UNIVERSIDADE FEDERAL DO PARANÁ
SETOR DE CIÊNCIAS JURÍDICAS
FACULDADE DE DIREITO
NÚCLEO DE MONOGRAFIAS

PETIÇÕES ELETRÔNICAS NO PROCESSO CIVIL BRASILEIRO

CURITIBA
2006

JOÃO LUIZ PIANOVSKI VIEIRA

PETIÇÕES ELETRÔNICAS NO PROCESSO CIVIL BRASILEIRO

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel no Curso de Graduação em Direito do Setor de Ciências Jurídicas da Universidade Federal do Paraná.

Orientador: Professor Edson Ribas Malachini

CURITIBA

2006

TERMO DE APROVAÇÃO

JOÃO LUIZ PIANOVSKI VIEIRA

PETIÇÕES ELETRÔNICAS NO PROCESSO CIVIL BRASILEIRO

Monografia aprovada como requisito parcial para obtenção do grau de Bacharel no Curso de Graduação em Direito do Setor de Ciências Jurídicas da Universidade Federal do Paraná, pela seguinte banca examinadora:

Orientador: _____
PROF. EDSON RIBAS MALACHINI

Examinador: _____
PROF. MANOEL CAETANO FERREIRA FILHO

Examinador: _____
PROF. ELTON VENTURI

Curitiba, 25 de outubro de 2006

Agradeço a todos aqueles que, com sua inestimável colaboração, tornaram este trabalho possível: ao bondoso Deus, que tanto me proporcionou; a meus pais, fonte inesgotável de afeto, auxílio e compreensão; ao Professor Malachini, pela confiança e pela orientação na exploração de tão delicado tema, e a meus amigos, pelos engrandecedores debates.

SUMÁRIO

RESUMO

Trata o presente trabalho das possibilidades trazidas pela informática de se levar a Juízo petições elaboradas por meio de um computador, com o uso da internet. As peças comumente produzidas no meio informático acabam por ser impressas e remetidas da mesma maneira como se faz há séculos: com o transporte físico de folhas de papel. No entanto, as infra-estruturas de chaves públicas, cujos mecanismos serão aqui objeto de análise, vieram para mudar esse panorama, firmando a segurança de uma nova modalidade de peticionamento. E assim fazem ao garantir a autenticidade e a integridade das peças processuais eletrônicas, por meio de assinaturas e certificados digitais, com elevados níveis de segurança, permitindo às partes ter confiança de que suas informações não serão interceptadas, indevidamente lidas ou alteradas após deixarem seus equipamentos e adentrarem a grande rede. As assinaturas e certificados digitais, produto da criptografia assimétrica, já são objeto de debates na seara jurídica nacional, estando atualmente reguladas por medida provisória de que se trata neste estudo. Para além disso, experiências apontando no sentido da virtualização do processo em território nacional não faltam: o tema da informática jurídica – isto é, os computadores servindo ao direito – é fértil e suscita grandes questionamentos, tais como a instituição de um processo completamente virtual, a utilização de documentos eletrônicos como meio de prova e o próprio conceito de documento, passagens que se visitará com brevidade – por pertinentes, porém periféricas – para clarificar a problemática da viabilidade fática de se utilizarem petições eletrônicas. Trazem-se à tona, ainda, indagações processuais carecedoras de resposta, buscando, outrossim, traçar visão geral da legislação e das instalações pátrias no que concerne ao tema.

Palavras-chave: informática jurídica; petições eletrônicas, assinaturas digitais, certificados digitais, autenticidade, integridade, processo virtual, criptografia, infra-estruturas de chaves públicas.

INTRODUÇÃO

A informática já é perenemente aplicada no dia-a-dia da prática jurídica. Textos são processados por meio de computadores, mensagens são enviadas igualmente através deles e os bancos de dados são ferramentas de que se valem inúmeros profissionais do direito. Mas há muito mais a se aproveitar. Quando um arquivo é produzido num equipamento e, depois de impresso, passa tão-somente a jazer no disco rígido, seu potencial é precocemente ceifado[1].

A presença crescente do mundo digital, mesmo entre as classes menos favorecidas, é um fato. Tome-se também por base a necessidade de se agilizarem as tarefas dos profissionais do direito e as facilidades que as novas tecnologias permitem, podendo ser implantadas em vários procedimentos do processo civil com mais vantagens que prejuízos. Configura-se o cenário para que a implantação dessas novas técnicas seja desejável, em que pese a resistência contra o emprego de meios eletrônicos no processo civil já apontada por Dinamarco[2].

Em face da complexidade do mundo moderno, que força uma perene revisão de nossos conceitos, as pessoas já adquiriram uma maior flexibilidade em relação a mudanças, sejam elas procedimentais ou de comportamento.

Com o direito, apesar de se desejar sua adaptação às transformações na velocidade destas, forçoso reconhecer que tal não ocorre de maneira tão fácil. A estrutura do mundo jurídico necessita de alguma tenacidade, o que implica em verificação de conformidade, em face do sistema vigente, para as novidades que surgem. Até que se sedimentem entendimentos sobre novas realidades, muito há de se discutir. E, quando se pensa em justiça, não poderia ser de outro modo. Silva bem sintetiza esse raciocínio:

> (...) o meio jurisprudencial, pela natureza mesma das funções que exerce – extremamente voltadas à segurança e à certeza do direito das pessoas –, tende a ser naturalmente conservador e, portanto, pouco permeável às novidades tecnológicas que possam apresentar qualquer possibilidade de dúvida quanto à fidedignidade dos dados que fornecem.[3]

1 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 155.

2 DINAMARCO, Candido Rangel *apud* ALMEIDA FILHO, José Carlos de Araújo e CASTRO, Aldemario Araujo. *Manual de informática jurídica e direito da informática*, p. 201.

3 SILVA, João Carlos Pestana de Aguiar. *As provas no cível*, p. 116.

Se é certo que a tenacidade do ordenamento deve ser respeitada, igualmente é que o direito não pode se imobilizar diante de inovações de relevo. Sendo inevitável a adoção do crescente aparato tecnológico, extremamente conveniente, acaba este por se instalar muitas vezes baseando-se em analogias, antes mesmo de regulação legal específica. Tanto é assim que algumas dessas novidades já são ferramentas de que se valem os profissionais do direito, por força de pioneiras experiências.

Desafio como poucos é a internet para o direito. Se de um lado permite a prática de vários atos ilícitos, igualmente habilita a consecução de legítimos interesses, cujos detentores desejam de todo modo suplantar os riscos da Grande Rede que prejudiquem a realização de seus negócios. Afirma Silva[4] que além de não existir uma autoridade a poder controlar a internet – característica sua da maior relevância –, o ambiente desta é contaminado pela volatilidade, pela mutabilidade e pelo anonimato, caráter este criador de obstáculos à aplicação do ordenamento. Como contraponto, há custos reduzidos, precisão, alta velocidade e facilidade de acesso, sem falar na falta de barreiras financeiras, temporais e espaciais, que aliás trazem consigo a necessidade de reavaliar certos conceitos processuais, como o de territorialidade.

No Brasil, as declarações de imposto de renda são hoje quase em sua totalidade entregues em meio digital. As eleições se valem de urnas eletrônicas. E agora a informática vem para revolucionar o processo civil: com o processo que se virtualiza, os profissionais do direito terão maior facilidade na elaboração de peças processuais, podendo buscar informações necessárias de maneira automatizada – não são raros os casos em que, diante de ser indispensável absoluta certeza de um dado encontrar-se ou não nos autos, eles precisem ser folheados página a página. O número de idas e vindas dos cadernos processuais poderá ser drasticamente reduzido – ou mesmo eliminado, no caso do processo integralmente virtual. Todas as partes do processo poderão usufruir de notável mobilidade, podendo exercer suas funções de onde estiverem.

A aceitação de meios eletrônicos pelas repartições públicas implicará em verdadeira transformação no mundo jurídico. Entre os resultados dessa mudança

4 SILVA, João Carlos Pestana de Aguiar. *As provas no cível*, p. 370.

situam-se protocolos e contratos eletrônicos, a publicação dos atos (que importará em notável acréscimo de sua publicidade fática, com conseqüente democratização da informação), a intimação por meio eletrônico, a transformação da atividade advocatícia.

Importa destacar que, em termos de economia e sustentabilidade, a eliminação de parte dos documentos impressos e de muitos deslocamentos físicos de que carecem os profissionais do direito colaborará, de modo bastante direto, para a perpetuação do sistema e à manutenção dos recursos do planeta[5].

A tecnologia permitirá que autos sejam arquivados por prazos ainda mais longos; as informações processuais poderão ser mais minuciosas e facilmente consultadas, com a agilidade e a precisão que só os novos mecanismos podem proporcionar[6].

Tais vantagens da comunicação eletrônica, de um modo geral, já são bem conhecidas. Faltavam a segurança e a autenticidade, que segundo preleciona Guedes são verdadeiros pressupostos da existência da comunicação eletrônica. Na primeira, englobar-se-iam a confiabilidade dos sistemas dedicados à recepção e ao envio de dados, bem como a possibilidade de se confirmar a concretização dos atos praticados. Já a autenticidade responderia, no âmbito objetivo, pela correspondência entre o conteúdo enviado e aquele recebido; na seara subjetiva, de outra parte, pela certeza de que o emissor e o receptor são aqueles que deveriam ser, de fato, os participantes da relação processual[7].

Esses dois pontos eram suficientes para abalar a credibilidade da prática de atos processuais por meio eletrônico, em razão de os profissionais do direito, no envio de instrumentos processuais por essa via, não se importarem somente com suas vantagens, mas também – e prudentemente – com a segurança de que suas peças sejam remetidas de maneira segura e sem interceptações, com uma probabilidade razoável de inexistirem fraudes.

Se antes não se vislumbravam meios eficientes e totalmente eletrônicos de

5 O que se verificou até o momento foi que o computador, ao invés de reduzir os gastos de papel, intensificou-os.

6 Digna de nota a informação de que, na Justiça do Trabalho, programa de computador verifica a admissibilidade de recursos, elaborando despachos-padrão: LIMA, George Marmelstein. *e-Processo:* uma verdadeira revolução procedimental.

7 GUEDES, Jefferson Carús. *Comunicação processual eletrônica na lei dos Juizados Especiais Federais*.

documentos nesse meio terem validade jurídica, com autenticidade e integridade garantidas, a criptografia, ao permitir a feitura de assinaturas e certificados digitais, é o fundamento desse novo processo que se anuncia.

No presente trabalho, após sucinta introdução histórica ao notável avanço da informática sobre as atividades de nossos dias, observar-se-á a composição dos documentos eletrônicos, passando-se a seguir ao modo de operação dos mecanismos criptográficos na aposição de assinaturas e certificados digitais sobre esses documentos. Será igualmente examinada a estrutura da ICP-Brasil, infra-estrutura de chaves públicas estabelecida por medida provisória que pretende fundamentar a utilização dessas inovações no Brasil.

Também sob o aspecto legislativo, revisitar-se-ão normas que permitiram historicamente a utilização de instrumentos processuais eletrônicos no processo civil brasileiro, sendo ainda objeto de reflexão as pertinentes normas em vigor e os projetos de lei em trâmite.

Questionar-se-á, além disso, a viabilidade de um processo integralmente virtual, anotando-se as experiências já realizadas nesse sentido no Brasil e os desafios que advêm da virtualização dos trâmites processuais.

1. HISTÓRICO

1.1 A DESCOBERTA DO VIRTUAL

Lévy leciona que "a palavra virtual vem do latim medieval *virtualis*, derivado por sua vez de *virtus*, força, potência. Na filosofia escolástica, é virtual o que existe em potência e não em ato. (...) A árvore está virtualmente presente na semente"[8]. Prossegue o autor afirmando que o virtual sempre existiu[9], apesar de se apresentar como algo novo. Consiste na possibilidade existente em todas as coisas, não se contrapondo ao real, mas sendo instrumento de aperfeiçoamento de uma dada realidade por meio da solução de problemas. Nessa linha, o ciberespaço permitiria a virtualização da escrita, libertando-a do papel e permitindo sua livre circulação. Oliveira, valendo-se do entendimento de Lévy, anota[10] que a possibilidade de uma pessoa ter acesso a um processo em tempo real significa a virtualização da distância entre ela e o juízo. O processo virtual igualmente virtualizaria a informação, atingindo-se um elevado grau de publicidade anteriormente inatingível.

Enquanto a digitalização implica somente na transferência de um determinado conteúdo para o computador[11], a virtualização vai além, atribuindo a esta máquina as funções mecanizadas exercidas pelos chamados servidores burocráticos, cabendo então ao ser humano apenas as atividades envolvendo a criatividade[12].

No direito, a aplicação da cibernética foi vislumbrada inicialmente por Norbert Wiener, considerado "pai da cibernética"[13].

---

8 OLIVEIRA, Bruno Augusto Santos. *Juizado virtual*: o deslocamento do centro de gravidade ontológico do processo-papel para a problemática da eficiência da justiça.

9 LÉVY, Pierre *apud* FAGÚNDEZ, Paulo Roney Ávila. *A virtualidade,* pp. 152-153.

10 OLIVEIRA, Bruno Augusto Santos. *Juizado virtual:* o deslocamento do centro de gravidade ontológico do processo-papel para a problemática da eficiência da justiça.

11 O digital e o eletrônico dizem mais respeito à forma que à substância: OLIVEIRA, Bruno Augusto Santos. *Juizado virtual:* o deslocamento do centro de gravidade ontológico do processo-papel para a problemática da eficiência da justiça.

12 OLIVEIRA, Bruno Augusto Santos. *Juizado virtual:* o deslocamento do centro de gravidade ontológico do processo-papel para a problemática da eficiência da justiça.

13 LUCCA, Newton da. *Títulos e contratos eletrônicos*, p. 50.

1.2 DOS ÁTOMOS AOS BITES

No início, as pessoas se valiam de expressões corporais para expressar sua vontade, sendo a comprovação dos negócios feita por meio de testemunhos, como nas assembléias realizadas na Roma Antiga para a realização dos atos jurídicos. Em momento posterior, a escrita e o papel viriam a se prestar para a materialização das provas, juntamente com a assinatura, traço identificador da autoria das declarações. O documento em papel serviu então de fundamento ao desenvolvimento do direito, que dele se vale para a formulação de inúmeros conceitos[14]. A relação entre o direito e o papel é, destarte, muito estreita, razão pela qual desvincular este daquele soa extremamente desafiador.

A civilização anteriormente tinha por unidade estrutural os átomos, naturalmente palpáveis, característica essa da qual o mundo jurídico obviamente se valia. De fato, até os anos oitenta, o direito – apesar de regular a propriedade intelectual informática – vislumbrava o computador como apenas mais uma máquina. Mas uma nova unidade estrutural começou a se estabelecer: o bite, que alcança espaço cada vez maior no cotidiano da atualidade[15].

Uma rede de computadores em especial pode ser considerada a responsável pelo enorme trânsito de bites que se estabeleceu: a internet, criada diante das necessidades militares que se impuseram nos Estados Unidos da América como uma rede de computadores interligada sem central, de modo a resistir à perda de frações suas sem prejuízos ao seu funcionamento, peculiaridade esta particularmente útil diante de possíveis ataques militares[16]. Hoje a internet já alçou papel de indispensabilidade na vida dos cidadãos – mesmo daqueles que com ela não interagem diretamente –, sendo objeto de designação em texto normativo (Norma 004/95, item 3, "a" do Ministério do Estado das Comunicações) como

> nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o software e os dados contidos nestes computadores[17].

14 VOLPI NETO, Angelo. *Ata notarial de documentos eletrônicos.*
15 CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 100 e LIMA NETO, José Henrique Barbosa Moreira. *Aspectos jurídicos do documento eletrônico*.
16 PORTA, Marcos de Lima. *A importância da internet na justiça*, p. 357.
17 LUCCA, Newton da. *Títulos e contratos eletrônicos*, p. 61.

Na legislação pátria, o uso de meios eletrônicos foi primeiramente referido no art. 10, § 2º da Lei Federal nº 6.404/1976 (Lei de Sociedades por Ações), dada a autorização de se substituírem os livros sociais por registros eletrônicos[18]. Já no que se refere à prática de atos processuais, em termos legislativos, a Lei Federal nº 8.245/1991 (Lei do Inquilinato), em seu art. 58, IV passou a prever o uso de fax. Todavia, tratava a hipótese legal da citação do réu, não sendo muito bem aceito esse mecanismo. Marcacini anota que tal provavelmente se deu por ter sido implantado esse meio eletrônico logo de início em tão importante ato processual, sendo que a forma de comunicação tampouco foi regulada adequadamente[19].

No início daquela década de 1990, em sentido contrário à jurisprudência do Supremo Tribunal Federal e do Superior Tribunal de Justiça, a interposição de recursos por fac-símile passou a ser aceita nos Tribunais Regionais Federais e nos Tribunais Estaduais, desde que posteriormente juntados os originais[20].

1.3 CAMINHOS ABERTOS PELA LEI FEDERAL Nº 9.800/1999

A Lei Federal nº 9.800/1999 suscitou discussões acerca do uso de meios eletrônicos no processo civil brasileiro. O art. 1º da referida lei permite "às partes a utilização de sistema de transmissão de dados e imagens tipo fac-símile ou outro similar, para a prática de atos processuais que dependam de petição escrita". A interpretação de que o correio eletrônico estaria compreendido na expressão "outro similar" deu azo a que muitas varas judiciais estaduais e tribunais (como o TJPR, por meio de seu Decreto nº 46/2001) validassem a recepção de peças processuais por esse meio[21]. Nessa seara, alerta Atheniense[22] que a aferição da autenticidade do remetente não foi objeto de grande atenção, para o que provavelmente colaborou a necessidade expressa no art. 2º da lei e em seu parágrafo único, determinando a juntada do *original em papel* até cinco dias após a remessa eletrônica ou após o

18 LUCCA, Newton da. *Títulos e contratos eletrônicos*, p. 45.
19 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 156-158.
20 GUEDES, Jefferson Carús. *Comunicação processual eletrônica na lei dos Juizados Especiais Federais*.
21 GUEDES, Jefferson Carús. *Comunicação processual eletrônica na lei dos Juizados Especiais Federais.*
22 ATHENIENSE, Alexandre Rodrigues. *Da validade legal dos atos processuais praticados pelo meio eletrônico.*

término do prazo (nos atos sujeitos a ele), o que desprestigia a validade do remetido eletronicamente.

No Superior Tribunal de Justiça há julgados – notadamente da Primeira Turma – atribuindo eficácia à petição remetida por correio eletrônico, como o seguinte:

> PROCESSUAL CIVIL - RECURSO - APRESENTAÇÃO - CORREIO ELETRÔNICO - INTERNET - POSSIBILIDADE - LEI 9.800/99.
> I - O art. 1º, da Lei 9.800/99, outorga às partes a faculdade de utilizar sistema de transmissão de dados e imagens tipo fac-símile ou outro similar, para a prática de atos processuais que dependam de petição escrita.
> II - É plenamente eficaz, como ato processual, a petição remetida por correio eletrônico (Internet), quando os originais, devidamente assinados, são entregues até cinco dias da data do término do prazo recursal. Inteligência da Lei nº 9.800/99. (...)
> (EDcl no AgRg no Ag 389.941/SP, Rel. Ministro HUMBERTO GOMES DE BARROS, PRIMEIRA TURMA, julgado em 27.05.2003, DJ 16.06.2003 p. 263)

Se de um lado a aludida lei foi inovadora, permitindo, conforme Marcacini[23], uma gradual assimilação da tecnologia por parte dos profissionais do direito, há limitações em seus dispositivos que impedem a aplicação de um verdadeiro processo virtual, como aquela do art. 5º, que estabelece a não-obrigatoriedade de os órgãos judiciários disporem de equipamentos receptores. Fundamentalmente, porém, na esteira do pensamento de Wambier, Wambier e Medina[24], é a imprescindibilidade de ser feito o procotolo dos originais no prazo da lei que afasta a efetivação de um autêntico processo virtual fundamentado na Lei Federal nº 9.800/1999.

---

23 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 161.

24 WAMBIER, Luiz Rodrigues; WAMBIER, Teresa Arruda Alvim; MEDINA, José Miguel Garcia. *Breves comentários à nova sistemática processual civil, II:* Leis 11.187/2005, 11.232/2005, 11.276/2006, 11.277/2006 e 11.280/2006, p. 25.

2. O DOCUMENTO ELETRÔNICO

Apesar das referências que fazem a documento, nem o Código Civil nem a respectiva carta processual o definem, razão pela qual tal tarefa ficou a cargo da doutrina[25].

Carnelutti compreendeu documento como "uma coisa representativa de um fato", sendo portanto resultado da atividade do Homem, dado que representativa[26]. Chiovenda, por sua vez, o definiu como: "toda representação material destinada a reproduzir determinada manifestação do pensamento". Já para Pontes de Miranda, documento é "toda coisa em que se expressa por meio de sinais, o pensamento"[27].

Tais entendimentos concebiam o documento como uma "coisa" representada pela da fusão do pensamento e do meio sobre o qual este era registrado[28].

Ocorre que, como preleciona Cabral, na representação eletrônica as informações que constituem o documento não se confundem com a mídia em que estão gravadas[29]. Os documentos eletrônicos não se prendem ao meio em que estão armazenados, e é exatamente isso que os torna surpreendentemente flexíveis. De fato, compreender o documento eletrônico exige um pouco de abstração, como alerta Marcacini[30], que definiu esse tipo de documento como "uma seqüência de *bits* que, traduzida por meio de um determinado programa de computador, seja representativa de um fato"[31].

Bite (ou *bit*, no idioma de origem), acrônimo do inglês *binary digit*[32], é a

25 PARENTONI, Leonardo Netto. *A regulamentação legal do documento eletrônico no Brasil.*
26 LIMA NETO, José Henrique Barbosa Moreira. *Aspectos jurídicos do documento eletrônico.*
27 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 63-64.
28 A idéia de outros autores relacionou-se mais com o escrito que com o produto de sua união a um meio físico, no que aparentemente se aproximam mais das necessidades contemporâneas de conceituação de documento, apesar de limitarem a representação à forma escrita.
29 O autor observa que esta separação entre meio e mensagem é revolucionária para a análise da prova, e demandará cuidados por parte dos processualistas.
30 Em semelhante sentido, por afirmar que "não se pode querer entender o documento digital sob características cartáceas": VOLPI NETO, Angelo. *Ata notarial de documentos eletrônicos*.
31 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 66-67. Apesar dos debates doutrinários, a Medida Provisória nº 2.200/2001 deve imobilizar o conceito do que seria documento eletrônico no Brasil, ao estabelecer que ele será assim considerado se houver a utilização de chaves públicas: ALMEIDA FILHO, José Carlos de Araújo e CASTRO, Aldemario Araujo. *Manual de informática jurídica e direito da informática*, pp. 177-178.

unidade de contagem de um sistema binário, em que os dígitos podem ter o valor zero ou um. É nessa linguagem binária que se baseia o código-fonte dos documentos eletrônicos. Sendo os computadores, rigorosamente, máquinas *de cálculo* muito possantes, é essa arquitetura que permite o processamento de informações por eles[33]. Lembra Cabral que os bites são usualmente agrupados em conjuntos[34] tais como as letras são agrupadas para formar palavras. Havendo uma dada ordem de dígitos para a constituição de um documento eletrônico, reproduzir-se tal ordem implica em cópia perfeita do original, pois inexistem bites falsos[35]. Como eventual adulteração nessa seqüência de dígitos é dificilmente verificável, apesar de ser facilmente possível, imperativo o uso de criptografia de dados para preservá-la.

Não se questiona que os documentos eletrônicos sejam indiretamente representativos[36], por ser necessário recorrer-se a aparelhagem adequada para perceber seu conteúdo. Entrementes, o mesmo se dá em relação a fitas cassete, discos e outros materiais, que curiosamente não têm sua validade e materialidade questionada no direito brasileiro da mesma maneira com que são desafiados os documentos eletrônicos.

Um dos grandes mitos que dizem respeito ao documento eletrônico colocam em dúvida a sua materialidade. Ora, os problemas de espaço nos computadores, nas mídias e a velocidade de transmissão de dados bem revelam que os bites são materiais. Ainda que não sejam tangíveis e possam ser – mediante comando humano, em regra – rapidamente apagados, duplicados ou transmitidos, isso não quer dizer que não existam. Explica Greco que os bites "são entidades magnéticas e, portanto, à sua maneira, realidades materiais, ainda quando não perceptíveis pelos sentidos humanos"[37].

Na seara da segurança documental, muitos vêem a sua representação eletrônica como mais segura que o tão defendido documento tradicional. Se as seqüências de bites requerem cuidados, diferente não é com o papel, que, frágil e único em sentido material, não pode ser exposto à água e agentes biológicos,

32 LUCCA, Newton de. *Títulos e contratos eletrônicos*: o advento da informática e suas conseqüências para a pesquisa jurídica, p. 118.
33 KAMINSKI, Omar e VOLPI, Marlon Marcelo. *A evolução da certificação digital no Brasil*, pp. 249-250.
34 Inicialmente, o padrão adotado era o baite (*byte*), formado por oito bites.
35 CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, pp. 101-102.
36 CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, pp. 120-123.
37 GRECO, Leonardo. *O processo eletrônico*, p. 88.

requerendo ainda, geralmente, o manuseio direto, tornando-o mais vulnerável. O problema é que a memória em que os bites componentes do documento eletrônico são armazenados é geralmente adulterável, daí a importância de meios garantidores da integridade da seqüência, como assinaturas e certificados digitais.

Em que pesem todas as diferenças explicitadas, os documentos eletrônicos não deixam de ser meios reais de representar fatos[38], assim como aqueles tradicionais. Trata-se, inclusive, de núcleo da conceituação de documento informático adotada pelo Decreto nº 513/1997, do Presidente da República Italiana: "representação informática dos atos, fatos e dados juridicamente relevantes"[39].

Para que, conforme o exposto, um documento possa representar também no futuro os fatos que registra hoje, deve ele ter por características a durabilidade e a inalterabilidade. Assim como o papel em sua forma primitiva, o documento eletrônico despido de proteção pode ser alterado não só por atos humanos (estes dolosos ou não, sendo que na primeira hipótese haverá fraude[40]), mas também por fatores externos ou por problemas técnicos[41].

Dentre as alterações possíveis de se fazer em um documento, calha relevar a antedatação. Antedatar um documento é possível tanto no meio tradicional como na representação eletrônica. Para forjar uma data nesta, basta modificar a data do sistema no momento da assinatura. Há meios, porém – como se verá à frente –, para certificar a data no documento eletrônico, evitando essa ardilosa fraude[42]. Além disso, no peticionamento eletrônico, mais especificamente, os documentos emitidos pelo juízo – tais como recibos de protocolo, na forma do art. 160 da carta processual civil –, presumir-se-ão verdadeiramente datados, diante da fé pública do agente emissor.[43]

Outra fraude imaginável seria a reprodução espúria de um documento. De

38 LUCCA, Newton da. *Títulos e contratos eletrônicos*, p. 89.

39 CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, pp. 120-123.

40 Como os programas de computador, de uma maneira ou de outra, processam as informações neles inseridas – ao se digitar uma senha, por exemplo, os dígitos devem ser pelo programa recebidos e interpretados – é possível que algum invasor tenha acesso a essas informações por meio de programas ditos espiões.

41 BLUM, Renato M.S. Opice. *O processo eletrônico*, p. 44.

42 Além da certificação digital feita diretamente sobre o documento atestando a sua data, para provar a existência de um documento eletrônico de uma dada data em diante pode-se pensar na publicação ou no registro do código-fonte impresso das assinaturas digitais correspondentes ou dos "resumos" dos documentos, únicos estatisticamente e portanto com força probatória.

43 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 77.

início, esclareça-se que por original, do latim *originalis*, denota-se, no conceito de De Plácido e Silva, o primeiro, o primitivo, o que vem da origem[44]. Complementa Rêgo que o original, independentemente do número de vias, é uno, consubstanciando-se no instrumento que materializa a vontade humana ensejadora do ato ou negócio jurídico, e tão somente manterá a condição de original no meio em que se aperfeiçoar[45].

Ocorre que, no caso específico do documento eletrônico, a informação reproduzida a qualquer tempo – *no mesmo meio,* sublinhe-se – será igualmente o original, pois o documento é a seqüência de bites, independente do meio em que armazenada. Não há meios para distinguir o original da cópia sem vincular o documento a uma mídia física, o que seria desnaturar esse tipo documental. Poderá haver cópia de um documento eletrônico, no entanto, se for transcrita a sua versão em outro meio, como o papel. O contrário é igualmente verdadeiro. Quanto a estas duas hipóteses, algumas peculiaridades merecem menção: primeiramente, a cópia eletrônica de um documento físico, se for assinada digitalmente, deve ser compreendida como certidão, pois em via de representação distinta do original; a cópia impressa de uma seqüência de bites, por outro lado, deverá conter apenas a imagem gráfica visualizável desse documento, sem o código da assinatura digital, uma vez que a conferência desta só é possível em confronto com os bites do documento armazenado digitalmente[46].

Por derradeiro, em sentido indicativo da receptividade dos documentos eletrônicos, note-se que as informações disponibilizadas na Grande Rede pelo Poder Judiciário merecem confiança, conforme já decidiu o Superior Tribunal de Justiça[47]:

> PROCESSUAL – PRAZO – JUSTA CAUSA – INFORMAÇÕES PRESTADAS VIA INTERNET – ERRO – JUSTA CAUSA – DEVOLUÇÃO DE PRAZO – CPC, ART. 182.
> - Informações prestadas pela rede de computadores operada pelo Poder Judiciário são oficiais e merecem confiança. Bem por isso, eventual erro nelas cometido constitui "evento imprevisto, alheio à

44 RÊGO, Paulo Roberto de Carvalho. *O Registro de Títulos e Documentos:* um instrumento jurídico para segurança da sociedade.
45 RÊGO, Paulo Roberto de Carvalho. *O Registro de Títulos e Documentos:* um instrumento jurídico para segurança da sociedade.
46 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 68-70.
47 LIMA, George Marmelstein. *e-Processo:* uma verdadeira revolução procedimental.

> vontade da parte e que a impediu de praticar o ato.". Reputa-se, assim, justa causa (CPC, Art. 183, § 1º), fazendo com que o juiz permita a prática do ato, no prazo que assinar. (Art. 183, § 2º).
> (STJ, REsp 390561/PR, Rel. Ministro HUMBERTO GOMES DE BARROS, PRIMEIRA TURMA, julgado em 18.06.2002, DJ 26.08.2002 p. 175)

> RECURSO ESPECIAL. Divergência. Precedente do STJ. Diário da Justiça. Site na internet.
> Indicado como paradigma acórdão do próprio STJ, com referência ao Diário da Justiça da União, órgão de publicação oficial, e com a reprodução do inteiro teor divulgado na página que o STJ mantém na Internet, tem-se por formalmente satisfeita a exigência de indicação da fonte do acórdão que serve para caracterizar o dissídio. (...)
> (STJ, REsp 327687/SP, Rel. Ministro RUY ROSADO DE AGUIAR, QUARTA TURMA, julgado em 21.02.2002, DJ 15.04.2002 p. 225)

Também prestigiou as informações fornecidas no ambiente virtual o Tribunal de Justiça de São Paulo[48], como se vê a seguir:

> INVENTÁRIO – Certidão negativa quanto à dívida ativa da União, obtida por meio da Internet. Não aceitação, com ordem de juntada de outra, fornecida pela Secretaria da Receita Federal. Portaria da Procuradoria-Geral da Fazenda Nacional que concede a esse documento os mesmos efeitos da certidão negativa comum. Aplicação do disposto na Lei Federal nº 9.800/1999. Recurso a que se dá provimento
> (TJSP, 1ª Câmara de Direito Privado, Agravo nº 139.645-4, Rel. Luís de Macedo, j. em 16.11.1999)

48 BLUM, Renato M.S. Opice. *O processo eletrônico:* assinaturas, provas, documentos e instrumentos digitais, p. 61.

3. POSSIBILIDADES DESVENDADAS PELA CRIPTOGRAFIA

Para que qualquer instrumento processual tenha validade jurídica, suas autenticidade e integridade são requisitos fundamentais. Uma análise viável e segura dessas condições em meio eletrônico, diante da vulnerabilidade desse ambiente, só poderá ocorrer mediante fortes garantias de proteção dos dados envolvidos. É aí que entra em cena a criptografia.

A criptografia é uma técnica de embaralhamento de mensagens. Ensina Cabral que se a palavra advém do grego “escrita oculta”, identificando-se com a arte de escrever em código de modo a tornar a mensagem legível apenas ao seu destinatário autorizado[49].

Em que pese o grande desenvolvimento da técnica nos últimos anos, suas origens remontam a longínquo passado: já em 1510 Johannes Trithemius, considerado “pai da criptografia moderna”, publicara seu “Poligrafia”, primeiro livro a abordar essa arte que, como contraponto, tem a criptoanálise, dedicada a decifrar seus códigos[50].

A evolução da criptografia foi notável na Segunda Guerra Mundial, em que foram aplicadas máquinas capazes de criptografar um número até então impensável de mensagens[51]. Essa veia militar da criptografia é responsável por muitas das restrições que sua aplicação enfrenta hoje em dia. O receio de muitos em relação ao livre acesso a essas técnicas de codificação de mensagens reside no possível uso destas por criminosos, que teriam o sigilo de suas comunicações garantido. Em razão disso, até o ano 2000 os Estados Unidos da América impunham severas proibições à exportação de produtos de criptografia. Na França, as regras rígidas de antes alcançavam o próprio uso interno da técnica, e na Federação Russa, já em 1995, criptografia não autorizada foi proibida[52].

Se as máquinas de meados do século vinte trouxeram grande avanço à criptografia, o que dizer dos computadores da atualidade: tanto a criptografia como a

---

49 CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 108-109.

50 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 9-11.

51 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 9-11.

52 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 13-14.

criptoanálise tiveram suas aplicações possibilitadas de maneira exponencialmente maior. Há de se destacar que foi igualmente a informática a responsável por aproximar a criptografia do cidadão comum, de maneira transparente mas presente desde transações bancárias até o decodificador necessário à recepção do sinal de televisão paga[53].

Na história da criptografia moderna, um programa de computador foi de grande destaque: o PGP, ou "Pretty Good Privacy" (privacidade satisfatória, em tradução livre), criado por Phillip Zimmermann. O autor do programa, pretendendo a massificação da criptografia e também protestar em favor das liberdades civis ameaçadas por projetos governamentais de restrição de acesso à criptografia, divulgou gratuitamente, em 1991, o código-fonte do PGP pela internet. As investigações a que Zimmermann foi submetido – mais tarde arquivadas – não impediram que, em pouco tempo, o PGP fosse visto como padrão de criptografia no mundo virtual. Curiosamente, para lançar ao mundo a versão posteriormente elaborada do programa, feita para o ambiente Windows, Zimmermann reproduziu o código-fonte do PGP em doze livros que, com base em autorização judicial fundamentada na liberdade de expressão, conseguiu exportar[54].

O uso da criptografia pelo cidadão veio para ficar. A uma, porque se seu uso for proibido a fiscalização será inviável, diante da dificuldade extrema em se comprovar que um emaranhado de números no arquivo de alguém constitui um documento cifrado. A duas, já alertava o criador do PGP, Phillip Zimmermann, que a proibição da criptografia limitá-la-ia aos fora-da-lei[55]. E a três, finalmente, porque vetar o uso de tão fundamental meio de proteção de conteúdos enviados eletronicamente obstaria o desenvolvimento das transações eletrônicas, de tanta importância na atualidade.

A relevância da criptografia se destaca ao se compreender que os registros eletrônicos não protegidos – incluindo-se aí as mensagens de correio eletrônico – são adulteráveis de modo a não deixar vestígios, ainda que o programa incumbido de seu tratamento não forneça essa opção, pois há programas específicos para

53 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 12-13.
54 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 15-18.
55 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 127.

tanto. Dentre outras falhas de segurança, anote-se que certos servidores de correio eletrônico enviam mensagens sem confirmar a autenticidade do remetente sequer por meio de senha.

Violáveis são também os sistemas que cuidam das senhas de acesso. Os operadores do sistema – ou quem indevidamente venha a fazer as suas vezes – a elas poderão ter acesso, eis que ficam cadastradas. Portanto, não se fala em prova confiável nesse caso, uma vez que a senha pode ser do conhecimento de outras pessoas que não o titular[56].

No que se refere ao uso da criptografia para facilitar o trabalho de criminosos, igual destino pode se dar a tantas outras práticas legais – andar de automóvel, por exemplo. A irrazoabilidade de proibi-las decorre das inúmeras vantagens obtidas com sua aplicação. Além disso, ainda que fosse possível interceptar uma comunicação criptografada, os mais modernos meios afastam a possibilidade de ela poder ser decifrada por terceiros. A essa realidade os investigadores deverão se conformar, buscando outros meios de prova do cometimento de delitos[57].

Marcacini diz que a importância da criptografia é tão grande no mundo contemporâneo, com o necessário tráfego intenso de informações – que no entanto trafegam por meio vulnerável –, que poder-se-ia falar em um *direito à criptografia*, tendente a proteger garantias individuais[58].

Cabral lembra que a necessidade de se proteger uma informação tem relação direta com o risco de sua interceptação[59]. Nessa linha, o trânsito de documentos pela internet, para ter valor jurídico, deve se valer da mais potente criptografia disponível.

Um dos tipos de criptografia é a chamada simétrica, conhecida também por criptografia de chave privada. Nela, a chave (número também chamado de senha) que codifica a mensagem tem uma correspondente inversa que a descodifica. Ilustrativamente, há os exemplos clássicos de codificação de mensagens, recuando

56 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 109-111.
57 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 130.
58 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 151-152.
59 CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 110.

ou avançando um determinado número de letras no alfabeto. Veja-se: avançando uma letra no alfabeto (chave com valor 1), a mensagem “recuar tropas” se transformaria em “sfdvbs uspqbt”. Para se decodificar a mensagem, ao invés de avançar uma letra (+1), deverá o leitor *recuar* (-1) um algarismo.

Marcacini ensina que esse método é também chamado de criptografia de chave privada, uma vez que o destinatário da mensagem deverá ter conhecimento da chave utilizada para embaralhar a mensagem. Mas não é só: também o algoritmo, isto é, o critério utilizado para codificar o conteúdo (em outras palavras, a fórmula cuja incógnita é a chave privada – no exemplo dado, [+x] para codificar e [-x] para decodificar) deverá ser do conhecimento do receptor. Não é um sistema inútil hoje em dia, apesar de sua vulnerabilidade ser expressiva, o que não lhe confere muito crédito. Sério inconveniente do sistema é que, de alguma maneira, remetente e destinatário deverão convencionar o algoritmo e a chave utilizados na codificação, o que nem sempre é possível de modo seguro. Por isso, a utilidade maior que se vislumbra é no caso de uma pessoa querer ocultar suas próprias informações, hipótese em que ela deverá memorizar as funções utilizadas na encriptação[60].

A criptografia simétrica não pode ser utilizada visando a efeitos jurídicos, porque é impossível demonstrar a terceiros que um determinado documento advém do remetente nela indicado. Explica-se: se a chave de codificação deve ser do conhecimento do remetente e do destinatário, este pode ter, ele próprio, codificado a mensagem. Além disso, inviabiliza-se a comunicação com mais de uma pessoa, já que todas – cujos interesses podem não ser comuns – deverão ter acesso à chave[61].

Para suplantar esses inconvenientes, viria a criptografia assimétrica, também conhecida como criptografia de chave pública, proposta em 1976 por Whitfield Diffie e Martin Hellman. Embora os passos iniciais desse tipo de criptografia datem de 1976, seu conhecimento geral é muito mais recente. Talvez por isso tanto se imagine que não há como atribuir segurança a documentos eletrônicos[62].

---

60 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 18-21.

61 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 23-25.

62 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 80-81 e 90-91.

Na criptografia assimétrica, o algoritmo calcula duas chaves – combinações de dígitos geradas aleatoriamente – relacionadas de maneira matemática: uma pública e outra privada. Ambas[63] são distintas e servem para codificar e decodificar mensagens. Uma decifra o conteúdo protegido pela outra, porém são independentes e relacionam-se matematicamente de modo que é inviável descobrir-se uma delas com base unicamente na outra.

A chave privada deve ser guardada pelo titular com máximo cuidado e sigilo, enquanto que a pública deve ser divulgada publicamente por meio da grande rede.

Para que não seja viável descobrir-se uma chave privada a partir do conhecimento da correspondente chave pública, ou vice-versa, a criptografia assimétrica se vale de funções matemáticas sem retorno, sem operação inversa. Por isso, não há como dar exemplos ilustrativos como os de criptografia simétrica simples, em que substituir letras por seus pares, avançando ou recuando no alfabeto, é uma possibilidade. Mas essa complexidade, complementa Marcacini, não afasta a criptografia moderna da população, do usuário leigo: todas essas operações são feitas de maneira transparente pelos programas de computador da atualidade, não se exigindo do usuário mais do que alguns cliques. Em verdade, há várias aplicações de criptografia assimétrica já em uso sem que o usuário sequer delas tome conhecimento, como as operações bancárias via internet ou de comércio eletrônico. Nesses casos, porém, a codificação serve somente para evitar a interceptação dos dados[64].

O sistema funciona da seguinte maneira, como preleciona Cabral[65]: um documento assinado com uma chave privada não poderá ser decifrado com essa mesma chave – apenas a correspondente chave pública estará apta a fazê-lo. O inverso é igualmente verdadeiro. Assim, de posse da chave pública de uma pessoa, amplamente disponível, qualquer um pode verificar se um dado documento foi de fato assinado por ela. Caso a chave pública fornecida decodifique a mensagem, isto quer dizer que o conteúdo fora codificado com a correspondente chave privada – de conhecimento exclusivo do titular. Restará, portanto, garantida a autenticidade da assinatura. Da mesma maneira, se não se desejar o acesso de um terceiro que não

63 Tais chaves não são de livre escolha do usuário, apesar de serem gerados por comando dele.
64 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 26-31.
65 CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 110.

o destinatário ao documento, basta codificá-lo com a chave pública deste. Assim, somente o possuidor da chave privada – o destinatário – será capaz de ler a mensagem. Este terá a chave pública do remetente – disponível publicamente – para verificar se a assinatura advém mesmo de quem alega tê-la produzido; outrossim, com base na sua chave privada – cujo conhecimento só ele detém – poderá decifrar o conteúdo a ele dirigido.

É possível assinar documentos apenas com a chave privada do subscritor ou somente com a chave pública do destinatário. No entanto, no primeiro caso qualquer pessoa poderia ler o conteúdo do documento, apesar de provada sua origem; já no segundo, apesar de garantidos o sigilo e a integridade do conteúdo, não haveria segurança quanto à identidade do remetente. Assim, o ideal é que o assinante aplique duas chaves ao documento: a sua chave privada e a chave pública do destinatário.

Destaque-se que o algoritmo[66] criptográfico – isto é, as operações que o programa realiza com base na chave[67] – não deve necessariamente ser sigiloso. Ao contrário, quanto maior for a publicidade de seus cálculos, maior será sua credibilidade[68]. O que determinará a segurança da criptografia é, sim, a consistência da chave[69], que maior será na medida em que haja mais combinações possíveis para ela. Isso se consegue aumentando-se o seu número de bites, isto é, a quantidade de dígitos que compõem a chave[70].

No que se refere à segurança da criptografia de chave pública, entusiasma-se Marcacini afirmando que “por mais fantástico que possa parecer, não há, hoje, poder computacional instalado sobre a Terra que seja suficiente para decifrar este

66 Também chamado de fórmula.

67 O que se altera nas operações de codificação é apenas a chave, já que o algoritmo é sempre igual: MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 25.

68 Comumente, imagina-se que a criptografia tem a ver com códigos escondidos. De fato, a chave privada e o conteúdo da mensagem são coisas a se ocultar, mas não os mecanismos criptográficos. Tanto o algoritmo como o programa de computador que com ele trabalhará, para serem considerados seguros, devem ter todos os seus cálculos e meios de segurança conhecidos. A confidencialidade do cifrado deve ser posta à prova, devendo permanecer inviolável àqueles que não possuam a chave, mesmo com todas as investidas da comunidade científica: MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 41-43.

69 A chave é produzida com base no algoritmo.

70 CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 111.

código".[71]

Neste tocante cumpre averbar que, apesar de toda a segurança proporcionada pela criptografia, as senhas comuns não deixarão de fazer parte do cotidiano do profissional do direito. Esses códigos relativamente simples servirão para reforçar os elos da corrente elaborada pela criptografia, dificultando o acesso às chaves e documentos no computador do usuário. Cabral[72] menciona como alternativa às senhas a biometria, ciência que permite a identificação de pessoas com base em seu corpo, já implantada no Brasil em atividades cotidianas, em locais como clubes e academias de ginástica. As partes do corpo mais analisadas seriam a impressão digital, os olhos, a face e a voz – neste caso, destaca o autor que há sistemas destinados a testar a espontaneidade do usuário ao responder a perguntas de cunho pessoal. Apesar da elevada confiabilidade das técnicas de biometria na identificação de pessoas, há respeitáveis críticas no que se refere à sua implementação[73].

Para que a técnica criptográfica seja o caminho para uma segurança efetiva – pois apesar de não ser absolutamente inviolável, como todos os outros sistemas conhecidos, tem notável eficácia aliada a muitas outras vantagens – deve o usuário se valer de criptografia forte, com algoritmos consistentes e chaves de tamanhos grandes o suficiente[74]. A razão para que sejam necessárias chaves com muitos números é que, em tese, é possível obter a chave privada a partir da chave pública. Marcacini anota que o algoritmo RSA, por exemplo, é fundado na multiplicação de dois números primos elevados, cujo produto seja um número de muitos dígitos. Fatorar um número extenso, isto é, encontrar os números primos que multiplicados nele resultam, é razoavelmente impossível com o atual estágio da tecnologia. Por isso, chaves de 1024 bites são tidas como seguras[75].

71 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 30.

72 CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 115.

73 Uma das críticas direcionadas à biometria é que de uma maneira ou de outra os dados do indivíduo são convertidos em bites para armazenamento, o que possibilita fraudes. Ainda, há sempre a questão de crimes contra a liberdade, em que a utilização de um pedaço do corpo seria o objetivo primordial dos criminosos, com todo tipo de conseqüência trágica que pode disso resultar. Afinal de contas, ao se lidar com biometria não se pode, por exemplo, negar o fornecimento de impressões digitais mediante coação, enquanto que negar a posse de chaves criptográficas e as senhas correspondentes é muito mais plausível.

74 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 40.

75 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 46.

Confrontando aqueles que, para questionar o sistema criptográfico, apegam-se a uma remota possibilidade de a chave ser quebrada (como se não fosse possível falsificar um documento em papel), tem-se a lúcida lição de Marcacini:

> Além da impossibilidade técnica, para o estágio atual de desenvolvimento, é razoável mencionar também o argumento da impossibilidade econômica. Ainda que "apenas" uns cinco mil computadores pudessem quebrar uma senha no espaço de, digamos, um ano, que segredo ou assinatura valeriam tanto quanto o uso econômico de tal potencial de processamento? Ou, se forem tão valiosos, não haveria meio mais barato de obtê-los?[76]

Logicamente, as chaves que hoje são tidas como seguras poderão não o ser amanhã, com o avanço dos computadores e com progressos nas ciências matemáticas que facilitem o rompimento das chaves. No entanto, um computador que suplante os processadores de hoje, decifrando a chave por eles gerada, será capaz de produzir códigos criptográficos assimétricos muito mais complexos, os quais ele já não será possante o suficiente para depurar.

Por certo, como conseqüência dessa evolução tecnológica pode ser necessária a reassinatura periódica de documentos a serem arquivados por longo tempo. Nesse sentido, bem alerta Marcacini que, no ambiente jurídico, a criptografia é uma "via de mão dupla": enquanto serve à segurança de documentos eletrônicos, viabilizando o uso de assinaturas digitais e protegendo a integridade e o sigilo desses documentos, cria problemas jurídicos outros[77].

A boa notícia é que podem surgir sistemas criptográficos ainda mais eficientes que a criptografia assimétrica, sem necessariamente inutilizar as capacidades desta. Lima refere que possivelmente caberá à criptografia quântica esse papel[78]. Por outro lado, citando Simon Sign, questiona o autor a possibilidade de órgãos governamentais de países desenvolvidos já terem logrado a decodificação dos sistemas assimétricos de criptografia, ocultando essa informação.

Desconsiderando essa hipótese, a melhor tática para terceiros contornarem o sistema criptográfico, dada a sua segurança, seria a apropriação da chave privada

76 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 47-48.
77 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 6-7.
78 LIMA, George Marmelstein. *e-Processo:* uma verdadeira revolução procedimental.

de posse do titular.

Por isso, a chave privada – que não deverá ser armazenada no computador do usuário, realce-se[79] – também deve ser protegida por meios criptográficos, de modo que, ainda que alguém tenha acesso ao arquivo da chave, só seja ela acessível a partir da digitação de uma complexa senha. A preocupação com o cuidado da chave privada faz todo sentido, uma vez que qualquer um que dela se aposse enquanto válida poderá assinar documentos como se o titular da chave fosse. Nas palavras de Marcacini, a responsabilidade por esse cuidado é toda do usuário, que é "o único guardião da chave privada. A ninguém mais compete protegê-la e mantê-la distante de pessoas mal-intencionadas"[80]. Prosseguindo, comenta Marcacini:

> (...) ninguém mais tem acesso à sua chave privada, e só esse fato já permite perceber que a criptografia de chave pública chega a ser mais segura do que o mais desenvolvido dos sistemas, em que, em algum lugar, por mais protegida que esteja, a senha do usuário está cadastrada. A desvantagem é que não teremos a quem culpar, pela eventual negligência em manter a chave privada segura, já que a apropriação indevida dessa chave pode ser considerada o maior risco que afeta a segurança do sistema.[81]

Já as chaves públicas, por outro lado, contêm dados individualizadores do usuário e são identificadas por uma numeração conhecida por "impressão digital". Essa referência se dá por ser esse número estatisticamente único, o que permite a associação de uma pessoa à sua chave. Levando-se em conta que para o documento ter força probante a autenticidade da chave deve ser demonstrável a terceiros, a relação de confiança quanto à titularidade de uma chave pode vir a se basear na publicação das "impressões digitais" de chaves públicas. Caso a aptidão

79 "...quando apagamos um arquivo do disco rígido, ele é apagado apenas logicamente, não fisicamente. Ou seja, é como se o computador apenas "esquecesse" que o arquivo apagado está lá, de modo a não mais mostrá-lo no diretório e a permitir que outros arquivos sejam gravados no espaço que ele ocupa. Mas, fisicamente, a informação continua ali, e assim permanecerá até que outro arquivo venha a ser gravado "por cima". Existem programas de computador que podem recuperar estes arquivos "apagados", o que nos leva à conclusão de que apagar um arquivo logicamente não é algo suficientemente seguro. Por outro lado, há programas que apagam fisicamente os arquivos...": MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 50.

80 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 51.

81 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 115.

probatória não seja necessária, mera confirmação junto à parte transacionante se mostra razoável. O método mais evidente para o estabelecimento da aludida confiança, como se verá, é porém a certificação digital[82].

A criptografia lastreada no sistema de chaves públicas permite a aludida segurança jurídica da comunicação, conferindo a documentos assinados digitalmente aptidão probatória perante terceiros, uma vez que garante a autenticidade e impede a adulteração e a leitura não autorizadas do arquivo, o que poderia acontecer facilmente com um conteúdo desprotegido[83].

Como mostra da segurança desse sistema, há notícia de que a tecnologia das chaves públicas tem servido ao pagamento de contas pelo governo em movimentações que se aproximam de quatrocentos bilhões de reais[84].

No que se refere aos pontos fracos do sistema criptográfico de chave pública, de outra parte, Marcacini menciona a possibilidade de terceiros se apropriarem indevidamente de chave privada e a problemática da autenticidade da chave pública"[85].

O roubo da chave privada, aqui entendido como a aplicação de coação física para obtê-la (assim como outros códigos necessários ao seu pleno uso) é semelhante ao encontrado no mundo dos documentos tradicionais, em que alguém pode ser forçado a assinar um documento manualmente. No caso, igualmente a solução será demonstrar o uso indevido da chave por outros meios de prova. Poderão, outrossim, ser utilizados métodos de segurança que permitam a revogação instantânea de um par de chaves pelo usuário.

Já a questão da autenticidade da chave pública é enfrentada pelos certificados digitais, tema adiante abordado.

---

82 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 55.

83 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 117.

84 FIGUEIREDO, José Antônio *apud* ZONZIN, Janaína. *Identidade do futuro.*

85 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 91-92.

4. ASSINATURAS DIGITAIS

Em toda a história da humanidade, mesmo nos já tão conhecidos papéis e pessoas, conferiu-se à questão da autenticidade papel de relevo, dadas as dúvidas que sempre acompanharam a questão[86]. Como os atos e documentos geram responsabilidades, é certo que deve haver essa preocupação.

Segundo o dicionário de De Plácido e Silva, a autenticidade, oriunda do latim *authenticus* – que expressa autoridade, validade e aprovação – indica que o documento ou ato é verdadeiro, exato e conforme a lei[87]. Aguiar Dias, por sua vez, considera autêntico documento "que faz autoridade de prova ou de solenidade, por expressar, só por si, a observância das formalidades a que estava sujeito. A autoridade é a qualidade do documento autêntico"[88].

Ressalte-se adicionalmente o entendimento de Moacyr Amaral Santos, para quem autenticidade é "a certeza de que o documento provém do autor nele indicado". Autor, por sua vez, seria aquela pessoa a quem se atribui a paternidade do documento[89].

Quanto ao documento tradicional, a tarefa de atribuir-lhe segurança jurídica foi assumida pela assinatura de próprio punho, acompanhada de selos, carimbos e papéis especiais. Na lição de Carnelutti, a função dessa manifestação manuscrita é essencialmente a de indicar, declarar e provar[90]. Não em sentido diverso fluem os termos do art. 368 do Código de Processo Civil, segundo os quais a autoria em regra se comprova pela assinatura do autor.

Cabe indagar, então, sobre a natureza da assinatura digital, que pretende garantir a autoria e a integridade de um documento constituído por uma seqüência de bites, ao qual a assinatura tradicional não pode ser aposta.

A propósito, desde 1995 já há leis em âmbito mundial tratando do tema. No Estado norte-americano de Utah, entrou em vigor naquele ano a primeira lei a regulamentar o uso de assinaturas eletrônicas. Nos dias atuais, em quase todos os

86 BLUM, Renato M.S. Opice. *O processo eletrônico*, p. 43.
87 RÊGO, Paulo Roberto de Carvalho. *O Registro de Títulos e Documentos:* um instrumento jurídico para segurança da sociedade.
88 AGUIAR DIAS, José de *apud* RÊGO, Paulo Roberto de Carvalho. *O Registro de Títulos e Documentos:* um instrumento jurídico para segurança da sociedade.
89 AMARAL SANTOS, Moacyr *apud* MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 70-71 e 75-76.
90 BLUM, Renato M.S. Opice. *O processo eletrônico*, p. 47.

Estados Unidos há lei ou projeto de lei tratando do assunto, que viria a ser abordado na Europa em 1997, pioneiramente na Alemanha e posteriormente na Itália[91].

Historicamente, a primeira menção legislativa às assinaturas digitais no Brasil data de 1996, como sinaliza Marcacini:

> No Brasil, a primeira disposição a tratar do tema foi a Instrução Normativa nº 17, de 11 de dezembro de 1996, editada pelo Ministério da Administração Federal e Reforma do Estado, que determinou que "*no prazo de 360 (trezentos e sessenta) dias serão implementadas aplicações que tratem da utilização de documentos eletrônicos e do uso de assinatura digital"* (art. 4º, § 6º) no âmbito das atividades governamentais. Apenas após quase quatro anos viria a ser baixado regulamento mais específico sobre o tema, o Decreto nº 3.587, de 5 de setembro de 2000, que institui a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal (ICP-Gov). Referido Decreto estabelece normas básicas para a implantação do uso de criptografia de chave pública pela Administração Pública Federal, com o intuito de conferir segurança às comunicações eletrônicas entre os entes administrativos, prevendo ainda uma futura e progressiva substituição dos documentos físicos por meios eletrônicos.[92]

Inicialmente, explique-se, por cautela, que a assinatura digital não remete à figura de uma imagem transportada para o computador da assinatura autógrafa convencional, também chamada de assinatura digitalizada. Tal procedimento não ofereceria segurança alguma, permitindo que qualquer um copiasse e reproduzisse o gráfico correspondente. E, apesar da utilidade de senhas de acesso para proteção da assinatura digital, esta não se confunde com aquelas.

A assinatura digital seria, para Cabral, "um código que identifica o remetente e pode ser anexado a uma mensagem transmitida eletronicamente"[93].

Já Marcacini compreende a assinatura digital como "o resultado de uma complexa operação matemática, que utiliza uma função digestora e um algoritmo de criptografia assimétrica, e tem, como variáveis, a mensagem a ser assinada e a chave privada do usuário (ambas vistas pelo computador como *números*)"[94].

---

91 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 59-60 e LUCCA, Newton da. *Títulos e contratos eletrônicos*, p. 91.

92 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 61-62.

93 CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, pp. 113 e 124.

94 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 37.

A assinatura digital obtida por meios criptográficos difere substancialmente daquela tradicional – manuscrita em papel – sob variados aspectos. De início, consigne-se que o que determina a autenticidade de uma assinatura feita à mão é exatamente a similitude dela com o padrão do assinante, que se repete em todas as vezes nas quais sua marca pessoal é reproduzida. A assinatura digital, diferentemente, é única para cada documento, não podendo ser reconhecida por comparação com aquela aposta em outro arquivo ou com um padrão arquivado.

A razão para que a assinatura digital de uma dada pessoa seja única para cada documento é que este é uma variável da fórmula. Trata-se, como preleciona Marcacini, de uma relação lógico-matemática entre a assinatura e o documento, ao passo que a ligação de uma assinatura autógrafa é física, pois deverá constar da mesma folha de papel documental[95].

Brasil enumera outros diferenciais da assinatura eletrônica em relação ao conceito tradicional de firma. Em primeiro lugar, enquanto a assinatura manuscrita é pessoal, indelevelmente relacionada a manifestações corpóreas do indivíduo – podendo ser periciada grafologicamente –, a similar digital é um sinal fornecido por outrem consistente em um conjunto de algarismos ininteligível. Além disso, a firma digital é em tese transferível, uma vez que, não acompanhando o corpo do titular, poderia ser hipoteticamente cedida[96].

Apesar das citadas diferenças, a expressão “assinatura” contida no art. 371 da carta processual civil não afasta a sua representação digital, na opinião de Marcacini. E a razão para tanto é que a assinatura eletrônica cumpriria as mesmas funções daquela convencional, permitindo a identificação da autoria de um documento com elevada probabilidade de certeza, sendo igualmente um sinal distintivo, único e exclusivo de uma dada pessoa. Assim, ampliar o conceito de assinatura para além de traços personalizados feitos de próprio punho não afrontaria as tradições jurídicas, tampouco a língua portuguesa[97].

Sabendo-se o que é uma assinatura digital, resta analisar-se de que maneira ela se vale da criptografia assimétrica para ser produzida. Nessa linha, é didática a

95 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 38.
96 BRASIL, Angela Bittencourt. *Assinatura digital não é assinatura formal.*
97 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 83-84.

explicação de Marcacini:

> (...) a assinatura digital é produzida cifrando a mensagem com a (...) chave *privada*, o que só poderá ser decifrado com a chave pública. Ou seja, se for possível decifrar a mensagem com o uso da chave *pública*, é sinal de que ela só pode ter sido codificada com a chave *privada* correspondente e, portanto, somente aquele que detém esta chave *privada* poderia tê-lo feito. Note-se, com isso, que a "conferência" da assinatura é tarefa que qualquer um pode realizar, dado que a chave *pública*, como diz o seu nome, pode e deve ser amplamente divulgada e distribuída.[98]

Para evitar a necessidade de codificar a mensagem por inteiro, o que demandaria elevado trabalho de processamento e resultaria em arquivos demasiado grandes, a assinatura digital não é produzida sobre a mensagem, mas sim sobre um resumo dela[99], obtido através da aplicação de uma função digestora[100] sobre seu conteúdo. Essa função se fundamenta em operações matemáticas sem retorno, do mesmo modo como as operações que resultam em dígitos verificadores quaisquer. Isso quer dizer que com base unicamente nesse resumo não é possível desvendar o conteúdo do documento, ou mesmo ajustar um resumo a um documento diferente daquele que o originou. Tome-se por exemplo um determinado número de CPF. Se qualquer dos nove algarismos desse cadastro for modificado, os dígitos verificadores acusarão a irregularidade. Por outro lado, apenas com base nos dígitos controladores, não é possível descobrir-se os nove números principais. A função digestora trabalha de maneira semelhante, com a diferença de se valer de códigos incomparavelmente maiores, a ponto de o resumo de uma determinada mensagem ser estatisticamente único[101]. É como se os dígitos verificadores do CPF fossem exclusivos a ponto de permitirem, por si sós, a identificação da pessoa[102]. Qualquer alteração no documento assinado, por mínima que seja (como a inserção de um espaço adicional entre palavras) modifica totalmente o resultado do resumo. Conclui-se, portanto, que é suficientemente segura a aplicação da chave privada do

98 MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 33-34.

99 A doutrina se refere também à correspondência em inglês – *message digest* ou *hash* criptográfico.

100 O inglês *hash function* é termo igualmente corrente para designar essa função.

101 Em razão disso, Marcacini afirma que a existência desse resumo demonstra a existência da mensagem.

102 De modo semelhante a uma impressão digital, como acusa Rezende: REZENDE, Pedro Antônio Dourado de. *Sistema de Pagamento Brasileiro e ICP – Brasil.*

subscritor tão somente sobre esse resumo.[103]

Na conferência da assinatura, o computador calcula o resumo da mensagem recebida e o compara ao contido de modo codificado na assinatura, verificando assim a integridade do documento enviado, isto é, se o conteúdo do documento assinado é o mesmo daquele recebido. Se ele houver sido interceptado e modificado, os resumos diferirão. Noutra ponta, sendo o documento decifrável com a chave pública do suposto subscritor, somente a chave privada deste pode ter sido aplicada na geração da assinatura, pelo que se confirma a autenticidade do documento[104].

A assinatura digital poderá ser integrada ao documento – que continuará igualmente legível – ou salva como um arquivo em separado, vinculado inexoravelmente, porém, ao conteúdo do documento quando da elaboração da assinatura. Múltiplas assinaturas diversas são possíveis, tanto em um caso como no outro. E, sempre, alterando-se o conteúdo do documento, a firma é invalidada.

Ademais, como todo arquivo digital pode receber uma assinatura eletrônica, vislumbra-se a possibilidade – anteriormente inexistente – de se assinar vídeos e sons. Ao invés de assinar a transcrição do depoimento prestado em audiência, assina-se digitalmente o próprio arquivo contendo o desenrolar desta em áudio e vídeo.

Contra a assinatura digital, pesam a falta de penetração na consciência coletiva de que o método é seguro, assim como a possibilidade de que a certificação em outros países não seja merecedora de confiança, o que deverá se repercutir no comércio internacional ainda por algum tempo com a confirmação dos negócios por meios tradicionais[105].

Outro ponto de disparidade em relação à rubrica autógrafa a se sublinhar é a noção de falsificação de assinatura digital. O tema é abordado por Marcacini, com a ressalva de que os procedimentos sejam fundamentados em criptografia forte e confiável:

103MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 33-34.

104MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 36.

105GRECO, Leonardo. *O processo eletrônico*, p. 89.

> (...) quanto a um documento assinado eletronicamente pelo uso de criptografia assimétrica, a argüição de falsidade só poderá ser baseada em "*falsidade de assinatura*". (...) Dentro deste prisma, é de se dizer que o documento eletrônico assim assinado é dotado de um maior grau de confiabilidade que o próprio documento tradicional. Modificado um único *bit*, o próprio *software* de criptografia, ao conferir a assinatura, acusará que o documento adulterado não corresponde a ela. Já o documento cartáceo necessita de um exame pericial para constatar-se eventual alteração; e, com o evoluir da técnica, certamente surgem meios mais e mais poderosos para alterar documentos físicos.
> Por *"falsificação da assinatura digital"*, por sua vez, deve ser entendida a criação de um par de chaves falso, atribuído ao suposto signatário. A verdadeira assinatura digital, legitimamente gerada pelo seu titular, não tem como ser falseada. No fundo, inexiste falsidade a ser apurada no próprio documento eletrônico; o problema em análise se resume exclusivamente na verificação da autenticidade da chave pública.[106]

Ao se pensar em falsidade, pensa-se também em segurança, do mesmo modo como sempre foram enfrentadas as assinaturas tradicionais. Um problema novo que pode ocorrer em uma infra-estrutura de chaves públicas é a possibilidade – aparentemente, a fraude mais perigosa – de violação do sigilo de uma chave privada, com a sua conseqüente utilização para assinar documentos indevidamente. O titular da chave, por continuar tendo acesso a ela, dificilmente saberá se algum terceiro dela se apropriou antes de ser comunicado sobre fraude perpetrada em seu nome.

Visando a aumentar a proteção do sistema digital, Kaminski e Volpi recomendam procedimento para dificultar ao máximo fraudes em assinaturas digitais. Baseia-se na conjunção de três preceitos, quais seriam, o "ter", o "ser" e o "saber". O primeiro diria respeito a algum elemento portátil pelo usuário, como um cartão magnético contendo a chave privada. O "ser", por sua vez, referir-se-ia a características do corpo do assinante, como a leitura da íris dos olhos, enquanto que o último seria um conhecimento exclusivo do usuário, como uma senha. Quanto mais elementos destes presentes, maior será a probabilidade de ser autêntica a expressão de vontade[107].

Como exemplo desse procedimento, fala-se na utilização de um cartão

106MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 95.
107KAMINSKI, Omar e VOLPI, Marlon Marcelo. *A evolução da certificação digital no Brasil*, p. 250.

eletrônico conhecido por *smart card* para a elaboração de assinaturas digitais. Um leitor apropriado, conectado ao computador, faria a leitura as informações contidas no cartão e então o usuário estaria apto a assinar documentos digitalmente. O uso de senhas e de técnicas de biometria – como a leitura da impressão digital – para validar o uso do cartão[108] seriam medidas de segurança adicionais[109].

Por fim, outro aspecto de relevância diz respeito às atribuições dos notários e registradores. Entende Brasil que o reconhecimento de firmas por parte dos notários, bem como o arquivamento de assinaturas realizado em cartório, ambos nos termos da Lei de Registros Públicos e do art. 236 da Constituição Federal, dá-se somente sobre a assinatura gráfica manual, com características pessoais e aposta num documento de papel. Apesar da semelhança de propósitos e de nomenclatura, seria a assinatura digital sinal identificador de natureza jurídica diversa, pelo que não afrontaria a Constituição Federal eventual atribuição das atividades cartorárias cibernéticas a outrem que não os tabeliães[110].

108Na eventualidade de roubo do cartão, os certificados garantidores da autenticidade da assinatura digital – dos quais se tratará adiante – podem ser rapidamente revogados.

109*Ellen Gracie assina convênio para certificação digital.*

110BRASIL, Angela Bittencourt. *Assinatura digital não é assinatura formal.*

5. CERTIFICAÇÃO DIGITAL

A certificação digital veio ao Brasil em 1996, estando hoje presente desde celulares GSM às páginas dos bancos na internet. Com base nela, fala-se, para o futuro, em documentos de identidade digitais em microdispositivos portáteis, dada a segurança do sistema, que se não é infalível é extremamente alta. Além disso, o preço dos certificados deverá cair vertiginosamente nos próximos anos[111]. Para tornar a certificação acessível ao cidadão, destaquem-se ainda o potencial dos órgãos representantes de classes – tais como sindicatos – ou empresas públicas como os Correios e a Caixa Econômica Federal.

A grande utilidade dos certificados digitais decorre, como alerta Marcacini, de uma diferença entre as assinaturas criptográficas e as manuais. Enquanto estas têm um vínculo com o corpo da pessoa do titular, identificável por meio das características de seus traços, não há, no caso da assinatura digital, relação direta entre as chaves criptográficas e o corpo do signatário. Assim, para garantir autenticidade à chave pública com a qual conferir-se-á uma assinatura, os certificados eletrônicos de autenticidade revelam-se uma alternativa[112]. Buscando definir o certificado digital, explica Marcacini que

> (...) o certificado nada mais é do que a assinatura eletrônica de uma pessoa, lançada sobre a chave pública de outra. Ou seja, uma primeira pessoa, com o uso de sua chave *privada*, assina a chave *pública* de uma segunda pessoa. Conhecendo a chave pública daquela primeira pessoa, posso conferir a assinatura dada em certificação da chave pública da segunda. Por fim, confiando na primeira pessoa, acreditarei que a chave pública da segunda pessoa é verdadeira.[113]
>
> Do ponto de vista jurídico, esses certificados teriam, a princípio, o significado de uma declaração, dada pelo agente certificante, de que a chave pública em questão realmente pertence ao titular indicado.[114]

111KULIKOVSKI, Sérgio *apud* ZONZIN, Janaína. *Identidade do futuro.*

112Outra maneira de reconhecimento da validade e da eficácia de chaves públicas é, ainda, a assinatura de um documento físico pelas partes reconhecendo as chaves públicas fornecidas como suas. Imagina Marcacini também a possibilidade de a notoriedade de chaves públicas atribuir-lhes autenticidade, caso em que a prudência do magistrado determinaria ser cabível ou não a aceitação da assinatura: MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 94-95.

113MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 53-54.

114MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 93.

Especialistas em informática e profissionais do direito vêm entendendo que a certificação digital é o meio mais seguro para a prática de atos judiciais em meio eletrônico[115].

De fato, em decisão sobre o tema, inclinou-se o Supremo Tribunal Federal pela certificação digital como caminho para a aceitação de assinatura eletrônica. Veja-se:

> Ato processual: recurso: chancela eletrônica: exigência de regulamentação do seu uso para resguardo da segurança jurídica. 1. Assente o entendimento do Supremo Tribunal de que apenas a petição em que o advogado tenha firmado originalmente sua assinatura tem validade reconhecida. Precedentes. 2. No caso dos autos, não se trata de certificado digital ou versão impressa de documento digital protegido por certificado digital; trata-se de mera chancela eletrônica sem qualquer regulamentação e cuja originalidade não é possível afirmar sem o auxílio de perícia técnica. 3. A necessidade de regulamentação para a utilização da assinatura digitalizada não é mero formalismo processual, mas, exigência razoável que visa impedir a prática de atos cuja responsabilização não seria possível.
> (STF, AI 564765/RJ, Primeira Turma, Relator Min. Sepúlveda Pertence, publicado em 17/03/2006)

O certificado, como visto, é uma *opção* a ser aposta sobre a chave pública, dando segurança a quem dela se valer para conferir uma assinatura. É que a autoridade certificadora, por meio de sua chave privada, assina a chave pública de alguém, atestando sua autenticidade.

Sob outro aspecto, saliente-se que nos certificados eletrônicos existe a possibilidade de inclusão de variadas informações de relevo, consistindo um diferencial em relação à assinatura manuscrita. Como exemplo, cita Marcacini a menção no certificado à representação legal exercida pelo assinante[116].

Necessariamente deve ser especificada nos certificados a sua validade, mas de todo modo poderão ser revogados, hipótese em que deverão constar de publicação acessível por todos. Outras informações que se fazem necessárias no certificado são o nome do titular, a chave pública da autoridade emissora e um número de série exclusivo.

115SOUZA, Giselle *apud OAB defende uso da certificação digital contra as fraudes.*

116MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 104-105.

Para Cabral, o documento eletrônico assinado e certificado digitalmente subsumir-se-ia à órbita dos arts. 368 e 371 do Código de Processo Civil, aceitando-se a autoria do signatário e presumindo-se verdadeiras as declarações naquele constantes em relação a este, de modo igual ao que ocorre com os documentos particulares de papel[117].

A segurança que o certificado busca proporcionar se baseia no risco de falsidade da chave pública. Afinal, é possível que uma chave desse tipo pertença de fato a outra pessoa que não aquela a quem é atribuída, uma vez que qualquer um pode gerar um par de chaves e atribuí-lo falsamente a outrem. Se o usuário se valer de chave pública inidônea para codificar um documento, não só este ficará inacessível ao verdadeiro destinatário como poderá ser aberto pelo falsário.

O problema da verdadeira identidade, lembra Marcacini, não é exclusivo das chaves públicas: a possível falsidade de dados apostos na chave criptográfica existe de igual maneira no documento de papel. A solução, aponta, é a *confiança*, não surpreendentemente a que fundamenta a aceitação do documento palpável, uma vez que sua elaboração pode ter sido embasada em fraude contra a autoridade de identificação[118]. A confiança que se tem na autoridade certificadora ou na própria pessoa – caso seja esta a lhe fornecer a chave diretamente – é que determinará o crédito a ser atribuído pelo usuário a uma dada chave.

O caminho da regulamentação de certificados digitais no Congresso Nacional iniciou-se com a Proposição nº 1.483/1999, da Câmara dos Deputados, ao qual foi apensado mais tarde o de nº 1.589/1999, dada a convergência de abordagem[119]. O tema, porém, já é objeto de discussão há vários anos, como lembrado por Kaminski e Volpi, segundo quem “o processo de implantação dessa tecnologia vem se mostrando lento e dificultoso”, devido aos trâmites necessários para que seja regulamentada[120].

Mesmo com as dificuldades de regulamentação, já se visualizam aplicações de certificados digitais. O Superior Tribunal de Justiça disponibiliza em sua “Revista

117CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 113.
118MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 51-52.
119KAMINSKI, Omar e VOLPI, Marlon Marcelo. *A evolução da certificação digital no Brasil*, pp. 252-253 e 263.
120KAMINSKI, Omar e VOLPI, Marlon Marcelo. *A evolução da certificação digital no Brasil*, p. 263.

Eletrônica de Jurisprudência" decisões jurisprudenciais cujo conteúdo foi certificado eletronicamente para maior credibilidade. A Imprensa Oficial do Estado de São Paulo, por sua vez, lançou o diário oficial virtual, com informações assinadas por certificado digital e com valor de original[121]. De outra parte, também está prevista a implementação da certificação eletrônica no CNJ e no STF. Além disso, o número de certificados digitais emitidos conforme o padrão da ICP-Brasil – objeto de tópico posterior – já ultrapassou os quinhentos mil, conforme o ITI – Instituto Nacional de Tecnologia da Informação. Até o fim desta década, essa quantia deverá chegar a vinte milhões, aponta a Câmara Brasileira de Comércio Eletrônico.[122] Vale menção também à área fiscal, na qual a Receita Federal lançou a nota fiscal eletrônica, já em uso no país. O "Sistema Público de Escrituração Digital" (SPED), projeto que lhe deu origem, consiste na "substituição da emissão de livros e documentos contábeis e fiscais em papel por documentos eletrônicos com certificação digital, garantindo assim a sua autoria, integridade e validade jurídica"[123].

Como contraponto às vantagens da implantação de estruturas certificatórias no Brasil, Greco[124] enumera o grande investimento necessário, bem como a credibilidade – idealmente fundada em fiscalização e técnica rigorosos – que "nem o registro de pessoas naturais e o de imóveis conseguiram adquirir no Brasil" de modo satisfatório, segundo o autor.[125] Como eventual amenizador caso esses aspectos se confirmem, é de se referir o Projeto de Lei nº 6.825/2002, que busca instituir a contratação de seguro sobre as atividades de certificação digital, o que por certo facilitaria a aceitação desse mecanismo pela sociedade[126].

Saliente-se, por derradeiro, que ao contrário da tendência verificada no Brasil, em âmbito mundial tende-se a reconhecer as assinaturas digitais livres, não certificadas por entidades autorizadas[127].

---

121 LIMA, George Marmelstein. *e-Processo.*
122 *Brasil já tem 500 mil certificados digitais emitidos pelo padrão oficial.*
123 *Sistema Público de Escrituração Digital.*
124 GRECO, Leonardo. *O processo eletrônico,* pp. 90-91.
125 GRECO, Leonardo. *O processo eletrônico,* p. 91.
126 KAMINSKI, Omar e VOLPI, Marlon Marcelo. *A evolução da certificação digital no Brasil*, p. 259.
127 ROGNETTA, Giorgio *apud* MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 53-54.

6. A DISCIPLINA JURÍDICA DE INSTRUMENTOS PROCESSUAIS ELETRÔNICOS

Os atos processuais por meio eletrônico já foram vislumbrados quando da elaboração da nova redação do art. 170 do Código de Processo Civil – resultado da reforma processual de 1994 –, segundo Marcacini, pois a expressão "uso de outro meio idôneo" em juízos e tribunais incluiria a eletrônica lastreada em mecanismos confiáveis[128]. A recente Lei Federal nº 11.341/2006, a seu turno, alterou o parágrafo único do art. 541 do Código de Processo Civil, autorizando a prova de divergência jurisprudencial por meio de decisões constantes de meios eletrônicos. Ademais, dispositivos como as Leis Federais nºs 10.259/2001 e 11.280/2006, adiante analisadas, igualmente caminham no sentido da aceitação de meios eletrônicos no processo. Não obstante, muitas vozes têm questionado a aplicação dessa via ao processo judicial, demonstrando várias opiniões preocupação com a situação de princípios processuais como a documentação escrita.

Fato é que em breve os documentos eletrônicos deverão ser a regra – trata-se, talvez, da maior esperança para a celeridade e a efetividade que as reformas pelas quais vem passando a carta processual civil tanto desejam –, pelo que regulá-los se mostra essencial, em que pese a possibilidade de enxergá-los sob as normas atuais[129].

A indispensabilidade dessa regulamentação já foi sentida quando a Terceira Turma do Superior Tribunal de Justiça afastou a possibilidade do uso de correio eletrônico para os fins da Lei Federal nº 9.800/1999 no Recurso Especial 594.352/SP. Entendeu-se que inexistiria regulamentação sobre o tema, tampouco técnica para verificar a idoneidade do documento e de seu subscritor[130].

Além de inexistirem normas federais a regulamentar a informatização – o que acaba por ampliar o campo de liberdade dos tribunais com espeque no parágrafo único do art. 154 do Código de Processo Civil –, a legislação atual contém certos requisitos frontalmente incompatíveis com os instrumentos eletrônicos,

128MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 156-158.

129BLUM, Renato M.S. Opice. *O processo eletrônico,* p. 65.

130WAMBIER, Luiz Rodrigues; WAMBIER, Teresa Arruda Alvim; MEDINA, José Miguel Garcia. *Breves comentários à nova sistemática processual civil, II:* Leis 11.187/2005, 11.232/2005, 11.276/2006, 11.277/2006 e 11.280/2006, pp. 28-29.

mesmo considerando-se que a lei brasileira adota o princípio da liberdade de forma – consubstanciado no art. 332 do Código de Processo Civil –, como no caso do testamento particular, que só poderá ser escrito de próprio punho. Do mesmo modo, a regra do art. 1.525 do Código Civil, no qual se consigna a necessidade de firma manuscrita para requerer habilitação para casamento. Diante de regras com essa característica, Greco explica que serão mais facilmente substituíveis por seus correspondentes eletrônicos aqueles documentos para os quais a assinatura seja o único foco de autenticidade[131].

Segundo Cabral, inexistindo norma específica tratando dos documentos eletrônicos, dever-se-á aplicar a eles o Código de Processo Civil[132]. Com base nesse entendimento, a título exemplificativo, Marcacini ensina que, no que se refere ao ônus da prova em sede de argüição de falsidade de chave pública[133], ter-se-ia hipótese de contestação de autoria do documento. Tomando por base o art. 389, II do Código de Processo Civil, competiria à parte produtora do documento provar a autenticidade da chave, assim como na argüição de falsidade de assinatura em documento tradicional[134]. Noutro passo, sendo argüido o uso indevido de chave pública autêntica por terceiros, o ônus da prova caberá a quem defender tal tese.

Ressalvadas são as regras da carta processual civil que não se harmonizam com a natureza de tais inovações[135]. Exemplo é o art. 370, III, uma vez que a impossibilidade física de assinar manualmente não necessariamente afasta a capacidade de assinar por meio digital. Outra disposição inaplicável é a que trata do preenchimento abusivo do documento assinado, pois qualquer alteração documental posterior à assinatura eletrônica acaba por invalidá-la. Ainda, não há como se atribuir a documentos eletrônicos não assinados a credibilidade prevista no Código de Processo Civil para os similares em papel, pois aqueles são extremamente vulneráveis[136].

131GRECO, Leonardo. *O processo eletrônico,* p. 88.

132Silva frisa que os arts. 131, 332 e 335 são compatíveis com os meios de autenticação digital, o que acontece igualmente com outros dispositivos, como os dos arts. 386-395 e 420-443: SILVA, João Carlos Pestana de Aguiar. *As provas no cível*, p. 386.

133Realce-se que no caso de documentos públicos, o ônus da prova é sempre do impugnante, dada a presunção de veracidade daqueles.

134MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, p. 96.

135CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, pp. 120-123.

136MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 90-91.

Questão pertinente diz respeito à cifragem de dados que se mostrarem necessários à instrução processual. Se sua exibição for cabível, podem ser aplicadas as regras presentes atualmente na legislação. Recusando-se a parte de modo ilegítimo a exibir dados legíveis, caberia a pena de confissão ficta; no caso de um terceiro deixar de exibir dados inteligíveis injustificadamente, a única alternativa será a incursão nas sanções do crime de desobediência, pois em princípio medida de busca e apreensão seria inútil[137].

Ausentes normas jurídicas particulares, poderá ainda o juiz se fundamentar naquilo que ordinariamente acontece, a teor do art. 335 do Código de Processo Civil.

Por certo, muitas mudanças na legislação processual são necessárias, pois, como alertam Lima e Fonseca[138], ela não está pronta para o novo processo que nasce[139]. A automação do processo, a segurança dos dados processuais, a prova documental[140] e questões também delicadas como o conceito de jurisdição deverão implicar em revisão das normas processuais. Lima acrescenta que, para além da modernização dos atos do processo, há regras incompatíveis com a celeridade processual almejada, como o prazo de sessenta dias para contestação da Fazenda Pública, igualmente beneficiada pela agilidade conferida pelo computador[141].

Corroborando a necessidade de adaptações no Código de Processo Civil em face das inovações tecnológicas, tem-se o exemplo ilustrativo de seu art. 385, segundo o qual a prova por meio de fotografia deverá ser acompanhada do negativo pertinente. O documento eletrônico correspondente a esse tipo de prova – a fotografia digital – sabidamente não se vale de negativos, e não obstante se tornou preponderante até mesmo em países subdesenvolvidos.

Sublinhe-se, quanto a essas mudanças que certamente haverão de ser feitas, a lição de Lima Neto quanto ao documento eletrônico no direito comparado: relata o autor que no direito alienígena o documento escrito não é tido por referência em relação ao eletrônico, que além do mais tem particularidades no que se refere à

137MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 151-152.

138LIMA, George Marmelstein; FONSECA, Reynaldo Soares da *et al. Elementos para reforma do Código de Processo Civil.*

139Em semelhante entendimento, por entender insuficiente a regulação da matéria no direito brasileiro: CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 125.

140No mesmo sentido: ALMEIDA FILHO, José Carlos de Araújo e CASTRO, Aldemario Araujo. *Manual de informática jurídica e direito da informática*, pp. 174-175.

141LIMA, George Marmelstein. *e-Processo.*

técnica informática cuja regulação a interpretação não consegue suprir[142].

Com efeito, na falta de lei, a incerteza que se instala desestimula o uso dessas novas tecnologias, mais uma razão para que sejam regulamentadas. A necessidade de regulamentação de assinaturas informáticas, a título de exemplo, já foi afirmada pelo Supremo Tribunal Federal, em votação unânime:

> (...) Assinatura digitalizada não é assinatura de próprio punho. Só será admitida, em peças processuais, após regulamentada. Equívoco material pela alusão à regulamentação da recente lei viabilizadora do correio eletrônico na prática de atos processuais não é bastante para qualquer mudança no resultado do julgamento. Embargos rejeitados.
> (STF, RMS-AgR-ED 24257/DF, Rel. Min. Ellen Gracie, Primeira Turma, publicado em 14/02/2003)

Wambier, Wambier e Medina anotam[143] que os atos processuais por meio eletrônico, enquanto sua regulamentação não for projetada para além do art. 8º, § 2º da Lei 10.259/2001, continuarão a ser objeto de discordância, notadamente por ser imperativa disciplina sobre a autenticidade, a integridade, a validade jurídica e a interoperabilidade[144].

No que se refere aos moldes dessa legislação a ser elaborada, por fim, Lima e Fonseca defendem que a melhor técnica legislativa para autorizar o uso de meios eletrônicos no processo seja genérica, tratando apenas dos requisitos essenciais de segurança sem se referir a técnicas ou métodos específicos[145].

6.1 LEI FEDERAL Nº 10.259/2001

A Lei Federal nº 10.259/2001, embora se destaque mais nos Juizados Especiais Federais, tem amplo emprego para além destes, como destaca Guedes. A

142LIMA NETO, José Henrique Barbosa Moreira. *Aspectos jurídicos do documento eletrônico.*

143WAMBIER, Luiz Rodrigues; WAMBIER, Teresa Arruda Alvim; MEDINA, José Miguel Garcia. *Breves comentários à nova sistemática processual civil, II,* p. 28.

144Enquanto há quem entenda, como Blum, que a legislação atual confere ao documento eletrônico assinado digitalmente força probatória equivalente à daquele manualmente assinado, uma vez obedecido ao disposto nos arts. 368, 370 e 371 da carta processual civil, há entendimento em sentido aparentemente diverso, como o de Silva, para quem certificados e assinaturas digitais não são suficientes à estabilidade jurídica: BLUM, Renato M.S. Opice. *O processo eletrônico,* pp. 52-53 e SILVA, João Carlos Pestana de Aguiar. *As provas no cível*, p. 375.

145LIMA, George Marmelstein; FONSECA, Reynaldo Soares da *et al. Elementos para reforma do Código de Processo Civil.*

mencionada lei inova ao permitir o recebimento de petições por meio eletrônico (art. 8º, § 2º: "Os tribunais poderão organizar serviço de intimação das partes e de recepção de petições por meio eletrônico"), desde que haja organização e previsão regimental por parte dos Tribunais Regionais Federais[146]. Dentre os desafios que essa proposta apresenta, na visão do autor, há o horário de expediente previsto no art. 172, § 3º do Código de Processo Civil, que poderá ser repensado – refletindo-se no instituto da preclusão – com a possibilidade de se receber petições em qualquer horário no protocolo eletrônico.

Nos termos da lei em comento, o Tribunal Regional Federal da 4ª Região implantou o processo eletrônico dos Juizados Especiais Federais de sua região. O sistema, chamado de *e-proc*, busca um processo integralmente digital. A garantia de autenticidade e de origem dos documentos é, nos termos do art. 4º da Resolução nº 13/2004 – que regula o *e-proc* –, baseada na geração de chaves eletrônicas[147].

Outros Tribunais Regionais Federais, também em atenção à Lei 10.259/2001, já organizaram serviços de recepção de petições por meio eletrônico[148].

6.2 LEI FEDERAL Nº 11.280/2006

No Código de Processo Civil, o art. 154 bem dispõe a finalidade instrumental do processo, que garante a aceitação do ato processual realizado em desconformidade com a norma se atingir sua finalidade. A Lei Federal nº 11.280/2006 alcançou a referida regra, nela inserindo um parágrafo único, semelhante a disposições existentes em outros países, que possibilita expressamente a prática – disciplinada por normas regimentais – de atos processuais por meios eletrônicos, "atendidos os requisitos de autenticidade, integridade, validade jurídica e interoperabilidade da Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil".

Wambier, Wambier e Medina defendem que "a implementação das regras

146GUEDES, Jefferson Carús. *Comunicação processual eletrônica na lei dos Juizados Especiais Federais.*

147WAMBIER, Luiz Rodrigues; WAMBIER, Teresa Arruda Alvim; MEDINA, José Miguel Garcia. *Breves comentários à nova sistemática processual civil, II,* pp. 25-26.

148LIMA, George Marmelstein. *e-Processo.*

referidas no parágrafo único do art. 154 exigirá novas reformas processuais, tendentes a ajustar não só os aspectos procedimentais, mas também questões relacionadas aos institutos fundamentais do direito processual civil e ao denominado 'e-processo'"[149].

Diante das técnicas dessa natureza já postas em prática, como os juizados virtuais, necessário se faz verificar o respeito à sistemática da ICP-Brasil – analisada logo a seguir – por tais implementações[150].

149WAMBIER, Luiz Rodrigues; WAMBIER, Teresa Arruda Alvim; MEDINA, José Miguel Garcia. *Breves comentários à nova sistemática processual civil, II,* p. 29.

150CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 125.

7. A ICP-BRASIL E A MEDIDA PROVISÓRIA Nº 2.200/2001

Cumpre inicialmente consignar o entendimento de Reinaldo Filho, para quem infra-estrutura de chaves públicas é "um conjunto de regimes normativos, procedimentos, padrões e formatos técnicos que viabilizam o uso em escala da criptografia de chaves públicas em rede digital aberta"[151], sendo sua precípua função, por meio de autoridades certificadoras, adicionar segurança no uso de chaves públicas e certificados digitais destinados a garantir a autenticidade, a integridade e a validade jurídica de documentos eletrônicos. As ICP permitem o estabelecimento da cadeia de confiança, fundamento do sistema de certificação digital, pois a confiança nas assinaturas é estabelecida pela autoridade certificadora – e não pelas partes. Estas confiam naquela e manifestam essa confiança ao autorizar seus programas de computador a aceitarem os certificados daquela autoridade como válidos.

A Medida Provisória nº 2.200, de agosto de 2001, criou a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil – e estabeleceu as condições de validade jurídica de documentos eletrônicos no Brasil. Nos termos de seu art. 1º, a ICP-Brasil destina-se a "garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica".

A ICP-Brasil é definida, pela página governamental a ela dedicada na internet, como

> um conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública.[152]

A aludida medida provisória, que já gera debates acerca de sua constitucionalidade, estabeleceu que documentos eletrônicos assinados digitalmente com certificados emitidos sob a égide da ICP-Brasil presumem-se verdadeiros. O dispositivo não definiu em detalhes a organização da ICP-Brasil – previu apenas seus órgãos no art. 2º –, do que ficou incumbido o regulamento.

---

151 REINALDO FILHO, Demócrito. *A ICP-Brasil e os poderes regulatórios do ITI e do CG.*
152 *ICP Brasil.*

Essa medida provisória, com força de lei, está atualmente com a numeração 2.200-2, de 24 de agosto de 2001, após alterações textuais. Trata-se do primeiro e único diploma legal a regular meios de segurança para documentos eletrônicos e deverá ser revogado pelo Projeto de Lei nº 7.316/2002, com maior abrangência normativa.

A medida provisória dividiu tarefas entre as autoridades certificadoras e autoridades de registro, coordenadas por um Comitê Gestor – composto de maneira eclética –, cadastradas e fiscalizadas pela Autoridade Certificadora Raiz.

Às autoridades de registro cabem tão somente a identificação e o cadastro de usuários, que poderão obter, junto às autoridades certificadoras, certificados digitais com pares de chaves criptográficas baseadas na tecnologia da criptografia assimétrica.[153]

As críticas feitas pela OAB à medida provisória em comento vão desde os procedimentos de segurança implementados na ICP-Brasil até a opção por uma só chave raiz oficial, sem paralelo no mundo. A fé própria do Poder Judiciário impediria igualmente que este dependesse do Poder Executivo para validar seus atos[154].

Chama a atenção – Cabral afirma tratar-se do dispositivo mais relevante do diploma – o parágrafo primeiro do art. 10 da Medida Provisória, que estabelece a presunção de veracidade *erga omnes* das declarações apostas em documentos eletrônicos em relação aos seus signatários, desde que tais documentos sejam assinados com processo de certificação regulado pela ICP-Brasil. Tal disposição se assemelha às dos arts. 368 do Código de Processo Civil e 219 do Código Civil de 2002, incumbindo-se o ônus da prova ao subscritor. Cabral entende que apesar do foco na integridade do conteúdo do documento (declarações), silenciou a medida provisória no que se refere à sua autenticidade, referida no art. 369 do Código de Processo Civil[155].

Críticas à medida provisória são também desferidas por Atheniense, para quem norma de tamanha importância – estabelecendo os fundamentos da validade jurídica do documento eletrônico – não deveria ter sido elaborada por ato do Poder

153CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 125.
154KAMINSKI, Omar e VOLPI, Marlon Marcelo. *A evolução da certificação digital no Brasil*, pp. 259-260.
155CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 125.

Executivo. Afirma o autor, ainda, que a existência de um certificado único – com o suposto objetivo de assegurar a interoperabilidade entre as AC – é uma desnecessária afronta à privacidade, porque pode haver perfeita interação através de padrões tecnológicos comuns, como o X.509[156], enquanto que com a adoção de um certificado único facilita-se a devassa das informações referentes ao usuário, fator responsável pela recusa dos países europeus em utilizar tal sistema[157].

Rezende igualmente censura os procedimentos estabelecidos pelo diploma normativo instituidor da ICP-Brasil, que no seu entender permite a subversão da capacidade de os usuários buscarem por si sós o controle da segurança dos documentos eletrônicos. Outro ponto negativo para o autor é a falta de transparência dos procedimentos realizados pelos credenciados, dado que auditáveis somente internamente pelo órgão credenciador – conforme resoluções do Comitê Gestor –, não sendo permitida a auditoria por parte da sociedade ou do Poder Público dos mecanismos que irão presumir verdadeiro um documento em relação ao signatário[158].

O mesmo Rezende[159] entende ser motivo de grande preocupação a validade jurídica, no sistema instituído pela medida provisória, de um certificado auto-assinado – o da Autoridade Certificadora Raiz da ICP-Brasil, eis que ela própria o assina para apresentar-se – como gerador de presunção da identidade do signatário[160]. Segundo ensina, meios haveriam para forjar esta autocertificação, com dificuldades à caracterização do crime, em contraposição a benefícios que o tornariam atraente a falsificadores, podendo introduzir desequilíbrios desanimadores no ordenamento jurídico.

Passa-se à crítica de Rezende[161] sobre as possibilidades de revogação de

---

156O padrão X.509, da International Standards Organization (ISO) é muito utilizado em certificação e é de livre implementação. Fundamenta-se em uma estrutura piramidal, podendo a chave pública ser assinada somente uma vez pelo certificante, que a seu turno pode ter sido certificado por um certificador-raiz: MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 53-54.

157ATHENIENSE, Alexandre Rodrigues. *A privacidade na "ICP-Brasil".*

158REZENDE, Pedro Antônio Dourado de. *Sistema de Pagamento Brasileiro e ICP – Brasil.*

159REZENDE, Pedro Antônio Dourado de. *Sistema de Pagamento Brasileiro e ICP – Brasil.*

160Nos moldes da medida provisória, só a AC-Raiz pode apresentar-se a si própria com presunção de veracidade no meio regulado por aquele dispositivo, o que para Rezende é contrário ao estabelecido no art. 236 da Constituição Federal. Nos Estados Unidos, tal modelo teria sido rechaçado justamente por causa da problemática da segurança: REZENDE, Pedro Antônio Dourado de. *Sistema de Pagamento Brasileiro e ICP – Brasil.*

161REZENDE, Pedro Antônio Dourado de. *Sistema de Pagamento Brasileiro e ICP – Brasil.*

chaves. O Comitê Gestor previu, nas normas que editou, dois tipos de revogação. Varia a iniciativa, que pode ser do titular ou do certificador. A revogação de uma chave privada por iniciativa do titular, buscando evitar os efeitos nefastos de seu vazamento, consiste em procedimento questionável. Presumivelmente, a iniciativa de revogação decorrerá da quebra indevida do sigilo da chave, o que, como visto, provavelmente só se detectará após a ocorrência da fraude. Por outro lado, revogar uma chave por iniciativa do certificador seria procedimento a ser tomado diante da suspeita de falsidade ideológica do titular. Tanto em um caso como noutro, confirmadas as expectativas de uso indevido da chave, a revogação só neutralizaria os efeitos caso pudesse retroagir, hipótese em que as possibilidades de fraude aumentariam exponencialmente.

A impossibilidade de se realizar auditoria externa nas certificadoras pode fazer da revogação retroativa um problema maior que o vazamento de chaves privadas ou a falsificação de certificados, defende Rezende[162], pois ter-se-á que confiar na palavra do revogador, não havendo outros meios para saber se a data de revogação foi forjada artificiosamente.

Sobre os órgãos de cúpula da ICP-Brasil, preleciona o referido autor[163] que o ITI – Instituto Nacional de Tecnologia da Informação, na condição de Autoridade Certificadora Raiz – e o Comitê Gestor atuam sobre as atividades de certificação digital no país com propósitos próprios de agências reguladoras, pois podem direcionar as atividades dos credenciados em consonância com interesses públicos definidos juridicamente.

7.1 O COMITÊ GESTOR

A atividade normativa na ICP-Brasil, incluindo a definição de regras para a operação das autoridades certificadoras e de registro, é exercida pelo Comitê Gestor – integrado também por representantes da sociedade, o que lhe confere autonomia frente ao poder político central –, restando uma parcela residual à Autoridade Certificadora Raiz, à qual compete dar execução aos atos normativos. Essa competência residual, não prevista no Projeto de Lei nº 7.316/2002, consubstancia-

162REZENDE, Pedro Antônio Dourado de. *Sistema de Pagamento Brasileiro e ICP – Brasil.*
163REZENDE, Pedro Antônio Dourado de. *Sistema de Pagamento Brasileiro e ICP – Brasil.*

se naquilo que não for de encontro às resoluções do Comitê Gestor[164]. Para Reinaldo Filho[165], a atividade normativa deve se firmar como exclusiva desse comitê, como se verifica no citado projeto de lei, que possivelmente revogará a atual medida provisória.

A função do Comitê Gestor, na prática e apesar de todas as atribuições que lhe são confiadas, será a de definir políticas gerais de certificação, a serem executadas pela Autoridade Certificadora Raiz, sobre a qual recairão igualmente o credenciamento, a auditoria e a supervisão dos prestadores de serviço credenciados, com fulcro no art. 4º, parágrafo único da medida provisória, que autoriza a delegação, por parte do Comitê Gestor, de atribuições à Autoridade Certificadora Raiz[166].

7.2 AUTORIDADE CERTIFICADORA RAIZ

Importa destacar o papel da Autoridade Certificadora Raiz (AC Raiz) da ICP-Brasil, cujo par de chaves criptográficas e o correspondente certificado digital foram gerados em novembro de 2001. Apesar de ter funções semelhantes às outras autoridades certificadoras, é regida por algumas peculiaridades, como a necessidade de vinculação ao Ministério da Ciência e Tecnologia. Assim como as outras autoridades da cadeia certificadora, com exceção daquela no nível mais baixo (que é a que poderá emitir certificados ao usuário final), pode gerar certificados apenas para as autoridades certificadoras de nível imediatamente inferior[167].

A existência de uma autoridade certificadora raiz, que estabelece as políticas gerais de certificação e na qual todas as certificadoras hierarquicamente inferiores devem confiar, é uma maneira de expandir, com sua respeitabilidade, a validade dos certificados emitidos por estas. Este foi o modelo adotado pela ICP-Brasil, com uma estrutura hierarquizada e vertical de âmbito nacional[168].

Dispositivos da Medida Provisória nº 2.200/2001 especificam a quem incumbirá o papel de AC Raiz e suas funções, como se vê a seguir:

164REINALDO FILHO, Demócrito. *A ICP-Brasil e os poderes regulatórios do ITI e do CG.*
165REINALDO FILHO, Demócrito. *A ICP-Brasil e os poderes regulatórios do ITI e do CG.*
166REINALDO FILHO, Demócrito. *A ICP-Brasil e os poderes regulatórios do ITI e do CG.*
167KAMINSKI, Omar e VOLPI, Marlon Marcelo. *A evolução da certificação digital no Brasil*, p. 257.
168REINALDO FILHO, Demócrito. *A ICP-Brasil e os poderes regulatórios do ITI e do CG.*

> Art. 5º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.
> Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.
> (...)
> Art. 12º Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação - ITI, com sede e foro no Distrito Federal.
> Art. 13º O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.
> Art. 14º No exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei.

7.3 AUTORIDADES CERTIFICADORAS

A autoridade certificadora[169] (AC) é uma instituição credenciada destinada à expedição de identidades digitais certificadas aos interessados, vinculando pares de chaves criptográficas a seu titular mediante contraprestação periódica. Após receber o pedido de emissão de certificado das Autoridades de Registro (AR), que previamente verificaram a real identidade – por meios tradicionais – do tomador de serviço, valem-se da criptografia assimétrica para apor seu certificado na chave pública do titular (a chave privada é de exclusivo controle e conhecimento deste). A chave pública é então disponibilizada na página da certificadora na grande rede, ficando acessível a todos para verificação da autenticidade de assinaturas, enquanto que a chave privada fica em poder do interessado para a codificação de seus documentos.[170]

Em outras palavras, às autoridades certificadoras (AC), objeto do art. 6º da Medida Provisória nº 2.200/2001, cabe gerar, distribuir e gerenciar chaves públicas e

169A Serasa e o Serpro são exemplos de autoridades certificadoras já credenciadas: KAMINSKI, Omar e VOLPI, Marlon Marcelo. *A evolução da certificação digital no Brasil*, p. 261.
170CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 113.

certificados digitais, segundo uma estrutura técnica e normativa, dando segurança ao sistema, cumprindo papel similar ao dos notários na certificação tradicional. Cabral compara essas autoridades a um cartório virtual[171].

Na ICP-Brasil, especificamente, as autoridades certificadoras (AC) se situam na hierarquia certificatória um nível abaixo da AC Raiz, por quem são credenciadas, cabendo a elas emitir certificados digitais aos usuários finais[172].

A fé pública do ente certificante público, por gerar presunção simples de autenticidade, serve para inverter o ônus da prova em desfavor daquele que se eventualmente se insurja contra o certificado, como anota Marcacini, para quem as funções de autoridade certificadora possivelmente incorporar-se-ão às já exercidas pelos tabeliães, dotados de fé pública e com investidura feita pelo Estado[173].

Na visão de Marcacini, tanto técnica como juridicamente, todos poderão assinar as chaves públicas de outrem – que é o que as autoridades certificadoras fazem. No caso de entes certificantes privados, porém, ensina o autor que

> (...) se algumas cautelas foram tomadas pelo ente certificante, como, por exemplo, colher do cliente uma declaração escrita em papel, reconhecendo a chave como sua, esta sim, dado que proveniente daquele contra quem se quer fazer a prova, poderia demonstrar a autenticidade da chave pública assinada pelo ente certificador privado. Ademais, se a certificação eletrônica privada, por si só, não faz prova contra o titular da chave, por certo gera obrigações para o certificador em relação a terceiros que tenham acreditado nele.[174]

Segundo a Medida Provisória nº 2.200/2001, a criação de uma autoridade certificadora é livre e independe de autorização específica, sendo que, se atendidos aos requisitos estabelecidos pela ICP-Brasil, poderá a AC criada se credenciar junto a ela (art. 8º do citado dispositivo legal), passando a integrar sua infraestrutura e com isso tendo o raio de validade de seus certificados – que poderão ser aplicados em qualquer documento – expandido, conferindo-lhes valor probante contra terceiros em todo o território nacional[175]. Quanto ao uso de chaves públicas na

171CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 113.
172REINALDO FILHO, Demócrito. *A ICP-Brasil e os poderes regulatórios do ITI e do CG.*
173MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 97 e 102.
174MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia, pp. 98-100.
175REINALDO FILHO, Demócrito. *A ICP-Brasil e os poderes regulatórios do ITI e do CG.*

esfera pública, caberia aos próprios Poderes o estabelecimento de uma infra-estrutura pertinente.

Poderão algumas certificadoras atestar a data e a hora de produção do documento, elementos úteis perante terceiros[176]. No caso, porém, a certificação se dará sobre o próprio documento, e não mais sobre a chave pública. Mostra-se, na hipótese, conveniente a publicação do ato, para que se afaste a possibilidade de a data certificada ser forjada. De todo modo, averbe-se que, para o peticionamento eletrônico, deverá bastar o art. 370, IV do Código de Processo Civil, segundo o qual a partir da apresentação em juízo considera-se datado o documento.

Uma autoridade certificadora da ICP-Brasil chama a atenção por reunir de modo mundialmente pioneiro apenas instituições ligadas à Justiça: é a AC-JUS, ou Autoridade Certificadora da Justiça. Integram-na, podendo ter seus documentos por ela certificados, o Conselho da Justiça Federal, o Superior Tribunal de Justiça, os cinco Tribunais Regionais Federais, assim como o Conselho Nacional de Justiça, os demais tribunais superiores e o Colégio Notarial[177].

Além da AC-JUS, como exemplos de autoridades certificadoras credenciadas, destaquem-se, entre os órgãos públicos, a Secretaria da Fazenda, a Presidência da República, o Serpro e a Caixa Econômica Federal[178].

7.4 AUTORIDADES DE REGISTRO

As autoridades de registro (AR) têm por missão verificar a real identidade daquele que se apresenta como titular de um determinado par de chaves, em sua presença, para – uma vez confirmada a veracidade daquela – encaminhar pedido de emissão de certificado à autoridade certificadora à qual estão vinculadas. O art. 7º da Medida Provisória nº 2.200/2001, que trata das AR, estabelece que o registro de suas atividades cabe a elas próprias. Kaminski e Volpi, que noticiam ter a Associação dos Notários e Registradores do Brasil solicitado o seu credenciamento como Autoridade de Registro, anotam que a estrutura para se estabelecerem as AR,

176CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, pp. 113-114.
177BASTOS, Roberta. *Integração tecnológica do Poder Judiciário é tema de encontro realizado no STJ.*
178*OAB anuncia lançamento de certificação digital para advogados.*

que deverá ser a mais ampla possível, poderá ter por base outras já existentes, como os registros notariais, correios e casas lotéricas[179].

179KAMINSKI, Omar e VOLPI, Marlon Marcelo. *A evolução da certificação digital no Brasil*, pp. 257 e 262.

8. A ICP-OAB

A Ordem dos Advogados do Brasil, por meio de seu Conselho Federal, buscando preservar o sigilo e a independência, instituiu sistema próprio de infraestrutura de chaves públicas para certificação de advogados, a ICP-OAB, em funcionamento desde outubro de 2002. Pretende a OAB recadastrar seus inscritos para a emissão de novo cartão de identidade de advogado, com certificação digital, por meio da Casa da Moeda do Brasil, válido em todo o território nacional por três anos[180].

Em alguns Estados já é possível ao advogado a obtenção de seu certificado digital da ICP-OAB, que é interoperável com a ICP-Brasil[181] e igualmente está sob a égide da Medida Provisória nº 2.200/2001.

Nesse tocante, é de se destacar que há campanha no sentido de que o certificado digital utilizado na prática profissional da advocacia deverá ser aquele fornecido pela entidade autorizada legalmente[182], isto é, a Ordem dos Advogados do Brasil, conforme o Estatuto da Advocacia (Lei Federal nº 8.906/1994). Por essa razão, o advogado não deveria adquirir certificados de terceiros para a prática de atos da profissão. No que se refere à validade do certificado emitido pela OAB, o art. 10, § 2º da Medida Provisória nº 2.200/2001 a confirmaria, pois é desnecessária a certificação pela ICP-Brasil se houver o reconhecimento da parte transacionante (no caso, seja na comunicação entre o Poder Judiciário e a OAB, seja entre esta e o inscrito), caso em que o certificado utilizado será igualmente válido[183].

Os tribunais que reconhecerem o sistema de certificação da OAB, além de verificarem a autenticidade da assinatura, poderão consultar instantaneamente o cadastro de advogados aptos no momento do recebimento da petição. Além disso, esse padrão tecnológico exige menores investimentos em infra-estrutura[184].

180ATHENIENSE, Alexandre Rodrigues. *Da validade legal dos atos processuais praticados pelo meio eletrônico.*

181ATHENIENSE, Alexandre Rodrigues. *Da validade legal dos atos processuais praticados pelo meio eletrônico.*

182Em sentido oposto, há notícia de que o Governo Federal e o Poder Judiciário teriam determinado que os sistemas de certificação digital por eles utilizados só poderiam ser prestados e contratados dentro da ICP-Brasil, de modo a excluir a aceitação da identificação digital da OAB: *OAB anuncia lançamento de certificação digital para advogados.*

183ATHENIENSE, Alexandre Rodrigues. *Campanha "Advogado, não compre certificado digital de empresas particulares" – Esclarecimento.*

No Tribunal de Justiça do Estado de Rondônia já existe o protocolo eletrônico de peças – sem necessidade de juntada posterior de papéis –, mediante a utilização da certificação subordinada à ICP-OAB. Para usar o sistema, implantado neste ano, o causídico deve adquirir identidade digital junto à Seção da OAB no Estado. O mecanismo implantado no TJRO está em consonância com a Lei Federal nº 11.280/2006 e emite recibo eletrônico para confirmar o recebimento da petição, com horário certificado pelo Observatório Nacional[185].

184ATHENIENSE, Alexandre Rodrigues. *Da validade legal dos atos processuais praticados pelo meio eletrônico.*

185*ICP-OAB é usada pela primeira vez em peticionamento eletrônico.*

9. O PROCESSO VIRTUAL

A Emenda Constitucional nº 45/2004 veio para incluir na Carta Magna, em seu art. 5º, o inciso LXXVIII, como demonstração da preocupação em acelerar a prestação jurisdicional. Tal dispositivo assegura a todos "a razoável duração do processo e os meios que garantam a celeridade de sua tramitação" como garantia fundamental. A respeito do tema, é lúcida a reflexão de Marinoni:

> (...) no que diz respeito especificamente à celeridade dos procedimentos, não é preciso dizer que a demora do processo jurisdicional sempre foi um entrave para a efetividade do direito de acesso à justiça. Sim, já que não tem sentido que o Estado proíba a justiça de mão própria, mas não confira ao cidadão um meio adequado e tempestivo para a solução dos seus conflitos. Se o tempo do processo, por si só, configura um prejuízo à parte que tem razão, é certo que quanto mais demorado for o processo civil mais ele prejudicará alguns e interessará a outros. Seria ingenuidade inadmissível imaginar que a demora do processo não beneficia justamente àqueles que não tem interesse no cumprimento das normas legais.[186]

A grande esperança de uma vigorosa aceleração na prestação da tutela jurisdicional é depositada no chamado processo virtual. Nele, o máximo de atos possível é realizado por meio eletrônico, com plena validade jurídica. É a chamada virtualização, com a qual, na esteira do entendimento de Oliveira, o processo se foca menos na ordenação do processo-papel e mais na eficiência da Justiça, mais célere, simples, publicizada e segura[187].

Como demonstração de iniciativas nesse caminho, o trabalho realizado nos Juizados Especiais Federais, nos quais se destaca vigorosamente a virtualização do processo em âmbito nacional, tem produzido resultados excelentes, embora as questões tratadas sejam de menor valor financeiro, como é de se esperar. Um dos Tribunais Regionais Federais a implantar o processo eletrônico – dispensando a apresentação de documento em papel após o protocolo da petição eletrônica – foi o da 4ª Região. Nos Juizados Especiais Federais da aludida região, a segurança dos

186MARINONI, Luiz Guilherme. *O custo e o tempo do processo civil brasileiro.*

187OLIVEIRA, Bruno Augusto Santos. *Juizado virtual:* o deslocamento do centro de gravidade ontológico do processo-papel para a problemática da eficiência da Justiça.

dados no chamado *e-proc*[188] é baseada na geração de chaves criptográficas.

Pode-se pensar que, inicialmente, a aceitação de petições enviadas pela internet concorra com outras alternativas, tais como a entrega pessoal de peças gravadas em meio magnético ou em papel a ser digitalizado posteriormente. Não foi este o caso do *e-proc*. Veja-se que, segundo o julgamento a seguir, sequer é facultada a utilização de meios convencionais nos processos de sua competência:

> MANDADO DE SEGURANÇA. ATO PRESIDENTE TRF4. OBRIGAÇÃO DE UTILIZAÇÃO DO PROCESSO ELETRÔNICO (EPROC) NOS JUIZADOS ESPECIAIS FEDERAIS.
> 1. A instituição do processo eletrônico é decorrência da necessidade de agilização da tramitação dos processos nos Juizados Especiais Federais, representando a iniciativa o resultado de um enorme esforço institucional do Tribunal Regional da 4a Região e das três Seções Judiciárias do sul para que não se inviabilize a prestação jurisdicional à população, diante da avalanche de ações que recai sobre a Justiça Federal, particularmente nos Juizados Especiais Federais.
> 2. O sistema em implantação é consentâneo com os critérios gerais da oralidade, simplicidade, informalidade, economia processual e celeridade que devem orientar os Juizados Especiais, previstos no art. 2º da Lei 9.099/95, e que são aplicáveis aos Juizados Especiais Federais, conforme disposto no art. 1º da Lei 10.259/2001.
> 3. A sistemática implantada assegura o acesso aos equipamentos e aos meios eletrônicos às partes e aos procuradores que deles não disponham (Resolução nº 13/2004, da Presidência do TRF/4ª Região, art. 2º, §§ 1º e 2º), de forma que, a princípio, ninguém tem o acesso à Justiça ou o exercício da profissão impedido em decorrência do processo eletrônico.
> - Segurança denegada.
> (TRF4, MS 2004.04.01.036333-0, Corte Especial, Relator João Surreaux Chagas, publicado em 19/10/2005)

No Juizado Virtual, o processo é acessível de qualquer lugar do mundo, por página segura, maximizando a publicidade. As petições recebidas, assinadas digitalmente de modo a garantir a origem e o conteúdo, são juntadas automaticamente pelo sistema e é emitido um protocolo eletrônico[189]. O executor de cada ato processual fica registrado, com data e hora. Também com base em assinaturas digitais criptografadas os juízes assinam sentenças, com um clique, o

188A nomenclatura dos sistemas de processo eletrônico varia. Por exemplo, o sistema do Tribunal Regional Federal da 1ª Região recebeu o nome de “e-Jufe”.

189Como formas de recibo de petições enviadas eletronicamente, pode-se cogitar um código como o recebido na entrega da declaração de Imposto de Renda, ou então – o que seria mais seguro – a expedição de um comprovante digital assinado eletronicamente pelo juízo.

que lhes permite resolver problemas urgentes sem se deslocar à sede da Justiça[190]. Cópias de segurança redundantes em vários locais são igualmente característica do sistema. Ademais, o uso de certificação nos Juizados Especiais Federais controla o acesso das partes ao processo, mediante cadastro e uso de senha[191] e, visando a reforçar a segurança, os atos processuais não podem sofrer modificações após adentrarem o sistema[192].

Surpreendentemente, o custo médio de um processo eletrônico no *e-proc*, em que, além da otimização do trabalho, são dispensados insumos como papel, tinta, grampos e etiquetas, é de vinte reais, contra *oitocentos* necessários no modelo tradicional[193].

Lima busca enumerar as peculiaridades próprias do processo eletrônico: publicidade[194], velocidade, comodidade, facilidade de informação, com sua conseqüente democratização; menor contato pessoal; rotinas e decisões jurídicas automatizadas; autos digitalizados; ampliação do conceito espacial de jurisdição; participação de técnicos de informática[195] em questões processuais; cuidado com a segurança dos dados processuais; extensão dos poderes processuais dos magistrados; validação das provas digitais e o surgimento de nova categoria de excluídos processuais[196]. Porta acrescenta a transparência, a proteção ao meio ambiente e efetiva implementação do ordenamento jurídico[197]. Se por um lado muitas dessas características são vantajosas, outras podem ser uma ameaça à legitimidade do processo judicial, na visão daquele autor, segundo quem as possibilidades de fraude se multiplicam e a punição por seu cometimento enfrenta

190*Processo eletrônico.*

191Atheniense critica as experiências que vêm sendo feitas em termos de processo eletrônico acessível por meio de senhas e sem assinaturas digitais da OAB, pois – segundo afirma – além da desarmonia com que vêm sendo implantados, a identificação do peticionante fica vulnerável e é incerto se ele de fato pode exercer a advocacia: ATHENIENSE, Alexandre Rodrigues. *Da validade legal dos atos processuais praticados pelo meio eletrônico.*

192CUNHA, Vagner Bispo da. *A intimação por correio eletrônico e as questões controvertidas.*

193NERY, Fernando Loschiavo. *A virtualização dos processos judiciais (e-proc) e a dispensabilidade de autenticação documental por tabelião.*

194É certo que na teoria também os processos de papel são públicos. Questiona-se, porém, a efetividade dessa publicidade, que usualmente demanda deslocamentos físicos nem sempre possíveis. Com o processo virtual, ainda que a pessoa não tenha acesso a computadores, poderá comparecer em juízos próximos de sua residência – nos quais idealmente haverá computadores disponíveis para consulta, com o auxílio de servidores – para lá tomar conhecimento de autos em trâmite noutra localidade.

195Tanto o monitoramento e a correção de falhas nos sistemas como a elaboração de perícias, fundamental no cenário que se desenha, ficarão a cargo dos especialistas em informática.

196LIMA, George Marmelstein. *e-Processo.*

197PORTA, Marcos de Lima. *A importância da internet na justiça,* p. 362.

obstáculos como a identificação do fraudador, que poderá ademais se encontrar nas mais diversas localidades do planeta.

Apesar dos riscos cogitados por muitos, o secretário-geral do Conselho Nacional de Justiça, juiz federal Sérgio Tejada, esclarece que há planos de se implantar o processo eletrônico em todo o Poder Judiciário[198], no que o Brasil deve ser pioneiro. Entusiasma-se Tejada com as vantagens da virtualização do processo: para ele, o processo virtual é a mudança, muito além de simplesmente informatizar a burocracia. Complementa que segundo pesquisa "(...) o tempo médio de julgamento de um processo na Justiça brasileira é de cerca de 700 dias. Já nos Juizados Especiais que já utilizam a tramitação eletrônica, esse tempo cai para 37 dias"[199]. O conselho pelo juiz secretariado, que ficará mais acessível com o uso do processo virtual – hoje é necessário ir a Brasília ou remeter o material por correio para lá dar entrada em um processo, enquanto que virtualmente isso será possível instantaneamente de qualquer parte do globo – desenvolve um sistema baseado em *software livre*[200] a ser disponibilizado sem custo a todos os tribunais[201].

Outra iniciativa de virtualização do processo se vislumbra no Supremo Tribunal Federal, que já tem mais de 250 mil processos totalmente virtuais em andamento[202]. Pretende-se que os recursos extraordinários sejam processados de forma eletrônica.

Para além das enumeradas, há mais especialidades a se desvendar com o uso da internet no processo, algumas já em prática, outras em tese.

Exemplificando a prática, aponta-se que nas Varas Federais da 4ª Região, o correio eletrônico é utilizado para envio de cartas precatórias e outras comunicações de atos processuais, conforme disposto no Provimento nº 1/2000 da Corregedoria[203].

---

198 *Sistema de Processo Eletrônico tem projeto piloto aprovado pelos ministros do STF.*

199 *Processo virtual brasileiro não tem precedentes no mundo inteiro.*

200 Os programas de computador conhecidos por software livre, cujo código-fonte é livremente acessível – o que não se confunde com gratuidade –, apesar dos atrativos, podem nem sempre ser a solução mais adequada a ser implementada. Deve-se analisar, na escolha entre programas livres ou proprietários, o aproveitamento dos investimentos já feitos e o dinheiro a ser despendido com cada tipo de programa, entre outras ponderações, como alerta Bruno A. S. Oliveira: OLIVEIRA, Bruno Augusto Santos. *Juizado virtual:* o deslocamento do centro de gravidade ontológico do processo-papel para a problemática da eficiência da Justiça.

201 GARCIA, Sergio Renato Tejada *apud CNJ elabora programa de processo virtual que pode ser estendido para todo o Judiciário.*

202 GARCIA, Sergio Renato Tejada *apud Sistema de Processo Eletrônico tem projeto piloto aprovado pelos ministros do STF.*

203 LIMA, George Marmelstein. *e-Processo.*

Outrossim, é possível aos advogados que atuam em processos em curso na Justiça Federal da referida região o pagamento via internet[204] de custas, tanto em primeira como em segunda instância[205].

No campo das possibilidades, por fim, assinala-se que, logrando o documento eletrônico demonstrar a possibilidade de resguardar autenticidade e integridade, os títulos executivos – os quais segundo Borba deverão deixar progressivamente o meio documental tradicional[206] – poderão eventualmente passar a ser aceitos nos termos do art. 614 do Código de Processo Civil, ao que não se opõe o pensamento de Greco[207]. Demonstra essa inclinação a exposição de Lucca:

> Na nova redação que se pretende dar ao art. 566 do Código de Processo Civil, assim ficaria tal dispositivo:
>
> "Pode promover a execução forçada o credor por obrigação expressa em documento por lei considerado título executivo extrajudicial, redigido por escrito ou constante de registro eletrônico autorizado."
>
> O acréscimo da expressão "ou constante de registo eletrônico autorizado" parece traduzir a inequívoca intenção de dar ao título com suporte eletrônico a mesma força daquele materializado no pedaço de papel.[208]

204Dentre os inúmeros meios de pagamento utilizáveis em transações eletrônicas, Cabral cita a carteira virtual, o boleto bancário, o reembolso postal, o depósito em conta (inclusive via banco eletrônico), o débito em conta telefônica, o cheque eletrônico, o crédito pré-pago e o cartão de crédito virtual: CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 117.

205*Advogados do Sul podem pagar pela Internet as custas processuais do TRF e da Justiça Federal.*

206BORBA, Gustavo Tavares *apud* GRECO, Leonardo. *O processo eletrônico,* p. 81.

207GRECO, Leonardo. *O processo eletrônico,* p. 81.

208LUCCA, Newton da. *Títulos e contratos eletrônicos,* p. 61.

10. A NECESSÁRIA INTEGRAÇÃO DO PODER JUDICIÁRIO

A integração entre os sistemas dos diversos órgãos jurisdicionais mostra-se condição da plena operabilidade do peticionamento eletrônico, bem como requisito para a viabilização de algumas de suas maiores vantagens.

Ocorre que, conforme analisa Cerdeira[209], os tribunais brasileiros, com fundamento na autonomia que lhes é dedicada, têm se informatizado sem o adequado planejamento, resultando em protocolos de comunicação incompatíveis. Em que pese a semelhança entre as informações de um e de outro tribunal, cada um as trata com programas de computador diferenciados, sem que tivesse havido ao menos o estabelecimento de um padrão de intercomunicação de dados. E a importância desse padrão não é menor, já que, como é cediço, também na informática há normas de caráter técnico a permitir compatibilidade de equipamentos e informações. A grande rede mundial é notório exemplo do que se pode conseguir com diretivas comuns para o intercâmbio de informação.

No que se refere aos tribunais, a criação do Conselho Nacional de Justiça, competente para definir normas de caráter geral para a serem seguidas por eles, pode reverter esse quadro.

As vantagens de um protocolo de comunicação comum seriam da maior relevância: pesquisas de dados tornar-se-iam possíveis no âmbito de todos os tribunais, com reflexos no controle da prestação jurisdicional e na efetiva aplicação das decisões (na esfera penal, por exemplo, condenações produziriam resultados em todos os Estados da Federação). Na remessa de autos de um órgão jurisdicional a outro, não seria necessário qualquer recadastramento de informações, abrindo-se ainda a possibilidade de remeterem-se autos integralmente virtuais por meio do chamado “malote digital”. Não menos relevantes seriam os benefícios da integração do Poder Judiciário com outros órgãos, como a Receita Federal e cartórios extrajudiciais.

A semente dessa comunhão de informações já se vislumbra no convênio Bacenjud, entre o Banco Central do Brasil e o Poder Judiciário, permitindo ao primeiro a imediata constrição judicial de numerário (“penhora online”) por meio da

209CERDEIRA, Pablo de Camargo. *Informatização dos sistemas jurídicos e os protocolos de informação.*

internet[210].

Nesse tocante, destaca-se o projeto da Rede Informática do Poder Judiciário – Infojus –, que busca a interligação de todas as unidades e instâncias do Poder Judiciário no Brasil. Este projeto, em razão do qual o Supremo Tribunal Federal instituiu Comissão Interdisciplinar, por meio da Portaria nº 156/2000[211], poderá servir de estrutura para a implantação de meta ainda mais ousada, que seria a rede de comunicação internacional da Justiça, atualmente denominada de Iudicis[212].

Como um dos pilares da integração almejada, ter-se-ia ainda o Sistema Nacional de Integração das Bases de Dados da Justiça Federal e do Superior Tribunal de Justiça. Dentre seus benefícios de grande destaque a serem implantados, cita-se a compilação de dados processuais relevantes em uma única base, propiciando importantes avanços na utilização do Rol Nacional dos Culpados e na verificação de distribuição de processos[213].

Menke anota que qualquer infra-estrutura que pretenda atingir a coletividade deve ser fundada na interoperabilidade, devendo ser possível a comunicação entre os diversos equipamentos envolvidos; nesse sentido, o modelo adotado pela Medida Provisória nº 2.200/2001 – idêntico ao da Alemanha e ao de outros países – seria apropriado em termos de interoperabilidade, por se basear em um tronco comum a sua normatização. Preleciona ainda o autor que, no caso de uma infra-estrutura de chaves públicas, para que seus usuários sintam a confiança necessária no sistema, normas e padrões compatíveis devem ser estabelecidos. A neutralidade tecnológica, vista por alguns como inafastável, deve ser vista com cautela, pois do contrário pode ser um desserviço aos sistemas de determinação de autoria dos documentos eletrônicos. Nessa seara, destaca Menke que pouca atenção tem sido dispensada no Brasil à necessidade de reassinatura, após um certo período, de documentos eletrônicos arquivados por longo tempo, uma vez que o passar dos anos pode tornar ineficazes as técnicas criptográficas neles aplicadas,

---

210CERDEIRA, Pablo de Camargo. *Informatização dos sistemas jurídicos e os protocolos de informação.*

211PORTA, Marcos de Lima. *A importância da internet na justiça,* p. 368.

212LIMA, George Marmelstein. *e-Processo.*

213BASTOS, Roberta. *Integração tecnológica do Poder Judiciário é tema de encontro realizado no STJ.*

descartando sua aptidão como prova[214].

Finalmente, calha destacar a título de exemplo que, buscando a interoperabilidade, com fundamento na plataforma de dados do Sistema “Justiça Moderna”, do Tribunal de Justiça do Distrito Federal, este tribunal, bem como os de Mato Grosso, Goiás, Mato Grosso do Sul, Maranhão e Tocantins teriam firmado convênio de integração de dados informáticos[215].

214MENKE, Fabiano. *Considerações sobre a interoperabilidade aplicada à infra-estrutura de chaves públicas.*

215*Tribunais firmam convênio de integração de informática.*

11. PROJETOS DE LEI EM ANDAMENTO

11.1 PROJETO DE LEI DA OAB

Por iniciativa da Ordem dos Advogados do Brasil – Seção de São Paulo, surgiu o Projeto de Lei nº 1.589/1999, da Câmara dos Deputados, que caracteriza como documento eletrônico aquele assinado digitalmente com certificação baseada em chave pública. Estabelece, ainda, a presunção de veracidade em relação ao signatário quanto às declarações contidas no documento eletrônico, equiparando-o assim ao regulado pelo art. 368 do Código de Processo Civil, como afirma Greco[216]. A certificação da chave pública, para os mencionados efeitos, deverá ser realizada por tabelião nos termos do projeto, que ainda trata de autoridades certificadoras em outros países, aceitando o valor de suas certificações se houver acordo internacional com o Brasil[217].

Parentoni observa que, ainda que as disposições do referido projeto coincidam de uma maneira geral com os da Medida Provisória nº 2.200/2001, no modelo de certificação digital diferem de modo cristalino. É que o art. 8º da medida provisória opta por um modelo misto, que confere tanto a cartórios como a empresas privadas delegadas a possibilidade de certificação de documentos eletrônicos, admitindo ainda a certificação fundada em certificados não governamentais, com empresas especializadas autenticando documentos, valendo-se de tecnologia própria. O Projeto de Lei nº 1.589/1999, no entanto, prefere o modelo de certificação pública[218], obrigando ao uso de certificados governamentais submetidos à ICP-Brasil e destinando aos particulares uma função secundária, descartando a presunção de validade de seus certificados[219].

A Medida Provisória nº 2.200/2001 seguiria opção mais vantajosa no entender do autor, uma vez que o consumidor pode escolher pelo certificado de sua conveniência. Prossegue Parentoni opinando que os cartórios seriam ineficientes e de serviços custosos, enquanto que as empresas certificadoras privadas com atuação internacional seriam estáveis, atenderiam a rigorosos padrões de

---

216No mesmo sentido: BLUM, Renato M.S. Opice. *O processo eletrônico,* p. 59.
217GRECO, Leonardo. *O processo eletrônico,* p. 90.
218Arts. 24 e 25 do projeto.
219PARENTONI, Leonardo Netto. *A regulamentação legal do documento eletrônico no Brasil.*

segurança, teriam preços mais contidos – em razão da concorrência internacional – e permitiriam a compatibilidade da ICP-Brasil com padrões globais. Nesse sentido, o art. 236 da Constituição Federal, que trata dos serviços notariais e de registro, não impediria a certificação por empresas internacionais, em conjunto com os tabeliães, como autoriza a Medida Provisória nº 2.200/2001[220].

11.2 O PROJETO DE LEI DA AJUFE

Em contraponto ao Projeto de Lei nº 1.589/1999, a Associação dos Juízes Federais – AJUFE apresentou, em 2001, outro projeto tratando da aplicação da informática ao processo, abordando o peticionamento eletrônico através do uso de senhas junto aos tribunais, com a dispensa de posterior apresentação de documentos em papel[221].

O referido projeto, que assumiu o número 5.828/2001 na Câmara dos Deputados, onde já foi aprovado, recebeu o nº 71/2002 no Senado Federal. Apesar das críticas por parte de alguns setores da OAB, há quem defenda que a proposta desta complementa o aludido projeto ao invés de enfrentá-lo[222].

Almeida Filho reserva críticas ao projeto em comento, que seria muito tímido para uma efetiva implementação de processo virtual, não condizendo ainda com a realidade brasileira e sendo possivelmente inaplicável, eis que admite o processo eletrônico apenas parcialmente. Na sua ótica, aparentemente "o legislador pretende criar meios eletrônicos para a prática dos atos processuais e não um processo eletrônico do início ao fim"[223]. É de se reconhecer, porém, que há considerável avanço no projeto no que se refere ao peticionamento eletrônico, eis que prevê a obrigatoriedade de disponibilização de serviços para o recebimento de peças eletrônicas por parte das pessoas jurídicas de direito público – excetuados os municípios – e a obrigação de os órgãos do Poder Judiciário instituírem sistema de comunicação eletrônica[224].

220PARENTONI, Leonardo Netto. *A regulamentação legal do documento eletrônico no Brasil.*

221LIMA, George Marmelstein; FONSECA, Reynaldo Soares da *et al. Elementos para reforma do Código de Processo Civil.*

222LIMA, George Marmelstein; FONSECA, Reynaldo Soares da *et al. Elementos para reforma do Código de Processo Civil.*

223ALMEIDA FILHO, José Carlos de Araújo. *Processo civil eletrônico.*

224*Ellen Gracie entregará a Aldo Rebelo moção de apoio ao processo judicial virtual.*

12. CONSIDERAÇÕES FINAIS

A virtualização do processo é um fato. Apoiada na criptografia de dados, que agora permite a elaboração de documentos eletrônicos seguros, anuncia que dominará o processo brasileiro rapidamente, esteja regulada de modo específico pelo direito ou não. Caberá, portanto, ao sistema normativo a tarefa de recepcioná-la. Em igual sentido ensina Maximiliano[225], afirmando que

> o Direito não pode isolar-se do ambiente em que vigora, deixar de atender às outras manifestações da vida social e econômica; e esta não há que de corresponder imutavelmente às regras formuladas pelos legisladores. Se as normas positivas se não alteram à proporção que evolve a coletividade, consciente ou inconscientemente a magistratura adapta o texto preciso às condições emergentes e imprevistas.[226]

A discussão sobre a aplicação de meios eletrônicos no processo deve ser imperiosamente ágil, pois enquanto se ponderam seus benefícios e prejuízos, sua implementação cresce assustadoramente, com profundas mudanças em curso. Como asseverou Marinoni, a digitalização dos processos "virá num piscar de olhos. Os processualistas não estão preparados. Os tribunais não estão preparados. Os juízes não estão preparados. Os advogados não estão preparados. E quem está?"[227].

É certo que, em grande parte, a idéia que se tem da internet como um ambiente sem lei em muito se relaciona com a ausência de debates jurídicos sobre o tema. Não que se pretenda alegar a segurança absoluta com o uso da rede – o que seria certamente utópico em qualquer meio lastrado no relacionamento humano – mas, como se viu, a comunicação eletrônica pode ser extremamente vulnerável ou extremamente segura, sendo essa mutação efeito do uso da criptografia. A consciência coletiva, no entanto, associa essa espécie de comunicação mais à primeira característica, talvez por desconhecimento[228].

Como bem afirma Cunha, o caminho mais provável para a resistência

---

225MAXIMILIANO, Carlos. *Hermenêutica na aplicação do direito,* p. 129.

226LIMA NETO, José Henrique Barbosa Moreira. *Aspectos jurídicos do documento eletrônico.*

227MARINONI, Luiz Guilherme. *O custo e o tempo do processo civil brasileiro.*

228O senso comum desconsidera também que, havendo a prática de ilícitos virtuais, a autoria poderá ser determinada por peritos especializados em provas digitais, que no Brasil ainda não são muitos: BLUM, Renato M.S. Opice. *O processo eletrônico,* p. 36.

coletiva contra os meios eletrônicos será o de ser suplantada pela eficácia destes[229]. Afinal, as empresas do setor privado em muito já se beneficiaram da aplicação da tecnologia – que adotaram maciçamente –, assim como em parte o mundo jurídico também já o faz.

No que se refere à ICP-Brasil, mais precisamente, só o tempo dirá se seus certificados serão aceitos pelo mercado ou se este se autoregulamentará.

Com fundamento na ICP-Brasil ou não, acredita-se que, demonstradas as vantagens do processo eletrônico, tornando seus resultados visíveis aos Três Poderes e a todos os profissionais do direito, bem como fazendo uma transição prudente e gradual de modo a permitir que os atores processuais possam absorver as complexidades das inovações tecnológicas, aberto estará o caminho para a virtualização completa do processo no país, com condições de aumentar a celeridade e a acessibilidade da prestação da tutela jurisdicional.

Disso resultará um maior acesso à Justiça, acompanhado de menores custos, de modo que causas de montas menores poderão ter sua viabilidade reforçada. Por outro lado, a redução de atos burocráticos permitirá melhor aproveitamento de pessoal, aliado à maior velocidade dos expedientes ordinatórios.

Confirmando-se a menor morosidade processual em todos os setores, vislumbra-se até mesmo um maior crescimento econômico do país, fundado em taxas de juros mais atraentes – decorrentes de uma prestação jurisdicional mais eficiente. Resta o desafio de regular os atos processuais por meio eletrônico e de ensinar os profissionais do direito a utilizar tais tecnologias da melhor maneira possível.

À guisa de conclusão, se os computadores permitem à humanidade alçar novos vôos, muitas vezes – feliz ou infelizmente – como condição de sustentabilidade das rotinas que esta pôs em prática, não se pode olvidar a lição de Cabral, segundo quem “os computadores somente processam dados. O poder do conhecimento, da informação, da criação, é privativo dos seres humanos. (...) E são estes mesmos homens que usam sua razão também para fins torpes e ilícitos”[230].

229CUNHA, Vagner Bispo da. *A intimação por correio eletrônico e as questões controvertidas.*
230CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas*, p. 131.

REFERÊNCIAS

Advogados do Sul podem pagar pela Internet as custas processuais do TRF e da Justiça Federal. In: Tribunal Regional Federal da 4ª Região. Disponível em <http://www.trf4.gov.br/trf4/noticias/ noticia_final.php?id=1822>. Acesso em 19 mar. 2006.

ALMEIDA FILHO, José Carlos de Araújo. *Processo civil eletrônico.* Disponível em <http://www.processoeletronico.com.br>. Acesso em 21 ago. 2006.

ALMEIDA FILHO, José Carlos de Araújo e CASTRO, Aldemario Araujo. *Manual de informática jurídica e direito da informática.* Rio de Janeiro: Editora Forense, 2005.

ALVIM, José Eduardo Carreira. *Alterações do código de processo civil.* 2. ed. Rio de Janeiro: Impetus, 2006.

ATHENIENSE, Alexandre Rodrigues. *Da validade legal dos atos processuais praticados pelo meio eletrônico.* In: O direito e as novas tecnologias. Disponível em <http://atheniense.blogs.com/dnt/informtica_jurdica/index.html>. Acesso em 25 abr. 2006.

BLUM, Renato M.S. Opice. *O processo eletrônico:* assinaturas, provas, documentos e instrumentos digitais. In: BLUM, Renato M.S. Opice (Coord.) e outros. Direito eletrônico – a internet e os tribunais. Bauru, SP: EDIPRO, 2001.

BRASIL, Angela Bittencourt. *Assinatura digital não é assinatura formal.* Jus Navigandi, Teresina, ano 5, n. 48, dez. 2000. Disponível em: <http://jus2.uol.com.br/doutrina/ texto.asp?id=1783>. Acesso em: 21 jun. 2006.

CABRAL, Antonio do Passo. *A eficácia probatória das mensagens eletrônicas.* In: Revista de Processo, ano 31, n. 135, maio de 2006. São Paulo: Revista dos Tribunais, 2006.

CARVALHO, Ivan Lira de. *Os Juizados Especiais Federais e as comunicações processuais eletrônicas.* Aspectos da Lei nº 10.259/2001. Jus Navigandi, Teresina, ano 6, n. 53, jan. 2002. Disponível em: <http://jus2.uol.com.br/doutrina/ texto.asp?id=2501>. Acesso em: 23 ago. 2006.

CERDEIRA, Pablo de Camargo. *Informatização dos sistemas jurídicos e os protocolos de informação.* In: Âmbito Jurídico, Rio Grande, 23, 30/11/2005. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link= revista_artigos_leitura&artigo_id=270>. Acesso em 24 ago. 2006.

CUNHA, Vagner Bispo da. *A intimação por correio eletrônico e as questões controvertidas.* Disponível em: <http://www.uj.com.br/publicacoes/doutrinas/ default.asp? action=doutrina&iddoutrina=2288>. Acesso em: 22 jul. 2006.

Ellen Gracie entregará a Aldo Rebelo moção de apoio ao processo judicial virtual. In: Supremo Tribunal Federal. Disponível em <http://www.stf.gov.br/noticias/imprensa/ultimas/ler.asp?CODIGO= 190248&tip=UN>. Acesso em 24 jul. 2006.

FAGÚNDEZ, Paulo Roney Ávila. *A virtualidade.* In: ROVER, Aires José (Org.). Direito e informática. Barueri, São Paulo: Manole, 2004.

GRECO, Leonardo. *O processo eletrônico.* In: GRECO, Marco Aurelio; MARTINS, Ives Gandra da Silva (Coord.). Direito e internet – relações jurídicas na sociedade informatizada. São Paulo: Revista dos Tribunais, 2001.

GUEDES, Jefferson Carús. *Comunicação processual eletrônica na Lei dos Juizados Especiais Federais.* In: Busca Legis. Disponível em <http://www.buscalegis.ufsc.br/arquivos/hsr424.htm>. Acesso em 21 jul. 2006.

ICP Brasil. Disponível em <http://www.icpbrasil.gov.br>. Acesso em 20 mai. 2006.

KAMINSKI, Omar e VOLPI, Marlon Marcelo. *A evolução da certificação digital no Brasil.* In: BLUM, Renato M.S. Opice (Coord.) e outros. Direito eletrônico – a internet e os tribunais. Bauru, SP: EDIPRO, 2001.

LIMA, George Marmelstein. *e-Processo:* uma verdadeira revolução procedimental. Jus Navigandi, Teresina, ano 7, n. 64, abr. 2003. Disponível em: <http://jus2.uol.com.br/ doutrina/texto.asp?id=3924>. Acesso em: 18 mai. 2006.

LIMA, George Marmelstein; FONSECA, Reynaldo Soares da *et al. Elementos para reforma do código de processo civil.* Sugestões dos juízes federais. Jus Navigandi, Teresina, ano 8, n. 186, 8 jan. 2004. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=4664>. Acesso em: 29 jul. 2006.

LIMA NETO, José Henrique Barbosa Moreira. *Aspectos jurídicos do documento eletrônico.* Jus Navigandi, Teresina, ano 2, n. 25, jun. 1998. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1780>. Acesso em: 17 ago. 2006.

LUCCA, Newton de. *Títulos e contratos eletrônicos:* o advento da informática e suas conseqüências para a pesquisa jurídica. In: LUCCA, Newton de e SIMÃO FILHO, Adalberto. Direito & internet – aspectos jurídicos relevantes. 2. ed. São Paulo: Quartier Latin, 2005.

MARCACINI, Augusto Tavares Rosa. *Direito e informática:* uma abordagem jurídica sobre criptografia. Forense, Rio de Janeiro, 2002.

MARINONI, Luiz Guilherme. *O custo e o tempo do processo civil brasileiro.* Disponível em: <http://www.professormarinoni.com.br/admin/users/05.pdf>. Acesso em: 22 jul. 2006.

MAXIMILIANO, Carlos. *Hermenêutica e aplicação do direito.* 19. ed. Rio de Janeiro:

Forense, 2002.

MENKE, Fabiano. *Considerações sobre a interoperabilidade aplicada à infra-estrutura de chaves públicas.* Disponível em <http://iti.br/twiki/pub/Forum/ArtigoB01/ b01-menke.rtf>. Acesso em 20 ago. 2006.

NERY, Fernando Loschiavo. *A virtualização dos processos judiciais (e-proc) e a dispensabilidade de autenticação documental por tabelião.* Uma análise prognóstica de suas implicações no cenário jurídico moderno. Jus Navigandi, Teresina, ano 8, n. 215, 6 fev. 2004. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=4795>. Acesso em: 22 ago. 2006.

OAB anuncia lançamento de certificação digital para advogados. In: Ordem dos Advogados do Brasil – Conselho Federal. Disponível em <http://www.oab.org.br/ noticia.asp?id=7719>. Acesso em 30 ago. 2006.

OAB defende uso da certificação digital contra as fraudes. In: Ordem dos Advogados do Brasil – Conselho Federal. Disponível em <http://www.oab.org.br/ noticia.asp?id=6428>. Acesso em 15 jun. 2006.

OLIVEIRA, Bruno Augusto Santos. *Juizado virtual:* o deslocamento do centro de gravidade ontológico do processo-papel para a problemática da eficiência da justiça. Jus Navigandi, Teresina, ano 8, n. 464, 14 out. 2004. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=5812>. Acesso em: 24 mai. 2006.

PAIVA, Mário Antônio Lobato de. *Peticionamento eletrônico.* Jus Navigandi, Teresina, ano 8, n. 122, 4 nov. 2003. Disponível em: <http://jus2.uol.com.br/ doutrina/texto.asp? id=4353>. Acesso em: 25 jul. 2006.

PARENTONI, Leonardo Netto. *A regulamentação legal do documento eletrônico no Brasil.* Jus Navigandi, Teresina, ano 9, n. 772, 14 ago. 2005. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=7154>. Acesso em: 21 ago. 2006.

Processo eletrônico. In: Tribunal Regional Federal da 4ª Região. Disponível em: <http://www.trf4.gov.br/trf4/institucional/ institucional.php?no=164>. Acesso em 19 ago. 2006.

RÊGO, Paulo Roberto de Carvalho. *O Registro de Títulos e Documentos:* um instrumento jurídico para segurança da sociedade. Histórico, desenvolvimento e a era digital. Jus Navigandi, Teresina, ano 7, n. 60, nov. 2002. Disponível em: <http://jus2.uol.com.br/ doutrina/texto.asp?id=3382>. Acesso em: 22 abr. 2006.

REZENDE, Pedro Antônio Dourado de. *Sistema de Pagamento Brasileiro e ICP - Brasil.* Jus Navigandi, Teresina, ano 6, n. 56, abr. 2002. Disponível em: <http://jus2.uol.com.br/ doutrina/texto.asp?id=2845>. Acesso em: 23 jul. 2006.

SILVA, João Carlos Pestana de Aguiar. As provas no cível. Rio de Janeiro: Forense,

2003.

Sistema Público de Escrituração Digital. Disponível em <http://www.receita.fazenda.gov.br/Sped/Default.htm>. Acesso em 20 ago. 2006.

VOLPI NETO, Angelo. *Ata notarial de documentos eletrônicos.* Disponível em <http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=3132>. Acesso em 05 jun. 2006.

WAMBIER, Luiz Rodrigues; WAMBIER, Teresa Arruda Alvim; MEDINA, José Miguel Garcia. *Breves comentários à nova sistemática processual civil, II:* Leis 11.187/2005, 11.232/2005, 11.276/2006, 11.277/2006 e 11.280/2006. São Paulo: Revista dos Tribunais, 2006.