise do nível de erro (*ELA- Error Level Analysis*), o redimensionamento entre outras ferramentas. Informa, ainda que (p. 152): "O formato de compressão JPEG, geralmente o mais utilizado em fotografias digitais, acarreta uma perda de qualidade de imagem".

Como curiosidade, a informação desse autor de que "a visão humana é mais sensível à cor verde, por este motivo o número de pixel dessa cor é o dobro dos demais, pois a mesma dever ter maior precisão pela sua influência na qualidade perceptual da imagem" (2013, p. 144).

Segundo Evandro Della Vechia (2014, p. 107, em nota de rodapé):

> *Exchangeable Image File Format* (EXIF) é uma especificação seguida por fabricantes de câmeras digitais, visando à gravação de informações sobre a captura de imagens, dados do equipamento entre outros. Essas informações são gravadas junto ao arquivo da imagem propriamente dita, na forma de metadados.

5.1.2 *CD e DVD*

Na lição de Joel Ribeiro Fernandes (2013, p. 47):

> Um dos marcadores mais utilizados na análise de um áudio é o espectro do mesmo, que é obtido pela representação gráfica da amplitude da onda (intensidade) versus a sua frequência, isto é, amplitude no eixo vertical (Y) e frequência no eixo horizontal (X) [...]
>
> Outra ferramenta útil é a análise estatística do *pitch* na fala do locutor. O *pitch* corresponde à sensação fisiológica do timbre da voz e sua medida é expressa em Hz, estando relacionada à variação da frequência fundamental. (2013, p. 55)

Ressalta a perda de elementos do sinal quando o áudio está gravado no formato *MP*3, com alta taxa de compressão (2013, p. 72). Já o formato *RAW* tem compressões sem perdas (2013, p. 124-5). Sugere *softwares* para análise: *Sound Forge*, *Adobe Audition*, etc (2013, p. 87). Assevera que: "A garantia da integridade de um áudio é dada de forma mais adequada pela aplicação de um algoritmo de *hash*, pois, a partir desse momento, uma mínima modificação na estrutura lógica do arquivo será facilmente detectada" (2013, p. 90).

5.1.3 *Página na internet*

Materializa-se a imagem mediante ata notarial ou as teclas "print screen" (PrtScn) do teclado. "O processo de captura de uma imagem da tela para salvar, imprimir ou compartilhar é conhecido como captura de tela." *In http://windows.microsoft.com/pt-br/windows/take-screen-capture-print-screen#take-screen-capture-print-screen=windows-7* é possível obter mais informações.

5.1.4 *Programa de computador*

Cada programador tem um jeito de programar, que se equipara a uma assinatura. Desse modo, é possível verificar quem produziu o programa.

5.1.5 *Correspondência eletrônica (e-mail*)

O servidor informa qual a conta de *e-mail* que deve enviar e para a qual deve enviar. Para saber qual a máquina que enviou há programa que detecta a sequência binária que se assemelha ao número do chassi de um carro. Analisando o disco rígido, pelo endereço de IP é possível verificar quem enviou, sendo possível verificar se houve acesso remoto ao computador.

Há, portanto, possibilidade de, por perícia, verificar se um documento, independentemente do suporte, possui as características necessárias para constituir meio de prova.

O Instituto Nacional de Tecnologia da Informação estabelece as trilhas para possibilitar a auditoria em sistemas:

> *"i. Histórico das transações de sistemas que estão disponíveis para a avaliação com o objetivo de provar a correção de sua execução comparada com os procedimentos ditados pela política de segurança.*

> *ii. rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria.*
>
> *iii. conjunto cronológico de registros que proporcionam evidências do funcionamento do sistema. Estes registros podem ser utilizados para reconstruir, revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para rastrear o uso do sistema, detectando e identificando usuários não autorizados"* (BRASIL. Instituto Nacional de Tecnologia da Informação, 2007).

Igualmente, a análise de metadados (sic) é útil para verificar a integridade do arquivo. Joel Ribeiro Fernandes (2013, p. 97) afirma que:

> Esse tipo de análise permite o conhecimento das características de áudios ou de imagens digitais, mostrando a data da criação dos mesmos, o tipo de formato no qual estão armazenados, os *softwares* que realizaram alguma modificação, o tamanho, a organização, ou seja, a identificação de dados usados para auxiliar na identificação, na descrição e na localização da informação digitalizada.

Para a solicitação de perícia, consoante Evandro Della Vechia (2014, p. 66-7), é preciso o histórico do caso, com detalhes e quesitos objetivos, tais como para a falsificação de documentos (2014, p. 68):

> - Existem imagens de documentos públicos ou privados no material questionado? Quais?
>
> - O conjunto de equipamentos enviados para perícia tem condições de produzir documento similar ao apresentado em anexo?
>
> - O documento apresentado em anexo foi produzido pelo conjunto de equipamentos submetidos à perícia?
>
> - O documento questionado é autêntico?

Para o rastreamento de *e-mails* (correspondências eletrônicas), o mesmo autor sugere os quesitos, os quais devem ser adaptados caso a caso:

> - Verificar a origem (endereço IP, cidade, empresa, etc) do e-mail recebido dia ##/##/## com assunto "Abre teu olho!
>
> - Verificar a origem dos e-mails recebidos em nome de "Tiburcio da Silva" (tiburciodasilva171@gmail.com).

Portanto, para um bom resultado da perícia, é necessária objetividade nos quesitos.

6 CONCLUSÃO

Cada vez mais os documentos eletrônicos podem ser utilizados como prova. Igualmente, as informações existentes na internet podem constituir subsídio para as partes e para o juiz. Além da obtenção por meios legais,

a credibilidade da prova está relacionada à possibilidade de verificar a integridade e a respectiva autoria. Se antes a perícia grafodocumentoscópica era suficiente, hoje há necessidade de um setor de perícias de documentos em diversos suportes.

REFERÊNCIAS

ATHENIENSE, Alexandre. *Comentários à Lei nº 11.419/06 e as Práticas Processuais por meio Eletrônico nos Tribunais Brasileiros*. Curitiba: Juruá, 2010.

BRASIL. Instituto Nacional de Tecnologia da Informação. *Glossário ICP-Brasil*. Versão 1.2. Brasília, DF: ICP, 2007. Disponível em: <http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/Glossario/Glossario_ICP_Brasil_Versao_1.2_novo-2.pdf>. Acesso em: 08 out. 2014.

BRASIL. Instituto Nacional de Tecnologia da Informação. *Glossário ICP-Brasil*. Versão 1.4. Brasília, DF: ICP, 2010. Disponível em: <http://www.iti.gov.br/images/icp-brasil/Normas%20ICP-Brasil/Glossario/GLOSSaRIOV1.4.pdf>. Acesso em: 07 jul. 2014.

BRASIL. Instituto Nacional de Tecnologia da Informação. *Homepage*. Disponível em: <www.iti.gov.br>. Acesso em: 07 jul. 2014.

BRASIL. *Lei nº 5.869*, de 11 de janeiro de 1973. Institui o Código de Processo Civil. Disponível em: <www.senado.gov.br>. Acesso em: 19 set. 2014.

BRASIL. *Lei nº 10.406*, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406.htm>. Acesso em: 08 out. 2014.

BRASIL. *Lei nº 13.105*, de 16 de março de 2015. Código de Processo Civil. Disponível em: <www.senado.gov.br>. Acesso em: 01 jun. 2015.

CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais*. São Paulo: Saraiva, 2011.

DELLA VECHIA, Evandro. *Perícia Digital*: da investigação à análise forense. Campinas, SP: Millenium Editora, 2014.

FERNANDES, Joel Ribeiro. *Perícias em Áudios e Imagens Forenses*. Campinas, SP: Millenium Editora, 2013.

LEMOS, André. *Cibercultura, Tecnologia e Vida Social na Cultura Contemporânea*. 2. ed., Porto Alegre: Sulina, 2004.

LÉVY, Pierre. *Cibercultura*. Trad. Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

MARINONI, Luiz Guilherme; ARENHARDT, Sérgio Cruz. *Comentários ao Código de Processo Civil*. V. 5, t. 2, São Paulo: Revista dos Tribunais, 2000.

MARQUES, Antônio Terêncio G. L. *A Prova Documental na Internet*. Curitiba: Juruá, 2006.

PARENTONI, Leonardo Netto Parentoni Netto. *Documento Eletrônico*: aplicação e interpretação pelo Poder Judiciário. Curitiba: Juruá, 2007.

SOUZA, Carlos Affonso Pereira de. Contratos Eletrônicos e Responsabilidade Civil de Provedores. In: FUNDAÇÂO GETÚLIO VARGAS. *Direito Eletrônico*. Direito Rio. Programa de Capacitação em Poder Judiciário. Realização FGV, TRT4 e Escola Judicial do TRT4.

LEGISLAÇÃO

A legislação brasileira básica sobre internet compreende:

Lei nº 9.609/1998 (Lei de *software*): Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. (Definição de *software*);

Medida Provisória nº 2.200/01: institui a infraestrutura de chaves públicas brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

Lei nº 11.280/06: acrescentou o parágrafo único ao artigo 154 do CPC.

Lei nº 11.341/06: altera o parágrafo único do art. 541 do Código de Processo Civil - Lei nº 5.869, de 11 de janeiro de 1973, para admitir as decisões disponíveis em mídia eletrônica, inclusive na Internet, entre as suscetíveis de prova de divergência jurisprudencial.

Lei nº 11.419/06: 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;

Lei nº 12.965/14: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Lei nº 13.105, de 16 de março de 2015: novo Código de Processo Civil.

TERMOS TÉCNICOS

Algoritmo assimétrico: É um algoritmo de criptografia que usa duas chaves: uma chave pública e uma chave privada, onde a chave pública pode ser distribuída abertamente enquanto a chave privada é mantida secreta. Os algoritmos assimétricos são capazes de muitas operações, incluindo criptografia, assinaturas digitais e acordo de chave (BRASIL. Instituto Nacional de Tecnologia da Informação, 2010).

PIN (Personal Identification Number): Sequência de números e/ou letras (senha) usadas para liberar o acesso à chave privada, ou outros dados armazenados na mídia, somente para pessoas autorizadas.

PUK (Personal Identification Number Umblocking Key): Chave para desbloqueio do número de identificação pessoal (PIN), o qual normalmente fica bloqueado após várias tentativas inválidas.

Como o PIN, a senha PUK deve ser guardada de forma segura, pois ambas permitem, em dispositivos como tokens e smart cards, o acesso à chave privada de um titular de certificado. (BRASIL. Instituto Nacional de Tecnologia da Informação, 2010).

Arquivo digital: Conjunto de bits que formam uma unidade lógica interpretável por computador e armazenada em suporte apropriado (BRASIL. Arquivo Nacional, 2004).

Programa de computador: é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados (BRASIL, 1998).

Na Lei nº 12.965/14, constam ainda as definições:

Art. 5º Para os efeitos desta Lei, considera-se:

I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II - terminal: o computador ou qualquer dispositivo que se conecte à internet;

III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP (BRASIL, 2014).

REFERÊNCIAS

BRASIL. Arquivo Nacional. *Subsídios para um dicionário brasileiro de terminologia arquivística*. Rio de Janeiro: Conselho Nacional de Arquivos, 2004. Disponível em: <http://www.arquivonacional.gov.br/download/dic_term_arq.pdf>. Acesso em: 08 out. 2014.

BRASIL. Instituto Nacional de Tecnologia da Informação. *Glossário ICP-Brasil*. Versão 1.4. Brasília, DF: ICP, 2010. Disponível em: <http://www.iti.gov.br/images/icp-brasil/Normas%20ICP-Brasil/Glossario/GLOSSaRIOV1.4.pdf>. Acesso em: 07 jul. 2014.

BRASIL. *Lei nº 9.609*, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/ L9609.htm>. Acesso em: 05 jul. 2015.

BRASIL. *Lei nº 12.965*, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em: 05 jul. 2015.