

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE NACIONAL DE DIREITO

A ASSINATURA DIGITAL NO DIREITO BRASILEIRO

GUILHERME DIEGUES MONTEIRO

RIO DE JANEIRO

2008

GUILHERME DIEGUES MONTEIRO

A ASSINATURA DIGITAL NO DIREITO BRASILEIRO

**Trabalho de conclusão de curso
apresentado à Faculdade de Direito da
Universidade Federal do Rio de Janeiro,
como requisito parcial para obtenção do
título de Bacharel em Direito.**

Orientadora: Prof.^a Ms. Cíntia Muniz de Souza

RIO DE JANEIRO

2008

Monteiro, Guilherme Diegues.

A assinatura digital no direito brasileiro / Guilherme Diegues Monteiro. – 2008.

82 f.

Orientadora: Cíntia Muniz de Souza.

Monografia (graduação em Direito) – Universidade Federal do Rio de Janeiro, Centro de Ciências Jurídicas e Econômicas, Faculdade de Direito.

Bibliografia: f. 61 - 62.

1. Requisitos do ato jurídico - Monografias. I. Souza, Cíntia Muniz de. II. Universidade Federal do Rio de Janeiro. Centro de Ciências Jurídicas e Econômicas. Faculdade de Direito. III. Título.

CDD 343.231

GUILHERME DIEGUES MONTEIRO

TÍTULO DO TRABALHO: A ASSINATURA DIGITAL NO DIREITO BRASILEIRO

**Trabalho de conclusão de curso
apresentado à Faculdade de Direito da
Universidade Federal do Rio de Janeiro,
como requisito parcial para obtenção do
título de Bacharel em Direito.**

Data de aprovação: 25 de novembro de 2008.

Banca Examinadora:

Cíntia Muniz de Souza – Orientadora e Presidente da Banca Examinadora
Prof.^a Ms. da Faculdade Nacional de Direito - UFRJ

Fábio Wanderley
Prof. Ms. da Faculdade Nacional de Direito - UFRJ

Vera Maria Smid Paes de Barros
Prof.^a Ms. da Faculdade Nacional de Direito - UFRJ

RESUMO

MONTEIRO, G. D. **A assinatura digital no direito brasileiro**. 2008. 82 f. Monografia (Graduação em Direito) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2008.

Este trabalho analisa questões relevantes acerca da assinatura digital no direito brasileiro. Para a compreensão do tema o trabalho está dividido em três partes. A primeira parte explica os conceitos envolvidos no tema, assim como, princípios utilizados pela matéria. A segunda parte expõe a legislação nacional promulgada que conferiu segurança jurídica ao uso das assinaturas digitais no Brasil, esclarecendo também, a Infra-estrutura de Chaves Públicas Brasileira criada. Por fim, a terceira parte do trabalho expõe a atual situação jurídica da assinatura digital no Brasil, descrevendo os diversos usos que a assinatura digital vem tendo, tanto em âmbito governamental, em suas três esferas, dando ênfase ao processo eletrônico e seus diversos sistemas implantados, assim como, na sociedade civil.

Palavras Chave: Assinatura digital, Medida Provisória 2.200-2/01, ICP-Brasil, documento eletrônico, processo eletrônico.

ABSTRACT

MONTEIRO, G. D. **The digital signature in the brazilian law**. 2008. 82 p. Monograph (Law Graduate) – Federal University of Rio de Janeiro, Rio de Janeiro, 2008.

This work analyses relevant matters about the digital signature in the brazilian law. For the comprehension of the theme this work is divided in three parts. The first part explains the concepts involved in the theme, and also the principles used by the field. The second part exposes the national legislation promulgated that gave legal security to the use of the digital signature in Brazil, showing also the brazilian Public Key Infrastructure criated. At last, the third part of this work exposes the current legal situation of the digital signature in Brazil, describing the several uses that has been given to the digital signature, both under governmental, in his three spheres, giving emphasis to the eletronic suit and his several implanted systems, as also, in the civil society.

Keywords: Digital signature, MP2.200-2/01, Brazil-PKI, eletronic document, eletronic suit.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho tem como objetivo apresentar uma análise sobre o modelo brasileiro de assinatura digital. Para tanto, serão apresentados os conceitos técnicos básicos envolvidos, a tecnologia utilizada, a legislação promulgada, jurisprudência acerca do tema e uma breve introdução ao modelo internacional.

A *internet* alterou sensivelmente o mundo em que vivemos. Desde as relações pessoais às financeiras, caminhamos para uma imersão profunda de nossas vidas na grande rede. Já são vastas as possibilidades oferecidas por esse incrível mecanismo de comunicação, porém, serão ainda mais notáveis os avanços sociais ao se incorporar a *internet* de maneira segura e eficaz à sociedade.

Como cediço, o direito persegue a realidade, no caso em tela não se foge a essa regra. No entanto, é desleal esse encaicho, já que o direito caminha vagarosamente, tendo como lastro um penoso processo legislativo, enquanto a *internet* voa à velocidade da luz. Urge a necessidade de estudos sobre o tema que fundamentem, dessa forma, um processo legislativo mais célere e preciso nessa matéria, afinal, a questão já não é mais se devemos, mas sim como devemos utilizar a *internet* em benefício do Direito.

A assinatura digital sana um dos maiores problemas da comunicação eletrônica, a **confiabilidade**. O mecanismo cria uma “identidade virtual” confiável para as pessoas, possibilitando a segura identificação dos usuários na *internet*.

Seu uso garante tanto a autenticidade como a integridade de documentos eletrônicos. Dessa forma, a assinatura digital vem, enfim, possibilitar o efetivo e seguro ingresso do Direito no meio eletrônico, revolucionando a sociedade em que vivemos.

Percebendo essas oportunidades, o Brasil já deu seus primeiros passos na implementação dessa incrível ferramenta. Foi criada a Infra-Estrutura de Chaves Públicas Brasileira, ICP-Brasil, tendo a mesma a adesão a cada dia de mais setores da sociedade.

Por meio do estudo da doutrina acerca do tema, sendo boa parte dela encontrada inclusive na própria Internet, da pesquisa da legislação federal de regulamentação da assinatura digital e da pesquisa de jurisprudência de relevantes tribunais superiores pátrios

(STF, STJ e TST), realizaremos uma exposição do modelo criado no Brasil para regulamentação do uso da assinatura digital, assim como analisaremos em traços gerais o atual patamar do uso desse mecanismo em nosso direito.

Para tanto, o trabalho foi dividido em três seções. A primeira apresenta os conceitos técnicos básicos sobre o tema, demonstrando os mecanismos tecnológicos envolvidos no uso das assinaturas eletrônicas, assim como, a lei modelo internacional proposta pela Organização das Nações Unidas e seus princípios reconhecidos. A segunda seção delimita o marco legal da assinatura digital no Brasil, analisando essa legislação de forma a apresentar seus dispositivos mais significativos. Continuando, temos a terceira seção que sintetiza como o Brasil está tratando o tema em diversas áreas de nossa sociedade, em âmbito estatal e civil.

Pelo exposto, demonstraremos que a assinatura digital já se encontra regulamentada pelo Direito brasileiro e seu uso está se disseminando tanto em âmbito governamental como na sociedade civil.

Esse mecanismo veio para revolucionar o modo como encaramos as relações eletrônicas e os benefícios que o direito pode extrair desses meios de comunicação. Diversas serão as vantagens trazidas pela incorporação da assinatura digital ao dia-a-dia jurídico, sendo notáveis os ganhos na administração da justiça brasileira.

2 CONCEITOS

Para entendermos o processo de certificação digital, que é o meio de assinarmos digitalmente um documento, precisamos compreender previamente alguns conceitos implícitos ao tema, como o algoritmo, a criptografia e a função *hash*.

2.1 Algoritmo

Um algoritmo é uma função matemática complexa que executa um conjunto de processos para efetuar um cálculo, ou seja, uma seqüência de instruções executada até que determinada condição se verifique. Em uma analogia poderíamos dizer que um algoritmo seria uma receita, os passos necessários para se realizar uma tarefa.

2.2 Criptografia simétrica x criptografia assimétrica

De origem grega, a palavra criptografia significa: “a arte de escrever em códigos de forma a esconder a informação em um texto incompreensível.”¹ Chamamos a informação codificada de texto cifrado. O procedimento de codificação é chamado de cifragem, sendo o procedimento inverso, ou seja, de obter a informação original a partir do texto cifrado, chamado de decifragem.

Atualmente existem dois tipos de criptografia: a simétrica e a assimétrica. A criptografia simétrica se utiliza de apenas uma chave para realizar a cifragem e a decifragem

¹ AULETE, Francisco; VALENTE, Antonio. Dicionário Aulete Digital. **Net**, nov. 2008. Disponível em: <<http://www.auletedigital.com.br>>. Acesso em: 10 set. 2008.

da informação por meio do algoritmo. Como a mesma chave deve ser utilizada na cifragem e na decifragem, todas as partes devem ter conhecimento da chave que cifra e decifra os dados.

Já a criptografia assimétrica utiliza algoritmos que trabalham com chaves duplas, ou seja, chaves distintas. Uma é a chave privada e a outra a chave pública, ambas geradas simultaneamente pelo algoritmo e relacionadas entre si; são um par de chaves. A operação executada por uma, só pode ser revertida pela outra. A chave privada é mantida em sigilo, só sendo conhecida pelo seu dono. Já a chave pública é de acesso geral, disponibilizada e tornada acessível a qualquer indivíduo que deseje se comunicar com o proprietário da chave privada correspondente.

2.3 Função de *hash*

A função de *hash* gera um resumo, ou seja, uma função de *hash* resume em uma linha de código um documento inteiro, por exemplo. Dessa forma, ganha-se muito em desempenho (velocidade e tempo) quando se utiliza uma função de *hash* na criptografia, pois, os algoritmos criptográficos são em geral complexos e lentos. Utiliza-se, então, a função de *hash* para resumir o documento e em seguida criptografa-se o resumo, ganhando-se tempo no processo de geração da assinatura digital.

2.4 Assinatura eletrônica x assinatura digital

Não se deve confundir a assinatura eletrônica com a assinatura digital. Enquanto a primeira se trata de um gênero, a segunda é uma de suas espécies. Assinatura eletrônica se refere a qualquer mecanismo de identificação do remetente de uma mensagem eletrônica, não sendo, necessariamente, aplicada a criptografia para tanto. Já a assinatura digital se trata da assinatura eletrônica feita por meio de um certificado digital, ou seja, utilizando-se a

criptografia assimétrica e garantido-se sua propriedade por meio de uma Infra-estrutura de Chaves Pública (ICP).

A assinatura digital é um mecanismo de proteção de dados que circulam na rede. Sua importância reside em permitir uma identificação inequívoca do criador de um documento eletrônico, assim como de garantir a integridade deste documento. Em termos práticos, é um código inserido em um documento eletrônico por meio da chave criptográfica pessoal. Com o par desta chave, a chave pública, de conhecimento geral, é possível checar a procedência e integridade deste documento.

Sendo assim, ao recebermos um documento digitalmente assinado, programas farão a checagem desta assinatura e informarão se ela é válida e se o documento foi alterado em algum momento.

Os programas de computador, a fim de checar uma assinatura digital realizam duas operações: calculam o *hash* do documento e decifram a assinatura com a chave pública do emitente. Obtendo-se sucesso na operação, a assinatura está correta, o que significa que foi gerada pela chave privada corresponde à chave pública utilizada na verificação e que o documento está íntegro. Se a chave pública não decifrar corretamente o documento, a assinatura está incorreta, o que significa que pode ter havido alterações no documento ou na assinatura.

A assinatura digital fornecerá, dessa forma, duas certezas: **autenticidade**, garantia da autoria em um documento ou identificação em uma transação; **integridade**, fidelidade do documento recebido em relação ao original enviado.

Ao termos sucesso na checagem de uma assinatura digital com uma chave pública, podemos afirmar com convicção que aquele documento foi gerado pelo detentor da chave privada correspondente, sendo assim **autêntico**. Além disso, também podemos afirmar que o documento não teve seu conteúdo alterado no caminho que percorreu, estando assim **íntegro**.

2.5 Certificado digital

O certificado digital é o documento eletrônico assinado digitalmente que dá validade à assinatura digital, isto é, ele associa uma pessoa ou entidade a uma chave pública.

A fim de se garantir a validade do certificado digital disponível na rede, ou seja, que ele realmente corresponde à pessoa, física ou jurídica, que se diz seu titular, surgiram as Autoridades Certificadoras (AC), que atestam a identidade do dono dessas chaves. Dessa forma, ao receber um documento assinado digitalmente podemos nos dirigir ao site da Autoridade Certificadora e obter o certificado digital correspondente à pessoa que o enviou. Este, além de conter os dados dessa pessoa também contém a chave pública a ser utilizada.

Um certificado digital contém, em geral, informações como o nome da pessoa ou da entidade a ser associada à chave pública, o período de validade do certificado, a chave pública a ser utilizada para checagem da assinatura digital, o nome e assinatura da entidade que assinou o certificado, seu número de série, o algoritmo utilizado, entre outras.

Em alguns países as autoridades certificadoras são pessoas jurídicas privadas, por essa razão, podem ser acreditadas ou não, conforme possuam aval de alguma autoridade governamental para prestarem esse serviço. No Brasil, como veremos, AC podem ser pessoas jurídicas privadas, no entanto, toda a ICP esta subordinada ao controle governamental sendo, dessa forma, toda a ICP acreditada.

O certificado digital possui um período de validade. Só é possível assinar um documento digitalmente com esse certificado enquanto ele é válido. Já a checagem dos documentos assinados digitalmente por esses certificados pode ser feita a qualquer tempo, mesmo após o certificado expirar.

Após a revogação ou expiração do certificado, todas as assinaturas realizadas com este certificado tornam-se inválidas, mas as assinaturas realizadas antes da revogação do certificado continuam válidas se houver uma forma de garantir que esta operação foi realizada durante o período de validade do certificado, como por exemplo com a técnica do carimbo de tempo que adiciona uma data e hora à assinatura, permitindo determinar quando o documento foi assinado.

O certificado digital pode ser revogado antes do período definido para expirar, nesse caso, ele deve ser incluído na Lista de Certificados Revogados (LCR) que é a pública. A publicação dessas listas se dá com a periodicidade que a AC definir, podendo essas listas ser consultadas a qualquer momento para se verificar se um certificado se encontra válido ou não.

A validade dos certificados reforça a cadeia de confiança, mantendo-a atualizada e renovando também o vínculo entre o usuário e a AC. Essa renovação é importante até mesmo para o caso de uma substituição da chave privada por uma outra tecnologicamente mais avançada ou devido a possíveis mudanças ocorridas nos dados do usuário. Essas alterações têm como objetivo tornar mais robusta e segura a cadeia.

2.6 UNCITRAL e princípios internacionais

A Comissão de Direito em Comércio Internacional das Nações Unidas (United Nations Commission on International Trade Law – UNCITRAL), formada em 1966, realizou desde então, inúmeros grupos de estudo de forma a possibilitar o comércio internacional de maneira mais segura. Como resultado desses grupos de estudo surge, em 1996, a lei modelo sobre comércio eletrônico², reeditada em 1998, com uma série de explicações destinadas inclusive ao corpo legislativo de países que queiram regular a matéria. Não obstante, em 2001 surge a lei modelo de assinatura eletrônica³, já prevista na lei modelo anterior. Essas duas previsões trouxeram a possibilidade de uma regulação mais uniforme em âmbito internacional.

O sucesso dos objetivos da UNCITRAL é comprovado pela aprovação de leis, baseadas nessas leis modelo em países como China, República da Coreia, participantes da comunidade da Grã Bretanha, Canadá e Estados Unidos (a nível estadual e federal).

² ORGANIZAÇÃO DAS NAÇÕES UNIDAS – UNCITRAL. Model Law on Electronic Commerce with Guide to Enactment, with additional article 5 bis as adopted in 1998. 1996. Disponível em: <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html> Acesso em: 03 nov. 2008.

³ ORGANIZAÇÃO DAS NAÇÕES UNIDAS – UNCITRAL. Model Law on Electronic Signatures with Guide to Enactment. 2001. Disponível em: <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html> Acesso em: 03 nov. 2008.

O êxito dessa iniciativa se deu, em sua maior parte, pelos princípios estabelecidos nestes documentos que, se adotados na formulação de ordenamentos locais, tornarão estes compatíveis mundialmente.

Dois são os princípios essenciais a serem observados pela matéria, são eles: **Neutralidade Tecnológica e Equivalência Funcional.**

2.6.1 Neutralidade tecnológica

Tendo em vista o respeito à liberdade das partes e governos para escolherem a tecnologia que melhor atenda aos seus interesses, bem como objetivando evitar sua defasagem com o surgimento de novas tecnologias, englobando todas as situações fáticas relacionadas, o princípio da neutralidade tecnológica visa evitar que a legislação restrinja a tecnologia utilizada nesses documentos eletrônicos, como a forma de armazenamento, a transmissão de dados e o mecanismo de segurança, por exemplo.

Na matéria aqui em questão, a segurança digital, apesar do aparente entendimento pacífico de que a neutralidade tecnológica é o melhor caminho⁴, alguns entendem não haver necessidade de se adotá-la. Argumenta-se que o temor em tornar-se obsoleta a tecnologia da assinatura digital é equivocado uma vez que se tem buscado, pelos últimos 2500 anos, descobrir a fórmula matemática que possibilitaria tornar a criptografia assimétrica obsoleta. Dessa maneira, deveria se optar unicamente pela criptografia assimétrica, por ser mais segura e a única a garantir, para ambas as partes, a segurança necessária, além das vantagens da tecnologia utilizada para a criptografia assimétrica já fazer parte do domínio público, ou seja, não haver custo adicional com licenciamento da patente de muitos dos programas utilizados.

Como veremos, em que pese essa tese, a legislação pátria vem, majoritariamente, seguindo o princípio da neutralidade tecnológica.

⁴ Foi o entendimento proferido no Congresso Internacional de Direito e Tecnologias da Informação, realizado nos dias 3 a 4 de Outubro de 2002, no auditório do STJ, Brasília-DF.

2.6.2 Equivalência funcional

Partindo da premissa de que as legislações das nações estabelecem como requisitos o “documento original”, a “assinatura manuscrita ou de próprio punho” e até mesmo o “papel”, esse princípio não tenta substituir esses elementos, mas simplesmente fazer com que os documentos eletrônicos preencham os mesmos requisitos e funcionalidades que os físicos. Assim, preenchendo os mesmos objetivos, os documentos eletrônicos e seus elementos, como a assinatura eletrônica e os dados armazenados digitalmente, poderão receber a mesma proteção legal conferida aos documentos clássicos.

Como ressalta Renato Opice Blum em seu manual:

O princípio da equivalência funcional é o principal argumento da tecnologia jurídica dos documentos virtuais. Por este conceito, o documento eletrônico cumpre as mesmas funções do documento em suporte papel e não pode ser rejeitado pelo simples fato de se encontrar em meio magnético ou eletrônico.⁵

Dessa forma, os países poderão aderir às leis modelo ou regular a matéria, sem necessitar alterar suas legislações nacionais. Tal fato torna viável a aplicação das leis modelo inclusive no Brasil, apesar da presença dos elementos citados em diversas leis nacionais como o Código Civil de 2002, por exemplo.

⁵ BLUM, Renato M. S. Opice. **Manual de Direito Eletrônico e Internet**. São Paulo: Aduaneiras, 2006. 54 p.

3 MARCO LEGAL DA CERTIFICAÇÃO DIGITAL NO BRASIL

3.1 Medida Provisória 2.200-2, de 24 de agosto de 2001⁶

No Brasil, em 24 de agosto de 2001, foi promulgada pelo então presidente da República Fernando Henrique Cardoso a Medida Provisória 2.200-2 (MP 2.200-2/01) que deu início à implantação do sistema nacional de certificação digital instituindo a **Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil)**. Analisemos, então, o disposto neste marco digital-legal nacional.

Primeiramente, como acima mencionado, logo em seu Art. 1º a MP 2.200-2/01 institui a ICP-Brasil e determina seus fins precípuos: “garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.”⁷

Em seguida, em seu Art. 2º, define a composição da ICP-Brasil que detém uma autoridade gestora de políticas, o Comitê Gestor (CG-ICP), e uma cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz (AC-Raiz), Autoridades Certificadoras (AC) e Autoridades de Registro (AR). Trata-se de uma estrutura hierárquica em forma de pirâmide onde a Autoridade Certificadora Raiz se encontra em seu topo, abaixo dela se encontram as Autoridades Certificadoras e em nível subalterno a estas as Autoridades de Registro.

Podemos então resumir a ICP-Brasil como um conjunto de entidades, padrões técnicos e regulamentos, elaborados para suportar um sistema criptográfico com base em certificados digitais, com a finalidade de assegurar maior segurança nas transações eletrônicas e incentivar a utilização da Internet como meio para a realização de negócios e atos jurídicos.

Em seu Art. 12 a MP 2.200-2/01 transforma o Instituto Nacional de Tecnologia da Informação (ITI) em autarquia federal vinculada ao Ministério da Ciência e Tecnologia,

⁶ Anexo – Texto Integral da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

⁷ BRASIL. Medida provisória nº 2.200-2, de 24 de agosto de 2001. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 27 AGO. 2001.

determinando logo em seguida, como disposto no Art. 13, que o ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira. Sendo assim, a supramencionada estrutura piramidal da ICP-Brasil tem em seu ápice o ITI, como AC Raiz.

Vale ressaltar, que a MP 2.200-2/01 em seu Art. 8º prevê a possibilidade de atuarem como AC e AR tanto os órgãos e as entidades públicos como as pessoas jurídicas de direito privado. Ou seja, somente há previsão da AC Raiz ser especificamente o ITI, de resto, a MP 2.200-2/01 abre espaço para qualquer empresa ou órgão, público ou privado participar da cadeia, se em conformidade com os critérios estabelecidos pelo Comitê Gestor da ICP-Brasil.

Pelo exposto, podemos notar que adotamos um modelo onde o governo brasileiro por meio de uma autarquia federal, o Instituto Nacional de Tecnologia da Informação, realiza a função de Autoridade Certificadora Raiz, gerando toda uma estrutura de confiabilidade à cadeia que vem abaixo do ITI.

Em relação ao tema aqui abordado, é de suma importância citarmos o teor constante do Art. 10 §1º da MP 2.200-2/01, afinal, é onde se encontra a fundamentação de confiabilidade de toda a cadeia de certificação digital brasileira, isso por que, este artigo confere **presunção de veracidade** aos documentos eletrônicos assinados digitalmente, ou seja, aos documentos eletrônicos gerados fazendo-se uso de certificados emitidos pela ICP-Brasil. Dessa forma, este artigo tornou a assinatura digital um instrumento válido juridicamente no Brasil.

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.⁸

Este artigo denota a adoção do supracitado princípio da **equivalência funcional**, igualando os documentos eletrônicos aos documentos em papel, suprimindo a lacuna legislativa que faltava para tornar esses documentos, e os atos jurídicos deles derivados, válidos e aceitos juridicamente no Brasil.

Também de amplo relevo é o disposto no §2º do Art. 10 que vem para observar o segundo princípio internacionalmente aceito para o tema, a **neutralidade tecnológica**,

⁸ BRASIL. Medida provisória nº 2.200-2, de 24 de agosto de 2001. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 27 AGO. 2001.

acalmando as críticas dos partidários às ICP independentes do controle direto do governo, como acontece em outros países. Esse parágrafo abre espaço para a utilização de qualquer meio de comprovação de autoria e integridade de documentos eletrônicos, no entanto, não os embute da mencionada presunção de veracidade.

§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.⁹

Dessa forma, a lei prevê a possibilidade de técnicas alternativas de comprovação de autoria ou o uso da própria técnica de assinatura digital, porém, em cadeia de certificação não garantida pela ICP-Brasil, mas ressalta alguns pontos a serem observados. Note-se que essas técnicas devem ser previamente estipuladas e conhecidas, sendo aceitas pelas partes, ou, devem ser aceitas pelas pessoas a quem forem opostos esses documentos eletrônicos.

Assim, o uso de outras técnicas ou até mesmo da certificação digital, porém, não garantida pela ICP-Brasil, é legalmente previsto no Brasil, sendo juridicamente válido. O que são diversas são as qualidades atribuídas a documentos eletrônicos assinados eletronicamente utilizando-se ou não a ICP-Brasil. Enquanto na ICP-Brasil esses documentos gozam da presunção de veracidade, externamente a ela os métodos utilizados para tanto precisam ser acreditados pelas partes.

Ressalte-se que o exposto não vincula apenas as partes envolvidas no ato jurídico. Com a promulgação da MP 2.200-2/01 não pode a Administração Pública negar o reconhecimento de documento eletrônico assinado digitalmente, tanto no executivo, no legislativo ou judiciário. Como veremos adiante, é exatamente por esse caminho que nossa Administração Pública está seguindo já que a cada dia mais órgãos dos três poderes aderem ao uso e criam regras para regular o trâmite de documentos eletrônicos digitalmente assinados.

Paralelamente, além do seu uso na sociedade civil e aceitação da Administração Pública desses atos jurídicos, está a própria incorporação desta magnífica ferramenta a esses órgãos estatais, agilizando sobremaneira a burocracia que macula nossa enferrujada máquina

⁹ BRASIL. Medida provisória nº 2.200-2, de 24 de agosto de 2001. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 27 AGO. 2001.

estatal, de forma segura e confiável, possibilitando inclusive a implementação de um e-Gov¹⁰ eficaz.

Podemos, pelo exposto, dizer que a MP 2.200-2/01 foi um marco regulatório no ordenamento jurídico brasileiro já que fundou as bases da ICP-Brasil, sistema que, como veremos adiante, expande sua abrangência a cada dia nos mais diversos setores da nossa sociedade.

3.2 Comitê Gestor

Como acima salientado, o Comitê Gestor da ICP-Brasil (CG-ICP), possui grande relevância na cadeia. Ele atua como uma espécie de conselho deliberativo que tem por atribuição principal coordenar a implantação e o funcionamento da ICP-Brasil, definindo as normas técnicas a serem observadas pela mesma. Mediante a edição de resoluções que são previamente analisadas pela Comissão Técnica Executiva (COTEC), que assiste e dá suporte técnico ao órgão deliberativo, o CG-ICP regula a infra-estrutura.

As resoluções são aplicadas e cumpridas pela Autoridade Certificadora Raiz, que é o Instituto Nacional de Tecnologia da Informação, autarquia federal vinculada à Casa Civil da Presidência da República ao qual aprofundaremos análise mais adiante.

O detalhamento da estrutura e das competências do Comitê Gestor estão nos Arts. 3^o e 4^o da MP 2.200-2/01 além do recente decreto nº 6.605, de 14 de outubro de 2008. O Art. 3^o prevê a função, o vínculo à Casa Civil e a composição do mesmo:

Art. 3^o A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República,

¹⁰ Governo eletrônico, ou *e-gov*, do inglês *electronic government*, é uma tendência global. Governos de todo o mundo têm concentrado esforços no desenvolvimento de políticas e definições de padrões em termos de tecnologias da informação e comunicação, comumente chamadas de TICs, visando construir uma arquitetura interoperável a fim de munir os cidadãos com acesso a informações e serviços. De modo geral, aceita-se a noção de governo eletrônico como ligada à prestação de serviços públicos por meio eletrônico, ou seja, utilizando-se recursos de tecnologia da informação, em caráter remoto e disponível no sistema 24/7 ou seja, vinte e quatro horas por dia, sete dias por semana. Wikipédia. Disponível em: <http://pt.wikipedia.org/wiki/Governo_eletr%C3%B4nico> Acesso em: 27 out. 2008.

e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.¹¹

O disposto no artigo acima transcrito é repetido no Art. 20 do decreto nº 6.605/08. Pelo exposto, podemos perceber o caráter heterogêneo da composição do Comitê Gestor, o que lhe dá mais legitimidade e fundamentação para atuar. São de se observar dois aspectos relevantes neste artigo, primeiro, a presença da sociedade civil no Comitê, iniciativa louvável do legislador como forma de dar estabilidade, transparência e confiabilidade ao sistema. Em segundo, o § 10 do mesmo que prevê a que a coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República, permanecendo, dessa forma, o controle estatal sobre a cadeia.

O Art. 40 da MP 2.200-2/01 determina as competências do CG-ICP que podem ser resumidas em: I - coordenar a implantação e o funcionamento da ICP-Brasil; II - estabelecer os critérios e normas para o credenciamento e atuação das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil; III - estabelecer as regras operacionais da AC Raiz; IV - fiscalizar a AC Raiz; e VII - avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional.

O CG-ICP, como salientado, conta com uma Comissão Técnica Executiva, COTEC, a quem cabe assistir e dar suporte técnico ao mesmo, conforme especificado nos Arts. 4º e 5º do decreto nº 6.605/08, além de uma Secretaria Executiva cuja competência está especificada nos Arts. 6º e 7º do mesmo decreto.

Outras disposições sobre o Comitê Gestor e sobre a Comissão Técnica Executiva encontram-se no decreto nº 6.605, de 14 de outubro de 2008, nas Resoluções do Comitê Gestor da ICP-Brasil e nas Instruções Normativas e outros documentos.

¹¹ BRASIL. Medida provisória nº 2.200-2, de 24 de agosto de 2001. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 27 AGO. 2001.

3.3 Instituto Nacional de Tecnologia da Informação – AC Raiz

O Instituto Nacional de Tecnologia da Informação, ITI, foi transformado em uma autarquia federal vinculada à Casa Civil da Presidência da República, pela MP 2.200-2/01 em seu Art. 12. Seu objetivo é manter a Infra-Estrutura de Chaves Públicas Brasileira.

O ITI é a Autoridade Certificadora Raiz, AC Raiz, da Infra-Estrutura de Chaves Públicas Brasileira legitimado pelo Art. 13 da MP 2.200-2/01. Isso significa que o Brasil possui uma infra-estrutura pública, mantida e auditada por um órgão público, no caso, o Instituto Nacional de Tecnologia da Informação, que segue regras de funcionamento estabelecidas pelo CG-ICP.

Como tal é a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. O modelo de Infra-estrutura adotado pela ICP-Brasil foi o de certificado com raiz única.

Cabe ao ITI credenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos, como previsto no Art. 5^o da MP 2.200-2/01:

Art. 5^o 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 subsequente 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.
¹²

As principais atribuições do ITI são as de auditar, credenciar e fiscalizar as Autoridades Certificadoras que postularem o seu credenciamento na ICP-Brasil para fornecer

¹² BRASIL. Medida provisória nº 2.200-2, de 24 de agosto de 2001. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 27 AGO. 2001.

certificados digitais para os usuários finais. Cabe ressaltar, que por determinação da MP 2.200-2/01 em seu Art. 50 parágrafo único, como transcrito acima, o ITI não pode fornecer certificados digitais para os consumidores.

O processo de credenciamento perante o ITI consiste num procedimento complexo que prevê pormenorizada auditoria das instalações, rotinas, documentos e práticas das entidades candidatas. Em suma, se o interessado provar ter capacidade técnica e organizacional para emitir certificados e para gerenciar listas de certificados revogados, se garantir a segurança da integridade e segurança de suas instalações, e outros tantos requisitos previstos nas normas, ele será credenciado pelo ITI e passará a ter autorização para emitir certificados digitais com o atributo da presunção de que trata o parágrafo primeiro do Art. 10 §10 da MP 2.200-2/01.

Vale observar, que o credenciamento perante o Instituto Nacional de Tecnologia da Informação não é obrigatório para que as Autoridades Certificadoras possam emitir certificados digitais. Como salientado acima, o disposto no §20 da MP 2.200-2/01 prevê a possibilidade da utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Além disso, compete ao ITI estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital. Neste vetor, o ITI tem como sua principal linha de ação a popularização da certificação digital e a inclusão digital, atuando sobre questões como sistemas criptográficos, software livre, hardware compatíveis com padrões abertos e universais, convergência digital de mídias, entre outras.¹³

A AC é o principal componente de uma Infra-Estrutura de Chaves Públicas e é responsável pela emissão dos certificados digitais. O usuário de um certificado digital precisa confiar na AC. Sendo assim, para que sejam emitidos certificados, as AC devem estar de acordo com os deveres e obrigações descritos em um documento chamado de Declaração de Práticas de Certificação, DPC. A DPC é pública, permitindo que as pessoas saibam como foi emitido o certificado digital.

A atividade mais relevante de uma AC é a de emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Cabe também à AC emitir listas de certificados revogados,

¹³ Instituto Nacional de Tecnologia da Informação, **Net**. Disponível em: <www.iti.gov.br> Acesso em: 28 out. 2008.

LCR, e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação, DPC. As AC desempenham como função essencial a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves pública/privada. Na hierarquia dos Serviços de Certificação Pública, as AC estão subordinadas à Autoridade Certificadora de nível hierarquicamente superior.

Todas as instituições envolvidas nessa cadeia são fiscalizadas e auditadas, assim como, seus procedimentos, instalações técnicas, sistemas envolvidos no serviço de certificação, bem como seu próprio pessoal. A não concordância com as regras acarreta em aplicações de penalidades, que podem ser inclusive o descredenciamento da AC.

Na estrutura da ICP-Brasil, imediatamente abaixo das AC vem as AR. São as Autoridades de Registro, empresas que estarão em contato direto com o usuário final da cadeia, a pessoa que deseja um certificado digital para assinar digitalmente seus documentos.

A Autoridade de Registro é a ponta inferior da cadeia, recebendo as solicitações de emissão de certificados digitais. Uma das tarefas de grande relevância dentro de uma ICP, que é desempenhada pelas AR, é a de identificar, mediante a **presença física** do indivíduo, os interessados em adquirir certificados digitais. Com efeito, caso não sejam tomadas todas as diligências cabíveis como a exigência da presença física e a atenta conferência da documentação apresentada no ato da identificação, corre-se o risco de atribuir um certificado digital a indivíduo criminoso que queira se passar por outra pessoa ou que simplesmente utilize falsa identidade para praticar atos ilícitos no meio virtual, sendo, portanto, atividade de suma importância a realizada pelas AR.

4 ATUAL SITUAÇÃO JURÍDICA DA ASSINATURA DIGITAL NO BRASIL

Antes da edição da MP 2.200-2/01 apenas empresas diretamente ligadas ao setor da informática ou empresas que tivessem bens valiosos na forma digital, como empresas de tecnologia e bancos, se interessavam pelo uso da assinatura digital. O sistema era particular, com empresas privadas fornecendo o serviço de certificação digital. O uso de tal tecnologia era muito mais interno do que externo, ou seja, era um serviço contratado para gerar confiabilidade entre a comunicação e transmissão de dados na *intranet*¹⁴ de uma empresa.

Afora esses casos, estavam as relações entre particulares onde ambos conheciam e aceitavam o uso dessa ferramenta. No entanto, juridicamente, não existia previsão alguma da obrigatoriedade de aceitação de documentos identificados por uma assinatura digital, tanto na nossa legislação como em nossa jurisprudência, o que restringia muito a difusão desse instrumento.

Afinal, para que seja realmente interessante o uso de uma tecnologia como esta é necessária a aceitação universal de sua implantação. A assinatura digital precisa ser conhecida e utilizada universalmente, só assim ela surtirá seus melhores efeitos para a sociedade. E, ao me referir em seu uso universal, quero dizer que a minha assinatura digital precisa ser aceita nos Estados Unidos da América, ou seja, os diferentes sistemas de diferentes países precisam se regular de alguma forma a aceitar como válidas juridicamente suas assinaturas digitais.

O desafio é enorme nesse sentido, problemas sensíveis criam obstáculos gigantescos a serem transpostos pelos estudiosos no assunto. No entanto, acredito que o uso de um único sistema para todo o mundo é inviável pelas diferenças entre as nações, desde culturais até legais. Dessa forma, a saída pode ser a auto-regulamentação interna por cada país, seguindo princípios básicos que amoldariam esses diferentes sistemas a uma forma relativamente padronizada. Os tratados internacionais de mútuo reconhecimento desses sistemas resolveriam o resto do problema jurisdicional.

Se a utópica difusão desse utensílio ainda se encontra distante da realidade mundial, em âmbito nacional não podemos dizer o mesmo. Após a edição da MP 2.200-2/01 o uso da

¹⁴ Resumidamente, o conceito de intranet pode ser interpretado como "uma versão privada da Internet", ou uma mini-Internet confinada a uma organização. Wikipédia. Disponível em: <<http://pt.wikipedia.org/wiki/Intranet>> Acesso em: 29 out. 2008.

assinatura digital no Brasil tem se popularizado cada vez mais em todos os âmbitos da nossa sociedade. A sociedade civil, como percussora, trouxe à tona as possibilidades de seu uso e o nosso legislador, acompanhando a vanguarda do direito internacional, veio a regular o seu uso em nosso ordenamento jurídico.

Como salientado no capítulo anterior, a presunção de validade conferida às assinaturas digitais pela MP 2.200-2/01 vem possibilitando a difusão do uso das mesmas no Brasil. Com o advento da ICP-Brasil pessoas físicas e jurídicas sentem-se mais seguros para realizar seus negócios e a administração pública finalmente abraçou essa prática em suas três esferas.

Executivo, legislativo e judiciário tem se mostrado receptivos à idéia e tentado, em diferentes velocidades e formas, maximizar suas administrações se utilizando da mesma. Como veremos, já são muitos os exemplos de sucesso na implantação do uso de certificados digitais.

4.1 No poder executivo

O primeiro dos três poderes a incorporar a assinatura digital como ferramenta administrativa foi o executivo por meio do Decreto 3.587, de 5 de setembro de 2000, que instituiu a Infra-Estrutura de Chaves Públicas do Poder Executivo, denominada ICP-Gov. Podemos dizer que a ICP-Gov foi a origem remota da ICP-Brasil.

Este decreto objetivava a tramitação segura de documentos eletrônicos já que havia um processo de substituição dos documentos físicos por aqueles, previsto inclusive em artigo do decreto.

No entanto, de acordo com o próprio decreto, seu âmbito de incidência se restringia apenas ao poder executivo, mais especificamente a Administração Pública Federal. Em relação às autoridades certificadoras o decreto agia de forma semelhante à ICP-Brasil, ou seja, poderiam ser empresas privadas a prestar esse serviço, se de acordo com as diretrizes de um órgão de controle estatal.

Ou seja, o Decreto 3.587/00 foi o precursor da MP 2.200-2/01. Ele inspirou o legislador a ampliar nacionalmente a abrangência da ICP, criando a ICP-Brasil que vigora em todo o território nacional e para todas as pessoas que se interessarem a adquirir um certificado digital. Após a edição da MP 2.200-2/01 o Decreto 3.587/00 foi revogado e o poder executivo aderiu à ICP-Brasil.

Como vimos, a iniciativa do poder executivo em utilizar a certificação digital em seu itinerário já aconteceu antes mesmo da criação da ICP-Brasil, no entanto, após seu surgimento o governo brasileiro tem usado essa técnica também em sua interação com o cidadão e as empresas.

Seguindo tendência mundial, o executivo tem imprimido esforços em implementar um *e-Gov* prático e amplo. Hoje, o particular já dispõe de diversos serviços fornecidos através dos sites governamentais, muitos deles somente possíveis pela aplicação da tecnologia aqui discutida. Como descrito no próprio site Governo Eletrônico¹⁵:

O que se pretende com o Programa de Governo Eletrônico brasileiro é a transformação das relações do Governo com os cidadãos, empresas e também entre os órgãos do próprio governo de forma a aprimorar a qualidade dos serviços prestados; promover a interação com empresas e indústrias; e fortalecer a participação cidadã por meio do acesso a informação e a uma administração mais eficiente.

O pregão, modalidade de licitação, é utilizado pela administração pública para a aquisição de bens comuns no mercado. A legislação pertinente ao assunto previu a possibilidade desse pregão ser realizado “por meio da utilização de recursos de tecnologia da informação, nos termos de regulamentação específica”¹⁶. Daí surgiu um dos recursos mais utilizados atualmente pelo executivo e que agiliza sobremaneira as negociações entre o governo e seus fornecedores, o Pregão On-line.

Diversos são os *sites* governamentais que prestam esse serviço. Em âmbito federal podemos citar o ComprasNet¹⁷, portal de compras do governo federal. Nele, existe a exigência expressa de que o interessado possua um certificado digital emitido pelo Serviço Federal de Processamento de Dados (SERPRO), uma das AC cadastradas no ICP-Brasil.

¹⁵ Site Governo Eletrônico, **Net**. Disponível em: <<https://www.governoeletronico.gov.br>> Acesso em: 04 nov. 2008.

¹⁶ BRASIL. Lei nº 10.520, de 17 de julho de 2002. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 18 JUL. 2002. (Art. 2º § 1º)

¹⁷ Site ComprasNet, **Net**. Disponível em: <<http://www.comprasnet.gov.br>> Acesso em: 28 out. 2008.

A Receita Federal é outra frente importante de atuação digital do governo. A instituição fornece diversos serviços às pessoas físicas e jurídicas, sendo que, para se ter acesso a muitos destes serviços é necessário um certificado digital.

Pessoas físicas são atendidas pelo Centro Virtual de Atendimento ao Contribuinte¹⁸ (*e-CAC*) que contém dados confidenciais que a Secretaria da Receita Federal fornece apenas ao próprio contribuinte, ou a procuradores previamente cadastrados pelo próprio contribuinte. O acesso só poderá ser efetivado mediante a utilização de um Certificado Digital, emitido por Autoridade Certificadora habilitada pela Secretaria da Receita Federal ou credenciada pela ICP-Brasil.

Serviços como obter cópia de declarações, cópia de pagamentos, realizar retificação de pagamentos, negociar parcelamento, pesquisar sua situação fiscal e alterar seus dados cadastrais são exemplos das possibilidades oferecidas às pessoas físicas.

Em relação às pessoas jurídicas, podemos citar os mesmos benefícios oferecidos às pessoas físicas, além de ferramentas específicas como o Sistema Integrado de Comércio Exterior¹⁹ (SISCOMEX), que é um instrumento informatizado por meio do qual é exercido o controle governamental do comércio exterior brasileiro. É uma ferramenta facilitadora que agrega competitividade às empresas exportadoras, na medida em que reduz o custo da burocracia. O sistema promove a integração das atividades de todos os órgãos gestores do comércio exterior, inclusive o câmbio, permitindo o acompanhamento, orientação e controle das diversas etapas do processo exportador e importador.

O Ministério da Fazenda, em parceria com a Receita Federal vem triunfando inclusive na criação da Nota Fiscal Eletrônica (*NF-e*). O instrumento que vem sendo implantado por um número crescente de contribuintes e pode ser conceituado como um “documento de existência apenas digital, emitido e armazenado eletronicamente, com o intuito de documentar, para fins fiscais, uma operação de circulação de mercadorias ou uma prestação de serviços, ocorrida entre as partes”.²⁰

A validade jurídica das *NF-e* é garantida pela assinatura digital do remetente, que é parte indispensável do processo, e pela recepção pelo Fisco do documento eletrônico, antes da ocorrência do Fato Gerador. Várias são as vantagens na adoção do sistema, tanto para o Fisco

¹⁸ Site da Receita Federal, seção e-CAC, **Net**. Disponível em:

<<http://www.receita.fazenda.gov.br/AtendVirtual/default.htm>> Acesso em: 20 out. 2008.

¹⁹ Site da Receita Federal, seção Siscomex, **Net**. Disponível em:

<<http://www.receita.fazenda.gov.br/Aduana/Siscomex/siscomex.htm>> Acesso em: 20 out. 2008.

²⁰ Site do Ministério da Fazenda, seção Portal Nacional da Nota Fiscal Eletrônica, **Net**. Disponível em:

<<http://www.nfe.fazenda.gov.br/portal/assuntoagrupado1.aspx>> Acesso em: 23 out. 2008.

como para o particular, sendo sensíveis a redução de custos de impressão e armazenagem de documentos fiscais, a redução do tempo envolvido nos trâmites que envolvem notas, como a entrada e saída de mercadorias das empresas, assim como, a parada de caminhões em Postos Fiscais de Fronteira para fiscalização, entre outros.

Até o dia 03 de novembro de 2008 já haviam sido autorizadas 41.841.612 (quarenta e um milhões, oitocentos e quarenta e um mil, seiscentos e doze) Notas Fiscais Eletrônicas, *NFe*, totalizando um montante de R\$ 890.801.154.140,18 (oitocentos e noventa bilhões, oitocentos e um milhões, cento e cinquenta e quatro mil, cento e quarenta reais e dezoito centavos) envolvidos nesses negócios, o que mostra a expressão desse mecanismo.²¹

Dessa forma, a Receita Federal representa um pólo importante de serviços prestados na *internet* sendo que muitos deles necessitam do uso dessa tecnologia de identificação pela seriedade envolvida nesses atos. A tendência é que cada vez mais serviços estejam atrelados à assinaturas digitais, inclusive atos que hoje são prestados sem essa observância como a declaração de imposto de renda. Afinal, atualmente não há garantia de autoria dessas declarações, tampouco de que elas não foram alteradas no seu curso, gerando uma insegurança jurídica muito grande.

Outro órgão significativo que já implantou o uso da certificação digital foi o Banco Central do Brasil. Internamente, como já citado, a certificação digital é amplamente utilizada, e, em relação aos usuários externos, muitas operações são realizadas utilizando-se os mesmos. O Sistema de Informações do Banco Central (SISBACEN) que disponibiliza diversos serviços utiliza a técnica em questão, assim como muitos contratos são fechados assinados digitalmente, como contratos de câmbio.

Seguindo o âmbito financeiro federal, a Caixa Econômica Federal é outra instituição que adotou internamente o uso da certificação digital para identificação e confirmação de atos de seus empregados, além de externamente, possibilitando que seus clientes realizem atos, incluindo contratos, pela Internet, com a segurança que o instituto emana. Vale ressaltar que a Caixa é inclusive uma Autoridade Certificadora de 1^o nível credenciada na ICP-Brasil, como veremos abaixo.

O rol de órgãos e serviços apresentado acima é apenas exemplificativo; é uma forma de tentar demonstrar como a assinatura digital está muito mais difundida pelo poder executivo brasileiro do que grande parte das pessoas pode imaginar. Se a tecnologia em si já é

²¹ Site do Ministério da Fazenda, seção Portal Nacional da Nota Fiscal Eletrônica, *Net*. Disponível em: <<http://www.nfe.fazenda.gov.br/portal/assuntoagrupado1.aspx>> Acesso em: 23 out. 2008.

simplesmente desconhecida por muitos, suas atuais aplicações são completamente desconsideradas. No entanto, pela velocidade com que o executivo em seus âmbitos federal, estadual e municipal vêm implantando o *e-Gov* e seus órgãos vem disponibilizando seus serviços de forma digital, dentro em breve a realidade será outra e mais e mais frutos serão colhidos.

Na Presidência da República, a principal utilização da tecnologia de certificação digital é o Sistema de Tramitação de Documentos Oficiais (SIDOF), é um sistema utilizado na tramitação de documentos oficiais entre os Ministérios e a Casa Civil da Presidência da República, instituído pelo Decreto nº 4.522, de 17 de dezembro de 2002.

Inclusive, no dia 23 de novembro de 2008 aconteceu, no Palácio do Planalto, a cerimônia de certificação digital do Presidente Luiz Inácio da Silva, onde lhe foi entregue um certificado digital do tipo A3²² da ICP-Brasil, emitido pela Autoridade Certificadora da Presidência da República – ACPR, cujo par de chaves foi gerado e armazenado em um *token*²³ criptográfico, inviolável e protegido por senha.

Atualmente, das oito Autoridades Certificadoras de 1^o nível, cinco estão ligadas ao nosso poder executivo, reforçando o acima exposto de que este poder se utiliza dessa tecnologia há muito e vem aumentando seu uso. São elas:

A Autoridade Certificadora Serpro (AC-SERPRO) foi a primeira autoridade certificadora credenciada pela ICP-Brasil. O Serviço Federal de Processamento de Dados (SERPRO), é uma empresa pública, vinculada ao Ministério da Fazenda. Foi criada em 1964 com o objetivo de modernizar e dar agilidade a setores estratégicos da Administração Pública brasileira. A Empresa, cujo negócio é a prestação de serviços em Tecnologia da Informação e

²² Na ICPBrasil estão definidos oito (08) tipos de certificados para titulares, classificados da seguinte forma: A1, A2, A3, A4, S1, S2, S3 e S4, e um tipo de certificado para Autoridades Certificadoras. Certificado de Assinatura Digital (A1, A2, A3 e A4) São os certificados usados para confirmação da identidade na web, correio eletrônico, transações online, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos com verificação da integridade de suas informações.

Certificado de Sigilo (S1, S2, S3 e S4) São os certificados usados para cifração de documentos, bases de dados, mensagens e outras informações eletrônicas. Glossário ICP-Brasil Versão 1.1, de 18 de março de 2006. Disponível em: <<http://www.iti.gov.br>> Acesso em: 15 out. 2008.

²³ O token é um dispositivo eletrônico, geralmente ligado a porta USB do computador, que gera uma nova senha numérica aleatória a cada 36 segundos ou segundo a programação previamente realizada, para ser utilizada como um fator de segurança adicional em transações financeiras realizadas pela Internet. Este sistema garante total privacidade em caso de roubo de senhas, através de programas espiões como os trojans.

O dispositivo armazena as chaves privadas e os certificados digitais, e possui vários algoritmos de criptografia como o RSA, DES e 3DES. Existe também a variante para smart cards, que é capaz de realizar as mesmas tarefas do token, mas que não é tão difundida. Site Wikipédia. Disponível em: <[http://pt.wikipedia.org/wiki/Token_\(chave_eletrônica\)](http://pt.wikipedia.org/wiki/Token_(chave_eletrônica))> Acesso em: 3 nov. 2008.

Comunicações para o setor público, é considerada uma das maiores organizações do setor na América Latina. Busca, desde a criação de seu Centro de Certificação Digital (CCD-SERPRO), em 1999, divulgar o uso dessa tecnologia para os vários segmentos com que trabalha.

A Autoridade Certificadora Caixa Econômica Federal (AC-CEF) é atualmente a única instituição financeira credenciada como Autoridade Certificadora na ICP-Brasil. Se utiliza, desde 1999, da tecnologia de certificação digital para prover a comunicação segura na transferência de informações referentes ao FGTS e à Previdência Social, no âmbito de seu projeto “Conectividade Social”, assim como, para a aceitação de contratos e movimentações financeiras realizados pela *internet*.

A Autoridade Certificadora da Presidência da República (AC-PR), foi criada em abril de 2002 por iniciativa da Casa Civil no âmbito do governo eletrônico e tem como objetivo emitir e gerir certificados digitais das autoridades da Presidência da República, ministros de estado, secretários-executivos e assessores jurídicos que se relacionem com a Presidência da República.

A Autoridade Certificadora Secretaria da Receita Federal (AC-SRF) foi a AC criada para que a SRF pudesse disponibilizar uma grande quantidade de serviços na web, com o objetivo de simplificar ao máximo a vida dos contribuintes e facilitar o cumprimento espontâneo das obrigações tributárias. Por meio dos serviços do Centro Virtual de Atendimento ao Contribuinte a SRF presta atendimento aos contribuintes de forma interativa, via *internet*, com uso de certificados digitais, garantindo a identificação inequívoca dos usuários.

A Autoridade Certificado Imprensa Oficial (AC-IMESP), é a Autoridade Certificadora Oficial do Estado de São Paulo e está credenciada e preparada para oferecer produtos e serviços de certificação digital para os poderes executivo, legislativo e judiciário, incluindo todas as esferas da administração pública, direta e indireta, nos âmbitos federal, estadual e municipal.

4.2 No poder legislativo

O poder legislativo brasileiro ainda encontra resistências em se tratando do uso da certificação digital como ferramenta de trabalho. Apesar da discussão e aprovação de diversos projetos relacionados ao tema que incidem sobre os outros poderes ou sobre particulares, poucas são as iniciativas legislativas visando a inclusão da assinatura digital em nosso processo legislativo, o que nos parece contraditório.

Nossas duas mais altas casas legislativas não tem a certificação digital inserida eficazmente como instrumento no processo legislativo. Tanto o Senado Federal como a Câmara dos Deputados, relutam em atualizar seus métodos, no entanto, podemos citar algumas tentativas e experiências que vem sendo realizadas.

A Câmara dos Deputados, por meio da sua Resolução nº 22 de 31 de março de 2004 alterou o regimento interno da casa em seu artigo 102, onde seus parágrafos 1º e 3º passaram a ter a seguinte redação:

Art. 102. A proposição de iniciativa de Deputado poderá ser apresentada individual ou coletivamente.

§ 1º Consideram-se Autores da proposição, para efeitos regimentais, todos os seus signatários, **podendo as respectivas assinaturas ser apostas por meio eletrônico** de acordo com Ato da Mesa.

[...]

§ 3º O *quorum* para a iniciativa coletiva das proposições, exigido pela Constituição Federal ou por este Regimento Interno, **pode ser obtido por meio das assinaturas de cada Deputado, apostas por meio eletrônico** ou, quando expressamente permitido, de Líder ou Líderes, representando estes últimos exclusivamente o número de Deputados de sua legenda partidária ou parlamentar, na data da apresentação da proposição²⁴.(grifo nosso)

Dessa forma, podemos perceber a preocupação da Câmara dos Deputados em tentar se adequar à era digital em que vivemos, no entanto, como anteriormente²⁵ explicado, as assinaturas eletrônicas são o gênero no qual as assinaturas digitais são uma espécie, sendo as assinaturas digitais as que realmente nos dão segurança física e jurídica para a realização de atos jurídicos digitais mais complexos.

Sendo assim, as alterações realizadas pela Resolução nº 22/04, apesar de abrirem espaço para a aderência à certificação digital, não obrigaram a casa a tanto, além de não fazer qualquer menção ao ICP-Brasil. Pelo exposto, as alterações podem até mesmo ser perigosas se o sistema de assinaturas eletrônicas não fornecer a segurança necessária a tais atos.

²⁴ BRASIL, Câmara dos Deputados. Resolução nº 22 de 31 de março de 2004. **Diário da Câmara dos Deputados**, Poder Legislativo, Brasília, DF, 01 ABR. 2004.

²⁵ Ver item 2.4 – Assinatura Eletrônica x Assinatura Digital

Percebendo isso o Centro de Informática da Câmara dos Deputados (CENIN) identificou a certificação digital como prioridade para garantir a autenticidade e o sigilo das informações que trafegam tanto pela sua rede interna como em processos com outros órgãos do governo brasileiro.

Sem caráter legislativo, ou seja, atuando de maneira técnica apenas, o CENIN elaborou uma estrutura de caráter heterogêneo, onde adquiriu 900 certificados emitidos por autoridades credenciadas à ICP-Brasil, para o uso dos parlamentares e da alta administração da Câmara, garantindo o necessário caráter oficial. O restante da estrutura faz uso de certificados emitidos pelos próprios servidores da Câmara dos Deputados, ou seja, externos à ICP-Brasil e, portanto, sem validade assegurada.

Atualmente os parlamentares podem propor projetos de leis pelo Sistema Informatizado de Legislação da Gestão Administrativa (SILEG) onde assinam digitalmente os documentos. No entanto, a real incorporação da ICP-Brasil ao processo legislativo, de seu início ao fim, assim como, ao dia a dia do nosso Congresso Nacional ainda não é uma realidade.

Apesar disso, o exemplo pode vir do âmbito estadual. Em iniciativa inédita a Assembléia Legislativa do Estado de São Paulo associou-se à Imprensa Oficial como Autoridade Certificadora e vem implantando práticas para o uso do *e-CPF*²⁶ que beneficiam os parlamentares e os funcionários através do ganho de tempo e da diminuição dos processos em papel.

Em que pese a lentidão em incorporar a certificação digital ao nosso parlamento por parte dos próprios parlamentares, os mesmos tem se mostrado atentos ao legislar externamente sobre o assunto.

A reforma realizada no processo eleitoral inseriu a utilização da urna eletrônica nas votações. A Lei nº 10.740 de 1º de outubro de 2003 alterou a Lei nº 9.504 de 30 de setembro de 1997 que trata das eleições, modificando o § 4º do Art. 59, como abaixo:

Art. 59 § 4º A urna eletrônica disporá de recursos que, mediante assinatura digital, permitam o registro digital de cada voto e a identificação da urna em que foi registrado, resguardado o anonimato do eleitor.

²⁶ O *e-CPF* é um documento eletrônico em forma de certificado digital. Ele funciona exatamente como uma versão digital do CPF. Ele garante a autenticidade e a integridade na comunicação entre as pessoas físicas e os diversos órgãos públicos. Identidade Digital. Disponível em: <<http://www.identidadedigital.com.br/pergunte/ecpf/info>> Acesso em: 04 nov. 2008.

Como expresso no parágrafo transcrito, a urna utiliza a assinatura digital para garantir a segurança do processo que é modelo mundial de eficiência, sendo sua implantação estudada por diversos países do mundo.

Com a popularização da certificação digital, passando esta a estar presente nos documentos mais básicos dos cidadãos, como CPF e RG, a tecnologia poderá ser utilizada também na identificação do cidadão no momento do voto, dispensando a busca pelo nome do cidadão em longas listas e sua assinatura manuscrita, tornando assim o processo ainda mais ágil e seguro, já que no modelo atual, o mesário libera a urna digitando o número do documento do cidadão, o que pode ser feito mesmo sem o cidadão estar presente, possibilitando fraudes, principalmente nos minutos finais do pleito, onde mesários mal intencionados votariam pelos faltantes.

Com a utilização da assinatura digital, a urna só seria liberada para votação após a inserção dessa assinatura no sistema da urna, o que só pode ser feito pelo próprio cidadão, portador da chave privada.

As possibilidades relacionadas ao escrutínio são gigantescas e revolucionárias, em exercício de imaginação podemos prever até mesmo que o processo supracitado restará obsoleto, já que com a popularização da assinatura digital o cidadão poderá votar de qualquer computador.

Se a aproximação de uma democracia direta pode ser considerada uma utopia pelos grandes entraves existentes, como ressalta Dalmo Dallari:

No momento em que os mais avançados recursos técnicos para captação e transmissão de opiniões, como terminais de computadores, forem utilizados para fins políticos será possível a participação direta do povo, até mesmo nos grandes Estados. Mas para isso será necessário superar as resistências dos políticos profissionais, que preferem manter o povo dependente de representantes.²⁷

Um modelo mais eficaz de democracia semidireta é plenamente possível. Institutos como o plebiscito e o referendo poderão ser utilizados mais regularmente dando ao cidadão mais poder e à democracia mais legitimidade, além da iniciativa popular que pode ganhar efetividade, já que hoje em dia é praticamente letra morta em nosso ordenamento jurídico.

Sobre a iniciativa popular já existe até mesmo projeto de lei estadual de nº 162/2008 proposto pelo deputado Rui Falcão da Assembléia Legislativa de São Paulo, que visa

²⁷ DALLARI, Dalmo de Abreu. **Elementos de Teoria Geral do Estado**. São Paulo: Saraiva, 2003. 24. ed. p.153

promulgar lei possibilitando a iniciativa popular por meio de assinatura digital colhida em *site*²⁸ da Assembléia Legislativa na *internet*. O projeto prevê ainda que para tanto serão observadas as normas técnicas de segurança emitidas pela ICP-Brasil. Vale lembrar, que o projeto já obteve inclusive parecer favorável da Comissão de Constituição e Justiça da Assembléia Legislativa.

A promulgação de uma lei como esta pode finalmente dar efetividade ao instituto da iniciativa popular. Se transportada para o âmbito federal esse exemplo, a tão temida subscrição por “no mínimo, um por cento do eleitorado nacional, distribuído pelo menos por cinco Estados, com não menos de três décimos por cento dos eleitores de cada um deles”²⁹ pode ser superada, tendo em vista o número crescente de usuários que a *internet* vem ganhando no Brasil a cada dia.

²⁸ O termo *website* (às vezes *web site*) designa um sítio virtual, um conjunto de páginas virtualmente localizado em algum ponto da web. Acontece que, com poucos anos de uso, o termo *website* ganhou a forma abreviada *site*, que passou a ser uma segunda acepção do termo original. *Site*, portanto, em inglês, passou a designar alternativamente um lugar real (no campo) ou virtual (na web). Wikipédia. Disponível em: <<http://pt.wikipedia.org/wiki/Site>> Acesso em: 04 nov. 2008.

²⁹ BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, 05 OUT. 1988. (Art. 61 §2º parte)

4.3 No poder judiciário

4.3.1 Disposições gerais

A presença da certificação digital no poder judiciário brasileiro já é marcante e tende a revolucionar a maneira como se é feita justiça no Brasil. Isso por que o processo vem sofrendo uma transformação em que ganha velocidade e agilidade.

A Lei nº 9.800, de 26 de maio de 1999, veio inovar em nosso ordenamento jurídico possibilitando a realização de atos processuais por meio de sistema de transmissão de dados. Essa lei previa que a petição poderia ser enviada por meio eletrônico, no entanto, as petições originais, em papel, deveriam ser protocoladas no respectivo órgão em até cinco dias da data do término do prazo a ser cumprido.

Apesar de inovadora a Lei 9.800, as vantagens do peticionamento eletrônico se encontravam restritas já que não havia segurança no processo, além do fato de que os autos em papel permaneciam sendo obrigatórios, dessa forma, nem mesmo a vantagem do não deslocamento ao tribunal existia já que os originais deveriam ser protocolados posteriormente. Vale lembrar, que sequer havia qualquer menção a meios de identificação do emitente.

Alguns anos depois, a promulgação da Lei nº 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial, compreendendo os processos civil, penal e trabalhista, bem como aos juizados especiais, em qualquer grau de jurisdição, efetivamente possibilitou nossos tribunais a, gradualmente, migrarem dos autos de papel para os autos digitais, protegidos pela tecnologia da assinatura digital.

Diversas são as iniciativas no nosso judiciário de adequação a essa nova realidade, no entanto, o que por um lado é muito bom por mostrar a vontade de nossas cortes em se modernizar, por outro lado precisa ser organizado, já que diversos são os sistemas atualmente utilizados e outros ainda sendo criados, gerando certa confusão ao operador de direito. Em que pese essa “*torre de babel*” que vem sendo construída, a adoção do processo eletrônico vem mostrando resultados expressivos onde é implementado, sendo, dessa forma, inegáveis suas vantagens.

As economias de tempo, recursos humanos e financeiros são brutais, dando ao nosso sistema judicial nova energia para se reformular e entrar de vez na era virtual em que vivemos, prestando uma justiça mais célere e transparente e ganhando novamente a confiança do cidadão que há tempos vê com descrença o sistema.

Percebendo essa oportunidade o judiciário criou a Autoridade Certificadora da Justiça (AC-JUS), com o intuito de massificar o uso de certificados digitais em todo o Poder Judiciário. A AC-JUS é AC de primeiro nível da ICP-Brasil, e a primeira do Poder Judiciário mundial, criada através de uma decisão conjunta, em 20 de dezembro de 2004, do Superior Tribunal de Justiça e do Conselho da Justiça Federal e teve inicialmente sua atuação voltada para o STJ, CJF e Justiça Federal, vindo, em 2005 a receber a adesão da alta cúpula da Justiça.

Por atuar como AC normativa, credencia outras AC, para que estas, adotando as regras por ela estabelecidas, emitam os certificados aos requerentes. Estão definidos os tipos de Certificado: Institucional, para órgãos da Justiça, Advogado, Empresarial, Cidadão e para Equipamento Servidor.

4.3.2 Processo eletrônico

A Lei 11.419, de 19 de dezembro de 2006 regula a informatização do processo judicial no Brasil, também conhecido como “processo eletrônico” ou “processo virtual”. Ela permite o uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais nos processos civil, penal e trabalhista, assim como nos juizados especiais e em qualquer grau de jurisdição.

Inicialmente vale ressaltar, que a lei se encontra em perfeita consonância com os princípios internacionais aceitos relacionados à matéria, os citados princípios da **neutralidade tecnológica** e da **equivalência funcional**.

O princípio da **neutralidade tecnológica** se encontra amplamente observado já no §2º do Artigo 1º da lei, como podemos observar abaixo:

Art. 1º O uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais será admitido nos termos desta Lei.

[...]

§ 2º Para o disposto nesta Lei, considera-se:

I - meio eletrônico qualquer forma de armazenamento ou tráfego de documentos e arquivos digitais;

II - transmissão eletrônica toda forma de comunicação a distância com a utilização de redes de comunicação, preferencialmente a rede mundial de computadores;

III - assinatura eletrônica as seguintes formas de identificação inequívoca do signatário:

a) assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica;

b) mediante cadastro de usuário no Poder Judiciário, conforme disciplinado pelos órgãos respectivos.³⁰

O texto do artigo transcrito demonstra a preocupação do legislador em seguir o princípio que tem como corolário a neutralidade, já que considera o meio eletrônico “qualquer forma” de armazenamento ou tráfico de documentos digitais, a transmissão dos mesmos por “toda forma”, além de utilizar o termo “assinatura eletrônica”, que, como vimos, é o gênero do qual a assinatura digital é espécie.

Observando-se o Art. 2º percebemos que realmente o legislador pretendeu prestigiar o princípio da **neutralidade tecnologia**, já que admite o peticionamento eletrônico mediante o uso de assinatura eletrônica, na forma do Art. 1º:

Art. 2º O envio de petições, de recursos e a prática de atos processuais em geral por meio eletrônico serão admitidos mediante uso de assinatura eletrônica, na forma do art. 1º desta Lei, sendo obrigatório o credenciamento prévio no Poder Judiciário, conforme disciplinado pelos órgãos respectivos.

§ 1º O credenciamento no Poder Judiciário será realizado mediante procedimento no qual esteja assegurada a adequada identificação presencial do interessado.

§ 2º Ao credenciado será atribuído registro e meio de acesso ao sistema, de modo a preservar o sigilo, a identificação e a autenticidade de suas comunicações.

§ 3º Os órgãos do Poder Judiciário poderão criar um cadastro único para o credenciamento previsto neste artigo.³¹

³⁰ BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 20 DEZ. 2006.

³¹ BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 20 DEZ. 2006.

A compreensão do artigo acima, em paralelo com o Art. 1º, demonstra que deverá ser utilizada assinatura eletrônica, no entanto, não restringe essa assinatura à digital emitida pela ICP-Brasil, permitindo outros métodos. Único detalhe é a necessidade do cadastramento prévio no Poder Judiciário.

Em relação ao princípio da **equivalência funcional**, este se encontra presente no Art. 11 que expressa perfeitamente a índole do preceito em questão:

Art. 11. Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais.³²

O dispositivo pode ser considerado mera norma de reprodução do disposto na MP 2.200/01 que já previa esse fato, no entanto, já que está em consonância com a mesma, nos parece interessante sua reprodução pela importância do conceito envolvido.

Continuemos, então, a análise da lei. O Art. 3º da mesma, em seu parágrafo único, traz alteração marcante no trâmite de protocolo dos atos processuais como se lê abaixo:

Art. 3º Consideram-se realizados os atos processuais por meio eletrônico no dia e hora do seu envio ao sistema do Poder Judiciário, do que deverá ser fornecido protocolo eletrônico.

Parágrafo único. Quando a petição eletrônica for enviada para atender prazo processual, serão consideradas tempestivas as transmitidas até as 24 (vinte e quatro) horas do seu último dia.³³

Afinal, não há a necessidade de funcionários protocolando petições impressas em balcões tumultuados, o ato agora é realizado automaticamente no momento em que o sistema recebe a petição, por programa de computador, dessa forma, os prazos poderão ser utilizados integralmente não ficando mais o operador preso a horários de funcionamento dos protocolos. Ressalte-se, que com essa alteração se fez justiça já que os prazos processuais são contados em dias e não em horas, dessa forma, é direito do operador protocolar sua petição até o último minuto do dia final do prazo.

O artigo 4º da lei 11.419/06 traz a inovação de que os tribunais poderão criar Diários da Justiça eletrônicos na internet para a publicação de atos judiciais, com a ressalva de que esses sites deverão ser assinados digitalmente, como abaixo:

³² BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 20 DEZ. 2006.

³³ BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 20 DEZ. 2006.

Art. 4º Os tribunais poderão criar Diário da Justiça eletrônico, disponibilizado em sítio da rede mundial de computadores, para publicação de atos judiciais e administrativos próprios e dos órgãos a eles subordinados, bem como comunicações em geral.

§ 1º O sítio e o conteúdo das publicações de que trata este artigo deverão ser assinados digitalmente com base em certificado emitido por Autoridade Certificadora credenciada na forma da lei específica.

§ 2º A publicação eletrônica na forma deste artigo substitui qualquer outro meio e publicação oficial, para quaisquer efeitos legais, à exceção dos casos que, por lei, exigem intimação ou vista pessoal.³⁴

Em consonância com o acima exposto está a previsão da lei, em seu artigo 9º, de que as intimações, citações e notificações realizadas nos processos eletrônicos serão realizadas por meio eletrônico, agilizando sobremaneira esses atos processuais, e mais uma vez ganhando tempo e dinheiro no procedimento.

Art. 9º No processo eletrônico, todas as citações, intimações e notificações, inclusive da Fazenda Pública, serão feitas por meio eletrônico, na forma desta Lei.

§ 1º As citações, intimações, notificações e remessas que viabilizem o acesso à íntegra do processo correspondente serão consideradas vista pessoal do interessado para todos os efeitos legais.³⁵

Outro mecanismo interessante é a possibilidade da implantação de sistemas que consigam detectar a prevenção, a litispendência e a coisa julgada, previsto no Art. 14 da lei, mais uma ferramenta que tornará o processo mais inteligente e seguro, poupando tempo dos juízes e serventuários da justiça.

Com o intuito de adequar o Código de Processo Civil (CPC) às novas disposições dessa lei, em suas disposições gerais a mesma prevê diversas alterações ao CPC. Dessa forma, em nada ficou obstaculizada a adoção das disposições da lei em nosso ordenamento jurídico.

José Eduardo Campos Neves resume bem o espírito do processo eletrônico:

Saliente-se que o sistema eletrônico viabiliza todas as regras, funções e objetivos do processo, que podem ser atingidos tanto pela mídia papel quanto pela mídia eletrônica, obtendo-se, porém, com essa última, ambiente clean, maior segurança, rapidez, economia e praticidade. Tanto na mídia papel, como na mídia eletrônica, há fases processuais – extremamente simplificadas nos Juizados – assinaturas e certificações. A nova mídia, porém, excita a criatividade da exegese das normas processuais, repensando

³⁴ BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 20 DEZ. 2006.

³⁵ BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 20 DEZ. 2006.

o procedimento, pois muitas das formalidades, antes exigidas, com ela tornam-se inúteis, supérfluas, ou sem objeto. Com o procedimento, estruturado pela informática, desaparecem os autos convencionais – com suas bizarrices, como a costura de capas, grampos, colchetes, carimbos e rubricas por folha – extinguem-se em boa parte as diligências para o cumprimento de mandados de citação e intimação, a movimentação física de Pessoas e documentos, as agendas clássicas, os arquivos/papel, a autenticação de documentos, as assinaturas ordinárias, os livros encadernados de registros de sentenças, os livros de carga de processos, e nessa seqüência os costumeiros ácaros, traças e vetores que os acompanham, et cetera.³⁶

Com o processo eletrônico estamos tendo a possibilidade de repensar procedimentos tumultuados ou pouco funcionais e eliminar procedimentos desnecessários. É uma grande chance de dinamizar, da forma que merece e precisa, o ato de se fazer justiça.

Programas de computador farão, de forma muito mais eficiente, boa parte do trabalho que hoje é feito por serventuários, liberando estes para outros tipos de tarefas e dando muito mais eficiência aos cartórios que atualmente são um dos grandes gargalos da justiça.

Podemos citar diversos exemplos de alterações que trarão agilidade ao processo, a contagem de prazos é uma, já que não precisará mais ser feita manualmente; o acesso aos autos também será visivelmente ampliado, até permanente, afinal, mesmo em momentos em que os mesmos necessitem de despacho do juiz, poderão ser acessados virtualmente sem problemas.

O armazenamento dos autos em meio digital trará muito mais segurança aos mesmos pela possibilidade de se fazer *backups*³⁷ em locais fisicamente diversos de onde se encontram os originais, dirimindo o risco de perda dos autos por desastres físicos como incêndios. Além da economia de espaço pelo arquivo digital, ganha-se recursos com a velocidade com que conseguiremos deslocar os autos, exterminando-se, inclusive, a possibilidade de extravio dos mesmos.

³⁶ NEVES. José Eduardo Campos. **Autos Digitais Eletrônicos** In: Propostas da Comissão de Altos Estudos da Justiça Federal. Internet, Brasília. Out. 2003, Disponível em: <<http://www.justicafederal.gov.br>> Acesso em: 12 jun. 2006.

³⁷ Em informática, cópia de segurança é a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados. Meios difundidos de cópias de segurança incluem CD-ROM, DVD, disco rígido externo, fitas magnéticas e a cópia de segurança externa (online). Esta, transporta os dados por uma rede como a Internet para outro ambiente, geralmente para equipamentos mais sofisticados, de grande porte e alta segurança. Site Wikipédia. Disponível em: <http://pt.wikipedia.org/wiki/Cópia_de_segurança> Acesso em: 05 nov. 2008.

Pelo exposto, o processo eletrônico veio para revolucionar a atuação da justiça brasileira. Após a promulgação da Lei 11.419/06 ele se tornou uma realidade e diversos tribunais pátrios já se adequaram a essa possibilidade regulando internamente, cada qual com suas particularidades, o trâmite desses autos virtuais.

Dentre esses sistemas de processamento eletrônico dos autos podemos citar o *e-STF* do Supremo Tribunal Federal, o *E-Pet* do Superior Tribunal de Justiça, o *e-Doc* da Justiça do Trabalho e o *e-Proc* da Justiça Federal. O rol é apenas exemplificativo já que existem diversos sistemas, além de projetos que visam a unificação do trâmite, como o *e-Jud* da Justiça Federal e o PROJUDI mantido pelo Conselho Nacional de Justiça.

4.3.2.1 *e-STF (Supremo Tribunal Federal)*

O Supremo Tribunal Federal (STF) possibilitou o envio de petições eletronicamente por meio da Resolução nº 287, de 14 de abril de 2004, criando assim o *e-STF*, no entanto, o sistema era baseado no modelo da Lei 9.800/99, ainda precário em vários aspectos. Em 2007, após a promulgação da Lei 11.419/06, o Supremo aderiu ao processo eletrônico, promulgando a Resolução nº 344, de 25 de maio de 2007 que regulamenta o meio eletrônico de tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais no Supremo Tribunal Federal por meio do *software*³⁸ *e-STF*.

A resolução prevê o protocolo pela internet, sendo este possível somente a usuários previamente cadastrados. Em relação a esse cadastro, a Portaria nº 73, de 30 de maio de 2007 do STF, veio para discriminar os detalhes referentes ao mesmo, assim como, as especificações técnicas dos arquivos eletrônicos que podem ser enviados pelo sistema.

A exemplo das legislações atinentes ao tema, a resolução determina, em seu Art. 6^o, que as intimações serão feitas por meio eletrônico, dispensando-se a sua publicação, e, seguindo a rotina de tentar viabilizar a totalidade dos autos de forma digital a resolução prevê que a assinatura dos documentos pelos ministros poderá ser feita de forma digital.

³⁸ Em computador ou sistema de computação, os elementos não físicos de processamento de dados, como programas, sistemas operacionais etc. AULETE, Francisco; VALENTE, Antonio. Dicionário Aulete Digital. **Net**, nov. 2008. Disponível em: <<http://www.auletedigital.com.br>>. Acesso em: 10 set. 2008.

Além do apresentado, a resolução prevê regras específicas para o trâmite do recurso extraordinário eletrônico, mostrando, desta forma, como seria interessante que as instâncias inferiores se adequassem ao sistema, já que a subida do recurso seria acompanhada da integralidade dos autos, sem problema algum. No entanto, se forem autos em papel, o recurso digital deverá ser acompanhado de diversas partes dos autos originais, como decisões, recursos e certidões, de primeira, segunda e instâncias superiores. A não adequação dessas outras instâncias acarretará na necessidade da digitalização de todos esses documentos no momento de ingresso do recurso extraordinário eletrônico.

Em 29 de novembro de 2007 o STF promulgou sua Resolução nº 350, para tratar sobre a certificação digital no peticionamento eletrônico do tribunal. A resolução institui o uso da certificação digital na prática de atos processuais, regulando seu trâmite. Vale ressaltar, que o tribunal somente aceitará os atos praticados utilizando-se certificados digitais emitidos por AC credenciada junto à ICP-Brasil, como está claro no parágrafo único do Art. 1º da resolução.

Dessa forma, o tribunal pretendeu cercar de maior segurança esse novo tipo de procedimento, no entanto, o Art. 2º da norma prevê que o uso do peticionamento eletrônico certificado digitalmente é facultativo.

Em relação ao tema o Supremo Tribunal Federal já se manifestou nos autos do Agravo de Instrumento nº 564.765-6 RJ de decisão que inadimitiu recurso extraordinário contra acórdão da 2ª Turma Recursal dos Juizados Especiais Federais do Estado do Rio de Janeiro. A decisão inadimitiu o recurso alegando que a petição era uma cópia, estando em cópia também a assinatura do advogado. A União, ora agravante, alega que a assinatura estaria na forma digitalizada.

O relator Ministro Sepúlveda Pertence votou pela manutenção da decisão que inadimitiu o recurso extraordinário, sendo voto vencido o Ministro Marco Aurélio. No presente trabalho é de grande valia fragmento do voto do relator que demonstra a inclinação do STF em aceitar a assinatura digital, refutando qualquer outra forma de assinatura eletrônica, como a digitalizada (copiada por xerox), como ato jurídico válido:

Na administração pública federal foi instituída a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil (MPr 2.200/2001), que visa ‘garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas

que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras’.

Atualmente, o órgão responsável pela emissão dos certificados digitais é o ITI- Instituto de Tecnologia da Informação.

No caso dos autos, não se trata de certificado digital ou versão impressa de documento digital protegido por certificado digital; trata-se de meta chancela eletrônica utilizada sem qualquer regulamentação e cuja originalidade não é possível afirmar sem o auxílio de perícia técnica.

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.³⁹

Vale ressaltar, que atualmente nem todos os tribunais de justiça ou tribunais federais estão associados ao recurso extraordinário eletrônico, porém, a tendência é de que cada vez haja uma adesão maior a essa prática.

4.3.2.2 *E-Pet (Superior Tribunal de Justiça)*

O *E-Pet* é o sistema de peticionamento eletrônico do Superior Tribunal de Justiça. O serviço permite o uso da internet para a prática de atos processuais, sem necessidade de petições escritas em papel, em todos os tipos de processos do Tribunal.

Em 24 de abril de 2007 o STJ promulgou a Resolução nº 2, posteriormente alterada pela Resolução nº 9, de 5 de novembro de 2007, que instituiu o recebimento de petição eletrônica no âmbito do Superior Tribunal de Justiça. A exemplo de outras legislações nesse sentido, a resolução prevê a necessidade do prévio credenciamento do usuário na corte para usufruir do sistema.

³⁹ BRASIL. Supremo Tribunal Federal. Processual Civil. Agravo de Instrumento nº 564.765-6 RJ, da 1ª Turma, Relator Ministro Sepúlveda Pertence. Brasília, DF, 14 de fevereiro de 2006. Disponível em: <<http://www.stf.jus.br>> Acesso em: 05 nov. 2008.

A desnecessidade da apresentação posterior de petições em papel, das petições enviadas por meio eletrônico marca a presença do princípio da **equivalência funcional** nesta norma, no entanto, o que realmente devemos destacar no âmbito deste trabalho é a disposição do artigo 4º da resolução, como se lê abaixo:

Art. 4º O acesso ao serviço de recebimento de petições depende da utilização pelo credenciado da sua identidade digital, a ser adquirida perante Autoridade Certificadora credenciada junto à Infra-Estrutura de Chaves Públicas Brasileira - ICP - Brasil.⁴⁰

Dessa forma, mais uma vez foi prestigiada a tecnologia em questão. O artigo supra transcrito demonstra o intuito da corte em aderir à ICP-Brasil na tentativa de possibilitar que o judiciário brasileiro colha, da maneira mais segura possível, todos os frutos que o processo eletrônico pode proporcionar, em que pese a desconsideração por parte da norma ao princípio da **neutralidade tecnológica** aqui não observado.

O próprio Superior Tribunal de Justiça, em julgado muito recente, do dia 07 de outubro de 2008, se pronunciou a respeito em sede de embargos de declaração opostos em face de acórdão prolatado pela Eg. 4.^a Turma desta Corte que não conheceu agravo regimental. O acórdão que não conheceu o agravo regimental se fundamentava no fato de que o mesmo havia sido protocolizado via fax, e o original não havia sido entregue no prazo estipulado pela Lei nº 9.800/99, que seria de cinco dias.

A embargante, em suas razões, alegava que o agravo regimental não teria sido interposto via "fax", mas sim pelo novo sistema de protocolo e assinatura digital, em 31 de março de 2008, pelo que dispensaria a apresentação da peça física dentro do prazo de cinco dias.

O Exmo. Sr. Ministro Carlos Fernando Mathias, relator dos embargos de declaração votou nos seguintes termos:

Assiste razão à embargante.

Com efeito, a Resolução n.º 02, de 24 de abril de 2007, regulamentou o recebimento de Petição Eletrônica no âmbito desta Corte, dispondo, em seu art. 1.º:

‘Art. 1º - Instituir o recebimento de petição eletrônica, no âmbito do Superior Tribunal de Justiça, que permite aos credenciados utilizar a Internet

⁴⁰ BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 20 DEZ. 2006.

para a prática de atos processuais, independente de petição escrita, nos processos de competência originária do Presidente, nos Habeas Corpus e nos recursos em Habeas Corpus.’

Assim, a utilização da Petição Eletrônica estava restrita aos processos originários, aos HC e RHC. Ocorre, porém, que a Resolução n.º 09, de 05 de novembro de 2007, alterou o artigo 1º, da Resolução n.º 02, estabelecendo que:

‘Art. 1º - O art. 1º da Resolução n. 2, de 24 de abril de 2007, publicada no Diário da Justiça de 27 subsequente, Seção I, página 215, passa a vigorar com a seguinte redação:

Art. 1º Fica instituído o recebimento de petição eletrônica, no âmbito do Superior Tribunal de Justiça, que permite aos credenciados utilizar a Internet para a prática de atos processuais, independente de petição escrita.’

Assevera o artigo 2.º da referida Resolução que a alteração passou a vigorar a partir de 1.º de fevereiro de 2008.

Assim, verifica-se que a embargante tem razão quanto à validade da petição eletrônica acostada aos fls. 135/142, revelando-se necessário, portanto, acolher os embargos de declaração, com efeitos modificativos, para afastado o erro material consistente na equivocada premissa de que interposto o recurso via "fax", apreciar as razões do agravo regimental interposto[...]’⁴¹

Podemos perceber, pelo exposto, que a corte já entende plenamente possível e legal a interposição de petição por meio eletrônico, utilizando-se a assinatura digital. Entendimento sustentado também pelo Ministro Arnaldo Esteves Lima em sede de agravo regimental oposto contra embargos de declaração, que alegava ser inexistente o recurso de embargos de declaração por se apresentar desprovido da assinatura dos advogados.

PROCESSUAL CIVIL. AGRAVO REGIMENTAL NOS EMBARGOS DE DECLARAÇÃO NO RECURSO ESPECIAL. PETIÇÃO ELETRÔNICA ASSINADA DIGITALMENTE. POSSIBILIDADE. AGRAVO IMPROVIDO.

1. Encontrando-se a petição eletrônica assinada digitalmente, porquanto se trata de credenciado, conforme permitem a Lei 11.419/06 e a Resolução 9/07 do Superior Tribunal de Justiça, é dispensável a assinatura de próprio punho do advogado.

2. Agravo regimental improvido.⁴²

⁴¹ BRASIL. Superior Tribunal de Justiça. Processual Civil. EDcl no AgRg no AGRAVO DE INSTRUMENTO nº 993.323 SP, Relator Ministro Carlos Fernando Mathias. Brasília, DF, 07 de outubro de 2008. Disponível em: <<http://www.stj.jus.br>> Acesso em: 05 nov. 2008.

⁴² BRASIL. Superior Tribunal de Justiça. Processual Civil. AgRg nos EDcl no RECURSO ESPECIAL nº 1.1015.543 RS, Relator Ministro Arnaldo Esteves Lima. Brasília, DF, 29 de maio de 2008. Disponível em: <<http://www.stj.jus.br>> Acesso em: 05 nov. 2008.

4.3.2.3 *e-Doc (Justiça do Trabalho)*

O Sistema Integrado de Protocolização e Fluxo de Documentos Eletrônicos (*e-DOC*) é o atual modelo utilizado pela justiça do trabalho. Criado pelo Tribunal Superior do Trabalho (TST), já tem a adesão de diversos Tribunais Regionais do Trabalho brasileiros. Por meio da Instrução Normativa nº 30 o TST regulou a informatização do processo judicial no âmbito da justiça do trabalho.

A disposição constante do Art. 3º da instrução normativa mencionada dispõe que “o envio de petições, de recursos e a prática de atos processuais em geral por meio eletrônico serão admitidos mediante uso de assinatura eletrônica”⁴³, além do conteúdo do Art. 4º que descreve em detalhes as assinaturas aceitas:

Art. 4º A assinatura eletrônica, no âmbito da Justiça do Trabalho, será admitida sob as seguintes modalidades:

I – assinatura digital, baseada em certificado digital emitido pelo ICP-Brasil, com uso de cartão e senha;

II – assinatura cadastrada, obtida perante o Tribunal Superior do Trabalho ou Tribunais Regionais do Trabalho, com fornecimento de login e senha.⁴⁴

No entanto, atualmente, a postura adotada na prática pela justiça do trabalho é de restringir o cadastramento a usuários que detenham certificados digitais emitidos pela ICP-Brasil. Tal postura tem sido legitimada nos Tribunais Regionais do Trabalho por suas próprias instruções normativas que, diferentemente da promulgada pelo TST, prevêm apenas a certificação digital como método de identificação e segurança dos documentos, ferindo, dessa forma, o princípio da neutralidade tecnológica.

Afora essa discrepância entre o texto legal e a postura da corte na gestão do sistema, as demais disposições da instrução normativa seguem o já demonstrado nos outros sistemas analisados como: ser um sistema facultativo, a necessidade do cadastro prévio do usuário, a

⁴³ BRASIL. Tribunal Superior do Trabalho. Instrução Normativa nº 30, de 13 de setembro de 2007, Poder Judiciário, Brasília, DF, 13 SET. 2007.

⁴⁴ BRASIL. Tribunal Superior do Trabalho. Instrução Normativa nº 30, de 13 de setembro de 2007, Poder Judiciário, Brasília, DF, 13 SET. 2007.

dispensa da apresentação de originais posterior consagrando o princípio da equivalência funcional, intimações, citações e notificações eletrônicas, entre outros.

Vale uma observação acerca da disposição do Art. 17 que institui a exclusividade da transmissão de cartas precatórias, rogatórias e de ordem, no âmbito da Justiça do Trabalho, na forma eletrônica, através do Sistema de Carta Eletrônica (CE), ficando dispensada a remessa física de documentos.

Além desse ponto, podemos destacar que o *e-Doc* se encontra amplamente difundido na justiça do trabalho, atualmente, de acordo com dados do site do TST, além desta corte superior, vinte e um Tribunais Regionais do Trabalho aderiram ao sistema, juntamente com Varas do Trabalho.

4.3.2.4 *e-proc (Juizados Especiais Federais da 4ª Região)*

Na vanguarda da justiça nacional, os tribunais sulistas do Brasil implantaram ambicioso sistema de peticionamento eletrônico no âmbito de seus Juizados Especiais Federais(4ª Região), o Sistema de Processamento Eletrônico de Ações (*e-proc*).

Isso aconteceu em decorrência do Art.8º §2º da Lei 10.259/01 (Lei que instituiu os Juizados Especiais no âmbito da Justiça Federal) que possibilitava a esses tribunais a organização de serviço de intimação das partes e de recepção de petições por meio eletrônico. Inicialmente, em 2003, o sistema tinha competência para poucos tipos de causas e estava instalado em um número reduzido de subseções.

Com a promulgação da Resolução nº 13, de 11 de março de 2004 e do Provimento nº 1, de 10 de maio de 2004 que complementou a mesma, pelo Tribunal Regional Federal da 4ª Região, o sistema foi regulamentado. A posterior promulgação da Lei 11.419/06 (Lei do Processo Eletrônico) em nada alterou o sistema que se encontrava em perfeita consonância com a mesma.

Em 31 de março de 2007 o *e-proc* foi adotado, definitivamente, como sistema processual único a ser utilizado por todos os juizados especiais federais do sul do Brasil (4ª Região), a partir dessa data não se admitiu mais ação alguma em meio físico.

Pela obrigatoriedade do uso do sistema no âmbito dos juizados, é de grande importância a disposição do §1º do Art. 2º da Resolução nº 13 que determina que em cada subseção deve ser instalada sala de auto-atendimento com sistema de escaneamento e computador ligado à *internet*. Dessa forma, foi garantido o princípio do acesso à justiça.

O e-proc prevê dois tipos de usuários, a saber: os externos, que são os magistrados e serventuários da justiça; e os internos, que são os advogados e procuradores.

Ponto de fraqueza do sistema é a falta de segurança por parte do usuário externo. O sistema não requer o uso de certificação digital para identificação do mesmo, tampouco para identificação ou proteção do documento eletrônico, sendo o uso de chaves eletrônicas, as chamadas senhas, o único meio de segurança externo, meio este frágil por estar sujeito a ataques de *crackers*⁴⁵.

Já para os usuários internos, mais especificamente os Juizes, o Art. 9º do provimento citado prevê que a assinatura dos documentos será feita de forma digital, garantindo assim a sua validade.

Como podemos perceber, o sistema tem suas vulnerabilidades, no entanto, entre prós e contras a balança pende claramente para um entendimento de que a experiência já provou ser deveras bem sucedida se tornando, inclusive, um exemplo.

De acordo com João Batista Lazzari, Juiz Federal, Coordenador do Processo Eletrônico da Justiça Federal em Santa Catarina em 2007, até o início de abril de 2007 foram recebidas pelos JEF da 4ª Região mais de 370 mil ações virtuais, das quais cerca de 210 mil foram julgadas e arquivadas até junho de 2007, levando um prazo médio, entre as datas de distribuição e da prolação da sentença, de 120 dias.⁴⁶

Além disso, informações do TRF da 4ª Região, apontam que um processo em papel pode levar mais de 600 dias para ser solucionado, enquanto um caso semelhante conduzido

⁴⁵ Cracker é o termo usado para designar quem pratica a quebra (ou cracking) de um sistema de segurança, de forma ilegal ou sem ética. Wikipédia. Disponível em: <<http://pt.wikipedia.org/wiki/Cracker>> Acesso em: 03 nov. 2008.

⁴⁶ LAZZARI, João Batista. **Justiça sem papel: uma realidade dos Juizados Especiais Federais do sul do Brasil**. Revista de Doutrina da 4ª Região, Porto Alegre, n. 18, jun. 2007. Disponível em: <http://www.revistadoutrina.trf4.jus.br/artigos/Edicao018/joao_lazzari.htm> Acesso em: 03 nov. 2008.

digitalmente pode ser resolvido em 50 dias.⁴⁷ Esses dados demonstram o poder do sistema e o potencial que iniciativa semelhante teria em âmbito nacional.

4.3.2.5 Modelos paralelos e projetos sendo implantados

4.3.2.5.1 STM e TSE

Na justiça militar existe o *e-STM*, no entanto, o modelo ainda segue os moldes da Lei 9.800/99, não fazendo qualquer referência a assinaturas digitais e, permanecendo a inconveniente necessidade de se protocolar a petição em papel, o que descaracteriza completamente o processo eletrônico.

O mesmo acontece com o nosso Tribunal Superior Eleitoral que permanece utilizando sistema atrelado à Lei 9.800/99, tendo como único avanço a possibilidade de se utilizar a internet para tanto, fato contraditório pela louvável gerência que o tribunal vem tendo sobre o sistema de urnas eletrônicas brasileiro, dentre os mais modernos do mundo, senão o mais.

4.3.2.5.2 e-Jud (Justiça Federal)

⁴⁷ Ordem dos Advogados do Brasil. **Tribuna do Advogado**. Número 7. Novembro de 2008.

O Sistema Processual Único da Justiça Federal (e-Jud) é um projeto da Justiça Federal que visa desenvolver um sistema único, compartilhado e descentralizado, que possibilite a gestão do processo em papel, híbridos e eletrônicos pelos seus órgãos.

Por meio do Acordo de Cooperação assinado em 21 de fevereiro de 2008, o Conselho Nacional de Justiça, o Conselho da Justiça Federal e os Tribunais Regionais Federais firmaram o objetivo de desenvolver, em 12 meses, o e-Jud.

O sistema pretende ser completo, atendendo a todas as necessidades da movimentação processual, observando, inclusive, o disposto na Lei nº 11.419/06. Visa, ainda, permitir a integração do sistema com outros sistemas do judiciário.

4.3.2.5.3 Justiça Estadual

Duas são as ferramentas mais relevantes atualmente utilizadas pelos Tribunais de Justiça brasileiros, o PROJUDI e o e-SAJ.

O Processo Judicial Digital (PROJUDI) é um *software* que permite a tramitação totalmente eletrônica de processos judiciais, via internet. O sistema foi desenvolvido em *software livre*⁴⁸ pelo Conselho Nacional de Justiça (CNJ) e distribuído, gratuitamente, a todos os órgãos interessados.

O sistema, que já se encontra em funcionamento em diversos Tribunais de Justiça, utiliza a tecnologia da certificação digital como ferramenta usada para assinatura das petições tramitadas no mesmo, existindo a exigência de que este certificado seja emitido pela ICP-Brasil.

Como de costume nesses tipos de sistemas, a intimação eletrônica do advogado dispensa a publicação em diário oficial em papel.

O Sistema de Automação do Judiciário (*e-SAJ*) é um portal de serviços. O sistema foi desenvolvido para a internet facilitando a troca de informações e agilizando o trâmite

⁴⁸ Software livre, segundo a definição criada pela Free Software Foundation é qualquer programa de computador que pode ser usado, copiado, estudado, modificado e redistribuído sem nenhuma restrição. Wikipédia. Disponível em: <http://pt.wikipedia.org/wiki/Software_livre> Acesso em: 03 nov. 2008.

processual por meio de diversos serviços voltados para os advogados, cidadãos e serventuários da justiça.

O portal esta em conformidade com a Lei 11.419/06, sendo que os serviços oferecidos viabilizam não só o peticionamento eletrônico como também a adoção do meio eletrônico para armazenamento, tramitação, comunicação e transmissão de documentos e arquivos digitais diversos, centralizando em um único local serviços como: Peticionamento eletrônico, consultas processuais, consultas de jurisprudência, diário da justiça eletrônico, conferência de documentos impressos com os originais em formato eletrônico, consulta de contratos e convênios das secretaria de administração, assim como conferência de certidões. Dessa forma, o *e-SAJ* se diferencia dos demais sistemas pela abrangência, pela centralização de diversos serviços em si.

O e-SAJ se muni dos certificados e assinaturas digitais e protocolização eletrônica de documentos para garantirem a segurança do sistema.

Característica desse sistema é a possibilidade de uma integração das instituições que participam da esfera do judiciário, já que dispõe de diversos serviços. Seu alto grau de adequabilidade permite que estas ferramentas sejam personalizadas e configuradas de acordo com as necessidades de cada órgão.

4.3.3 AC-OAB

Com a promulgação da MP 2.200-2/01 a Ordem dos Advogados do Brasil (OAB) se posicionou contra sua adesão à ICP-Brasil, propondo a criação de uma ICP-OAB. Em 23 de abril de 2002 o Provimento nº 97 promulgado pelo Conselho Federal da Ordem instituiu a Infra-estrutura de Chaves Públicas da Ordem dos Advogados do Brasil (ICP-OAB).

A iniciativa não teve muito sucesso, até por que, de acordo com a MP 2.200-2/01 o ICP-OAB se enquadrava no §2º do seu Art.10, ou seja, seus certificados não faziam parte da ICP-Brasil, dessa forma, os documentos assinados digitalmente pelos mesmos não gozavam da presunção de veracidade. Assim, os certificados emitidos pela ICP-OAB deveriam ser aceitos pelas partes envolvidas no ato jurídico.

Seguindo a postura contrária à ICP-Brasil o órgão lutou nos tribunais contra dispositivos que aderiram à mesma, vindo a levantar a inconstitucionalidade até mesmo da própria Lei 11.419/06 na ADI 3880.

Na ADI 3880 a OAB sustenta que seriam inconstitucionais os dispositivos que tratam do cadastro dos advogados, por entender ser ato de competência exclusiva da OAB, assim como, os dispositivos relativos ao Diário de Justiça eletrônico, pois, haveria ali uma restrição à publicidade. O órgão levantou também a inconstitucionalidade do artigo que dispõe sobre a regulamentação da lei por parte dos próprios tribunais, alegando que seria de competência da União.

Em que pese essas disputas judiciais ainda em curso, o órgão, que vinha há anos lutando pela aceitação de sua própria ICP-OAB independente da ICP-Brasil, cedeu e o Conselho Federal da Ordem promulgou, em 9 de outubro de 2007, o Provimento nº 120, alterando o Provimento nº 97, para aderir à ICP-Brasil.

A Ordem assinou, então, contrato de prestação de serviços com a autoridade certificadora Certisign, empresa privada, para que esta prestasse suporte à OAB, possibilitando sua entrada na ICP-Brasil, sem a necessidade de diversos investimentos em questões técnicas e de equipamento.

No Diário Oficial da União - Seção 1, do dia 5 de setembro de 2008, foi publicada a autorização de credenciamento da Autoridade Certificadora OAB (AC-OAB), vinculada à AC-Certisign. Dessa forma, contando com a estrutura necessária fornecida pela Certisign, a OAB agora já é uma autoridade certificadora da cadeia da ICP-Brasil, a AC-OAB, estando autorizada a emitir certificados digitais vinculados à ICP-Brasil.

Vale ressaltar, que as facilidades apresentadas pelo processo eletrônico diminuirão distâncias físicas, dando confiança aos advogados a ultrapassar fronteiras antes vistas com receio. Dessa forma, podemos prever uma maior incidência de advogados postulando fora dos estados onde estão inscritos originalmente.

Quanto a isso, o advogado deve observar o disposto no Estatuto da Ordem, Lei 8.906/94, em seu Art. 10 §2º, como abaixo transcrito:

Art. 10. A inscrição principal do advogado deve ser feita no Conselho Seccional em cujo território pretende estabelecer o seu domicílio profissional, na forma do regulamento geral.

[...]

§ 2º Além da principal, o advogado deve promover a inscrição suplementar nos Conselhos Seccionais em cujos territórios passar a exercer habitualmente a profissão considerando-se habitualidade a intervenção judicial que exceder de cinco causas por ano.⁴⁹ (grifo nosso)

Dessa forma, os advogados podem peticionar livremente pelos tribunais pátrios, no entanto, devem respeitar o limite de cinco causas estabelecido pelo Estatuto, a partir do qual deverão providenciar suas inscrições complementares nos respectivos Conselhos Seccionais. O destacado vale tanto para advogados que fazem uso da tecnologia da certificação digital como para os que utilizam outros meios de identificação e segurança.

No entanto, o advogado que tiver adquirido certificado emitido pela AC-OAB e promover inscrição suplementar poderá utilizar esse mesmo certificado para postular neste novo território, já que o certificado tem validade em todo o território nacional.

Em consonância com esse raciocínio está o fato de que, munido de certificado emitido pela AC-OAB, o advogado pode utilizá-lo para realizar atos em todos os órgãos que requeiram ou aceitem essa tecnologia como a Receita Federal, por exemplo, não estando restrito ao uso judicial.

O certificado digital emitido pela AC-OAB será disponibilizado ao usuário na própria carteira da ordem, e somente nela. As novas carteiras da OAB contém a tecnologia *smartcard*, ou seja, apesar de exteriormente aparentarem como um simples cartão plástico como as antigas carteiras, em seu interior são munidas de microprocessador e memória que pode armazenar vários tipos de informações, além de deter sofisticados mecanismos de segurança.

Dessa forma, o certificado emitido pela AC-OAB será armazenado nesta memória e fará parte da carteira de identificação do advogado. Apesar da aparente vantagem da desnecessidade de se possuir uma mídia segura externa à carteira para se ter o certificado, fazendo esse papel a própria carteira da ordem, como desvantagem temos a incompatibilidade.

Isso por que, a tecnologia *smartcard* ainda não se encontra difundida, sendo assim, a quase totalidade de computadores não possui dispositivo de leitura de cartões *smartcard* o que cria a necessidade do advogado adquiri-lo aumentando ainda mais o custo geral da tecnologia.

⁴⁹ BRASIL. Lei 8.906, de 04 de julho de 1994. Diário Oficial da República Federativa do Brasil, Poder Executivo, Brasília, DF, 05 JUL. 1994. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L8906.htm > Acesso em: 03 nov. 2008.

A disponibilização deste certificado por meio de mídia mais compatível atualmente, como o *token* que utiliza entrada *USB*⁵⁰ presente em grande número dos computadores usados hoje em dia, traria muitas facilidades aos advogados.

4.3.4 Sociedade civil

Fornecido por empresas privadas, os certificados digitais já eram utilizados pela sociedade civil antes mesmo da promulgação da MP 2.200-2/01. Apesar da seriedade e confiabilidade de várias dessas empresas, não existia dispositivo legal que obrigasse a aceitação de documentos eletrônicos assinados fazendo-se o uso de tais certificados.

Dessa forma, por conhecer a potencialidade da tecnologia e confiar nessas empresas, os particulares utilizavam as assinaturas digitais como forma de imprimir mais segurança aos seus negócios. A realidade hoje é outra. Empresas que já utilizavam a prática agora expandem seu uso interno e externo e as que não se sentiam à vontade, agora ganharam confiança pelo suporte legal criado.

A integração entre companhias cria cadeias complexas de comunicação e fornecimento gerando demanda por uma infra-estrutura de informações segura. A certificação digital vem para garantir a privacidade e integridade das informações que trafegam entre essas organizações. A identificação dos participantes e a integridade e sigilo entre as conexões são garantidos pela assinatura digital dessas transações.

Os certificados digitais possibilitam que funcionários assinem seus *e-mails*⁵¹ digitalmente garantindo o sigilo e a autoria das informações. Esses certificados também permitem muito mais segurança no acesso a redes corporativas, assim como, *laptops*⁵² podem

⁵⁰ Universal Serial Bus (USB) é um tipo de conexão Plug and Play que permite a conexão de periféricos sem a necessidade de desligar o computador. Wikipédia. Disponível em: <http://pt.wikipedia.org/wiki/Universal_Serial_Bus> Acesso em: 03 nov. 2008.

⁵¹ E-mail, correio-e (em Portugal, correio electrónico), ou ainda email é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação. Wikipédia. Disponível em: <<http://pt.wikipedia.org/wiki/E-mail>> Acesso em: 03 nov. 2008.

⁵² Um laptop (no Brasil, e também é chamado de notebook) ou computador portátil (em Portugal, abreviado frequentemente de portátil) é um computador portátil, leve, designado para poder ser transportado e utilizado em diferentes lugares com facilidade. Wikipédia. Disponível em: <<http://pt.wikipedia.org/wiki/Laptop>> Acesso em: 03 nov. 2008.

ter seus arquivos criptografados em diretórios exclusivos, só acessados com certificados digitais habilitados, dirimindo o risco da empresa em caso de perda, roubo ou furto do equipamento.

Além disso, grandes empresas perceberam por experiência, fenômeno pelos profissionais do direito claramente observado nos cartórios das Varas de nossos tribunais além dos escritórios de advocacia, que um dos principais problemas para administração de uma organização é o armazenamento dos documentos impressos gerados no dia-a-dia de sua operação. A necessidade de espaço físico cada vez maior para o armazenamento desses documentos diminui o espaço útil das empresas, assim como, cria uma dificuldade crescente na localização das informações.

A digitalização de documentos era vista com cautela pela sua fragilidade jurídica, no entanto, a equiparação destes aos documentos físicos tornou esta opção uma verdadeira solução para o problema. A garantia de integridade e autenticidade dos documentos assinados digitalmente revolucionou a forma de arquivamento e locomoção de documentos empresariais.

Não só as pessoas jurídicas mas também as pessoas físicas e profissionais liberais foram beneficiados pela tecnologia aqui discutida. Com ela, as pessoas podem se aproveitar dos serviços que o governo disponibiliza pela Internet, o *e-Gov*. Isso por que, cada vez mais serviços são oferecidos pelo governo eletrônico, possibilitando ao cidadão o pedido e acompanhamento de seu processo sem a necessidade do deslocamento até um posto de atendimento.

Os benéficos da assinatura digital também podem ser percebidos no comércio eletrônico. *Sites* de vendas já se utilizam da tecnologia para gerar um ambiente seguro para seus clientes, assim como, contratos eletrônicos podem ser assinados digitalmente pelas partes, com segurança, sem estas nunca terem se encontrado fisicamente.

A certificação digital já vem sendo utilizada também em relação aos direitos autorais já que atualmente, apesar do gigantesco conteúdo de informações presente na *internet*, não podemos de forma segura, atestar a integridade e autoria dessas informações. Assinando digitalmente suas obras os autores podem ter a certeza de que alterações em seus documentos, assim como plágios, serão facilmente identificados. Já os receptores terão a possibilidade de se verificar a autoria e integridade dos documentos que receberem.

Essas práticas já podem ser observadas nas posturas de cidadãos comuns, assim como, em bancos, empresas de cartão de crédito, profissionais liberais, universidades, no agronegócio entre outros.

Atualmente duas empresas privadas figuram como autoridades certificadoras de 1º nível da ICP-Brasil, a Certisign e a Serasa.

5 CONCLUSÃO

O presente trabalho apresentou os conceitos envolvidos na tecnologia da certificação digital, o amparo legal que teve criado no ordenamento jurídico pátrio, assim como, uma síntese do atual uso da mesma no Brasil.

Tal qual foi observada uma verdadeira revolução com a criação da imprensa ao passarmos da era manuscrita para a era impressa, estamos vivenciando nova revolução, uma revolução digital.

Os micro computadores alteraram de forma marcante a sociedade em que vivemos trazendo agilidade e eficiência onde quer que fossem implantados. Juntamente com essas incríveis máquinas surgiu o maior fenômeno da comunicação humana, a *internet*. Como ser vivo e mutante que a *internet* é, a mesma tem evoluído a cada dia nos mostrando novas possibilidades de aplicá-la ao nosso cotidiano.

Em contrapartida, testemunhamos um judiciário nacional lento e burocrático que afasta o cidadão da justiça pela sua descrença, salvo melhor juízo. Netos assumem causas iniciadas pelos seus avós gerando uma situação que beira o absurdo.

Em um país imerso em práticas burocráticas vemos, descrentes, a evolução da corrupção que rotulada de “jeitinho brasileiro” já passa a característica cultural da nação, sendo transmitida de pais para filhos e aceita socialmente. Entendemos que a lentidão e ineficácia do nosso judiciário acaba por gerar impunidade e somente contribuir para esse ciclo vicioso.

O Brasil precisa modernizar sua justiça a fim de colher os frutos do espírito de suas leis, afinal de contas, acreditamos que para a esmagadora maioria dos casos as leis existem, simplesmente não são aplicadas já que boa parte da população não recorre ao judiciário pela sua patente morosidade e pelas custas envolvidas. Isso feito, será visível o salto que a nação dará em direção a uma sociedade civilizada.

Como salientado, a *internet* se tornou uma ferramenta importante, podendo ser uma grande aliado nessa busca. Até pouco tempo, o direito via com certa cautela o uso de documentos eletrônicos, isso por que, sua integridade e autoria eram de difícil constatação, tornando sua validade jurídica questionável.

A incorporação das técnicas de criptografia assimétrica a esses documentos deu surgimento à tecnologia da certificação digital possibilitando que as barreiras supracitadas, integridade e autoria, fossem transpostas com segurança por meio da assinatura digital. Esses documentos apresentam diversas vantagens sobre os elaborados em papel, economizam espaço físico, insumos e recursos humanos em sua gestão.

A Medida Provisória 2.200-2 de 2001 veio para criar o suporte legal necessário à adoção, de forma juridicamente sustentável, dos documentos digitais. A norma criou a ICP-Brasil dando vida a uma cadeia de certificação digital de âmbito nacional. Além disso, a MP 2.200-2/01 igualou a validade jurídica de documentos digitais assinados fazendo-se uso de certificados emitidos pela ICP-Brasil, aos documentos em papel com assinaturas manuscritas, prestigiando, assim, o princípio internacionalmente aceito da equivalência funcional, pelo qual o documento eletrônico cumpre as mesmas funções do documento em papel, não podendo ser rejeitado pelo fato de se encontrar em meio eletrônico.

Vale lembrar, que a norma não excluiu de validade os documentos que não estivessem em conformidade com a ICP-Brasil, simplesmente condicionou a validade dos mesmos à mútua aceitação pelas partes envolvidas, consagrando, assim, o outro princípio regente da matéria, a neutralidade tecnológica, que visando o respeito à liberdade das partes para escolherem a tecnologia que melhor atenda aos seus interesses, bem como objetivando evitar sua defasagem com o surgimento de novas tecnologias, proíbe que a legislação restrinja a tecnologia utilizada nesses documentos eletrônicos.

Dessa forma, a sociedade brasileira teve criadas as fundações para uma evolução digital, em nossa opinião, tão necessária e diversos agentes nacionais começaram a se movimentar nesse sentido.

Tanto no estado brasileiro, em seus três poderes, como em âmbito privado, o uso da tecnologia da assinatura digital vem se difundindo em velocidades incríveis. Iniciativas como o *e-Gov* e o processo eletrônico são louváveis e essenciais, acompanhando a vanguarda do observado internacionalmente nesse sentido. Em paralelo, a sociedade vem incorporando, por parte de suas pessoas físicas e jurídicas, o uso da assinatura digital em seu cotidiano.

No entanto, salvo melhor juízo, grandes desafios precisam ser transpostos para que os benéficos dessa tecnologia sejam atingidos em sua plenitude.

Primeiramente, e de maior relevo, podemos citar a necessidade da popularização da informática. O ensino de informática deve ser ministrado desde as bases da educação de

nossas crianças. Todas as escolas do país, públicas ou particulares, precisam dispor de computadores conectados à internet. Não podemos, em pleno século XXI, admitir analfabetos digitais no Brasil, e, uma vez educada a população, computadores com acesso à internet precisam estar disponíveis aos que não puderem tê-los, para darmos fim à exclusão digital.

Em relação ao nosso judiciário é ainda de maior importância o supracitado. Afinal, o processo digital já é uma realidade em diversos tribunais pátrios, já sendo, inclusive, obrigatórios em algumas jurisdições.

Sendo assim, como forma de não cercearmos o acesso do cidadão à justiça, todos os tribunais que implantarem o processo eletrônico como único meio de se postular em juízo devem dispor de salas munidas de computadores com acesso à internet e ferramentas de digitalização. Além disso, os tribunais devem prezar pela acessibilidade de seus portais judiciais, pois, o uso desses sistemas por portadores de necessidades especiais precisa ser possibilitado, caso contrário, estará ocorrendo grave afronta à Constituição.

Ainda sobre o tema, precisamos ressaltar a necessidade da adoção de plataformas que não restrinjam o acesso a determinados sistemas operacionais ou *softwares*, e, caso contrário, que a restrição seja a *softwares* gratuitos disponibilizados na própria *internet*.

No processo de popularização do uso da tecnologia da assinatura digital a OAB terá relevante papel em relação aos advogados. Como visto, a OAB acaba de ser incorporada à ICP-Brasil como autoridade certificadora, a AC-OAB. Em nosso entendimento, a Ordem deve educar o advogado esclarecendo o uso da tecnologia e seus benefícios, além de estimular o advogado para tanto.

Outro desafio é o custo ainda elevado da aquisição de certificados digitais que ainda repeli ou até impossibilita a implantação da tecnologia por parte de muitas pessoas físicas e jurídicas. Certificados mais acessíveis tornarão real a possibilidade do ingresso em massa da sociedade ao uso dessa tecnologia. Inclusive, com a real disseminação dos serviços sociais utilizando a certificação digital, entendemos que o próprio governo deve fornecer certificados digitais gratuitos para as pessoas carentes para que estas sejam também beneficiadas.

Ponto que merece destaque é a necessidade do mútuo reconhecimento e comunicação entre os diversos sistemas de processos eletrônicos adotados pelo judiciário brasileiro. Acreditamos que não necessariamente precisamos caminhar para uma unificação dos modelos atuais de forma a termos apenas um sistema, mas de suma importância é a possibilidade do

trâmite entre sistemas, ou seja, os sistemas precisam permitir o trânsito de documentos eletrônicos entre si de forma inteligente e segura.

Em relação ao comércio e às jurisdições internacionais, entendemos que o desafio reside nos diversos países aceitarem mutuamente os diferentes sistemas adotados por cada um deles. Para isso, a solução parece residir na observação por parte de cada país aos princípios internacionais da matéria e às disposições das leis modelos, como as da UNCITRAL. Dessa forma, as legislações nacionais dos diversos países serão compatíveis e por meio de acordos, bilaterais ou até multilaterais, ou países poderão aceitar suas estruturas de certificação digital reciprocamente.

As assinaturas digitais são uma realidade no direito brasileiro. Entendemos que a dúvida em relação a elas já não é mais se devemos utilizá-las, mas sim, como devemos. Salvo melhor juízo, o Brasil precisa, para adquirir o status que almeja de nação de primeiro mundo, se modernizar. Defendemos que essa modernização passa necessariamente pelo uso da informática e suas ferramentas e, dentre essas ferramentas está a assinatura digital.

Consideramos que estamos caminhando no sentido correto, no entanto, os potenciais do uso dessa tecnologia são enormes e não podem ser subutilizados pela nossa sociedade. Estamos vivendo apenas o início de uma revolução digital que está por vir, e essa revolução, conduzida da maneira correta, trará muitos benefícios ao direito e à sociedade.

Pelo exposto, entendemos que o uso da assinatura digital pelo Direito brasileiro trará marcantes benefícios à sociedade. A aplicação da técnica deve ser estudada e regulada a fim de que o Direito extraia todo o proveito possível desse novo instituto.

REFERÊNCIAS

ALMEIDA FILHO, José Carlos Araújo. **Processo Eletrônico e Teoria Geral do Processo Eletrônico - A Informatização Judicial no Brasil**. Rio de Janeiro: Forense, 2007.

ATHENIENSE, Alexandre. **Internet e o Direito**. São Paulo: Inédita, 2000.

BLUM, Renato Opice (Org.); BRUNO, M.G.S. (Org.); ABRUSIO, J. C. (Org.). **Manual de Direito - Eletrônico e Internet**. São Paulo: Aduaneiras, 2006.

CERQUEIRA FILHO, Reginaldo de Castro. **Formação e eficácia probatória dos contratos por computador**. Jus Navigandi. Disponível em: <<http://jus2.uol.com.br/doutrina/texto.asp?id=3865>>. Acesso em: 13 nov. 2008.

CERTISIGN. **Net**. Disponível em: <<https://www.certisign.com.br/>> Acesso em: 12 jul. 2008.

CUSTÓDIO, Ricardo Felipe. **Análise Crítica da ICP-Brasil**. UFSC. Disponível em: <teses.eps.ufsc.br/defesa/pdf/8110.pdf> Acesso em: 30 jul. 2008.

DALLARI, Dalmo de Abreu. **Elementos da teoria geral do Estado**. 24. ed. São Paulo: Saraiva, 2003.

INFRA-ESTRUTURA DE CHAVES PÚBLICAS DO BRASIL - ICP-BRASIL. **Net**. Disponível em: <<https://www.icpbrasil.gov.br/>> Acesso em: 03 jul. 2008.

INSTITUTO NACIONAL DE TECNOLOGIA - ITI. **Net**. Disponível em: <<http://www.iti.gov.br/>> Acesso em: 23 jul. 2008.

KAMINSKI, Omar (Org.). **Internet Legal: o direito na tecnologia da informação**. Curitiba: Juará, 2006.

MENKE, Fabiano. **Assinaturas digitais, certificados digitais, infra-estrutura de chaves públicas brasileira e a ICP alemã**. Internet Legal. Disponível em: <<http://www.internetlegal.com.br/>> Acesso em: 20 abr. 2008.

MENKE, Fabiano. **Assinatura Eletrônica: aspectos jurídicos no direito brasileiro**. São Paulo: Revista dos Tribunais, 2005.

MORAES, Alexandre de. **Direito Constitucional**. 17. ed. São Paulo: Atlas, 2005.

ORDEM DOS ADVOGADOS DO BRASIL – OAB. **Net**. Disponível em:
<<http://www.oab.org.br/>> Acesso em: 23 jul. 2008.

PEREIRA, Caio Mário da Silva. **Instituições do direito civil: volume 3**. 20. ed. Rio de Janeiro: Forense, 2004.

RECEITA FEDERAL DO BRASIL. **Net**. Disponível em:
<<http://www.receita.fazenda.gov.br/>> Acesso em: 15 ago. 2008.

REZENDE, Pedro Antonio Dourado de. **As possíveis leis de assinatura digital no Brasil**. Disponível em <<http://www.cici.unb.br/docentes/pedro/trabs/leis.htm>>. Acessado em 15/01/08.

SANTOS, Moacyr Amaral. **Primeiras linhas de direito processual civil: volume 2**. 23. ed. São Paulo: Saraiva, 2004.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS – SERPRO. **Net**. Disponível em: <<http://www.serpro.gov.br/>> Acesso em: 12 jul. 2008.

SILVA JUNIOR, Ronaldo Lemos da (Org.); WAISBERG, Ivo (Org.). **Comércio Eletrônico**. São Paulo: Revista dos Tribunais, 2001.

UNCITRAL. **Net**. Disponível em: <<http://www.uncitral.org/>> Acesso em: 05 out. 2008.

ANEXOS

ANEXO A – Medida Provisória 2.200-2 de 24 de agosto de 2001. (Institui a ICP-Brasil)

ANEXO B – Organograma ICP-Brasil (12 de novembro de 2008)

ANEXO C – Lei 11.419 de 19 de dezembro de 2006. (Informatização do processo judicial)

ANEXO D – Relação de Tribunais que aceitam o uso da certificação digital em seus expedientes

ANEXO A: MEDIDA PROVISÓRIA 2.200-2, DE 24 DE AGOSTO DE 2001



Presidência da República

Casa Civil

Subchefia para Assuntos Jurídicos

MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 2001.

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º Compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;

II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Parágrafo único. O Comitê Gestor poderá delegar atribuições à AC Raiz.

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 subsequente 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. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Art. 7º Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Art. 8º Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.

Art. 9º É vedado a qualquer AC certificar nível diverso do imediatamente subsequente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

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

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

Art. 11. A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no [art. 100 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional](#).

Art. 12. 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. 13. O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.

Art. 14. No exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei.

Art. 15. Integrarão a estrutura básica do ITI uma Presidência, uma Diretoria de Tecnologia da Informação, uma Diretoria de Infra-Estrutura de Chaves Públicas e uma Procuradoria-Geral.

Parágrafo único. A Diretoria de Tecnologia da Informação poderá ser estabelecida na cidade de Campinas, no Estado de São Paulo.

Art. 16. Para a consecução dos seus objetivos, o ITI poderá, na forma da lei, contratar serviços de terceiros.

§ 1º O Diretor-Presidente do ITI poderá requisitar, para ter exercício exclusivo na Diretoria de Infra-Estrutura de Chaves Públicas, por período não superior a um ano, servidores, civis ou militares, e empregados de órgãos e entidades integrantes da Administração Pública Federal direta ou indireta, quaisquer que sejam as funções a serem exercidas.

§ 2º Aos requisitados nos termos deste artigo serão assegurados todos os direitos e vantagens a que façam jus no órgão ou na entidade de origem, considerando-se o período de requisição para todos os efeitos da vida funcional, como efetivo exercício no cargo, posto, graduação ou emprego que ocupe no órgão ou na entidade de origem.

Art. 17. Fica o Poder Executivo autorizado a transferir para o ITI:

I - os acervos técnico e patrimonial, as obrigações e os direitos do Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e Tecnologia;

II - remanejar, transpor, transferir, ou utilizar, as dotações orçamentárias aprovadas na Lei Orçamentária de 2001, consignadas ao Ministério da Ciência e Tecnologia, referentes às atribuições do órgão ora transformado, mantida a mesma classificação orçamentária, expressa por categoria de programação em seu menor nível, observado o disposto no [§ 2º do art. 3º da Lei nº 9.995, de 25 de](#)

[julho de 2000](#), assim como o respectivo detalhamento por esfera orçamentária, grupos de despesa, fontes de recursos, modalidades de aplicação e identificadores de uso.

Art. 18. Enquanto não for implantada a sua Procuradoria Geral, o ITI será representado em juízo pela Advocacia Geral da União.

Art. 19. Ficam convalidados os atos praticados com base na [Medida Provisória nº 2.200-1, de 27 de julho de 2001](#).

Art. 20. Esta Medida Provisória entra em vigor na data de sua publicação.

Brasília, 24 de agosto de 2001; 180ª da Independência e 113ª da República.

FERNANDO HENRIQUE CARDOSO

José Gregori

Martus Tavares

Ronaldo Mota Sardenberg

Pedro Parente

Este texto não substitui o publicado no D.O.U. de 27.8.2001

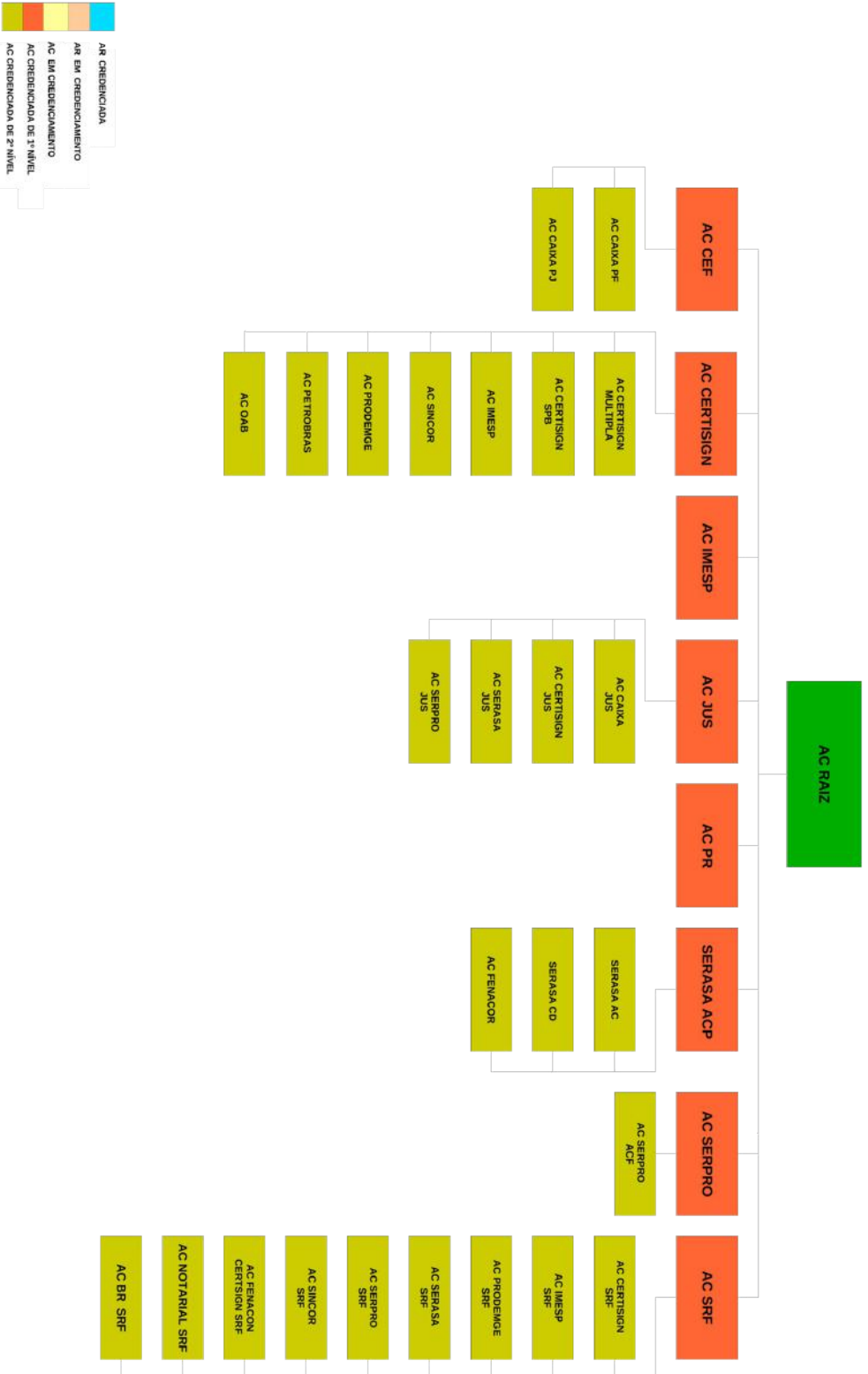
ANEXO B: ESTRUTURA DA ICP-BRASIL⁵³

⁵³ Instituto Nacional de Tecnologia da Informação. Net. Disponível em: <<http://www.iti.gov.br>> Acesso em: 13 nov. 2008.



Estrutura da ICP-Brasil

Atualizado: 30/10/2008



ANEXO C: LEI 11.419, DE 19 DE DEZEMBRO DE 2006



Presidência da República

Casa Civil

Subchefia para Assuntos Jurídicos

LEI Nº 11.419, DE 19 DE DEZEMBRO DE 2006.

Mensagem de veto

Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DA INFORMATIZAÇÃO DO PROCESSO JUDICIAL

Art. 1º O uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais será admitido nos termos desta Lei.

§ 1º Aplica-se o disposto nesta Lei, indistintamente, aos processos civil, penal e trabalhista, bem como aos juizados especiais, em qualquer grau de jurisdição.

§ 2º Para o disposto nesta Lei, considera-se:

I - meio eletrônico qualquer forma de armazenamento ou tráfego de documentos e arquivos digitais;

II - transmissão eletrônica toda forma de comunicação a distância com a utilização de redes de comunicação, preferencialmente a rede mundial de computadores;

III - assinatura eletrônica as seguintes formas de identificação inequívoca do signatário:

a) assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica;

b) mediante cadastro de usuário no Poder Judiciário, conforme disciplinado pelos órgãos respectivos.

Art. 2º O envio de petições, de recursos e a prática de atos processuais em geral por meio eletrônico serão admitidos mediante uso de assinatura eletrônica, na forma do art. 1º desta Lei, sendo obrigatório o credenciamento prévio no Poder Judiciário, conforme disciplinado pelos órgãos respectivos.

§ 1º O credenciamento no Poder Judiciário será realizado mediante procedimento no qual esteja assegurada a adequada identificação presencial do interessado.

§ 2º Ao credenciado será atribuído registro e meio de acesso ao sistema, de modo a preservar o sigilo, a identificação e a autenticidade de suas comunicações.

§ 3º Os órgãos do Poder Judiciário poderão criar um cadastro único para o credenciamento previsto neste artigo.

Art. 3º Consideram-se realizados os atos processuais por meio eletrônico no dia e hora do seu envio ao sistema do Poder Judiciário, do que deverá ser fornecido protocolo eletrônico.

Parágrafo único. Quando a petição eletrônica for enviada para atender prazo processual, serão consideradas tempestivas as transmitidas até as 24 (vinte e quatro) horas do seu último dia.

CAPÍTULO II

DA COMUNICAÇÃO ELETRÔNICA DOS ATOS PROCESSUAIS

Art. 4º Os tribunais poderão criar Diário da Justiça eletrônico, disponibilizado em sítio da rede mundial de computadores, para publicação de atos judiciais e administrativos próprios e dos órgãos a eles subordinados, bem como comunicações em geral.

§ 1º O sítio e o conteúdo das publicações de que trata este artigo deverão ser assinados digitalmente com base em certificado emitido por Autoridade Certificadora credenciada na forma da lei específica.

§ 2º A publicação eletrônica na forma deste artigo substitui qualquer outro meio e publicação oficial, para quaisquer efeitos legais, à exceção dos casos que, por lei, exigem intimação ou vista pessoal.

§ 3º Considera-se como data da publicação o primeiro dia útil seguinte ao da disponibilização da informação no Diário da Justiça eletrônico.

§ 4º Os prazos processuais terão início no primeiro dia útil que seguir ao considerado como data da publicação.

§ 5º A criação do Diário da Justiça eletrônico deverá ser acompanhada de ampla divulgação, e o ato administrativo correspondente será publicado durante 30 (trinta) dias no diário oficial em uso.

Art. 5º As intimações serão feitas por meio eletrônico em portal próprio aos que se cadastrarem na forma do art. 2º desta Lei, dispensando-se a publicação no órgão oficial, inclusive eletrônico.

§ 1º Considerar-se-á realizada a intimação no dia em que o intimando efetivar a consulta eletrônica ao teor da intimação, certificando-se nos autos a sua realização.

§ 2º Na hipótese do § 1º deste artigo, nos casos em que a consulta se dê em dia não útil, a intimação será considerada como realizada no primeiro dia útil seguinte.

§ 3º A consulta referida nos §§ 1º e 2º deste artigo deverá ser feita em até 10 (dez) dias corridos contados da data do envio da intimação, sob pena de considerar-se a intimação automaticamente realizada na data do término desse prazo.

§ 4º Em caráter informativo, poderá ser efetivada remessa de correspondência eletrônica, comunicando o envio da intimação e a abertura automática do prazo processual nos termos do § 3º deste artigo, aos que manifestarem interesse por esse serviço.

§ 5º Nos casos urgentes em que a intimação feita na forma deste artigo possa causar prejuízo a quaisquer das partes ou nos casos em que for evidenciada qualquer tentativa de burla ao sistema, o ato processual deverá ser realizado por outro meio que atinja a sua finalidade, conforme determinado pelo juiz.

§ 6º As intimações feitas na forma deste artigo, inclusive da Fazenda Pública, serão consideradas pessoais para todos os efeitos legais.

Art. 6º Observadas as formas e as cautelas do art. 5º desta Lei, as citações, inclusive da Fazenda Pública, excetuadas as dos Direitos Processuais Criminal e Infracional, poderão ser feitas por meio eletrônico, desde que a íntegra dos autos seja acessível ao citando.

Art. 7º As cartas precatórias, rogatórias, de ordem e, de um modo geral, todas as comunicações oficiais que transitem entre órgãos do Poder Judiciário, bem como entre os deste e os dos demais Poderes, serão feitas preferentemente por meio eletrônico.

CAPÍTULO III

DO PROCESSO ELETRÔNICO

Art. 8º Os órgãos do Poder Judiciário poderão desenvolver sistemas eletrônicos de processamento de ações judiciais por meio de autos total ou parcialmente digitais, utilizando, preferencialmente, a rede mundial de computadores e acesso por meio de redes internas e externas.

Parágrafo único. Todos os atos processuais do processo eletrônico serão assinados eletronicamente na forma estabelecida nesta Lei.

Art. 9º No processo eletrônico, todas as citações, intimações e notificações, inclusive da Fazenda Pública, serão feitas por meio eletrônico, na forma desta Lei.

§ 1º As citações, intimações, notificações e remessas que viabilizem o acesso à íntegra do processo correspondente serão consideradas vista pessoal do interessado para todos os efeitos legais.

§ 2º Quando, por motivo técnico, for inviável o uso do meio eletrônico para a realização de citação, intimação ou notificação, esses atos processuais poderão ser praticados segundo as regras ordinárias, digitalizando-se o documento físico, que deverá ser posteriormente destruído.

Art. 10. A distribuição da petição inicial e a juntada da contestação, dos recursos e das petições em geral, todos em formato digital, nos autos de processo eletrônico, podem ser feitas diretamente pelos advogados públicos e privados, sem necessidade da intervenção do cartório ou secretaria judicial, situação em que a autuação deverá se dar de forma automática, fornecendo-se recibo eletrônico de protocolo.

§ 1º Quando o ato processual tiver que ser praticado em determinado prazo, por meio de petição eletrônica, serão considerados tempestivos os efetivados até as 24 (vinte e quatro) horas do último dia.

§ 2º No caso do § 1º deste artigo, se o Sistema do Poder Judiciário se tornar indisponível por motivo técnico, o prazo fica automaticamente prorrogado para o primeiro dia útil seguinte à resolução do problema.

§ 3º Os órgãos do Poder Judiciário deverão manter equipamentos de digitalização e de acesso à rede mundial de computadores à disposição dos interessados para distribuição de peças processuais.

Art. 11. Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais.

§ 1º Os extratos digitais e os documentos digitalizados e juntados aos autos pelos órgãos da Justiça e seus auxiliares, pelo Ministério Público e seus auxiliares, pelas procuradorias, pelas autoridades policiais, pelas repartições públicas em geral e por advogados públicos e privados têm a mesma força probante dos originais, ressalvada a alegação motivada e fundamentada de adulteração antes ou durante o processo de digitalização.

§ 2º A arguição de falsidade do documento original será processada eletronicamente na forma da lei processual em vigor.

§ 3º Os originais dos documentos digitalizados, mencionados no § 2º deste artigo, deverão ser preservados pelo seu detentor até o trânsito em julgado da sentença ou, quando admitida, até o final do prazo para interposição de ação rescisória.

§ 4º [\(VETADO\)](#)

§ 5º Os documentos cuja digitalização seja tecnicamente inviável devido ao grande volume ou por motivo de ilegitimidade deverão ser apresentados ao cartório ou secretaria no prazo de 10 (dez) dias contados do envio de petição eletrônica comunicando o fato, os quais serão devolvidos à parte após o trânsito em julgado.

§ 6º Os documentos digitalizados juntados em processo eletrônico somente estarão disponíveis para acesso por meio da rede externa para suas respectivas partes processuais e para o Ministério Público, respeitado o disposto em lei para as situações de sigilo e de segredo de justiça.

Art. 12. A conservação dos autos do processo poderá ser efetuada total ou parcialmente por meio eletrônico.

§ 1º Os autos dos processos eletrônicos deverão ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garanta a preservação e integridade dos dados, sendo dispensada a formação de autos suplementares.

§ 2º Os autos de processos eletrônicos que tiverem de ser remetidos a outro juízo ou instância superior que não disponham de sistema compatível deverão ser impressos em papel, autuados na forma dos [arts. 166 a 168 da Lei nº 5.869, de 11 de janeiro de 1973 - Código de Processo Civil](#), ainda que de natureza criminal ou trabalhista, ou pertinentes a juizado especial.

§ 3º No caso do § 2º deste artigo, o escrivão ou o chefe de secretaria certificará os autores ou a origem dos documentos produzidos nos autos, acrescentando, ressalvada a hipótese de existir segredo de justiça, a forma pela qual o banco de dados poderá ser acessado para aferir a autenticidade das peças e das respectivas assinaturas digitais.

§ 4º Feita a autuação na forma estabelecida no § 2º deste artigo, o processo seguirá a tramitação legalmente estabelecida para os processos físicos.

§ 5º A digitalização de autos em mídia não digital, em tramitação ou já arquivados, será precedida de publicação de editais de intimações ou da intimação pessoal das partes e de seus procuradores, para que, no prazo preclusivo de 30 (trinta) dias, se manifestem sobre o desejo de manterem pessoalmente a guarda de algum dos documentos originais.

Art. 13. O magistrado poderá determinar que sejam realizados por meio eletrônico a exibição e o envio de dados e de documentos necessários à instrução do processo.

§ 1º Consideram-se cadastros públicos, para os efeitos deste artigo, dentre outros existentes ou que venham a ser criados, ainda que mantidos por concessionárias de serviço público ou empresas privadas, os que contenham informações indispensáveis ao exercício da função judicante.

§ 2º O acesso de que trata este artigo dar-se-á por qualquer meio tecnológico disponível, preferentemente o de menor custo, considerada sua eficiência.

§ 3º [\(VETADO\)](#)

CAPÍTULO IV

DISPOSIÇÕES GERAIS E FINAIS

Art. 14. Os sistemas a serem desenvolvidos pelos órgãos do Poder Judiciário deverão usar, preferencialmente, programas com código aberto, acessíveis ininterruptamente por meio da rede mundial de computadores, priorizando-se a sua padronização.

Parágrafo único. Os sistemas devem buscar identificar os casos de ocorrência de prevenção, litispendência e coisa julgada.

Art. 15. Salvo impossibilidade que comprometa o acesso à justiça, a parte deverá informar, ao distribuir a petição inicial de qualquer ação judicial, o número no cadastro de pessoas físicas ou jurídicas, conforme o caso, perante a Secretaria da Receita Federal.

Parágrafo único. Da mesma forma, as peças de acusação criminais deverão ser instruídas pelos membros do Ministério Público ou pelas autoridades policiais com os números de registros dos acusados no Instituto Nacional de Identificação do Ministério da Justiça, se houver.

Art. 16. Os livros cartorários e demais repositórios dos órgãos do Poder Judiciário poderão ser gerados e armazenados em meio totalmente eletrônico.

Art. 17. [\(VETADO\)](#)

Art. 18. Os órgãos do Poder Judiciário regulamentarão esta Lei, no que couber, no âmbito de suas respectivas competências.

Art. 19. Ficam convalidados os atos processuais praticados por meio eletrônico até a data de publicação desta Lei, desde que tenham atingido sua finalidade e não tenha havido prejuízo para as partes.

Art. 20. A Lei nº 5.869, de 11 de janeiro de 1973 - Código de Processo Civil, passa a vigorar com as seguintes alterações:

"Art. 38.

[Parágrafo único.](#) A procuração pode ser assinada digitalmente com base em certificado emitido por Autoridade Certificadora credenciada, na forma da lei específica." (NR)

"Art. 154.

Parágrafo único. (Vetado). [\(VETADO\)](#)

[§ 2º](#) Todos os atos e termos do processo podem ser produzidos, transmitidos, armazenados e assinados por meio eletrônico, na forma da lei." (NR)

"Art. 164.

Parágrafo único. A assinatura dos juízes, em todos os graus de jurisdição, pode ser feita eletronicamente, na forma da lei." (NR)

"Art. 169.

§ 1º É vedado usar abreviaturas.

§ 2º Quando se tratar de processo total ou parcialmente eletrônico, os atos processuais praticados na presença do juiz poderão ser produzidos e armazenados de modo integralmente digital em arquivo eletrônico inviolável, na forma da lei, mediante registro em termo que será assinado digitalmente pelo juiz e pelo escrivão ou chefe de secretaria, bem como pelos advogados das partes.

§ 3º No caso do § 2º deste artigo, eventuais contradições na transcrição deverão ser suscitadas oralmente no momento da realização do ato, sob pena de preclusão, devendo o juiz decidir de plano, registrando-se a alegação e a decisão no termo." (NR)

"Art. 202.

§ 3º A carta de ordem, carta precatória ou carta rogatória pode ser expedida por meio eletrônico, situação em que a assinatura do juiz deverá ser eletrônica, na forma da lei." (NR)

"Art. 221.

IV- por meio eletrônico, conforme regulado em lei própria." (NR)

"Art. 237.

Parágrafo único. As intimações podem ser feitas de forma eletrônica, conforme regulado em lei própria." (NR)

"Art. 365.

V- os extratos digitais de bancos de dados, públicos e privados, desde que atestado pelo seu emitente, sob as penas da lei, que as informações conferem com o que consta na origem;

VI - as reproduções digitalizadas de qualquer documento, público ou particular, quando juntados aos autos pelos órgãos da Justiça e seus auxiliares, pelo Ministério Público e seus auxiliares, pelas procuradorias, pelas repartições públicas em geral e por advogados públicos ou privados, ressalvada a alegação motivada e fundamentada de adulteração antes ou durante o processo de digitalização.

§ 1º Os originais dos documentos digitalizados, mencionados no inciso VI do **caput** deste artigo, deverão ser preservados pelo seu detentor até o final do prazo para interposição de ação rescisória.

§ 2º Tratando-se de cópia digital de título executivo extrajudicial ou outro documento relevante à instrução do processo, o juiz poderá determinar o seu depósito em cartório ou secretaria." (NR)

"Art. 399.

[§ 1º](#) Recebidos os autos, o juiz mandará extrair, no prazo máximo e improrrogável de 30 (trinta) dias, certidões ou reproduções fotográficas das peças indicadas pelas partes ou de ofício; findo o prazo, devolverá os autos à repartição de origem.

§ 2º As repartições públicas poderão fornecer todos os documentos em meio eletrônico conforme disposto em lei, certificando, pelo mesmo meio, que se trata de extrato fiel do que consta em seu banco de dados ou do documento digitalizado." (NR)

"Art. 417.

[§ 1º](#) O depoimento será passado para a versão datilográfica quando houver recurso da sentença ou noutros casos, quando o juiz o determinar, de ofício ou a requerimento da parte.

§ 2º Tratando-se de processo eletrônico, observar-se-á o disposto nos §§ 2º e 3º do art. 169 desta Lei." (NR)

"Art. 457.

.....

[§ 4º](#) Tratando-se de processo eletrônico, observar-se-á o disposto nos §§ 2º e 3º do art. 169 desta Lei." (NR)

"Art. 556.

[Parágrafo único.](#) Os votos, acórdãos e demais atos processuais podem ser registrados em arquivo eletrônico inviolável e assinados eletronicamente, na forma da lei, devendo ser impressos para juntada aos autos do processo quando este não for eletrônico." (NR)

Art. 21. [\(VETADO\)](#)

Art. 22. Esta Lei entra em vigor 90 (noventa) dias depois de sua publicação.

Brasília, 19 de dezembro de 2006; 185º da Independência e 118º da República.

LUIZ INÁCIO LULA DA SILVA

Márcio Thomaz Bastos

Este texto não substitui o publicado no DOU de 20.12.2006

ANEXO D: TRIBUNAIS QUE ACEITAM O USO DA CERTIFICAÇÃO DIGITAL EM SEUS EXPEDIENTES⁵⁴

⁵⁴ Ordem dos Advogados do Brasil. **Net**. Disponível em: <<http://www.oab.org.br>> Acesso em:05 nov. 2008.

Tribunais Superiores

STF

STJ

TST

Tribunais da Justiça Trabalhista

Tribunal Regional do Trabalho da 2ª Região (SP)

Tribunal Regional do Trabalho da 3ª Região (MG)

Tribunal Regional do Trabalho da 4ª Região (RS)

Tribunal Regional do Trabalho da 5ª Região (BA)

Tribunal Regional do Trabalho da 6ª Região (PE)

Tribunal Regional do Trabalho da 7ª Região (CE)

Tribunal Regional do Trabalho da 8ª Região (PA)

Tribunal Regional do Trabalho da 9ª Região (PR)

Tribunal Regional do Trabalho da 10ª Região (DF/TO)

Tribunal Regional do Trabalho da 13ª Região (PB)

Tribunal Regional do Trabalho da 14ª Região (RO/AC)

Tribunal Regional do Trabalho da 15ª Região (Campinas)

Tribunal Regional do Trabalho da 16ª Região (MA)

Tribunal Regional do Trabalho da 17ª Região (ES)

Tribunal Regional do Trabalho da 18ª Região (GO)

Tribunal Regional do Trabalho da 19ª Região (AL)

Tribunal Regional do Trabalho da 20ª Região (SE)

Tribunal Regional do Trabalho da 21ª Região (RN)

Tribunal Regional do Trabalho da 22ª Região (PI)

Tribunal Regional do Trabalho da 23ª Região (MT)

Tribunal Regional do Trabalho da 24ª Região (MS)

Tribunais de Justiça Estaduais

Tribunal de Justiça do Acre (Projudi)
Tribunal de Justiça do Alagoas (Projudi e e-Saj)
Tribunal de Justiça do Amazonas (Projudi e e-Saj)
Tribunal de Justiça da Bahia (Projudi)
Tribunal de Justiça do Ceará (Projudi)
Tribunal de Justiça do Distrito Federal (Projudi)
Tribunal de Justiça de Goiás (Projudi)
Tribunal de Justiça do Maranhão (Projudi)
Tribunal de Justiça do Mato Grosso (Projudi)
Tribunal de Justiça do Mato Grosso do Sul (e-Saj)
Tribunal de Justiça de Minas Gerais (Projudi)
Tribunal de Justiça do Pará (Projudi)
Tribunal de Justiça da Paraíba (e-Jus ou Projudi)
Tribunal de Justiça do Paraná (Projudi)
Tribunal de Justiça do Pernambuco (Projudi)
Tribunal de Justiça do Piauí (Projudi)
Tribunal de Justiça do Rio Grande do Norte (Projudi)
Tribunal de Justiça de Rondônia (Projudi e OAB-Cripton)
Tribunal de Justiça de Roraima (Projudi)
Tribunal de Justiça de São Paulo (e-Saj)
Tribunal de Justiça de Santa Catarina (e-Saj)
Tribunal de Justiça do Tocantins (Projudi)