O DOCUMENTO ELETRÔNICO E A ASSINATURA DIGITAL
(Uma visão geral)

Aldemario Araujo Castro
Procurador da Fazenda Nacional
Professor de Informática Jurídica e Direito da Informática
da Universidade Católica de Brasília
Brasília, 30 de outubro de 2001

I. DOCUMENTO ELETRÔNICO

Por documento entende-se a "coisa representativa de um fato" (Moacyr Amaral Santos). Nesta idéia, o termo "coisa" pode ser reputado como fundamental ou essencial e indicativo, ou não, da presença de algo material. O afastamento da materialidade por ser obtido pela mitigação da forma, assumindo importância decisiva o aspecto funcional do registro do fato. Por outro lado, a palavra em questão pode ser tomada no sentido de "tudo o que existe" ou "realidade absoluta (por oposição a aparência, ou representação)".

Assim, o documento eletrônico pode ser entendido como a representação de um fato concretizada por meio de um computador e armazenado em formato específico (organização singular de *bits* e *bytes*), capaz de ser traduzido ou apreendido pelos sentidos mediante o emprego de programa (*software*) apropriado. **(1)**

A partir do conjunto normativo aplicável **(2)** **(3)** e mesmo das considerações acerca da materialidade do documento são encontradas duas correntes jurídicas quanto à existência e validade dos chamados documentos eletrônicos **(4)**. Uma delas, sustenta a impossibilidade jurídica do documento eletrônico. A outra, admite a existência e a validade dos documentos eletrônicos. Esta última desdobra-se em duas vertentes: a que admite o documento eletrônico como realidade jurídica válida por si e a que somente aceita o documento eletrônico com o atendimento de certos requisitos, dada a sua volatilidade e a ausência de traço personalíssimo de seu autor.

Entendemos, afastando o critério de interpretação literal (e restritivo), fundado sobretudo nos arts. 368 ("escrito e assinado"), 369 ("reconhecer a firma do signatário"), 371 ("assinar"), 374 ("assinado"), 376 ("escreveu"), 386 ("entrelinha, emenda, borrão ou cancelamento"), entre outros, do Código de Processo Civil, que a existência e validade do documento eletrônico em si não pode ser recusada. Afinal, adotado um raciocínio hermenêutico sistemático **(5)** e consentâneo com a evolução histórica das tecnologias manuseadas pelo homem, verificamos o império da

liberdade de forma no direito pátrio. Não custa lembrar a aceitação inquestionável do contrato verbal. Assim, quem pode o mais pode o menos (argumento "*a maiori ad minus*").

A conhecida lei modelo da UNCITRAL (Comissão das Nações Unidas para leis de comércio internacional) sobre comércio eletrônico, que a busca a uniformização internacional da legislação sobre o tema, consagra em seu art. 5o.: "*Não se negarão efeitos jurídicos, validade ou eficácia à informação apenas porque esteja na forma de mensagem eletrônica*".

A utilização e aceitação jurídica do documento eletrônico é crescente, independentemente da aplicação, na sua confecção, de certas técnicas de segurança. Neste sentido, encontramos importantes decisões judiciais **(6)** e diplomas legais **(7)**.

Com certeza, a volatilidade e a ausência de traço personalíssimo do autor fragilizam o documento eletrônico. Surge, assim, o grande e crucial problema da eficácia ou validade probatória do mesmo, resolvido, como veremos adiante, por modernas técnicas de criptografia.

As dificuldades, no campo probatório, do "documento eletrônico puro" (desprovido de técnicas, acréscimos ou requisitos de "segurança") deverão ser superadas, na linha do livre convencimento, pelo recurso a todos os elementos e circunstâncias envolvidos na sua produção e transmissão.

Merece destaque a noção de cópia de documento eletrônico. Deve ser assim considerada "*... o documento eletrônico resultante da digitalização de documento físico, bem como a materialização física de documento eletrônico original*" (conforme o Anteprojeto de Lei apresentado pela OAB/SP).

A edição da Medida Provisória n. 2.200, de 28 de junho de 2001, responsável pela fixação do quadro regulamentório da assinatura digital no Brasil, suscitou um problema novo em relação à validade jurídica do documento eletrônico. Com efeito, o art. 1o. do diploma legal referido afirma: "*Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, (...)*". Como posto, é possível a interpretação de que a Medida Provisória não trata apenas da validade probatória do documento eletrônico, e sim, da validade jurídica do próprio documento em forma eletrônica.

Nossa opinião, na linha dos argumentos anteriormente apresentados, relacionados, sobretudo, com a liberdade de forma e admissão de contratos verbais no direito brasileiro, é de que a Medida Provisória n. 2.200, de 2001, trata, embora com redação deficiente, da validade ou eficácia probatória dos documentos eletrônicos.

Lembramos, neste particular, que o projeto de lei submetido à consulta pública pela Casa Civil da Presidência da República no final do ano 2000,

estabelecia que os documentos eletrônicos teriam o mesmo valor jurídico daqueles produzidos em papel desde que fosse assegurada a sua antenticidade e integridade **(8)**. A supressão da expressão "desde que" e a fixação de que a Infra-Estrutura de Chaves Públicas visa garantir a autenticidade, a integridade e a validade jurídica dos documentos eletrônicos, apontam para o aspecto funcional, para a agregação de um valor ou característica antes inexistente, para a validade probatória.

II. ASSINATURA DIGITAL

Como já vimos, se por um lado o documento eletrônico existe e é válido juridicamente, por outro lado, subsiste, diante de sua fugacidade, o crucial problema da eficácia ou validade probatória do mesmo. A indagação se impõe: como garantir autenticidade e integridade ao documento eletrônico? **(9)**

A resposta, para os padrões tecnológicos atuais, consiste na utilização da chamada assinatura digital baseada na criptografia assimétrica de chave pública (e chave privada). A rigor, num par de chaves matematicamente vinculadas entre si.

Neste ponto cumpre observar a realização da "máxima" de que os novos problemas trazidos pela tecnologia deverão ter solução buscada no âmbito tecnológico.

A criptografia consiste numa técnica de codificação de textos de tal forma que a mensagem se torne ininteligível para quem não conheça o padrão utilizado. Sua origem remonta às necessidades militares dos romanos (Escrita cifrada de César).

O padrão criptográfico manuseado para cifrar ou decifrar mensagens é conhecido como chave. Quando a mesma chave é utilizada para cifrar e decifrar as mensagens temos a denominada criptografia simétrica ou de chave privada, normalmente utilizada em redes fechadas ou computadores isolados. Quando são utilizadas duas chaves distintas, mas matematicamente vinculadas entre si, uma para cifrar a mensagem e outra para decifrá-la **(10)**, temos a criptografia assimétrica ou de chave pública, vocacionada para utilização em redes abertas como a Internet.

A criptografia moderna lança mão de conceitos técnicos avançados para a cifragem das mensagens: os algoritmos. Estes, numa visão singela, consistem em fórmulas matemáticas extremamente complexas, utilizadas para geração dos padrões ou chaves criptográficas.

Como funciona a assinatura digital (baseada na criptografia assimétrica) de um texto ou mensagem eletrônica? Na sistemática atualmente adotada, aplica-se sobre o documento editado ou confeccionado um algoritmo de autenticação conhecido como *hash* **(11) (12)**. A aplicação do algoritmo *hash* gera um resumo do conteúdo do documento conhecido como *message digest*, com tamanho em torno de

128 bits. Aplica-se, então, ao *message digest*, a chave privada do usuário, obtendo-se um *message digest* criptografado ou codificado. O passo seguinte consiste um anexar ao documento em questão a chave pública do autor, presente no arquivo chamado certificado digital. Podemos dizer que assinatura digital de um documento eletrônico consiste nestes três passos: a) geração do *message digest* pelo algoritmo *hash*; b) aplicação da chave privada ao *message digest*, obtendo-se um *message digest* criptografado e c) anexação do certificado digital do autor (contendo sua chave pública). Destacamos, neste passo, um aspecto crucial. As assinaturas digitais, de um mesmo usuário, utilizando a mesma chave privada, serão diferentes de documento para documento. Isto ocorre porque o código *hash* gerado varia em função do conteúdo de cada documento.

E como o destinatário do texto ou mensagem assinada digitalmente terá ciência da integridade (não alteração/violação) e autenticidade (autoria) do mesmo? Ao chegar ao seu destino, o documento ou mensagem será acompanhado, como vimos, do *message digest* criptografado e do certificado digital do autor (com a chave pública nele inserida). Se o aplicativo utilizado pelo destinatário suportar documentos assinados digitalmente ele adotará as seguintes providências: a) aplicará o mesmo algoritmo *hash* no conteúdo recebido, obtendo um *message digest* do documento; b) aplicará a chave pública (presente no certificado digital) no *message digest* recebido, obtendo o *message digest* decodificado e c) fará a comparação entre o message digest gerado e aquele recebido e decodificado. A coincidência indica que a mensagem não foi alterada, portanto mantém-se íntegra. A discrepância indica a alteração/violação do documento depois de assinado digitalmente.

É justamente este o mecanismo utilizado para viabilizar as chamadas conexões seguras na Internet (identificadas pela presença do famoso ícone do cadeado amarelo). Para o estabelecimento de uma conexão deste tipo, o servidor acessado transfere, para o computador do usuário, um certificado digital (com uma chave pública). A partir deste momento todas as informações enviadas pelo usuário serão criptografadas com a chave pública recebida e viajarão codificadas pela Internet. Assim, somente o servidor acessado, com a chave privada correspondente, poderá decodificar as informações enviadas pelo usuário.

Subsiste, entretanto, o problema da autenticidade (autoria). Portanto, a sistemática da assinatura digital (baseada na criptografia assimétrica) necessita de um instrumento para vincular o autor do documento ou mensagem, que utilizou sua chave privada, a chave pública correspondente. Em conseqüência, também o problema da segurança ou confiabilidade da chave pública a ser utilizada precisa ser resolvido. Esta função (de vinculação do autor a sua respectiva chave pública) fica reservada para as chamadas entidades ou autoridades certificadoras.

Assim, a função básica da entidade ou autoridade certificadora está centrada na chamada autenticação digital, onde fica assegurada a identidade do proprietário das chaves. A autenticação é provada por meio daquele arquivo chamado de certificado digital. Nele são consignadas várias informações, tais como:

nome do usuário, chave pública do usuário, validade, número de série, entre outros. Este arquivo, também um documento eletrônico, é assinado digitalmente pela entidade ou autoridade certificadora.

O sistema de criptografia assimétrica permite o envio de mensagens com total privacidade. Para tanto, o remetente deve cifrar o texto utilizando a chave pública do destinatário. Depois, ele (o remetente) deverá criptografar o texto com a sua chave privada. O destinatário, ao receber a mensagem, irá decifrá-la utilizando a chave pública do remetente. O passo seguinte será aplicar a própria chave privada para ter acesso ao conteúdo original da mensagem.

O processo de regulamentação da assinatura digital no Brasil pode ser dividido, até o presente momento, em 6 (seis) fases ou etapas. São elas:

1. Projetos

Num primeiro momento, notamos a presença de uma série de projetos de lei tratando do assunto. Vejamos os principais:

1.1. Lei Modelo das Nações Unidas sobre Comércio Eletrônico. Em 1996, a Organização das Nações Unidas, por intermédio da Comissão das Nações Unidas para leis de comércio internacional (UNCITRAL), desenvolveu uma lei modelo buscando a maior uniformização possível da legislação sobre a matéria no plano internacional. Na parte concernente a assinatura digital, a lei modelo consagra o princípio da neutralidade tecnológica, não se fixando em técnicas atuais e possibilitando a inovação tecnológica sem alteração na legislação. Deixa as especificações técnicas para o campo da regulamentação, mais afeita a modificações decorrentes de novas tecnologias.

1.2. Projeto de Lei n. 672, de 1999, do Senado Federal. Incorpora, na essência, a lei modelo da UNCITRAL.

1.3. Projeto de Lei n. 1.483, de 1999, da Câmara dos Deputados. Em apenas dois artigos, pretende instituir a fatura eletrônica e a assinatura digital (certificada por órgão público).

1.4. Projeto de Lei n. 1.589, de 1999, da Câmara dos Deputados. Elaborado a partir de anteprojeto da Comissão de Informática Jurídica da OAB/SP, dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital. Adota o sistema de criptografia assimétrico como base para a assinatura digital e reserva papel preponderante para os notários. Com fundamento no art. 236 da Constituição e na Lei n. 8.935, de 1994, estabelece que a certificação da chave pública por tabelião faz presumir a sua autenticidade, enquanto aquela feita por particular não gera o mesmo efeito. **(13)**

Deve ser registrado que o Projeto 1.589 está apenso ao 1.483 e, ambos, encontram-se sob a apreciação de uma comissão parlamentar especial na Câmara dos Deputados.

2. Edição de Decreto pelo Governo Federal

Com a edição do Decreto n. 3.587, de 5 de setembro de 2000, foi instituída a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal. Estava, então, criado um sistema de assinaturas digitais, baseado na criptografia assimétrica, a ser utilizado no seio da Administração Pública Federal.

3. Projeto de Lei submetido à consulta pública pelo Governo Federal

No mês de dezembro de 2000, a Casa Civil da Presidência da República submeteu à consulta pública um projeto de lei dispondo sobre a autenticidade e valor jurídico e probatório de documentos eletrônicos produzidos, emitidos ou recebidos por órgãos públicos. A proposta definia que a autenticidade e a integridade dos documentos eletrônicos decorreriam da utilização da Infra-Estrutura de Chaves Públicas criada por decreto meses antes. A proposição consagrava profundos equívocos, notadamente a não inclusão de documentos eletrônicos trocados entre particulares e a caracterização de que os documentos eletrônicos não tinham validade jurídica sem os procedimentos ali previstos.

4. Apresentação de substitutivo para apreciação de Comissão Especial da Câmara dos Deputados

No final do mês de junho de 2001, o Deputado Júlio Semeghini, Relator do Projeto de Lei n. 1.483 (e do Projeto de Lei n. 1.589 - apensado), apresentou Substitutivo aos projetos referidos, consolidando as propostas e agregando aperfeiçoamentos. O trabalho apresentado pelo relator decorreu de uma rotina de atividades, com início registrado em maio de 2000, envolvendo discussões internas e audiências públicas da Comissão Especial.

Em relação à assinatura digital, o Substitutivo adotou o sistema baseado na criptografia assimétrica, ressalvando a possibilidade de utilização de outras modalidades de assinatura eletrônica que satisfaçam os requisitos pertinentes. Estabeleceu, ainda, o Substitutivo, um modelo de certificação no qual podem atuar entidades certificadoras públicas e privadas, independentemente de autorização

estatal. Fixou, entretanto, que somente a assinatura digital certificada por entidade credenciada pelo Poder Público presume-se autêntica perante terceiros.

5. Edição da Medida Provisória 2.200

No dia 29 de junho de 2001, o Diário Oficial da União veiculou a Medida Provisória n. 2.200. Este diploma legal instituiu a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil para garantir a autenticidade e a integridade de documentos eletrônicos através da sistemática da criptografia assimétrica.

A organização da ICP-Brasil, a ser detalhada em regulamento, comporta uma autoridade gestora de políticas (Comitê Gestor da ICP-Brasil) e uma cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz (Instituto Nacional de Tecnologia da Informação - ITI), pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

À AC Raiz, primeira autoridade da cadeia de certificação, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC (de nível imediatamente subseqüente ao seu), sendo vedado emitir certificados para o usuário final. Às AC, órgãos ou entidades públicas e pessoas jurídicas de direito privado, compete emitir, expedir, distribuir, revogar e gerenciar os certificados de usuários finais. Às AR, entidades operacionalmente vinculadas a determina AC, compete identificar e cadastrar usuários, na presença destes, e encaminhar solicitações de certificados às AC.

O modelo centralizado adotado, vedando a certificação não derivada da AC Raiz, gerou profundas críticas **(14)**. Nas edições subseqüentes da MP n. 2.200, apesar de mantido o modelo centralizado **(15)**, único gerador da presunção de veracidade em relação ao signatário do documento eletrônico, admitiu-se a utilização de outros meios de comprovação de autoria e integridade, inclusive os que utilizem certificados não emitidos pela ICP-Brasil. Outro aspecto digno de nota é a definição de que o par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

6. Aprovação de substitutivo (com alterações) pela Comissão Especial da Câmara dos Deputados

No final de setembro de 2001, a Comissão Especial da Câmara dos Deputados aprovou, com várias alterações, o Substitutivo do Relator (Deputado Júlio Semeghini). A rigor, o novo texto ajustou-se a Medida Provisória da ICP-Brasil, aceitando a autoridade certificadora raiz. Foi criado um credenciamento provisório

até a completa operacionalização do modelo da ICP-Brasil.

Como afirmamos, o problema da identificação e da integridade dos documentos eletrônicos encontrou solução por meio da assinatura digital, baseada na criptografia assimétrica **(16)**. A assinatura digital, vale registrar, é apenas uma das espécies de assinatura eletrônica, abrangente de vários métodos ou técnicas, tais como: senhas, assinaturas tradicionais digitalizadas, chancela, biometria (íris, digital, timbre de voz), entre outras.

III. NOTAS

(1) "documento eletrônico: a informação gerada, enviada, recebida, armazenada ou comunicada por meios eletrônicos, ópticos, opto-eletrônicos ou similares." (art. 2o., inciso I do Projeto de Lei sobre documento eletrônico, assinatura digital e comércio eletrônico aprovado por Comissão Especial da Câmara dos Deputados).

(2) As principais normas com força de lei, no ordenamento jurídico brasileiro, aplicáveis aos documentos são as seguintes:

Código Civil:

"Art. 82. A validade do ato jurídico requer agente capaz, objeto lícito e forma prescrita ou não defesa em lei."

"Art. 129. A validade das declarações de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir."

"Art. 136. Os atos jurídicos, a que se não impõe forma especial, poderão provar-se mediante:

I - Confissão;

II - Atos processados em juízo;

III - Documentos públicos ou privados;

IV - Testemunhas;

V - Presunção;

VI - Exames e vistorias;

VII - Arbitramento."

"Art. 1.079. A manifestação de vontade, nos contratos, pode ser tácita, quando a lei não exigir que seja expressa."

"Art. 1.081. (...) Considera-se também presente a pessoa que contrata por meio de telefone."

Código de Processo Civil:

"Art. 131. O juiz apreciará livremente a prova, atendendo aos fatos e circunstâncias constantes dos autos, ainda que não alegados pelas partes; mas deverá indicar, na sentença, os motivos que lhe formaram o convencimento."

"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."

"Art. 244. Quando a lei prescrever determinada forma, sem cominação de nulidade, o juiz considerará válido o ato se, realizado de outro modo, lhe alcançar a finalidade."

"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."

"Art. 368. As declarações constantes do documento particular, escrito e assinado, ou somente assinado, presumem-se verdadeiras em relação ao signatário.

Parágrafo único. Quando, todavia, contiver declaração de ciência, relativa a determinado fato, o documento particular prova a declaração, mas não o fato declarado, competindo ao interessado em sua veracidade o ônus de provar o fato."

"Art. 369. Reputa-se autêntico o documento, quando o tabelião reconhecer a firma do signatário, declarando que foi aposta em sua presença."

"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;

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. 374. O telegrama, o radiograma ou qualquer outro meio de transmissão tem a mesma força probatória do documento particular, se o original constante da estação expedidora foi assinado pelo remetente.

Parágrafo único. A firma do remetente poderá ser reconhecida pelo tabelião, declarando-se essa circunstância no original depositado na estação expedidora."

"Art. 376. As cartas, bem como os registros domésticos, provam contra quem os escreveu quando:

I - enunciam o recebimento de um crédito;

II - contêm anotação, que visa a suprir a falta de título em favor de quem é apontado como credor;

III - expressam conhecimento de fatos para os quais não se exija determinada prova."

"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."

"Art. 386. O juiz apreciará livremente a fé que deva merecer o documento, quando em ponto substancial e sem ressalva contiver entrelinha, emenda, borrão ou cancelamento."

"Art. 388. Cessa a fé do documento particular quando:

I - lhe for contestada a assinatura e enquanto não se Ihe comprovar a veracidade;

II - assinado em branco, for abusivamente preenchido.

Parágrafo único. Dar-se-á abuso quando aquele, que recebeu documento assinado, com texto não escrito no todo ou em parte, o formar ou o completar, por si ou por meio de outrem, violando o pacto feito com o signatário."

(3) O novo Código Civil, já aprovado no âmbito do Congresso Nacional, não altera as considerações aqui formuladas. Com efeito, o seu art. 104 repete a fórmula do atual art. 82; o futuro art. 107 mantém os termos do art. 129 e o vindouro art. 212 conserva o espírito do atual art. 136. O futuro art. 428 contempla a contratação por telefone ou meio de comunicação semelhante, na linha do atual art. 1.081. Ademais, o novo art. 225 estabelece literalmente: "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." (Texto obtido no seguinte endereço eletrônico: http://www.intelligentiajuridica.com.br).

(4) "Vários são os trabalhos que vêm sendo desenvolvidos visando a negar ou afirmar a validade jurídica de documento quando gerado em meio digital, Cfr., entre tantos outros, os trabalhos de Ricardo Luis Lorenzetti, "Informática, Cyberlaw, E-Commerce", nesta obra coletiva; Frédérique Dupuis-Toubol, "Contracting on the Net: proof of transaction", ob. cit.; Silvânio Covas, "O COntrato no ambiente virtual. Contratação por Meio de Informática", ob. cit.; Davi Monteiro Diniz, Documentos Eletrônicos, Assinaturas Digitais, ob. cit.; José Henrique Barbosa Moreira Lima Neto, "Aspectos Jurídicos do Documento Eletrônico", ob. cit,; Giovanni Buonomo, Atti e Documenti in Forma Digitale, ob. cit.; Andrea Graziozi, "Premesse ad una teoria probatoria del documento informatico", ob. cit.; Paolo Piccoli e Giovanna Zanolini, "II Documento Elettronico e la Firma Digitale", ob. cit." Queiróz, Regis Magalhães Soares de. Assinatura Digital e o Tabelião Virtual. Nota 44. Pág. 385. Publicado em Direito e Internet. Aspectos Jurídicos Relevantes. EDIPRO.

(...) entendemos que quando assegurados os quatro requisitos acima exposto, seria teoricamente possível, em casos em que nõ saão exigidas formalidades específicas, atribuir-se validade jurídica ao documento eletrônico." Queiróz, Regis Magalhães Soares de. Assinatura Digital e o Tabelião Virtual. Págs. 385/386. Publicado em Direito e Internet. Aspectos Jurídicos Relevantes. EDIPRO.

"Quanto ao valor probatório, não há obstáculos para que o juiz no domínio de suas faculdades reconheça esses documento (eletrônicos), porém subsiste a incerteza com respeito à possibilidade de no caso se avaliar não tratar-se de um instrumento seguro. NO direito vigente existe então uma importante tendênciaencaminhada para a admissão dos documentos eletrônicos, tanto no que toca à sua validade quanto no que toca à sua eficácia probatória. Todavia, é necessário consagrar uma regra clara e especificar as condições técnicas nas quais esses documentos reúnam as qualidades de seguros e indeléveis." Lorenzetti, Ricardo Luis. Informática, Cyberlaw, E-commerce. Pág. 427. Publicado em Direito e Internet. Aspectos Jurídicos Relevantes. EDIPRO.

(5) "Contra, José Henrique Barbosa Moreira Lima Neto, entendendo que há várias leis que equiparam documento ao 'escrito', o que inviabilizaria a interpretação sistemática". Queiróz, Regis Magalhães Soares de. Assinatura Digital e o Tabelião Virtual. Nota 48. Pág. 386. Publicado em

Direito e Internet. Aspectos Jurídicos Relevantes. EDIPRO.

(6) "ARROLAMENTO - CERTIDÃO NEGATIVA DE TRIBUTOS FEDERAIS - Obtenção por consulta ao endereço eletrônico da Procuradoria-Geral da Fazenda Nacional. Validade. Existência de Portaria do Procurador-Geral da Fazenda Nacional (Portaria n. 414/98), conferindo a essa certidão os mesmo efeitos da certidão negativa expedida pelas unidades da Procuradoria. Recurso provido (TJSP - 8ª Câm. de Direito Privado; Ag. de Instr. n° 105.464.4/7-São Paulo-SP; Rel. Des. Cesar Lacerda ; j. 17.03.1999; v.u.).

ACÓRDÃO

Vistos, relatados e discutidos estes autos de AGRAVO DE INSTRUMENTO n° 105.464-4/ 7, da Comarca de SÃO PAULO, em que é agravante R.R., inventariante do ..., sendo agravado O JUÍZO:

ACORDAM, em oitava Câmara de Direito Privado do Tribunal de Justiça do Estado de São Paulo, por votação unânime, dar provimento ao recurso, de conformidade com o relatório e voto do Relator, que ficam fazendo parte do acórdão.

O julgamento teve a participação dos Desembargadores RICARDO BRANCATO (Presidente, sem voto), HAROLDO LUZ e EGAS GALBIATTI.

São Paulo, 17 de março de 1999.

CESAR LACERDA

Relator

VOTO

Cuida-se de agravo de instrumento inter-posto pelo .. , através de seu inventariante, R.R., nos autos do arrolamento dos bens deixados pela falecida, contra a respeitável decisão reproduzida a fls. 51 , que determinou a juntada de certidão negativa da Receita Federal, não aceitando documento acostado.

Sustenta a agravante que, com a determinação do Juízo para que fossem apresentadas certidões negativas de débitos fiscais, a certidão negativa da dívida ativa da União foi obtida junto à Receita Federal pela Internet. Assevera que a certidão expedida por consulta eletrônica foi validada, para todos os fins, pela Portaria n° 414/98, não havendo razão para seu indeferimento.

Recurso regularmente processado, com informações prestadas pelo MM. Juiz (fls. 63/ 64).

É o relatório.

O agravo comporta provimento.

Os elementos dos autos demonstram que o inventariante atendeu à exigência de comprovação de inexistência de tributos federais, mediante apresentação de certidão negativa obtida por consulta ao endereço eletrônico da Procuradoria-Geral da Fazenda Nacional, via Internet.

A expedição da referida certidão é fruto da evolução tecnológica e se amolda ao espírito desburocratizante que tem informado os tempos modernos, encontrando fundamento na Portaria n° 414, de 15.07.98, do Procurador-Geral da Fazenda Nacional, que estabelece:

"Artigo 1 ° - Fica instituída a Certidão Negativa quanto à Dívida Ativa da União, emitida por meio da

INTERNET.

§ 1 ° - Da certidão a que se refere este artigo, constará, obrigatoriamente, a hora e data da emissão.

§ 2° - A certidão a que se refere este artigo produzirá os mesmos efeitos da certidão negativa emitida por qualquer das unidades da Procuradoria-Geral da Fazenda Nacional e será válida por 30 dias. "

O Código de Processo Civil prevê que os atos e termos do processo não dependem de forma determinada, exceto quando a lei expressamente exigir (artigo 154).

O Diploma Processual também estatui que "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" (artigo 383).

A própria Receita Federal admite, mediante portaria, a validade da certidão negativa obtida por meio eletrônico, não havendo razão jurídica relevante para negar validade ao documento.

Diante do exposto, dá-se provimento ao recurso, para o fim de que seja aceita a certidão negativa obtida por meios eletrônicos.

São Paulo, 04 de março de 1999.

CESAR LACERDA

Relator"

(7) "Instrução Normativa SRF nº 86, de 22 de Outubro de 2001

DOU de 23.10.2001

Dispõe sobre informações, formas e prazos para apresentação dos arquivos digitais e sistemas utilizados por pessoas jurídicas.

O SECRETÁRIO DA RECEITA FEDERAL no uso da atribuição que lhe confere o inciso III do art. 209 do Regimento Interno da Secretaria da Receita Federal, aprovado pela Portaria MF no 259, de 24 de agosto de 2001, e tendo em vista o disposto no art. 11 da Lei nº 8.218, de 29 de agosto de 1991, alterado pela Lei nº 8.383, de 30 de dezembro de 1991, com a redação dada pelo art. 72 da Medida Provisória nº 2.158-35, de 24 de agosto de 2001, resolve:

Art. 1º As pessoas jurídicas que utilizarem sistemas de processamento eletrônico de dados para registrar negócios e atividades econômicas ou financeiras, escriturar livros ou elaborar documentos de natureza contábil ou fiscal, ficam obrigadas a manter, à disposição da Secretaria da Receita Federal (SRF), os respectivos arquivos digitais e sistemas, pelo prazo decadencial previsto na legislação tributária.

Parágrafo único. As empresas optantes pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte (Simples), de que trata a Lei nº 9.317, de 5 de dezembro de 1996, ficam dispensadas do cumprimento da obrigação de que trata este artigo.

Art. 2º As pessoas jurídicas especificadas no art. 1º, quando intimadas pelos Auditores-Fiscais da Receita Federal, apresentarão, no prazo de vinte dias, os arquivos digitais e sistemas contendo informações relativas aos seus negócios e atividades econômicas ou financeiras.

Art. 3º Incumbe ao Coordenador-Geral de Fiscalização, mediante Ato Declaratório Executivo (ADE), estabelecer a forma de apresentação, documentação de acompanhamento e especificações técnicas dos arquivos digitais e sistemas de que trata o art. 2º.

§ 1º Os arquivos digitais referentes a períodos anteriores a 1º de janeiro de 2002 poderão, por opção da pessoa jurídica, ser apresentados na forma estabelecida no caput.

§ 2º A critério da autoridade requisitante, os arquivos digitais poderão ser recebidos em forma diferente da estabelecida pelo Coordenador-Geral de Fiscalização, inclusive em decorrência de exigência de outros órgãos públicos.

§ 3º Fica a critério da pessoa jurídica a opção pela forma de armazenamento das informações.

Art. 4º Fica formalmente revogada, sem interrupção de sua força normativa, a partir de 1º de janeiro de 2002, a Instrução Normativa SRF nº 68, de 27 de dezembro de 1995.

Art. 5º Esta Instrução Normativa entra em vigor na data da sua publicação, produzindo efeitos a partir de 1º de janeiro de 2002.

EVERARDO MACIEL"

(8) "Art. 1o. Os documentos produzidos, emitidos ou recebidos por órgãos públicos federais, estaduais ou municipais, bem como pelas empresas públicas, por meio eletrônico ou similar, têm o mesmo valor jurídico e probatório, para todos os fins de direito, que os produzidos em papel ou em outro meio físico reconhecido legalmente, desde que assegurada a sua autenticidade e integridade.

Parágrafo único. A autenticidade e integridade serão garantidas pela execução de procedimentos lógicos, regras e práticas operacionais estabelecidas na Infra-Estrutura de Chaves Públicas Governamental - ICP-Gov."

(9) Encontramos, em diversos autores, a menção ou referência a outros requisitos, tais como: perenidade ou não repúdio. Entendemos que outros requisitos, além da integridade e autenticidade, não são essenciais para à segurança probatória do documento eletrônico ou são decorrências/conseqüências dos dois mencionados.

(10) Podemos figurar a seguinte analogia, acerca do par de chaves criptográficas (privada e pública), com finalidade exclusivamente didática. Imagine uma língua complicadíssima somente conhecida por dois seres especiais. Um deles, chamado CHAVE PRIVADA, vive no seu computador e só você conhece a sua identidade. O outro ser, chamado CHAVE PÚBLICA, perambula pela Internet, vivendo em qualquer computador. Existe um código de conduta entre estes dois seres no sentido de que uma mensagem traduzida por um deles, para aquela língua estranha, não mais será analisada pelo autor da tradução e só, somente só, pelo outro. Assim, os textos e mensagens que você confeccionar e forem traduzidos por CHAVE PRIVADA, seu hóspede virtual, somente serão entendidos por CHAVE PÚBLICA e vice-versa.

(11) "Uma função hash é uma equação matemática que utiliza texto (tal como uma mensagem de e-mail) para criar um código chamado message digest (resumo de mensagem). Alguns exemplos conhecidos de funções hash: MD4 (MD significa message digest), MD5 e SHS. Uma função hash utilizada para autenticação digital deve ter certas propriedades que a tornem segura para uso criptográfico. Especificamente, deve ser impraticável encontrar: - Texto que dá um hash a um dado valor. Ou seja, mesmo que você conheça o message digest, não conseguirá decifrar a mensagem. - Duas mensagens distintas que dão um hash ao mesmo valor". (Disponível em http://www.certisign.com.br/help_email/concepts/hash.htm. Acesso em 23 out. 2001)

(12) A rigor, a assinatura digital pode prescindir dos algoritmos de autenticação, a exemplo do hash. É possível a criação de uma assinatura digital com base no conteúdo da própria mensagem. Ao chegar no destinatário, a assinatura é decodificada e comparada com o conteúdo da mensagem. A coincidência entre a mensagem e a assinatura decodificada é indicativa da ausência de alteração. Os principais problemas desta sistemática estão relacionados com o tempo de envio e processamento (cifragem e decifragem de todo o conteúdo da mensagem; o todo transmitido tem o dobro do tamanho original) e as mensagens de conteúdo originalmente "estranho" (série de números aleatórios, coordenadas, etc). A introdução de funções hash ao processo de assinatura digital supera estas dificuldades.

(13) Cumpre destacar a existência de uma tendência internacional no sentido da iniciativa privada conduzir o comércio eletrônico em geral e as atividades de certificação em particular. No Brasil, principalmente em função do disposto no art. 236 da Constituição, subsiste a discussão acerca de eventual reserva desta atividade para determinada categoria de agentes (tabeliães ou notários). Pensamos que as atividades do tabelião são aquelas fixadas em lei, conforme prevê expressamente o §1o. do citado art. 236 da Constituição. Neste sentido, a lei pode deferir a outro ator social (e não ao tabelião) a condição de entidade ou autoridade certificadora.

(14) Veja algumas das críticas: a) de Marcos da Costa e Augusto Tavares da Comissão de Informática Jurídica da OAB de São Paulo (em http://www.cbeji.com.br/artigos/artmarcosaugusto05072001.htm); b) da CertSign (em http://www.certisign.com.br/imprensa_mix.html#); c) da Sociedade Brasileira de Computação (em http://www.sbc.org.br) e d) da OAB (logo adiante). A primeira nota da OAB: "A Ordem dos Advogados do Brasil vem a público manifestar o seu repúdio à nova Medida Provisória nº 2.200, de 29/06/2001, que trata da segurança no comércio eletrônico no País. A MP, editada às vésperas do recesso dos Poderes Legislativo e Judiciário, desprezou os debates que vêm sendo realizados há mais de um ano no Congresso Nacional sobre três projetos a esse respeito, um dos quais oferecido pela OAB-SP. Ao estabelecer exigência de certificações para validade dos documentos eletrônicos públicos e privados, a MP não apenas burocratiza e onera o comércio eletrônico, como distancia o Brasil das legislações promulgadas em todo o mundo. Pior: ao outorgar poderes a um Comitê Gestor, nomeado internamente pelo Executivo e assessorado por órgão ligado ao serviço de segurança nacional, o governo subtrai a participação direta da sociedade civil na definição de normas jurídicas inerentes ao conteúdo, procedimentos e responsabilidades daquelas certificações.

Tudo isso é motivo de extrema preocupação no que tange à preservação do sigilo de comunicação eletrônica e da privacidade dos cidadãos, num momento em que grampos telefônicos têm se proliferado país afora, afrontando, inclusive, o livre exercício da advocacia. Brasília, 03 de julho de 2001. Rubens Approbato Machado. Presidente nacional da OAB". A segunda nota da OAB: "A Ordem dos Advogados do Brasil reconhece a sensibilidade do Governo Federal em acolher as críticas e sugestões manifestadas na primeira edição da Medida Provisória nº 2.200, alterando-a substancialmente em pontos fundamentais, a saber: 1) determina que o par de chaves criptográficas seja gerado sempre pelo próprio titular e sua chave privada de assinatura seja de seu exclusivo controle uso e conhecimento (§ único do art. 8º); 2) eleva o número de representantes da sociedade civil no Comitê Gestor (art. 3º); 3) limita os poderes daquele Comitê à adoção de normas de caráter técnico (incisos II e IV do Art. 5º e caput do art. 6º), bem como lhe determina a observância de tratados e acordos internacionais no que se refere ao acolhimento de certificações externas (inciso VII do art. 5º); 4) estabelece que a identificação do titular da chave pública seja presencial (art. 9º); 5) limita os efeitos legais da certificação ao próprio signatário (§ 1º do art. 12º); e 6) utiliza outros meios de prova da autenticidade dos documentos eletrônicos, afastando, assim, a obrigação do uso nos documentos particulares de certificações da ICP-Brasil (§ 2 º do art. 12º). Entende a OAB que tais disposições são fundamentais para o restabelecimento de um ambiente que assegure a

privacidade, segurança e liberdade nas manifestações de vontade dos cidadãos realizadas por meio eletrônico. Independente desses verdadeiros avanços, a OAB continua certa de a disciplina do documento eletrônico, da assinatura digital e das certificações eletrônicas deva nascer de um amplo debate social, estabelecido em sede própria, qual seja, o Congresso Nacional, razão pela qual manifesta sua confiança em que a nova redação da MP não representará prejuízo ao andamento regular dos projetos de lei que tramitam atualmente em nosso Parlamento."

(15) "Discute-se, em nível mundial, segundo Henrique Conti, qual o melhor sistema de certificação a ser adotado. Pode-se criar uma hierarquia de certificadoras públicas ou privadas, baseado numa ceritficadora-raiz que possui as informações de todas as outras certificadoras. Nos Estados Unidos, segundo o convidado, esse modelo vem sendo duramente criticado, devido a preocupações com privacidade. Observa-se, portanto, uma tendência no sentido de implantar sistemas de certificação não hierárquicos, baseados no mútuo reconhecimento e troca de certificados entre várias certificadoras." Semeghini, Júlio. Voto no Substitutivo aos Projetos de Lei n. 1.483 e 1.589, ambos de 1999. Disponível em http://www.modulo.com.br/pdf/semeghini.pdf. Acesso em 22 out. 2001.

(16) "Ao tratar-se do tema assinatura digital em seu aspecto mais técnico, acaba-se fazendo relação direta aos algoritmos de autenticação. Entretanto, como a tecnologia caminha a passos largos, torna-se impossível garantir que a correlação entre uma assinatura digital e um algoritmo de autenticação venha a ser necessária dentro de algum tempo. Existe até mesmo a possibilidade de que a nomenclatura 'assinatura digital' acabe sendo substituída quando do abandono do uso dos algoritmos de autenticação." Volpi, Marlon Marcelo. Assinatura Digital. Aspectos Técnicos, Práticos e Legais. Axcel Books. 2001. Pág. 17.

IV. LISTA DE LINKS

Artigo ASPECTOS JURÍDICOS DO DOCUMENTO ELETRÔNICO.
Autor: José Henrique Barbosa Moreira Lima Neto.
www.jus.com.br/doutrina/docuelet.html

Artigo O DOCUMENTO ELETRÔNICO COMO MEIO DE PROVA.
Autor: Augusto Tavares Rosa Marcacini.
buscalegis.ccj.ufsc.br/arquivos/artigos/O_documento_eletronico_como_meio_de_prova.htm

Artigo VALIDADE JURÍDICA DE DOCUMENTOS ELETRÔNICOS. CONSIDERAÇÕES SOBRE O PROJETO DE LEI APRESENTADO PELO GOVERNO FEDERAL.
Autor: Aldemario Araujo Castro.
www.aldemario.adv.br/projetocc.htm
www.informaticajur.hpg.com.br/projetocc.htm

Representação gráfica da assinatura digital
Figura recuperada da pág. 25 da obra Assinatura Digital de Marlon Marcelo Volpi
www.infojurucb.hpg.ig.com.br/assdig.jpg

Representação gráfica da assinatura digital II

www.infojurucb.hpg.ig.com.br/quadroassdig.htm

Exemplo de MENSAGEM ASSINADA DIGITALMENTE
www.infojurucb.hpg.ig.com.br/assinada.gif

Exemplo de INDICAÇÃO DE ALTERAÇÃO da mensagem depois de assinada digitalmente
www.infojurucb.hpg.ig.com.br/violada.gif

Imagens de um certificado digital
www.infojurucb.hpg.ig.com.br/certificado1.gif
www.infojurucb.hpg.ig.com.br/certificado2.gif

Lei Modelo da UNCITRAL.
www.direitonaweb.adv.br/legislacao/legislacao_internacional/Lei_Modelo_Uncitral.htm
www.direitonaweb.adv.br

Projeto de Lei n. 1.589, de 1999.
www.informaticajur.hpg.ig.com.br/ploab.htm
www.informaticajur.hpg.ig.com.br

Infra-estrutura de chaves públicas do Poder Executivo Federal.
Decreto 3.587, de 5 de setembro de 2000
www.planalto.gov.br/ccivil_03/decreto/D3587.htm
www.planalto.gov.br

Substitutivo apresentado pelo Relator à Comissão Especial
www.modulo.com.br/pdf/semeghini.pdf
www.modulo.com.br

Medida Provisória n. 2.200, de 28 de junho de 2001
www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200.htm
www.planalto.gov.br

Medida Provisória n. 2.200-1, de 27 de julho de 2001
www.planalto.gov.br/ccivil_03/MPV/2200-1.htm
www.planalto.gov.br

Medida Provisória n. 2.200-2, de 24 de agosto de 2001
www.planalto.gov.br/ccivil_03/MPV/2200-2.htm
www.planalto.gov.br

Substitutivo (com alterações) aprovado pela Comissão Especial
www.cbeji.com.br/legislacao/PL4906-aprovado.htm
www.cbeji.com.br

Artigo ASSINATURAS ELETRÔNICAS - O PRIMEIRO PASSO PARA O DESENVOLVIMENTO DO COMÉRCIO ELETRÔNICO?
Autor: Henrique de Faria Martins

www.cbeji.com.br/artigos/artasselet.htm
www.cbeji.com.br

Artigo ASSINATURA DIGITAL NÃO É ASSINATURA FORMAL.
Autora: Angela Bittencourt Brasil
www.cbeji.com.br/artigos/artang02.htm
www.cbeji.com.br

Criptografia
www.catar.com.br/hg/leohomepage/criptografia.htm
www.gold.com.br/~colt45/danger/criptografia.html

Regime jurídico dos documentos eletrônicos e assinatura digital em Portugal. Decreto-Lei 290-D/1999
www.giea.net/legislacao.net/internet/assinatura_digital.htm

PGP (Pretty Good Privacy) - Programa gratuito (para fins não comerciais) para encriptação de arquivos utilizando o método das chaves públicas e privadas
www.pgpi.org