

3 DOCUMENTO ELETRÔNICO

3.1 NOÇÃO DE DOCUMENTO

Todo fluxo de informações que gravitam pelo aparato tecnológico da informática e telemática e, notadamente, através da Internet, em algum momento consubstancia-se em um invólucro que confere à informação um suporte de palpabilidade digital, ou seja, a informação cede sua imaterialidade inata a um suporte sob forma de arquivo eletrônico, num dos diversos formatos desenvolvidos pela informática, sejam estes um arquivo de texto, de imagem, de áudio, vídeo, banco de dados, etc.

A nova figura do documento eletrônico guarda semelhanças com o conceito tradicional de documento, este substancialmente atrelado à idéia de algo escrito. Em vertente etimológica, documento, do latim *documentum (docere)* significa mostrar, indicar, instruir (Cfe. DE PLÁCIDO E SILVA, 1963, p. 561). É “qualquer escrito usado para consulta, estudo ou prova, etc (...). Escritura destinada a comprovar um fato; declaração escrita, revestida de forma padronizada, sobre fato(s) ou acontecimento(s) de natureza jurídica” (FERREIRA, 2004, p. 327). Enfim, documento é aquilo que posterga ao incerto, sobremodo para o futuro, a vivificação latente de fenômenos pretéritos.

A compreensão do fenômeno do documento eletrônico perpassa, inelutavelmente, pela revisitação das concepções clássicas do documento. CHIOVENDA (1998, p. 51) entendia o documento como “toda representação material destinada a reproduzir determinada manifestação do pensamento, como voz fixada duradouramente (*vox mortua*)”. Nesse passo, SANTOS (1997, p. 385) toma o documento como “coisa representativa de um fato”.

3.2 SOBRE O DOCUMENTO ELETRÔNICO

O documento eletrônico, por sua vez, também cumpre o mesmo desiderato. Em essência, não se diferencia do documento tradicional no tocante à cristalização de fenômenos do mundo. Difere, no entanto, por constituir-se em meio etéreo, tal qual o conteúdo que encerra, isto é, a informação de fato, coisa ou idéia, que contém.

LEIVA (2000), renomado jurista chileno, conceitua documento eletrônico da seguinte maneira:

Por documento eletrônico deve entender-se toda expressão em linguagem natural ou convencional e qualquer outra expressão gráfica, sonora, e em imagens, recolhidas em qualquer tipo de suporte material, inclusive os suportes informáticos, com eficácia probatória ou qualquer outro tipo de relevância jurídica.

Oportuno, ademais, conhecer que o documento eletrônico, em última análise, no tocante a seu aspecto tecnológico, reduz-se a uma determinada seqüência formada por linguagem binária (*bits*) que é interpretada pelos computadores, revelando-se a informação nele contida. Ou seja, a revelação do conteúdo do documento eletrônico, aquele fato ou pensamento ali fixado, dependerá da intermediação de um computador que converterá a linguagem de máquina (seqüência de *bits*) à linguagem humana. Contudo, é um processo automático, imperceptível àquele que acessa o documento. A respeito de tal particularidade, MARCACINI (2002, p. 66) afirma que “o documento eletrônico é, então, uma seqüência de bits que, traduzida por meio de um determinado programa de computador seja representativo de um fato”.

Além disso, é preciso aceitar que o documento eletrônico é, também, um documento escrito, mas na linguagem própria do meio do qual dimana (*bits*). A mesma linguagem, ademais, que ao mesmo tempo constrói a informação e o formato do arquivo que a guardará, ou seja, tudo se reduz à seqüência binária.

Com isto, SANTOS (2000, p. 186) afirma que:

tanto o suporte informático quanto o suporte tradicional se enquadram no conceito legal de documento, porquanto ambos podem representar um ato ou fato jurídico, e (...) a validade desse suporte depende da sua capacidade de se manter íntegro e não deteriorável, porquanto suportes sujeitos a adulterações sem deixar vestígios perdem confiabilidade.

Há, por evidente, hodiernamente, grande parença entre o documento eletrônico e o documento tradicional escrito em papel, tanto que o Dicionário Aurélio já traz como uma das significações de documento: “5 *Inform.* Qualquer arquivo com dados gerados por um aplicativo”. ALMEIDA FILHO e CASTRO (2005, p. 174) apontam que “o documento eletrônico, hoje, é uma realidade que parece ser imutável. Desta forma, o desprestígio de nossos legisladores ao tema já se torna um grave problema”.

3.3 DOCUMENTO ELETRÔNICO E TRADICIONAL

Em muito se assemelham o documento eletrônico e o documento tradicional escrito ou impresso em papel. Segundo LEIVA (2000),

Os documentos eletrônicos possuem os mesmos elementos que um documento escrito em papel: a) constam em um suporte material (fitas, disquetes, circuitos, chips de memória, redes); b) contêm uma mensagem, o que está escrito usando a linguagem convencional dos dígitos binários (*bits*), entidade magnéticas que os sentidos humanos não podem perceber diretamente; c) estão escritos em um idioma

ou código determinado; d) podem ser atribuídos a uma pessoa determinada na qualidade de autor, mediante uma assinatura eletrônica, senha ou chave eletrônica.

Já DONEDA (2002, p. 204) refere que:

dos novos meios de transmissão de vontade disponibilizados pela tecnologia da informação, alguns, como o **documento eletrônico**, têm se mostrado aptos a desempenhar a **função que hoje a escrita e mesmo a que a forma pública desempenham (...)** [grifou-se].

Com efeito, há forte tendência de se buscar soluções para a substituição, tanto quanto for possível, dos documentos escritos para os documentos eletrônicos.

3.4 NORMAS INTERNACIONAIS ACERCA DO DOCUMENTO ELETRÔNICO

A UNCITRAL, órgão especial das Nações Unidas voltada ao comércio internacional, elaborou a chamada Lei Modelo, traçando diretivas a todos os países que se embrenhem na missão de legislar sobre a documentação eletrônica em seus ordenamentos jurídicos. Já em seu art. 5º trata da validade jurídica dos documentos eletrônicos, ao fixar que “não se negarão efeitos jurídicos, validade e exequibilidade às informações apenas por estarem na forma de mensagem de dados”. Logo, a validade que não possa ser negada, de acordo com a Lei Modelo analisada, reside no não rechaçamento da informação porquanto a forma eletrônica não deva ser proibida por lei. A eficácia, ou força executória, consoante se possa extrair do dispositivo em análise, é a viabilidade de os documentos eletrônicos serem úteis à realização daquilo a que se propõe o seu conteúdo. Em verdade, a suposta eficácia perseguida decorre da não negação da validade, sem o que não há repercussão do documento eletrônico no meio social.

MARTINS e MACEDO (2002, p. 75) aduzem que a referida Lei Modelo, ao ansiar pela equiparação dos documentos eletrônicos ao documento em papel, “preconiza, portanto, a denominada equivalência funcional, equiparando, para fins de validade jurídica, a mensagem eletrônica a qualquer documento tradicional”.

Todavia, mais proliferantes são as legislações internacionais que tratam da assinatura digital e certificação digital. Nesse lastro, convém citar a Lei de Assinatura Digital do Estado de Utah (EUA) elaborada em 1995. Relevante, também, é a Diretiva 1999/93 da Comunidade Européia que manifesta que a assinatura digital dá margem à iminente criação de serviços de expedição e gestão de certificados digitais.

3.5 ASSINATURA E CERTIFICAÇÃO DIGITAIS

A suposta fragilidade dos documentos eletrônicos, decorrente da facilitada alterabilidade que constitui a própria natureza destes meios, notadamente lhes usurpou, por um longo período, a viabilidade de

galgarem menor repúdio na concretização de relações jurídicas, bem como na sua prova. Aliada a esta névoa de incredulidade esteve a impossibilidade de aposição de assinatura, atributo que permite verificar a autenticidade e autoria do documento por ela adornado.

Pesquisando a história, GICO JÚNIOR (2000, p. 350) relata que:

provavelmente até o século XVI, não bastava que o documento contivesse apenas o nome, era necessário que se firmasse também o selo real ou o brasão da família para que fosse dada autenticidade. Este costume perdeu força quando os senhores feudais deixaram de ser analfabetos, podendo livremente escrever e ler os nomes escritos.

A assinatura pessoal solidificou-se com importância tamanha que alçou patamar de qualidade única à garantia de autoria e autenticidade, mormente incrustada nos documentos cartulares, isto é, externados em escritos sobre papel.

Na malha das relações jurídicas que fazem uso do suporte das tecnologias de informação, especialmente a Internet, no todo ou em parte de seu estágio constitutivo, a necessidade de segurança é o anseio mais candente. O atingimento desse propósito encontra na técnica a solução que pode conferir, de acordo com MENKE (2005, p. 40):

(1) maior certeza quanto à autoria de declarações de vontade; (2) maior garantia acerca da integridade dos documentos eletrônicos, ou seja, quanto ao fato de que não foram alterados; (3) maior garantia no que se refere ao sigilo dos documentos, informações e dados transmitidos.

Tal solução reflete na figura da assinatura digital. É a assinatura digital espécie do gênero assinatura eletrônica. Esta considerada como “um sem-número de métodos de comprovação de autoria empregados no meio virtual” (MENKE, 2005, p. 42). Desse modo, estão contemplados pelo gênero “assinatura eletrônica”, os métodos de identificação biométricos, números de identificação pessoal, senhas de operações bancárias, digitalização de assinatura manuscrita, etc. De acordo com o guia para a incorporação ao direito interno da Lei Modelo da UNCITRAL para o comércio eletrônico, tais métodos devem buscar o emprego em ambiente eletrônico, de tantas quantas forem possíveis das funções da assinatura manuscrita.

Adote-se que a assinatura digital, uma das aparições de maior evidência da assinatura eletrônica, “é o resultado de uma operação matemática, utilizando algoritmos de criptografia assimétrica” (MARCACINI, 2002, p. 32), que permite a “associação de um indivíduo a uma declaração de vontade veiculada eletronicamente (...)” (MENKE, 2005, p. 42). Está-se que a assinatura digital adere sobremaneira ao aspecto da demonstração de autoria do documento eletrônico. Trazem MARTINS e MACEDO (2002, pp. 11-12) que a assinatura digital constitui um “processo de assinatura eletrônica baseado em sistema criptográfico que pode comportar dois



sistemas: o assimétrico ou com chave pública e o simétrico ou de chaves privadas”.

E a criptografia apresenta-se, então, como o método técnico responsável pela assinatura e certificação digitais, e que permite a integridade, veracidade e autoria dos documentos eletrônicos. A relevância da criptografia, como método capaz de conferir segurança aos documentos eletrônicos, reside no fato de que um terceiro, desconhecedor do código de cifragem, não poderá conhecer o conteúdo do documento criptografado.

Há, entretanto, duas modalidades de criptografia: a simetria e a assimétrica. Na primeira modalidade, a criptografia simétrica, “uma mesma senha, ou chave, é utilizada tanto para codificar como para decodificar a mensagem” (MARCACINI, 2002, p. 28). É criptografia de chave privada porque tanto o autor do documento, ou emissor da mensagem, como aquele interessado, ou destinatário, que acessará seu conteúdo, deverão estar de posse da mesma diretriz cifradora.

A segunda modalidade (criptografia assimétrica) é que se mostra prestável à certificação digital de documentos eletrônicos. A assimetria que lhe caracteriza ampara-se no uso de duas chaves (diretrizes de codificação e decodificação), díspares, porém intrinsecamente interligadas, uma pública e outra privada. Destas, somente a chave privada é mantida em sigilo, pelo signatário da mensagem ou documento; a chave pública, por seu turno, pode ser disponibilizada livremente a terceiros.

A chave é um código especial inserido no arquivo do documento eletrônico. Em acepção técnica, as chaves de criptografia são “combinação de letras e números bastante extensa, que não são criadas pelo usuário, mas sim por programas de computador” (MENKE, 2005, p. 46). Ou seja, o documento que for cifrado (criptografado) pela chave privada, somente pode ser decifrado (decriptografado) pela chave pública univitelina àquela.

Ao contrário do que ligeiramente possa dar ensejo, a técnica de criptografia assimétrica aplicada na assinatura digital, por seu par de chaves, não tem o condão de lacrar o documento afetado por esta e torná-lo inacessível a terceiros. A finalidade, quando cuida de assinatura digital, é diversa; harmoniza-se com a função atestadora de autenticidade do documento assinado digitalmente. Lastreando tal entendimento, MARTINS e MACEDO (2002, p. 49) afirmam que “o sistema assimétrico de criptografia de dados (PKI, *Public Infrastructure* ou, em português, ICP, Infra-estrutura de Chaves Públicas) tem como objetivo a proteção da autoria de uma mensagem que circula na rede”. A garantia da integridade do documento assinado digitalmente nasce e é verificável pelo mesmo par de chaves.

A atratividade da criptografia assimétrica reside na sua segurança em nível superlativo, em razão da coerente impossibilidade prática de ser quebrado o código de chaves públicas e privadas.

A pretensa inquebrantabilidade das chaves de criptografia assimétrica é que confere credibilidade à segurança que apregoam. Decorre, especialmente, de

que o aparato tecnológico que as concebe é, diante da atual capacidade tecnológica desenvolvida, em tese, intransponível.

Além de fixar a autoria do documento eletrônico, a assinatura digital, por criptografia assimétrica, garante a integridade daquele, de tal modo que, ao ser acessado por um receptor qualquer, e este aplicar-lhe a conferência por chave pública correspondente, será possível saber se o documento, após assinado pelo emitente, com sua chave privada, sofreu qualquer alteração antes de chegar ao destinatário. É que, na aplicação da chave cifradora “o código é de tal forma sensível que qualquer alteração no documento, ainda que de um único *bit*, invalida a fórmula utilizada” (GICO JÚNIOR, 2000, p. 348).

Neste ponto, é salutar recordar os plúrimos formatos dos documentos eletrônicos, e que todos, independentemente do conteúdo que revelam, podem ser assinados digitalmente. Oportuna, nesse íterim, portanto, a exposição de GICO JÚNIOR (2000, p. 347):

Os atuais programas de criptografia são capazes de cifrar um documento eletrônico, seja ele texto (e.g. uma peça processual, um título de crédito eletrônico), som (e.g. uma audiência gravada, uma confissão) ou imagem (e.g. uma fotografia, um documento digitalizado) e marcá-lo com uma assinatura digital.

Enfim, assinado digitalmente o documento eletrônico, aplicado-se-lhe, pelo receptor, a chave pública, atestada a sua autenticidade e integridade, emerge, então, questão de ímpar pertinência, qual seja a certeza de que a chave privada realmente pertence à pessoa que assinou o documento eletrônico.

Como exemplifica MARCACINI (2002, p. 51), em termos de técnica para geração de assinaturas digitais,

uma pessoa pode gerar em seu computador quantos pares de chaves desejar, fornecendo nomes alheios, reais ou imaginários. Por outro lado, as chaves são geradas mediante cálculos matemáticos e eventos aleatórios, não havendo nenhum laço que as ligue à pessoa do usuário.

Entram em cena, pois, a certificação digital e as autoridades certificadoras.

Vê-se que a certificação digital cumpre a função de associar a pessoa ou entidade a uma determinada chave pública. O papel primordial dos certificados digitais é o de vincular, com fidedignidade bastante, determinada chave pública ao seu apregoado titular (Cfe. ITI, 2005). Notável, nesse íterim, trazer à baila que um certificado digital¹ é também um documento eletrônico e, via de regra, apresenta, como inafastáveis, informações sobre a quem está associada a chave pública da assinatura, o período de validade do certificado, o código da chave pública, o nome e assinatura da entidade emitente do certificado, e um

¹ Para a Lei Modelo da UNCITRAL sobre assinaturas eletrônicas, um certificado digital é toda mensagem de dados ou outro registro que confirme o vínculo entre um signatário e os dados de criação da assinatura.



número de controle interno de série de emissão. Opera, mesmo, como uma espécie de chancela afirmando que a chave pública tem por titular quem denota sê-lo. Por conterem um conjunto de informações publicáveis, os certificados digitais são disponibilizados em repositórios públicos, para que terceiros possam conferir a autenticidade das assinaturas digitais que vierem examinar.

Os entes que promovem a certificação digital, conhecidos como Autoridades Certificadoras ou Infra-Estruturas de Chaves Públicas, são serviços com finalidade de atribuir certificados digitais aos terceiros interessados que buscam utilizar assinaturas digitais. Uma autoridade certificadora pode ser entendida com um terceiro de confiança atuante na garantia das assinaturas digitais incluídas nos documentos eletrônicos. De acordo com MENKE (2005, p. 56), tais entidades “desempenham tarefa de gerenciar o ciclo de vida dos certificados, uma vez que, a qualquer momento, pode haver necessidade de revogar e emitir novos certificados (...)”.

No Brasil, o pilar da certificação digital foi erigido pela Medida Provisória nº 2.200-2, de 24 de agosto de 2001, sob a nomenclatura de Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil)². O ente presta-se, de acordo com o art. 1º da Medida Provisória em comento, a “garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras”. A configuração básica da ICP-Brasil abarca uma autoridade gestora de políticas e uma cadeia de autoridades certificadoras, destacando-se a Autoridade Certificadora Raiz (Cf. art. 2º). Consoante assevera MENKE (2005, p. 101),

A Autoridade Certificadora Raiz – AC Raiz é um dos pilares da Infra-Estrutura de Chaves Públicas Brasileira. A função da Autoridade Certificadora Raiz é desempenhada pelo Instituto Nacional de Tecnologia da Informação – ITI, autarquia federal vinculada à Casa Civil da Presidência da República.

Além de criar a Infra-Estrutura de Chaves Pública, a Medida Provisória 2.200-2 alcançou o mérito de versar sobre “os efeitos jurídicos produzidos por uma declaração de vontade assinada com certificado emitido no âmbito da ICP-Brasil bem como sobre os efeitos jurídicos emanados de outros meios de comprovação de autoria” (MENKE, 2005, p. 99).

Ao contrário, entretanto, do que primeiramente se possa sugerir, nada há de visionário no universo das assinaturas e certificações digitais. Ainda que a

técnica que lhes concebe seja complexa, e que aparentam ser soluções muito distantes da vida cotidiana, já têm sido objeto de situações às quais o legislador, ainda que em apáticas oportunidades, lhes dedicou tratamento, bem como outras levadas ao conhecimento do judiciário, além de fazerem parte do cotidiano da vida das pessoas, sem que disso se apercebam.

Mister se faz assentar que a Lei nº 10.740, de 1º de outubro de 2003, ao implantar o registro digital do voto, fixou a assinatura digital como mecanismo de segurança ao registro de votos em urna eletrônica³.

O Judiciário não esteve alheio ao fenômeno, ainda que tenha demonstrado maior cautela à rápida absorção da assinatura e certificação digital como aporte para o valor jurídico dos documentos eletrônicos.

A assinatura digital, aliás, galgou acolhimento pelos órgãos judiciários nos sistemas de peticionamento eletrônico, com vistas, reconhecidamente, à celeridade e economia processual⁴.

O assentamento do fenômeno de assinaturas digitais, porém, logrou modificar, ainda que vagarosamente, o entendimento jurisprudencial. Com propriedade, referindo-se à igualação da assinatura digital com a assinatura manuscrita, devendo-se-lhe atribuir isonômico valor, em Acórdão do Tribunal de Justiça de São Paulo, assim se pronunciou o relator: “a assinatura digital em nada interferiria em página da Internet, e, ademais, ao contrário do alegado **já existe regulamentação legal acerca da matéria, que aliás equipara documento assinado digitalmente ao documento cartáceo**” (TJSP. Emb. Dec. 345.203-4/0-01, Rel. Munhoz Soares, 12.08.2004) [grifou-se].

Enfim, a avultada importância e credibilidade conferida pelo Poder Judiciário aos sistemas de assinatura e certificação digital pode ser percebida na seguinte ementa da jurisprudência do TST:

AGRAVO. TRANSMISSÃO DO APELO POR E-MAIL. NECESSIDADE DE CERTIFICAÇÃO DIGITAL ACEITA PELA ICP-BRASIL. INAPLICABILIDADE DA LEI Nº 9.800/99. INTEMPESTIVIDADE. AUSÊNCIA DE DEMONSTRAÇÃO DO DESACERTO DO DESPACHO AGRAVADO. (...). **O envio de recurso por correio eletrônico é juridicamente aceitável apenas se houver certificação digital reconhecida pela ICP-Brasil, nos termos da MP 2.200-2/01. Logo, é juridicamente inexistente petição apresentada por intermédio de e-mail sem qualquer tipo de certificação digital (...)** (TST. AIRR 730172. 4ª T. Rel. Min. Ives Gandra Martins Filho, DJ 13.02.2004) [grifou-se].

³ “Art. 59 (...)”

⁴ A urna eletrônica disporá de recursos que, mediante assinatura digital, permitam o registro digital de cada voto e a identificação da urna em que foi registrado, resguardado o anonimato do eleitor.

⁴ Idéia similar pode ser encontrada em CARVALHO FILHO, 2005; e: “Considerando as vantagens propiciadas pela tecnologia de Infra-Estrutura de Chaves Públicas Brasileiras - ICP-Brasil, que permite a transmissão de dados de maneira segura, **criando facilidade de acesso e economia de tempo e de custos ao jurisdicionado**” (Instrução Normativa nº 28, TST) [grifou-se].

² Dado que o presente estudo não tem o escopo de analisar a atuação, constituição e funcionamento da Estrutura de Chaves Públicas Brasileira, recomenda-se, com vistas a pretensão aprofundamento: MENKE, Fabiano. **Assinatura eletrônica no direito brasileiro**. São Paulo: Revista dos Tribunais, 2005. Paralelamente, insta conhecer a legislação e regulamentação da ICP-Brasil, disponível do site da autarquia, em www.icpbrasil.gov.br.

