A Eficácia Probatória do Documento Digital

Christiano Vítor de Campos Lacorte

Advogado especialista em Direito da Informática. Bacharel em Direito, bacharel em Ciências da Computação, pós-graduado em Tecnologia da Informação, curso de extensão em Direito das Tecnologias da Informação e Direitos Autorais. Mestrando em Direito, Estado e Sociedade na Universidade Federal de Santa Catarina.

Resumo

Trata-se de artigo referente aos aspectos envolvidos na formação do documento digital, e na comparação deste com o documento físico. Da análise dos componentes que trazem valor probatório a este último, este trabalho passa à apresentação e avaliação dos elementos que conferem ao documento digital a denominada validade jurídica. Também se faz presente a apreciação de como a legislação estrangeira tem versado sobre o tema, e a análise dos textos legais pátrios que abordam a validade do documento digital.

SUMÁRIO

1. INTRODUÇÃO

Tornar a justiça brasileira mais eficiente: este tem sido o cerne das grandes discussões acerca da reforma do Judiciário. Como meio de se atingir este objetivo, muito se tem lembrado de uma maior – e melhor – utilização dos recursos de informática. Várias são as propostas de uso da tecnologia para melhorar os procedimentos judiciais, e dentre elas ganham destaque aquelas que se propõem a implementar a informatização do processo judicial. Esta tarefa passa, necessariamente, pelo uso de documentos digitais, os quais devem possuir elementos que lhes tragam validade jurídica. Esta é a questão que norteará este artigo.

O tema ganha ainda mais relevância quando se identifica que, já há algum tempo, não só a administração pública mas também as empresas privadas vêm buscando formas de substituir os documentos tradicionais, também denominados físicos, pelos seus correspondentes digitais. O volume de informações com que se lida atualmente, o acesso a elas, a necessidade de agilidade na sua distribuição, de forma que estejam disponíveis sempre que necessárias, são fatores que têm determinado essa migração para o documento digital.

No mundo jurídico, outros fatores além daqueles apresentados no parágrafo anterior motivam uma criteriosa análise a respeito da utilização do documento digital, merecendo destaque a possibilidade de se implantar um processo cada vez mais concernente com o princípio da publicidade, uma vez que o documento digital tem características que tornam mais fácil e menos dispendiosa a publicação e o acesso à informação, e também a oportunidade de melhor atender aos preceitos referentes à economicidade, já que os gastos envolvidos com armazenamento, impressão e transporte tendem a cair exponencialmente quando se adota uma adequada política de utilização dos recursos tecnológicos.

O estudo a respeito do documento digital passa, necessariamente, pela análise das características do documento físico, de forma a se identificar quais atributos que fazem dele a forma ainda hoje mais utilizada no mundo jurídico para o

registro de fatos, e se esses elementos podem ser reproduzidos – ou pelo menos seus efeitos – no seu correspondente digital.

Após a identificação das características que envolvem o documento físico, e constatado que o documento digital seria uma alternativa segura, deve-se questionar que motivos ensejariam, senão uma substituição completa, pelo menos uma mitigação do uso do primeiro com relação a este último. Faz-se necessário também o exame do documento digital, de modo que se perceba se este reúne condições para ser, de fato, um substituto viável ao documento físico. Após a abordagem das questões técnicas referentes ao documento digital, é aproriado o exame a respeito de como as leis vêm abordando essa questão, tanto no Brasil, quanto no exterior.

O objetivo deste trabalho, portanto, é demonstrar a viabilidade do documento digital, não como um substituto pleno do documento físico, mas sim como uma alternativa válida juridicamente e, em geral, capaz de oferecer grandes vantagens quando comparada ao seu correspondente físico.

Encerrando este intróito, deve-se destacar o papel do profissional do Direito como agente ativo na construção de uma estrutura mais funcional para a consecução das atividades jurídicas, de modo a obter melhor proveito dos recursos tecnológicos, utilizando-a como ferramenta idônea na persecução de um Direito cada vez mais eficiente e justo.

2. DOCUMENTO FÍSICO

Como apresentado anteriormente, antes de se dar início ao estudo do documento digital, torna-se necessária a análise dos conceitos que cercam o documento físico, de modo que seus elementos sejam compreendidos, e então se possa verificar se o documento digital reúne as condições necessárias para servir como alternativa ao primeiro.

2.1. CONCEITO

O documento físico, também denominado “documento tradicional”, ou apenas “documento”, é aquele cuja maior característica está na vinculação a um

suporte físico, ou seja, seu conteúdo está unido, de forma inseparável, a algo material, corpóreo. Antes de se avançar nessas características, vale uma breve análise dos significados dado ao termo "documento".

Para o Novo Dicionário Aurélio da Língua Portuguesa[1], "documento" é:

> 1. Qualquer base de conhecimento, **fixada materialmente** e disposta de modo que se possa utilizar para consulta, estudo, prova, etc. 2. **Escritura** destinada a comprovar um fato; **declaração escrita**, revestida de forma padronizada, sobre fato(s) ou acontecimento(s) de natureza jurídica. (...) *(grifou-se)*

Já em Michaelis – Moderno Dicionário da Língua Portuguesa[2], tem-se a seguinte definição para "documento":

> 1 **Instrumento escrito** que, por direito, faz fé daquilo que atesta; escritura, título, contrato, certificado, comprovante. **2 Escrito ou impresso** que fornece informação ou prova. 3 Qualquer fato e tudo quanto possa servir de prova, confirmação ou testemunho.(...). *(grifou-se)*

Percebe-se nestas definições a característica citada anteriormente: o documento possui um conteúdo que está ligado a um suporte físico. Outro ponto comum diz respeito à forma escrita, modo pelo qual, em geral, o documento se faria apresentar.

Deixando as definições léxicas e partindo para a doutrina jurídica, se percebe que os conceitos encontrados não guardam diferenças relevantes com relação às anteriores, ao contrário, reforçam a vinculação do conteúdo a um suporte material. Deste modo, para Chiovenda[3], documento seria toda a "**representação material** destinada a reproduzir determinada manifestação do pensamento" (grifou-se). Já Carnelutti[4] o descreve como "uma **coisa** representativa de um fato" (grifou-

---

[1] FERREIRA, Aurélio B. H. Novo Dicionário Aurélio da Língua Portuguesa. Rio de Janeiro: Nova Fronteira, 1986.

[2] MICHAELIS - Moderno Dicionário da Língua Portuguesa. São Paulo, Cia. Melhoramentos, 1998.

[3] CHIOVENDA *apud* GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva et al. **A segurança dos documentos digitais** . Jus Navigandi, Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2677>. Acesso em: 07 jul. 2005.

[4] CARNELUTTI *apud* CASTRO, Aldemario Araujo. **O Documento Eletrônico e O novo Código Civil**. Alfa-Redi: Revista de Derecho Informático. Disponível em: <http://www.alfa-redi.org/rdi-articulo.shtml?x=1256>. Acesso em: 10 set. 2005.

se), mediante a palavra escrita. Nesse sentido também lecionam, agora na doutrina pátria, Moacir Amaral dos Santos[5] e Humberto Theodoro Júnior[6].

Deixando as conceituações doutrinárias e procurando na legislação nacional definições para o vocábulo "documento", se percebe que raras são as normas que o explicam, optando o legislador pátrio por deixar tal tarefa, via de regra, a cargo da doutrina, como visto anteriormente. Porém, diversas referências ao termo "documento" são feitas nas normas brasileiras, por exemplo: no Código Civil, os artigos 212 inciso II, 215, 219, 1.151 § 1º, dentre outros; no Código Penal, temos, por exemplo, os artigos 297 ("Falsificação de Documento Público"), 298 ("Falsificação de Documento Particular"), 304 ("Uso de Documento Falso"), 305 ("Supressão de Documentos"); no Código de Processo Civil, temos os artigos 159, 202 §§1º e 2º, 283, 312, 355 , 364 a 399 (Título VIII, Capítulo VI, Seção V – "Da Prova Documental"), 861; e no Código de Processo Penal, os artigos 116; 135 § 1º; 145; 174 inciso II, 231 a 238 (Título XXX Capítulo IX – "Dos Documentos"), 400, e 513.

Da legislação analisada, apenas o Código de Processo Penal, no seu artigo 232, apresenta uma definição para documento, bastante restritiva, mas que vai ao encontro dos significados apresentados anteriormente:

> "Art. 232. Consideram-se **documentos** quaisquer **escritos**, **instrumentos** ou **papéis**, públicos ou particulares.
> Parágrafo único. À fotografia do documento, devidamente autenticada, se dará o mesmo valor do original." *(grifou-se)*

Deste modo, ao se examinar as definições apresentadas até agora, ratifica-se o entendimento de que o documento possui um **conteúdo** (relativo ao fato que se quer representar e, portanto, preservar), e que este encontra-se ligado – **inseparavelmente** – a um determinado **suporte físico** (em geral, o papel). Esta vinculação, é preciso ter em mente, se deve ao fato não haver, até então, outra

[5] SANTOS, Moacir Amaral *apud* GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva et al. **A segurança dos documentos digitais** . Jus Navigandi, Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2677>. Acesso em: 07 jul. 2005.

[6] THEODORO Jr., Humberto *apud* GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva et al. **A segurança dos documentos digitais** . Jus Navigandi, Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2677>. Acesso em: 07 jul. 2005.

forma de se registrar algo que não passasse pela inscrição em um suporte material, o qual guarda aquele conteúdo durante a sua vida útil.

Avanços tecnológicos trouxeram a possibilidade de separação entre conteúdo e suporte, dando ensejo a conceitos mais atuais de documento, construídos mais em razão da finalidade que da forma. Ver-se-á, mais adiante, que a principal característica dos **documentos digitais** reside justamente na **desvinculação** entre o conteúdo e o suporte do documento; a informação registrada poderá mudar de suporte sem que o documento seja perdido. Porém, antes se faz necessária uma breve análise dos elementos que trazem validade jurídica ao documento físico.

2.2. ASSINATURA MANUSCRITA

O documento físico, por si só, é um meio de prova deveras inexpressivo. Porém, se junto a ele se fizerem presentes outros elementos, sua eficácia como meio probatório tende a aumentar expressivamente. Um exemplo de como outros elementos agregam segurança a um documento físico pode ser encontrado naqueles em que o autor redige de próprio punho: mediante a análise grafotécnica pode se chegar a um resultado quanto à autoria daqueles escritos. Mais ainda, perícias realizadas no suporte utilizado, por exemplo, nas folhas de papel onde estão apostos os escritos, podem identificar vestígios de adulteração, o que seria uma forma de se comprovar a integridade do documento.

Porém, um elemento se destaca quanto à finalidade de identificação da autoria do documento e, por tal razão, lhe traz maior segurança jurídica: a assinatura manuscrita. Nos dizeres do professor Humberto Theodoro Júnior[7], "para que um documento seja eficaz como meio de prova, é indispensável que seja subscrito por seu autor e que seja autêntico". Dos exemplos apresentados no parágrafo anterior, e das palavras do professor Humberto Theodoro, dois elementos se destacam quando se trata da eficácia probatória de um documento: **autoria** e **integridade**.

[7] ZOCOLLI, Dinemar. Autenticidade e Integridade dos Documentos Eletrônicos: a Firma Eletrônica. In: Aires José Rover (Coord.). **Direito, Sociedade e Informática**. Florianópolis: Fundação Boiteux, 2000.

Estendendo a análise a respeito da assinatura manuscrita, descobre-se que, segundo os ensinamentos de Carnelluti[8], ela possui três funções básicas: indicativa (apontar quem é o autor do documento), declarativa (o autor assume a paternidade do que assinou, concordando com o conteúdo), probatória (concretiza materialmente as funções anteriores, de modo que possam ser verificadas por outrem). A presença destas funções é que permite a união consistente entre o conteúdo do documento e o seu signatário.

Portanto, uma vez reconhecida a falsidade da assinatura, o documento perde eficácia probatória – salvo a existência de outros elementos, como o caso de texto manuscrito –, em razão da inexistência da autenticidade, ou seja, não se pode imputar àquela pessoa a autoria do documento (perda da função indicativa). Há também a conseqüente extinção da função declarativa, já que não se pode ligar o signatário ao documento, tampouco se poderia falar em concordância deste com o que ali está registrado.

Uma observação interessante, e que decorre da inseparabilidade entre o conteúdo e o suporte no documento físico, reside no fato de que a assinatura é aposta no meio físico em que está registrado a informação, e uma vez que essa marca é também inseparável, ela passa a validar justamente aquele conteúdo ali fixado. Nas palavras de Dinemar Zoccoli[9], a assinatura é o elo entre o conteúdo e o autor do documento.

Diante do que foi apresentado, percebe-se que o documento digital apenas terá validade jurídica se atender às mesmas exigências demandadas do documento físico, ou seja, se for possível a verificação da autoria e da integridade. Cabe lembrar que no documento digital os elementos de validação devem estar vinculados ao conteúdo, e não ao suporte, como ocorre no documento físico, já que neste último há a inseparabilidade entre conteúdo e suporte, o que não ocorre no primeiro. Porém, antes de se verificar as características do documento digital, deve-

[8] CARNELUTTI *apud* ZOCOLLI, Dinemar. Obra citada. Páginas 178 e 179.

[9] ZOCOLLI, Dinemar. Autenticidade e Integridade dos Documentos Eletrônicos: a Firma Eletrônica. In: Aires José Rover (Coord.). **Direito, Sociedade e Informática**. Florianópolis: Fundação Boiteux, 2000.

se entender quais os motivos que levam a uma busca de alternativas ao documento físico.

2.3. DOCUMENTO FÍSICO: POR QUE BUSCAR ALTERNATIVAS?

Apresentadas as características do documento físico, e os elementos que fazem dele um meio probatório por excelência, afinal, da sua própria definição se depreende que tem por finalidade precípua o registro de algo de modo que possa ver verificado posteriormente, surge a pergunta: por que então substituí-lo, ou buscar alternativas a ele?

Antes da indicação dos pontos fracos do documento físico, deve-se ressaltar seus pontos fortes: em geral, não necessita de nenhum equipamento para que seu conteúdo seja conhecido, bastando luz suficiente para que possa ser visto; os meios físicos utilizados como suporte costumam ter uma durabilidade boa, desde que observadas condições adequadas de armazenamento. Além disso, não há como negar a praticidade de se ler um escrito de algumas poucas folhas de papel (desde que relativamente pequeno – um processo com mais de mil folhas já não tem um manuseio eficiente). Também se deve levar em consideração que os impressos geralmente possuem uma resolução bastante superior à maioria das telas de computadores, levando a uma acuidade perceptiva maior na leitura de documentos. Há também um conforto reflexivo maior quando se lê a partir do papel, quando comparado com a luz direta da tela do computador, a qual costuma levar a um cansaço visual mais rápido.

Porém, o documento físico também possui defeitos, e os mais relevantes estão ligados justamente a sua característica mais inerente: a presença de um suporte físico inseparável do conteúdo. O suporte mais utilizado é o papel, em razão de diversos aspectos, alguns deles elencados no parágrafo anterior. Porém, muitas são as razões que levam à busca de novas formas de se lidar com o registro de informações[10] :

[10] Os exemplos apresentados se referem ao papel, mas sem dificuldades podem ser transpostos a outros suportes

- Custos: os custos envolvidos com o documento físico estão diretamente ligados à quantidade de informação que se quer registrar. Assim, como essa quantidade é cada vez maior, também maior são os gastos relativos à aquisição do suporte sobre o qual se assentará a informação. Além disso, deve-se lembrar dos custos ecológicos: o papel mais comumente utilizado utiliza como matéria-prima a celulose, exigindo a derrubada de árvores, e quanto maior a quantidade demandada, maiores serão os recursos explorados; numa situação extrema, sem que se busque a renovação dos recursos de forma ordenada, pode levar a um esgotamento destes. A situação se repete para os demais insumos utilizados na produção do documento físico: tinta para impressão, materiais utilizados na fabricação de impressoras, copiadoras, etc.
- Transporte: o documento físico, para se fazer chegar aos destinatários daquela informação ali registrada, depende que o suporte que guarda o conteúdo seja a eles encaminhado. Este transporte pode ficar bastante caro quando pensamos em uma quantidade grande de documentos: um processo com alguns milhares de folhas tem um custo bastante alto de envio, e ainda requer que sejam observadas medidas de segurança de modo a não sofrer extravios durante a movimentação. Além disso, pode-se dizer que o transporte sempre será lento quando comparado às redes de transmissão de dados digitais, sobre as quais se movem os documentos digitais. A tecnologia traz novas expectativas quanto ao tempo para se ter acesso às informações, e os limites que se apresentam ao transporte dos documentos físicos, em geral, ficam aquém destas expectativas.
- Armazenamento: outro problema diretamente relacionado ao suporte corpóreo do documento físico: guardar enormes quantidades de documentos tem sido um problema tão grande quanto a própria quantidade de documentos sendo gerada. Salas, galpões, áreas dos mais diversos tipos têm surgido para a guarda de documentos – espaços estes que em determinado período já não serão suficientes.

Além disso, torna-se necessário um trabalho extenuante de catalogação do material armazenado de forma que seja possível acessá-lo depois. Também cabe destacar que esses locais devem ser preparados observando normas de preservação do suporte material do documento físico. Estas medidas – catalogação e preservação – envolvem mais custos e acrescem dificuldades ao uso do documento físico.

- Segurança: as medidas de segurança com relação ao documento físico, em geral, são complexas. Devem ser observadas condições que não levem à degradação do suporte que contém as informações, já que ele, uma vez deteriorado, leva junto a informação que guardava. Também deve se levar em conta a segurança quanto ao conteúdo do documento, ou seja, impedir que pessoas que não devam acessá-lo consigam fazê-lo, por exemplo, durante o transporte. Quando o documento está armazenado em um cofre, o nível de segurança é alto, porém, quando surge a necessidade de transportá-lo – o que, como apresentado, já envolve um custo operacional alto – outras medidas de segurança são requeridas, tornando ainda mais custosa a utilização .

Estas são algumas das razões que levam à persecução de alternativas ao uso do documento físico, o qual, ainda assim, continua a ser a forma por excelência de registro de informações. Pelos motivos apresentados, este cenário tende a apresentar alterações conforme barreiras venham a ser superadas, nem tanto de ordem técnica ou jurídica, como se verá no transcorrer deste trabalho, mas principalmente culturais. É certo que a cada ano essas barreiras culturais têm diminuído, de forma que o uso do documento digital já não é algo incomum.

3. DOCUMENTO DIGITAL

Antes de se passar a análise dos conceitos e características do documento digital, se faz pertinente uma breve explanação a respeito da terminologia utilizada neste trabalho. O termo “documento digital”, empregado neste

estudo, vai ao encontro dos trabalhos da Câmara Técnica do Documento Eletrônico (CTDE), do Arquivo Nacional. Esta Câmara, criada pelo Conselho Nacional de Arquivos (CONARQ), órgão do Arquivo Nacional, é um grupo de trabalho que tem por objetivo a "definição de normas, diretrizes, procedimentos técnicos e instrumentos legais sobre gestão arquivística e preservação dos **documentos digitais**, em conformidade com os padrões nacionais e internacionais"[11] (grifou-se). Cabe lembrar que o termo "documento eletrônico" era a expressão mais usual à época da criação do grupo (a Câmara Técnica do Documento Eletrônico foi criada, já com esta denominação, pela Portaria nº 8, de 23 de agosto de 1995).

Entre os resultados apresentados por este grupo, encontra-se o Glossário da Câmara Técnica do Documento Eletrônico[12], onde se encontram definições de diversos termos utilizados nos trabalhos do grupo. Destacam-se duas definições apresentadas no léxico citado, de modo a balizar a opção terminológica adotada neste trabalho:

> **Documento digital:** Unidade de registro de informações, codificada por meio de dígitos binários.
> **Documento eletrônico:** Unidade de registro de informações, acessível por meio de um equipamento eletrônico.

Como se pode depreender das delimitações elencadas, **documentos eletrônicos** são as unidades de registro **acessíveis mediante um equipamento eletrônico**: neste sentido, uma fita cassete de áudio ou uma fita VHS de vídeo, apesar de não serem gravadas em formato digital, devem ser entendidos como documentos eletrônicos.

Entretanto, o tipo de documento que possui as características analisadas no presente artigo é de fato o **documento digital**, aquele **formado por dígitos binários**, e sobre o qual incidem todas as demais considerações apontadas neste estudo, como a possibilidade de uma assinatura digital a ele vinculada, e a independência entre conteúdo e suporte físico. Não se trata aqui, portanto, do "documento eletrônico", razão pela qual se adotou a expressão "documento digital",

[11] A apresentação do grupo pode ser encontrada no site da Câmara Técnica do Documento Eletrônico, em http://www.arquivonacional.gov.br/conarq/cam_tec_doc_ele/index.asp

[12] O glossário da Câmara Técnica do Documento Eletrônico está disponível em http://www.arquivonacional.gov.br/conarq/cam_tec_doc_ele/download/ Glossario_CTDE_2004.pdf

e não a primeira. Resta lembrar que a utilização do termo “documento eletrônico” significando “documento digital” é bastante ampla, e não encontra maiores problemas, desde que se defina precisamente a acepção do termo que está sendo empregada. Porém, neste trabalho optou-se pela nomenclatura que se entendeu ser a mais precisa, tanto por melhor qualificar o objeto (“digital” indica melhor a formação do documento por “dígitos binários“), quanto por evitar confusão com aqueles documentos eletrônicos representados pela definição apresentada no mencionado glossário.

3.1. CONCEITO

Resolvidas as questões de terminologia, pode-se passar ao estudo do documento digital Como destacado anteriormente, as definições apresentadas para o termo “documento” tinham em comum a identificação de um conteúdo – a informação que se queria preservar para conhecimento futuro – fixado em um suporte corpóreo de forma inseparável. Esta acepção serve para o reconhecimento de apenas um tipo de documento: o físico, cujas características já foram apresentadas. O desenvolvimento de novas tecnologias permitiu o surgimento de novas formas de registros, e aquelas definições apresentadas já não servem mais para todos os tipos de documentos.

Assim, deve-se partir para a procura de um conceito mais geral de “documento”, o qual deixe de lado a necessidade de uma base corpórea na qual se fixará o conteúdo, e privilegie justamente a finalidade, qual seja, a de guardar um pensamento ou fato que se quer ter acesso no futuro. Deste modo, poder-se-ia dizer, simplesmente, que **documento** é o **registro de um fato**. Esta definição teleológica guarda correspondente no conceito encontrado no Glossário da Câmara Técnica do Documento Eletrônico[13]:

> **Documento:** Unidade de registro de informações qualquer que seja o suporte.

[13] O glossário da Câmara Técnica do Documento Eletrônico está disponível em http://www.arquivonacional.gov.br/conarq/cam_tec_doc_ele/download/ Glossario_CTDE_2004.pdf

Portanto, se novas tecnologias permitem uma nova forma de se realizar o registro de informações, não se pode deixar de considerá-las documentos. Nas palavras de Marcacini[14], "se a técnica atual, mediante o uso da criptografia assimétrica, permite registro inalterável de um fato em meio eletrônico, a isto também podemos chamar de documento".

Estas conceituações mais abrangentes para o termo documento, portanto, abrangem o documento digital. Porém, diante das peculiaridades deste tipo de documento, torna-se necessário uma definição de modo que se faça a diferenciação com o documento físico. Esta definição é bastante importante, haja vista que os elementos de aferição de autenticidade e integridade são diversos para cada um destes tipos de documento.

Em uma definição mais completa, Augusto Marcacini[15] definiu documento digital como "uma seqüência de bits que, captada pelos nossos sentidos com o uso de um computador e um software específico, nos transmite uma informação".

Uma conseqüência interessante, decorrente do modo como se estrutura o documento digital (uma seqüência de bits), está no sentido que se pode dar aos termos "original" e "cópia". Com documentos físicos, quando se tem a necessidade de compartilhar informação, a atividade a ser realizada é a de tirar cópias de um documento inicial, chamado original, de forma que essas reproduções possam ser levadas aos demais destinatários da informação. Já quando o documento "original" é uma seqüência de bits, uma reprodução dele significa exatamente a mesma seqüência de bits, razão pela qual o termo cópia talvez não seja o mais adequado, haja vista tratar-se mais propriamente de um clone do documento inicial, possuindo exatamente as mesmas características, e dele diferenciando-se apenas pelo momento da geração e do local de armazenamento em dado instante.

[14] MARCACINI, Augusto Tavares Rosa. **O Documento Eletrônico como meio de prova**. In: Infodireito [Internet] <http://www.infodireito.com.br/ > Acesso em: 10 jul. 2005.

[15] MARCACINI, Augusto. Obra citada – no artigo aludido, o autor adotou a nomenclatura "documento eletrônico" com o mesmo sentido de "documento digital" adotado neste artigo.

3.2. CRIPTOGRAFIA

Para avançar na análise da validade jurídica do documento digital, torna-se necessária uma breve apresentação da criptologia, ciência que engloba a criptografia (ciência que estuda a escrita em código) e a criptoanálise (ciência que estuda a quebra dos códigos criptográficos), cujas técnicas são primordiais para trazer ao documento digital os elementos capazes de lhe atribuir validade jurídica.

Na criptografia, o texto inicial, legível para todos, é denominado texto em claro. O processo de codificação do texto em claro é denominado cifragem, e o texto codificado recebe o nome de texto cifrado. A recuperação do texto inicial recebe o nome de decifragem.

Dois são os tipos de sistemas criptográficos: simétrico e assimétrico. O primeiro utiliza uma única chave para cifrar e decifrar o texto. Assim, para garantir o sigilo da informação, apenas o emissor e o receptor devem conhecer a chave. Um exemplo simples deste sistema está em definir, como chave, que a cada letra do alfabeto corresponde o número referente à sua ordem no abecedário (A=1, B=2, C=3, D=4). Assim uma mensagem cifrada com esta chave cujo resultado fosse "3141", pode ser decifrada com a mesma chave, resultando o texto em claro na palavra "CADA". O problema deste modelo reside exatamente nesse ponto: a chave utilizada para cifrar a mensagem deve ser compartilhada com todos os que precisam ler a mensagem, o que cria uma fragilidade.

Já a criptografia **assimétrica**, de especial relevância para o correto entendimento do funcionamento da assinatura digital, utiliza um par de chaves diferentes, mas que se relacionam matematicamente, sendo uma a chave pública (utilizada para cifrar a mensagem) e a outra a chave privada (utilizada para decifrar a mensagem). O texto cifrado por uma chave pública só pode ser decifrado pela chave privada correspondente. A chave privada, portanto, deve ser de conhecimento apenas de seu titular, enquanto a chave pública deve ser conhecida por aqueles que queiram enviar uma mensagem codificada ao primeiro.

O processo inverso é utilizado na assinatura digital: o signatário, com sua chave privada, firma o documento, e essa assinatura pode ser conferida por todos

aqueles que têm a chave pública correspondente. Essa operação será vista de forma mais detalhada no tópico 3.3 (“Assinatura Digital”).

Merecem abordagem também, neste breve intróito à criptografia, os conceitos de função *hash* e de *message digest*. A função *hash* utiliza cálculos matemáticos tendo por parâmetro o documento digital para criar um código chamado resumo de mensagem (*message digest*), que é único para aquele documento (seqüência de bits). O *message digest* possui um tamanho fixo, medido em bits, independente do tamanho do documento que a ele foi submetido, e que é determinado pelo *algoritmo* utilizado. O uso do resumo é importante em razão de um melhor desempenho, já que os algoritmos de criptografia assimétrica são bastante complexos e, por isso, lentos. A utilização do resumo no processo de cifragem com a chave privada reduz o tempo de operação para gerar a assinatura digital. A seguir, são apresentadas outras informações a respeito da assinatura digital.

3.3. ASSINATURA DIGITAL

A assinatura digital é o instrumento por meio do leva ao documento digital garantias de tal modo que este possa ter força probante, ou seja, é um elemento de credibilidade do documento digital, que permite a conferência da autoria e da integridade deste.

O primeiro aspecto a ser destacado sobre a assinatura digital, que é a modalidade de assinatura eletrônica – toda forma de se autenticar um documento digital – gerada por um sistema de criptografia assimétrica, está no fato de que ela em nada se assemelha à assinatura manuscrita, se tratando, na verdade, de um número resultante de funções matemática que utilizam, dentre outras variáveis, o próprio documento digital e a chave privada do subscritor[16]. A seguir é apresentada uma sucinta descrição de como ocorre o processo de assinatura digital de um documento e a sua validação.

[16] MARCACINI, Augusto Tavares Rosa. **O Documento Eletrônico como meio de prova**. In: Infodireito [Internet] <http://www.infodireito.com.br/ > Acesso em: 10 jul. 2005.

O signatário, já com o documento que deseja assinar digitalmente disponível, acessa um software de computador que, utilizando uma função hash, gera um resumo do documento (ver item 3.2) – deve-se ressaltar que este resumo é único, ou seja, nenhum outro documento digital pode gerar aquela seqüência numérica gerada pela função *hash* (coincidências deste tipo – mesmo resultado do *hash* para diferentes documentos, denominadas colisões – são raras de ocorrer, e indicam fragilidades dos algoritmos de cifragem; quanto maior a quantidade de colisões, mais vulnerável é aquele algoritmo). É por esta razão que as assinaturas digitais, mesmo que de um mesmo signatário, serão diferentes para cada documento assinado, diferente do que ocorre para a assinatura manuscrita, a qual o subscritor a repete nos diferentes documentos em que a apõe.

A seguir, o programa de computador aplica a chave privada do assinante ao resumo da mensagem, gerando uma nova seqüência de números, que só pode ser revertida por meio da chave pública que faz par com a chave privada utilizada – o resultado desta operação é a assinatura digital. Os destinatários daquele documento receberão junto a assinatura e para validá-la utilizarão um software, que primeiro utilizará a chave pública do signatário para obter o *hash* do documento, e então aplicará uma função *hash* no documento recebido e verificará se corresponde àquele que ele obteve da assinatura: se corresponder, a autoria e a integridade do documento estão confirmados, se não corresponder, ou a chave privada utilizada não é àquela correspondente à chave pública utilizada, ou o documento foi adulterado.

Apesar de o processo parecer complicado, a sua utilização é bastante simples, uma vez que a complexidade é, via de regra, encoberta pelos programas de computador, que realizam as operações e informam os resultados, restando aos usuários, em geral, apenas instruir quais documentos desejam assinar ou validar, e conferir os resultados das verificações das assinaturas.

A assinatura eletrônica, para realizar plenamente sua função de trazer segurança jurídica ao documento digital, deve possuir os seguintes atributos[17]:

[17] Cartilha do Instituto Nacional de Tecnologia da Informação, que pode ser obtida na Internet em <http://www.iti.br/twiki/bin/view/Main/Cartilhas> . Acesso em: 29/10/2005.

- ser única para cada documento, mesmo quando assinado por um mesmo signatário, uma vez que ela deve estar vinculada ao conteúdo, em razão da independência do documento digital com relação ao suporte em que está armazenado (diferentemente da assinatura manuscrita, que é repetida pelo signatário nos diversos documentos físicos que pretende firmar, repousando a assinatura no próprio suporte físico, validando o conteúdo em razão da inseparabilidade entre ele e o meio em que está acomodado);

- permitir a identificação unívoca (e inequívoca) do assinante, inclusive garantindo o não-repúdio (garantia de que de fato só aquela pessoa poderia ter assinado o documento digital);

- assegurar a conferência da integridade do documento (se ocorrer qualquer alteração após a aposição da assinatura, esta se torna inválida).

Portanto, uma característica que deve ser destacada, trazida ao documento digital pela assinatura digital, está no que se denomina de inalterabilidade[18] ou imutabilidade[19] lógica. O documento digital firmado por uma assinatura digital, cuja elaboração se dá em razão dos bits que compõem o teor do próprio documento, assegura que qualquer modificação posterior nele, mesmo a mera inclusão de um espaço em branco, leve à invalidação da assinatura. Deve-se lembrar que ser facilmente modificável é característico do documento digital, que com a ferramenta computacional adequada pode ser alterado sem deixar maiores sinais no meio onde estava armazenado. Deste modo, a inalterabilidade é dita "lógica" pelo fato não de impedir a modificação do documento, mas de impedir que o documento adulterado permaneça validamente assinado.

Importante ressaltar que a assinatura digital não serve para tornar o documento sigiloso, uma vez que a chave pública deve ser de conhecimento geral e será utilizada para auferir a utilização da chave privada na geração da assinatura digital. O sigilo de um documento digital pode ser obtida pelo processo inverso ao da

[18] ZOCOLLI, Dinemar. Autenticidade e Integridade dos Documentos Eletrônicos: a Firma Eletrônica. In: Aires José Rover (Coord.). **Direito, Sociedade e Informática**. Florianópolis: Fundação Boiteux, 2000.

[19] MARCACINI, Augusto Tavares Rosa. **O Documento Eletrônico como meio de prova**. In: Infodireito [Internet] <http://www.infodireito.com.br/ > Acesso em: 10 jul. 2005.

assinatura, ou seja, o emitente utiliza a chave pública do destinatário para criptografar o documento, e este último faz uso da respectiva chave privada, que é de seu exclusivo conhecimento, para decifrar o documento.

Compreende-se, então, que a assinatura digital foi a técnica encontrada para trazer aos documentos digitais os dois elementos que lhes trazem validade jurídica: autoria e integridade. A autoria é garantida em razão do fato de que para se gerar a assinatura digital ser necessário utilizar a chave privada do signatário, a qual somente ele tem acesso, e portanto ele é de fato o subscritor daquele documento. A integridade é assegurada também em razão da assinatura digital: esta, para ser gerada, além da chave privada do signatário, faz uso do conjunto de bits que corresponde ao próprio documento digital, de modo que qualquer alteração neste conjunto de bits leva a uma conseqüente invalidação da assinatura para aquele documento (conjunto de bits) utilizado na criação da assinatura – a mencionada inalterabilidade lógica do documento assinado digitalmente.

Pode-se questionar, então, se o mero uso da assinatura digital já torna suficientemente segura a utilização do documento digital. A resposta é negativa, salvo naqueles casos onde todos os envolvidos já se conhecem, trocaram entre si suas respectivas chaves públicas, e utilizam alguma técnica para confirmar se estão de fato utilizando as chaves corretas. Existe uma fragilidade no uso da assinatura digital para sistemas que envolvem uma grande quantidade de participantes, que não decorre especificamente da técnica empregada, mas sim da possibilidade de se fraudar a identidade real do signatário. Como? Com a criação de pares de chaves falsamente atribuídos a alguém por outrem que tenha interessem em fraudar a estrutura.

Deste modo, uma determinada pessoa, com a intenção de realizar fraudes, cria um par de chaves e distribui a chave pública indicando como sendo de um terceiro – para isto, invade o sistema de correio eletrônico deste último, ou então cria uma conta com o nome do terceiro em algum site, por exemplo, que ofereça este serviço gratuitamente. Aqueles que recebem esta chave não têm, a princípio, motivos para desconfiar da informação, afinal a receberam pelo próprio endereço de correio eletrônico do terceiro. A partir deste momento, o fraudador pode começar a enviar documentos digitais assinados como se fosse aquela pessoa, e aqueles que

os receberem utilizarão a chave pública encaminhada para validar, acreditando que de fato foi aquela pessoa que assinou, e não o fraudador. Também pode ocorrer destas pessoas enviarem documentos criptografados ao falsário, imaginando que estão enviando à pessoa em cujo nome foi gerado o par de chaves falsas, e o trapaceiro terá a chave privada capaz de decriptografar o documento.

Existe alguma forma de resolver este problema? Sim, por meio de um sistema de autenticidade das chaves públicas, ou seja, uma estrutura que confirme que aquela chave pública que está sendo utilizada para validar a assinatura digital de alguém (ou para criptografar um documento que será enviado a ela) é de fato desta pessoa. Surgiram então as infra-estruturas de chaves públicas e os sistemas de certificação digital.

3.4. INFRA-ESTRUTURAS DE CHAVES PÚBLICAS

As infra-estruturas de chaves públicas (ICP's) surgiram, portanto, da necessidade de se autenticar as chaves públicas utilizadas para validação de assinaturas digitais. Autenticação, nas palavras de Dinemar Zoccoli[20], significa "conferir o cumprimento dos requisitos exigíveis à confiabilidade da prova documental". Deste modo, busca-se a elisão da fragilidade do uso de sistemas que utilizam par de chaves para assinar documentos digitais no que se refere a confirmação de que aquelas chaves públicas que serão utilizadas para validar as assinaturas digitais são de fato de determinado signatário. O certificado digital é o instrumento utilizado para a validação das chaves públicas nestas estruturas, sendo ele próprio um documento digital, assinado digitalmente por uma autoridade certificadora, que contém diversos dados sobre o emissor e o titular do certificado, como nome do titular, identificação do algoritmo de assinatura, assinatura digital do emissor, validade do certificado, além da própria chave pública vinculada ao titular do certificado[21].

[20] ZOCOLLI, Dinemar. Autenticidade e Integridade dos Documentos Eletrônicos: a Firma Eletrônica. In: Aires José Rover (Coord.). **Direito, Sociedade e Informática**. Florianópolis: Fundação Boiteux, 2000. Pág. 186.

[21] Conforme definição do padrão X.509 da *International Communnications Union* (ITU)

As infra-estruturas de chaves públicas podem ser divididas em dois formatos básicos:

- Hierárquico: existe uma autoridade certificadora central (raiz), que autoriza a emissão de certificados pelas demais entidades daquela estrutura. Portanto, a AC-Raiz fica no topo da estrutura, e é auto-assinada (utiliza a própria chave privada para assinar o seu certificado). Por esta razão, a confiança é também centralizada, e é difundida aos demais certificadores da cadeia em razão na credibilidade depositada na AC-Raiz.

- Rede: há um conjunto de entidades certificadoras independentes, porém ligadas entre si por certificação cruzada, ou seja, criando relações de confiança uma nos certificados das outras.

O modelo central introduzido no Brasil pela Medida Provisória 2.200-02/2001, denominado ICP-Brasil, possui estrutura hierárquica, com certificação de raiz única. O Instituto Nacional de Tecnologia da Informação (ITI) é a Autoridade Certificadora Raiz (AC Raiz) desta infra-estrutura de chaves públicas, tendo por função básica "a execução das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor, atuando: na emissão, expedição, distribuição, revogação e gerenciamento de certificados de autoridades certificadoras de nível imediatamente inferior ao seu, chamadas Autoridades Certificadoras Principais; no gerenciamento da lista de certificados revogados (LCR), emitidos e vencidos; e na execução, fiscalização e auditoria das autoridades certificadoras, de registro e prestadoras de serviço de suporte habilitadas na ICP-BRASIL"[22].

Um ponto a ser destacado é de que os certificados digitais possuem prazos de validade: desse modo, uma determinada chave privada só pode ser utilizada para assinar um documento enquanto o certificado que dá validade à respectiva chave pública estiver válido. Além disso, o certificado pode ser suspenso – quando, por exemplo, pairarem dúvidas sobre o titular do certificado – ou revogado – nos casos de comprometimento da chave privada. Convém ressaltar, entretanto,

[22] http://www.iti.br/twiki/bin/view/Main/FaQ200324JunP

que apesar de não poder mais se utilizar aquela chave privada para assinar um documento, as infra-estruturas devem estar preparadas para continuar validando os documentos assinados quando o certificado ainda era válido, ou seja, os certificados devem permanecer armazenados por um tempo longo o suficiente para garantir a conferência das assinaturas digitais realizadas com as chaves privadas respectivas.

4. LEGISLAÇÃO

4.1. LEGISLAÇÃO ESTRANGEIRA

Já são décadas de existência dos documentos digitais, uma vez que surgiram junto com os próprios computadores. Entretanto, sua utilização só se tornou comum com a proliferação dos microcomputadores, e mais ainda, com o surgimento da internet, quando a adoção da tecnologia se viu estimulada, grande parte em razão das novas possibilidades de comunicação e interação, mas também em função dos valores econômicos e interesses comerciais envolvidos. A Era da Informação tem como uma de suas maiores características a *"desmaterialização de conceitos tradicionais, como o de documento"*[23]. Deve-se levar em conta que os avanços tecnológicos de uso comum pela sociedade muitas vezes levam tempo até serem absorvidos pela Direito. Assim foi com o documento digital; a legislação que trata dos documentos digitais apenas começa a surgir em meados da década de noventa. Era de se esperar que os países de maior renda fossem os primeiros a legislar sobre o tema, uma vez que são também eles os que fazem uso mais intenso da tecnologia.

Desta forma, em 1995, no estado de Utah, nos Estados Unidos, surge a primeira norma a respeito de documentos e assinaturas digitais (*Utah Digital Signature Act*[24]), notabilizada não só pela precedência como pelo detalhamento

[23] CASTRO, Aldemario Araujo. **Validade jurídica de documentos eletrônicos**. Jus Navigandi. [Internet]: <http://jus2.uol.com.br/doutrina/texto.asp?id=2028>. Acesso em: 10 set. 2005.

[24] Veja em <http://www.jus.unitn.it/users/pascuzzi/privcomp97-98/documento/firma/utah/udsa.html>

técnico nela contido[25]. Desde então os demais estados norte-americanos passaram a buscar a regulamentação do uso dos documentos e assinaturas digitais, como as normas dos estados da Califórnia[26] (*Digital Signature Regularions*), de Illinois (*Electronic Commerce Security Act*[27]), e da Georgia (*Electronic Records and Signature Act*[28]).

Na Europa, diversos países também já adotaram leis que tratam dos documentos e assinaturas digitais: Alemanha (*Signaturgesetz, SiG, Gesetz zur digitalen Signatur*[29]), Italia (*Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513*[30]), Inglaterra (*Electronic Communications Act, 2000*[31]), França (*Loi n°2000-230 du 13 mars 2000*[32]), Portugal (*Decreto-Lei n.º 290-D, de 2 de Agosto 1999*[33]), entre outros. Deve-se destacar a Diretiva 1999/93/EC[34] do Parlamento Europeu, que tem por objetivo nortear as nações européias no que se refere à produção legislativa a respeito de documento e assinatura digital, uma vez que normas divergentes poderiam significar barreiras à integração entre os países membros.

Na América do Sul, além do Brasil, como se verá mais adiante neste trabalho, outros países também disciplinam a questão dos documentos e assinaturas digitais. Por exemplo, o Chile o faz por meio do *Decreto Supremo n. 81 de 1999*[35], a Colômbia mediante a *Lei 527 de 1999*[36], e a Argentina com o *Decreto 427 de 1998*[37].

---

[25] MARCACINI, Augusto Tavares Rosa. **O Documento Eletrônico como meio de prova**. In: Infodireito [Internet] <http://www.infodireito.com.br/ > Acesso em: 10 jul. 2005.

[26] Veja em <http://www.ss.ca.gov/digsig/regulations.htm>

[27] Veja em http://www.findlaw.com/bills/ildigital.html

[28] Veja em http://gsulaw.gsu.edu/gsuecp/Act/Act.htm

[29] Veja versão em inglês em http://www.iuscomp.org/gla/statutes/SiG.htm

[30] Veja em http://www.interlex.it/testi/dpr51397.htm#6

[31] Veja em http://www.opsi.gov.uk/acts/acts2000/20000007.htm

[32] Veja em http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=JUSX9900020L

[33] Veja em http://www.pj.pt/htm/legislacao/dr_informatica/DL290_D_99.htm

[34] Veja em http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

[35] Veja em http://rechtsinformatik.jura.uni-sb.de/cbl/statutes/Chile81.html

[36] Veja em http://www.secretariasenado.gov.co/leyes/L0527_99.HTM

Como se verá a seguir, a legislação brasileira a respeito do matéria surgiu algum tempo depois dos textos legais de nossos países vizinhos, apesar de algumas iniciativas anteriores realizadas, porém, internamente ao Poder Executivo pátrio.

4.2. LEGISLAÇÃO BRASILEIRA

Atualmente, no Brasil, a norma que disciplina o uso dos documentos e assinaturas digitais tema é a Medida Provisória nº. 2.200-02, de 24 de agosto de 2001. É importante destacar que esta medida provisória, apesar de ter sido publicada há alguns anos, ainda está em vigor, em razão do que expressa o artigo 2º da Emenda Constitucional nº. 32, de 11/09/2001.

> Art. 2º As medidas provisórias editadas em data anterior à da publicação desta emenda continuam em vigor até que medida provisória ulterior as revogue explicitamente ou até deliberação definitiva do Congresso Nacional.

A medida provisória em questão instituiu a Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil), definindo como Autoridade Certificadora Raiz, conforme seu artigo 13, o Instituto Nacional de Tecnologia da Informação (ITI), estabelecida como autarquia federal vinculada ao Ministério da Ciência e Tecnologia, conforme expressa o artigo 12 deste texto normativo.

A norma, já em seu artigo 1º, declara que a ICP-Brasil tem por finalidade a garantia de autenticidade, integridade e validade jurídica dos documentos produzidos de forma eletrônica. O texto legal passa então à composição da infra-estrutura, a qual é formada pela Autoridade Certificadora Raiz (AC Raiz), pelas Autoridades Certificadoras (AC's) e pelas Autoridades de Registro (AR's).

Cabe destaque ao artigo 6º da Medida Provisória que, ao tratar das Autoridades Certificadoras (AC's), lhes traz a competência para emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular. Também são responsáveis pela emissão, expedição, distribuição, revogação e gerenciamento dos certificados, devendo colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes, além de manter registro de suas operações. O parágrafo único do artigo ora em comento trata de duas questões bastante sensíveis: a geração do par de chaves, que conforme o texto normativo

[37] Veja em http://www.informatica-juridica.com/anexos/anexo193.asp

deverá ser gerado sempre pelo próprio titular, e o conhecimento da chave privada de assinatura que, também se depreende da norma, será de ciência, uso e controle exclusivo do titular.

O artigo 7º trata das Autoridades de Registro que, vinculadas a uma Autoridade Certificadora, são responsáveis por identificar e cadastrar os usuários – na presença destes –, e encaminhar solicitações de certificados às Autoridades Certificadoras. As Autoridades de Registro, assim como as Certificadoras, também devem manter cadastradas as suas operações. O artigo 8º, por sua vez, aduz que poderão ser credenciados como Autoridades Certificadoras e Autoridades de Registro, desde que atendam critérios estabelecidos pelo Comitê Gestor da ICP-Brasil, órgãos e entidades públicos, bem como pessoas jurídicas de direito privado.

Chega-se então ao artigo 10 da Medida Provisória 2.200-02, de 2001, que trata de ponto central da norma: a validade dos documentos digitais (a expressão adotada no texto legal foi "documento eletrônico"). Assim, o *caput* do artigo diz que "consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória." O parágrafo 1º deste artigo equipara os documentos digitais assinados em conformidade com a ICP-Brasil aos documentos com assinatura manuscrita, fazendo referência expressa ao artigo 131 do Código Civil de 1916 (Lei nº. 3.071, de 1º de janeiro de 1916), que vigia à época da publicação da citada Medida Provisória. O referido artigo assim apregoava: "Art. 131 As declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários". O referido dispositivo legal encontra correspondência, literal, no artigo 219 do atual Código Civil (Lei nº. 10.406, de 10 de janeiro de 2002). De forma transparente, trazendo validade aos documentos digitais assinados em observância aos preceitos da ICP-Brasil, assim aponta o parágrafo 1º do artigo 10 da Medida Provisória 2.200-02/2001:

> § 1o As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil.

Porém, a citada Medida Provisória não se restringiu apenas aos documentos digitais assinados no âmbito da ICP-Brasil. O parágrafo 2º do artigo 10 faz menção expressa à utilização de outros meios de comprovação de autoria e

integridade de documentos digitais (no dispositivo legal chamados de “documentos em forma eletrônica”), inclusive para a utilização de certificados não emitidos pela ICP-Brasil, desde que esse meio de comprovação seja admitido pelas partes como válido, ou ainda que seja aceito pela pessoa a quem for oposto o documento, conforme apresentado a seguir:

> § 2o O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da **autoria** e **integridade** de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento. *(grifou-se)*

Nos próximos artigos, a Medida Provisória citada trata de outros aspectos relativos a criação e condições de funcionamento da ICP-Brasil. Foge ao escopo deste trabalho a análise mais aprofundada de outras normas que regulamentam o funcionamento da ICP-Brasil; porém, faz-se pertinente a referência a algumas delas: Decreto nº 3.996, de 31 de Outubro de 2001 (dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal), Decreto nº 4.414, de 07 de Outubro de 2002 (altera o Decreto no 3.996, de 31 de Outubro de 2001, que dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal), Decreto nº 4.689, de 07 de Maio de 2003 (aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação), bem como as resoluções e portarias do Comitê Gestor da ICP-Brasil.

Ainda com relação a validade jurídica do documento digital, cabe a lembrança do que dispõe o artigo 332 do Código de Processo Civil pátrio:

> 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.

Desta forma, ainda que não houvesse a Medida Provisória 2.200-02/2001 a tratar da validade dos documentos digitais assinados digitalmente, ainda assim não se poderia negar a legitimidade deste tipo de documento como meio probante, uma vez que não se pode falar que documentos digitais são, por si próprios, ilegais, nem tampouco imorais, e como visto anteriormente neste trabalho, reúnem condições técnicas que lhes trazem eficácia probatória. Pela mesma razão, como

bem lembra Augusto Marcacini[38], o documento digital tampouco confrontaria a previsão do inciso LVI do artigo 5º da Constituição Federal ("LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos"), justamente em razão do que já se notificou neste estudo – o documento digital, em si, não é ilegal. Porém, não se está dizendo que o documento digital não possa ser obtido de forma ilegal – no caso de uma interceptação de comunicação protegida por sigilo, por exemplo – , fato que, daí sim, ensejaria sua inadmissibilidade como elemento de prova, da mesma forma como ocorreria com qualquer outro meio probante obtido de forma viciada.

5. CONCLUSÃO

Diante do que foi apresentado, percebe-se que o documento digital se fará cada vez mais presente como forma de registro. As maiores barreiras a sua utilização não estão, como exposto, nos aspectos técnicos ou jurídicos, mas sim na mudança de cultura, diante do hábito arraigado de se utilizar o documento físico, ou seja, algo material, palpável, e cuja existência independe de um computador que possa armazená-lo e traduzi-lo. Porém, essa transformação cultural já está acontecendo; o uso dos meios informáticos é cada vez mais comum em todas as atividades, e se tornam ainda mais necessários na medida em que há o aumento expressivo do volume de informações com o qual os profissionais são obrigados a lidar.

No mundo empresarial, são intensos os esforços para se diminuir, e até substituir, a utilização do papel como fonte primária de registro e troca de informações, e o elemento principal desta empreitada é o documento digital. Se percebeu que, via de regra, o documento já nasce em um computador, e as empresas identificaram a possibilidade de obter grandes benefícios se estes documentos continuassem em meios digitais. Diante disso, não causa surpresa o fato de que o uso cada vez mais amplo do documento digital seja uma meta comum às mais variadas entidades atuantes no mercado.

[38] MARCACINI, Augusto Tavares Rosa. **O Documento Eletrônico como meio de prova**. In: Infodireito [Internet] <http://www.infodireito.com.br/ > Acesso em: 10 jul. 2005.

Na esfera pública, e em especial no Poder Judiciário, diversas são as iniciativas que prevêem a utilização de documentos digitais, motivadas pelas vantagens destacadas anteriormente neste trabalho. Ganham maior relevo aquelas que buscam à informatização dos processos judiciais, diante dos benefícios que podem trazer à sociedade: menor custo, maior agilidade, maior publicidade, melhor manuseio, maior segurança, apenas para elencar superficialmente os resultados que podem ser atingidos. Estas benesses não devem se restringir ao Poder Judiciário, mas sim se estender ao Legislativo e ao Executivo, vez que se vislumbra a possibilidade de fortalecimento da cidadania aos brasileiros.

Em relação aos profissionais do Direito, em especial aos advogados, ressalta-se que precisam ter a consciência de que estar atualizado tecnologicamente deve ser inerente à sua atuação. O advogado deve ter papel ativo na busca da melhor utilização da tecnologia para executar o seu mister. Não deve assumir uma postura passiva de apenas aguardar que o poder público decida a forma como se dará o estabelecimento de novas tecnologias – deve participar destas escolhas, compreender os desdobramentos implicados, e se preparar para eles. Por outro lado, também deve estar certo de que cada vez mais seus clientes exigirão capacitação para lidar com as melhores ferramentas para a execução de seus trabalhos. Nestes tempos de informação “na ponta dos dedos”, o nível de exigência quanto à qualidade de prestação de serviços tem atingido patamares mais elevados. O advogado deve estar pronto a atendê-los, sob pena de não sobreviver em um ambiente cada vez mais competitivo, e cada vez mais complexo.

Resta lembrar, portanto, que o documento digital já é uma realidade, e estará cada vez mais próximo, fará parte das atividades de forma tão corriqueira quanto o documento físico o faz hoje. Ao se ter mente os inquestionáveis avanços que serão obtidos com a utilização do documento digital, é possível prever que barreiras à sua utilização sejam cada vez mais reduzidas. No decorrer deste trabalho se verificou que fatores técnicos não são impeditivos à utilização do documento digital, ao contrário, o estado da técnica atual já permite se falar em validade jurídica deste documento. Este entendimento é convalidado com a demonstração de que os sistemas normativos brasileiro e estrangeiro já recepcionam o documento digital em sua plenitude.

6. REFERÊNCIAS

ARRUDA JÚNIOR, Itamar. **Documentos eletrônicos, autoridades certificadoras e legislação aplicável**. In: Âmbito Jurídico, nov/2001. Disponível em: <http://www.ambito-juridico.com.br/aj/int0010c.htm> Acesso em: 10 set. 2005.

BRASIL. Constituição Federal de 1988. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 22 fev. 1998. Disponível em: <http://www.planalto.gov.br>. Acesso em: 01 set. 2005.

BRASIL. Medida Provisória nº 2.200, de 11 de setembro de 2001. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 22 fev. 1998. Disponível em: <http://www.planalto.gov.br>. Acesso em: 01 set. 2005.

BRASIL, Ângela Bittencourt . **ASSINATURA DIGITAL** In: Site do Ministério da Ciência e Tecnologia. Disponível em: <http://www.mct.gov.br/legis/ Consultoria_Juridica /artigos /assinatura_digital.htm> Acesso em: 15 set. 2005

CASTELLS, Manuel. **A Galáxia da Internet**. São Paulo: Jorge Zahar, 2003.

CASTRO, Aldemario Araujo. **Validade jurídica de documentos eletrônicos**. Considerações sobre o projeto de lei apresentado pelo Governo Federal. Jus Navigandi. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2028>. Acesso em: 10 set. 2005.

CASTRO, Aldemario Araujo. **O Documento Eletrônico e O novo Código Civil**. Alfa-Redi: Revista de Derecho Informático. Disponível em: <http://www.alfa-redi.org/rdi-articulo.shtml?x=1256>. Acesso em: 10 set. 2005.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 2000.

GRECO, Marco Aurélio. **Internet e Direito**. São Paulo: Dialética , 2000.

KAMINSKI, Omar (Coord). **Internet Legal**. Curitiba: Juruá, 2003.

MARCACINI, Augusto Tavares Rosa. **O Documento Eletrônico como meio de prova**. In: Infodireito. Disponível em: <http://www.infodireito.com.br/ > Acesso em: 10 jul. 2005.

MONTENEGRO, Antonio Lindberg. **A Internet em suas Relações Contratuais e Extracontratuais**. Rio de Janeiro: Lumen Juris, 2003.

PAESANI, Liliane Minardi. **Direito de Informática**. São Paulo: Atlas, 2003.

PINTO, Marcio Morena. **Documento Electrônico: Uma Breve Análisie de seus Aspectos Jurídicos**. Disponível em: <http://www.alfa-redi.org/rdi-articulo.shtml?x=1559> Acesso em: 15 set. 2005

REINALDO FILHO, Demócrito (Coord.). **Direito da Informática – Temas Polêmicos**. Bauru: EDIPRO, 2002.

ROVER, Aires (Coord.). **Direito, Sociedade e Informática**. Florianópolis: Fundação Boiteux, 2000.

ROVER, Aires (Coord.). **Direito e Informática**. São Paulo: Editora Manole, 2003.

WACHOWICZ, Marcos (Coord.). **Propriedade Intelectual e Internet**. Curitiba: Juruá Editora, 2003.

ZOCOLLI, Dinemar. Autenticidade e Integridade dos Documentos Eletrônicos: a Firma Eletrônica. In: Aires José Rover (Coord.). **Direito, Sociedade e Informática**. Florianópolis: Fundação Boiteux, 2000. p. 177-192.