UNIVERSIDADE DE SÃO PAULO

ESCOLA POLITÉCNICA

AIRTON ROBERTO GUELFI

ANÁLISE DE ELEMENTOS JURÍDICO-TECNOLÓGICOS QUE COMPÕEM A ASSINATURA DIGITAL CERTIFICADA DIGITALMENTE PELA INFRA-ESTRUTURA DE CHAVES PÚBLICAS DO BRASIL - ICP-BRASIL.

São Paulo

2007

AIRTON ROBERTO GUELFI

ANÁLISE DE ELEMENTOS JURÍDICO-TECNOLÓGICOS QUE COMPÕEM A ASSINATURA DIGITAL CERTIFICADA DIGITALMENTE PELA INFRA-ESTRUTURA DE CHAVES PÚBLICAS DO BRASIL - ICP-BRASIL.

Dissertação apresentada à
Escola Politécnica da Universidade de São Paulo
para a obtenção do título de
Mestre em Engenharia Elétrica

São Paulo

2007

AIRTON ROBERTO GUELFI

ANÁLISE DE ELEMENTOS JURÍDICO-TECNOLÓGICOS QUE COMPÕEM A ASSINATURA DIGITAL CERTIFICADA DIGITALMENTE PELA INFRA-ESTRUTURA DE CHAVES PÚBLICAS DO BRASIL - ICP-BRASIL.

Dissertação apresentada à Escola
Politécnica da Universidade de São Paulo
para a obtenção do título de Mestre em Engenharia Elétrica

Área de Concentração:
Sistemas Eletrônicos

Orientador: Prof. Livre Docente
Pedro Luís Próspero Sanchez

São Paulo

2007

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, 09 de maio de 2007.

Airton Roberto Guelfi

Prof. Dr. Pedro Luís Próspero Sanchez

FICHA CATALOGRÁFICA

Guelfi, Airton Roberto
Análise de elementos jurídico-tecnológicos que compõem a assinatura digital certificada digitalmente pela infra-estrutura de chaves públicas do Brasil (ICP-Brasil) / A.R. Guelfi. – ed.rev. - São Paulo, 2007.
135 p.

Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.

1. Certificação digital (Aspectos jurídicos) – Brasil I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Sistemas Eletrônicos II.t.

DEDICATÓRIA

Dedico este trabalho à dois homens:
Meu pai, Antonio Guelfi,
por me ensinar a lutar;
Meu filho, João Antonio Tafarelo Guelfi
por ser a razão de minha luta.

AGRADECIMENTOS

Uma vitória nunca é conquistada isoladamente. É formada por auxílio e cooperação de um grupo.

Nesta oportunidade gostaria de render meus mais sinceros agradecimentos a todos aqueles que me auxiliaram nesta vitória:

A DEUS, acima de tudo, pela vida.

A meus pais, Antonio Guelfi (in memoriam) e Aparecida Garbeloto Guelfi pela dedicação, apoio e confiança.

Ao meu orientador, Professor Livre Docente Pedro Luís Próspero Sanchez, homem que aprendi a admirar e respeitar durante esta jornada em virtude dos ensinamentos que me levaram à conclusão do trabalho.

A Miki, pelo carinho e paciência.

Ao Mestre Engº. Ákio Nogueira Barbosa, pelas proveitosas discussões técnicas que contribuíram decisivamente.

À Mestre Jackeline Gonçalves da Silva, pelas pertinentes considerações que foram dirigidas.

Ao Natanael (Nata) e ao Cícero, por todo suporte técnico que me proporcionaram.

À Escola Politécnica da Universidade de São Paulo e ao Laboratório de Sistemas Integráveis por proporcionar total infra-estrutura.

A todos os amigos e amigas que torceram e acreditaram na minha vitória.

RESUMO

Este trabalho faz uma análise crítica dos elementos jurídicos-tecnológicos de uma assinatura digital certificada digitalmente. O primeiro aspecto a ser abordado advém da verificação da competência para o desenvolvimento da atividade de certificação, em decorrência da natureza jurídica do certificado digital. Consoante se verificou, o certificado digital é o instrumento hábil a assegurar a autenticidade dos documentos eletrônicos por meio de uma assinatura digital. Dessa forma, equipara-se ao ato de reconhecimento de firma, atividade notarial desenvolvida pelos Cartórios Notariais, de acordo com a competência fixada no artigo 236 da Constituição da República Federativa do Brasil. Todavia, segundo regra presente na Medida Provisória 2.200-2/01, desde 2001 essa atividade vem sendo desenvolvida sob a competência do Governo Federal, através do Instituto Nacional de Tecnologia da Informação – ITI (Autoridade Certificadora Raiz da Infra-estrutura de Chaves Públicas do Brasil. Como decorrência tem-se que a Medida Provisória 2.200-2/01 é inconstitucional, uma vez que não respeita regra de competência material fixada pela Constituição da República Federativa do Brasil para o desenvolvimento da atividade notarial. Sob um prisma tecnológico, têm-se que a ICP-Brasil, por meio de seu Comitê Gestor, fixa expressamente qual a tecnologia que deve ser empregada para a produção das assinaturas digitais. Neste caminho, até maio de 2006, entre outros, foi indicado o algoritmo criptográfico de função *hash* MD5 para a geração das assinaturas digitais com autenticidade e integridade garantidas por lei. Todavia, o MD5 perdeu sua utilidade em 2004, quando foi quebrado, ocasionando a possibilidade de fraudes, inclusive a geração de documentos eletrônicos forjados. Sem dúvida, a legislação brasileira vinha assegurando validade jurídica e força probante a documentos eletrônicos assinados com algoritmo criptográfico de função *hash* MD5 que poderiam ter sido forjados. Para que o documento eletrônico assinado digitalmente possa ser amplamente utilizado em relações sociais é preciso que regras jurídicas e tecnológicas sejam respeitadas, sob pena de se criar uma enorme insegurança social.

Palavras chave – Certificação digital; Assinatura digital; Infra-estrutura de Chaves Públicas.

ABSTRACT

This work presents a critical analysis of the technology and law aspects of certified digital signatures, and their implementation in Brazil. We discuss and verify the competency rules that apply to the certification activity according to the legal nature of the digital certificate. A digital certificate is the instrument that secures the authenticity of an electronic document by means of a digital signature. According to the article 236 of the Brazilian Constitution, authenticity certifications are of exclusive competence of public notaries. Nevertheless, based on an under constitutional statute, digital certification has being conducted by the Federal Government thru its National Institute of Information Technology (Instituto Nacional de Tecnologia da Informação – ITI), who is responsible for the Brazilian public key root certification authority. We found that the statute that supports those activities (Medida Provisória 2.200-2/01) is unconstitutional, and therefore invalid and unenforceable, since it does not satisfy constitutional rules of material competency.

Under a technology view, we find that the Managing Committee of the Brazilian Public Key Infrastructure explicitly defines the technology to be used in digital signatures. According to that ruling, until may 2006, among others, the MD5 hashing algorithm was used to generate digital signatures with statutory presumption of authenticity and integrity. Nevertheless, MD5 lost its technical usefulness in 2004, when it was broken, and became prone to fraud such as the generation of forged electronic documents. There is no doubt that Brazilian legislation gave legal value and probatory force to electronic documents signed using the already broken MD5 hashing algorithm that could very well had been forged.

Digitally signed electronic documents can only be successfully used if legal rules and the technological aspects be fully understood and respected. Otherwise, the result will be high levels of uncertainty in law relations.

Keywords – digital certification, digital signature, public key infrastructure.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

AC	Autoridade Certificadora
AC-RAIZ	Autoridade Certificadora Raiz
AC-SUB	Autoridade Certificadora Subseqüente
AR	Autoridade de Registro
ARs	Autoridades de Registro
Art.	Artigo de lei
CC	Código Civil
CEPESC	Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações
CF	Constituição da República Federativa do Brasil
CG	Comitê Gestor
CLT	Consolidação das Leis Trabalhistas
CP	Código Penal
CPC	Código de Processo Civil
CPP	Código de Processo Penal
Dec.	Decreto
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infra-estrutura de Chaves Públicas
ITI	Instituto Nacional de Tecnologia da Informação
LCR	Lista de Certificados Revogados

MD5 *Message-Digest algorithm 5.*

MP Medida Provisória

Par. Parágrafo

PL Projeto de lei

SERPRO Serviço Federal de Processamento de Dados

SHA1 *Secure Hash Algorithm*

UNCITRAL United Nations Commission on International Trade Law (Comissão das Nações Unidas para o Direito Mercantil Internacional)

SUMÁRIO

1 INTRODUÇÃO

O certificado digital tem por objetivo imediato a validade e a força probante dos documentos em formato eletrônico assinados digitalmente, assegurando os requisitos legais exigidos para os documentos.[1]

A atividade de certificação digital no Brasil vem sendo explorada de forma sistemática, sob a competência do Poder Executivo Federal. A finalidade primordial da atividade certificatória consiste na popularização do uso de certificados digitais, promovendo a inclusão digital.

O Instituto Nacional de Tecnologia da Informação - ITI é uma Autarquia Federal vinculada ao Ministério da Casa Civil da Presidência da República. O ITI exerce a função de Autoridade Certificadora Raiz – AC-Raiz na Infra-estrutura de Chaves Públicas – ICP, responsável pelo desenvolvimento administrativo da atividade de certificação.

A ICP-Brasil ainda é composta por um órgão normativo denominado de Comitê Gestor, responsável pela edição das normas técnicas utilizadas pela AC-Raiz na atividade e implementação de um sistema de certificação digital baseado em chaves públicas.

A atividade de certificação digital representa um elemento importante no desenvolvimento de vários setores da sociedade mundial. Para citarmos um, toma-se como exemplo o setor comercial, que tem crescido muito após a inclusão da Internet.

Em razão da atividade de certificação digital estar intrinsecamente ligada ao exercício dos poderes estatais, mister se faz, estarem presentes em sua estruturação a observância das regras de competência fixadas para o exercício desse poder.

Mas a validade e a força probante das assinaturas digitais não dependem apenas de aspectos jurídicos. Os aspectos tecnológicos também devem ser discutidos.

Com o decorrer do tempo, a tecnologia empregada na realização das assinaturas digitais torna-se obsoleta, trazendo à tona problemas nunca antes

---

[1] - Conforme o artigo 1.º da Medida Provisória 2.200-2/01.

enfrentados como, por exemplo, a perda da garantia de integridade do documento eletrônico.

1.1 Objetivos

O objetivo principal do presente trabalho desdobra-se em duas vertentes. A primeira, de caráter jurídico, consiste na fixação da natureza jurídica da certificação digital. Para essa fixação, levaremos em consideração a possibilidade do certificado digital conferir ou não presunção de legitimidade quanto a autoria do documento eletrônico. Com esta idéia, poderemos apontar quais normas de competência material fixada pela CF devem ser observadas para o desenvolvimento da atividade de certificação digital.

A definição da natureza jurídica da certificação digital representa o marco inicial para a análise da competência material constitucional para o desenvolvimento da atividade de certificação digital, e esta definição variará de acordo com a interpretação auferida da Medida Provisória 2.200-2/01.

Dessa forma, seremos capazes de convalidar ou repudiar o atual modelo de prestação do serviço público de certificação digital pelo Poder Executivo Federal, através do Instituto Nacional de Tecnologia da Informação, autarquia federal vinculada à Casa Civil da Presidência da República.

A segunda vertente, de caráter tecnológico, baseia-se no estudo dos problemas encontrados na utilização dos algoritmos de função de hash pela ICP-Brasil, no desenvolvimento da atividade de certificação digital, conforme previsão expressa da Declaração de Práticas de Certificação da AC-Raiz. Com a evolução da tecnologia, aspectos como algoritmos criptográficos de função *hash* poderão sofrer abalos que serão sentidos na segurança jurídica dos documentos eletrônicos.

1.2 Justificativas

A utilização das assinaturas digitais vem gradativamente ganhando espaço, em detrimento de artefatos milenares, como o papel e a tinta para escrever.

A assinatura digital confere segurança jurídica aos documentos eletrônicos que antes eram encarados com desprestígio, em virtude da falta de confiabilidade. Por meio da assinatura digital e do certificado digital é possível assegurar aos documentos eletrônicos os requisitos legais da autenticidade e integridade.

A concepção de certificado digital está atrelada à segurança jurídica que a assinatura digital confere. O certificado digital representa uma garantia estatal quanto à validade da assinatura digital. Apoiado nestas razões, vários são os países que já possuem uma estruturação estatal voltada para a exploração do serviço de certificação digital, incluindo-se neste quadro o Brasil.

Todavia, o exercício do poder público de certificação digital somente terá legitimidade se houver o respeito às regras legais de competência material fixadas pela Constituição Federal.

Outro ponto importante diz respeito a perpetuidade dos documentos. Os documentos eletrônicos somente possuem força probante se assegurados a autenticidade e a integridade do documento no passar dos anos. Qual será o impacto da evolução tecnológica diante da característica de perpetuidade que os documentos devem deter?

Uma análise técnica faz-se necessária para apontar possíveis falhas quanto à perpetuidade da integridade dos documentos eletrônicos assinados digitalmente. Os problemas enfrentados pelos algoritmos de função *hash* estão atrelados à integridade que a assinatura digital confere.

1.3 Trabalhos relacionados

A infra-estrutura de Chaves Públicas do Brasil (ICP-Brasil), representa o conjunto de regras e procedimentos que devem ser aplicados pelo Instituto Nacional de Tecnologia da Informação, no desenvolvimento da atividade de certificação digital.

A principal finalidade das respectivas regras e procedimentos corresponde em assegurar a autenticidade, integridade e validade jurídica dos documentos eletrônicos assinados digitalmente.

Os órgãos responsáveis por referida tarefa estão hierarquicamente subordinados à Casa Civil da Presidência da República, desenvolvendo o serviço público de certificação digital sob o exercício de poder do Poder Executivo Federal.

O trabalho de Silvestre[2] (2003) representa uma complementação paralela da presente dissertação. Realiza a análise da competência legislativa do Poder Executivo Federal para a implementação de uma Infra-estrutura de Chaves Públicas do Brasil e para a criação de uma autarquia federal para ocupar a posição de Autoridade Certificadora Raiz, através de ato normativo denominado "Medida Provisória". Naquele trabalho, o autor conclui pela incompetência legislativa do Poder Executivo Federal, tendo em vista que o rol de possibilidades aplicadas à utilização de medidas provisórias não vislumbra tal possibilidade.

1.4 Estrutura da dissertação

O capítulo 2 apresenta o estudo da evolução legislativa da Medida Provisória 2.200-2/01 e as principais tendências mundiais sobre o tema. Apresenta ainda um simplificado esboço atual sobre a competência notarial no ordenamento jurídico brasileiro.

O capítulo 3 traz uma apresentação das atuais regras e procedimentos oriundos da Infra-estrutura de Chaves Públicas do Brasil que devem ser seguidas pelo ITI, na prestação da atividade pública de certificação digital. O presente exame se faz necessário pois representa o atual conjunto de regras e procedimentos que serão analisados perante as regras de competência da Constituição Federal.

O capítulo 4 descreve os principais pontos jurídicos que circundam a utilização dos documentos eletrônicos. Neste caso, é apresentado um estudo sobre o documento eletrônico, e sua evolução no cenário jurídico brasileiro. A razão disto encontra-se no fato de que o certificado digital desenvolve papel primordial para a consideração jurídica dos documentos eletrônicos.

---

[2] **- SILVESTRE, Fábio André Chedid**. A ilegitimidade constitucional crítica da Infra-estrutura de Chaves Públicas Brasileira. Uma Semiótica do Poder.2003. 111 p. Dissertação de Mestrado. Universidade Federal de Santa Catarina. Programa de Pós-Graduação. Engenharia de Produção e Sistemas. Florianópolis (SC). 2003.

O capítulo 5 discorre sobre o exame da assinatura digital, trazendo suas implicações técnicas e jurídicas. O fundamento encontra-se na relação de autenticidade que o certificado digital implementa no uso da assinatura digital.

O capítulo 6 apresenta o trabalho realizado no sentido de fixar a natureza jurídica da certificação digital sob o aspecto funcional de conferir ou não presunção de legitimidade de autoria aos documentos eletrônicos, e por conseqüência, verificar a aplicação das regras de competência material fixadas na Constituição Federal. Podemos assim, apontar os principais requisitos jurídicos que devem ser levados em consideração no momento de se implantar uma ICP.

O capítulo 7 aborda a utilização dos algoritmos de função *hash* para a realização das assinaturas digitais e os principais aspectos dos problemas técnicos enfrentados diante da evolução natural da tecnologia.

Por fim, o capítulo 8 apresenta as principais conclusões e sugere possíveis trabalhos futuros relacionados.

2 ELEMENTOS LEGAIS

O direito, enquanto ordem coercitiva[3], é responsável pela regulamentação da vida social, impondo aos membros da sociedade regras que devem ser seguidas, com o propósito de alcançar a conduta humana pretendida para o bem estar social[4]. Quando o Código Penal - CP, em seu artigo 121, tipifica o crime de homicídio, procura induzir uma conduta humana diversa daquela capaz de produzir a morte de terceiro, preservando o bem maior que é a vida. Da mesma forma, o Código Civil, em seu artigo 104[5], fixa os requisitos mínimos para a validade jurídica dos atos jurídicos, descrevendo formas de agir, diretamente, protegendo as relações humanas que criam, alteram ou extinguem direitos e deveres. A fundamentação para essas proteções está representada pelo bem estar social que a proteção à vida e às relações humanas gera. Toda vez que uma específica situação interfere no bem estar social da comunidade, para o direito nasce a prerrogativa de coercitivamente impor uma solução para a controvérsia por meio de sanções, de forma a melhor atender aos anseios sociais.

Com os documentos eletrônicos, assinaturas digitais e certificados digitais não foi diferente. Partindo do pressuposto sobre qual o instrumento utilizado para fixar direitos e obrigações no tempo, conhecido como documento, passou a encontrar um novo paradigma com a criação do que denominamos “documento eletrônico”. Surgiu para a ciência jurídica a necessidade de regular coercitivamente este novo modelo documental, de forma a melhor atender aos anseios sociais. O mister de adaptar a nova realidade eletrônica aos conceitos legais clássicos de

---

3 - KELSEN, Hans. Teoria Geral do Direito e do Estado. 3ª. edição. São Paulo. Editora Martins Fontes. 2000. Hans Kelsen ensina que as normas jurídicas, ao contrário daquelas que não possuem força coercitiva, são impostas aos indivíduos mesmo contra sua vontade, descrevendo que “as ordens coercitivas são contrastadas com as que não possuem caráter coercitivo, que repousam na obediência voluntária. Isso é possível apenas no sentido de que uma estabelece medidas de coerção, ao passo que a outra não faz. E essas sanções são medidas coercitivas apenas no sentido de que certas posses são tiradas dos indivíduos em questão contra sua vontade, se necessário pelo emprego de força física.

4 - REALE, Miguel. Filosofia do direito. 20ª. edição. São Paulo. Editora Saraiva. 2002. Segundo o doutrinador, que usa dos ensinamentos de Scheler, o bem social será atingido sempre que o bem do indivíduo for preservado, como ponto essencial, sem prejudicar o bem do todo: “Na realidade, impõe-se preservar o bem do indivíduo como ponto final, como fim a que se deve tender de maneira dominante, mas ao mesmo tempo e correspondentemente, é mister salvo guardar e acrescer o bem do todo, naquilo que o bem social é condição do bem de cada qual.”

5 - “Art. 104. A validade do negócio jurídico requer: I – agente capaz; II – Objeto lícito, possível, determinado ou determinável; III – Forma prescrita ou não defesa em lei.”

documento e assinatura culminou no desenvolvimento legal de normas com a finalidade de situar o tema no arcabouço jurídico brasileiro.

As primeiras propostas de regulamentação da sistemática do documento eletrônico no Brasil surgiram no ano de 1.999, com os projetos de lei n.º 1.589/99[6] e projeto de lei n.º 1.483/99[7]. Entrementes, ambas propostas encontram-se em tramitação pelo Congresso Nacional, aguardando discussão e votação a fim de serem aprovadas, não possuindo, ainda, força de lei aplicável nas relações jurídico-sociais.

Atualmente, a "*validade jurídica, a autenticidade e a integridade"* do documento eletrônico, assinatura digital e certificação digital são asseguradas pela Medida Provisória 2.200-2/01, ou consoante disserta Rover e Veiga (2003, p. 01): "Em outras palavras, a MP dá o passo inicial para que uma infra-estrutura tecnológica, baseada na emissão de certificado e assinaturas digitais, seja criada a partir de regras e órgãos por ela definidos." [8]

Destarte, o presente capítulo discorre a respeito dos conceitos básicos sobre as normas jurídicas que aplicam-se na atividade de certificação digital, quando abordaremos os pontos sobre a validade jurídica e força probante do documento eletrônico na atual moldura legal brasileira. Seguindo neste raciocínio, o presente estudo buscará identificar os pressupostos legais exigidos pela referida Medida Provisória para assegurar a validade jurídica do diploma eletrônico.

2.1.Estrutura legal

Como descreve o artigo 1.º da Medida Provisória 2.200-2/01, a instituição da Infra-estrutura de Chaves Públicas Brasileira tem por finalidade garantir a autenticidade, integridade e validade jurídica dos documentos eletrônicos e as aplicações habilitadas que utilizem a certificação digital.

---

6 - O projeto de lei 1.589/99 foi apensado ao projeto de lei 1.483/99, por recomendação da Mesa Diretora da Câmara dos Deputados em 24 de Setembro de 1.999.

7 - O projeto de lei 1.483/99 foi apensado ao projeto de lei 4.906/01, por recomendação da Comissão especial destinada a proferir parecer técnico sobre o referido projeto de lei em data de 25 de Junho de 2.001.

8 - **ROVER, Aires José; VEIGA, Luiz Adolfo Olsen da.** In *"Validade jurídica de documentos eletrônicos assinados com infra-estruturas diferentes da ICP-Brasil.* 2003. Disponível em: http://www.buscalegis.ufsc.br/arquivos/artigoairesolsenbuscalegis.pdf . Acessado em 18 de Outubro de 2006.

A escassa doutrina sobre o assunto reconhece a referida Medida Provisória como fonte inicial de validade e legitimidade do documento eletrônico. Todas as regras de competência encontradas nos órgãos que compõem a ICP-Brasil são originalmente fixadas em seu texto. Os atos administrativos oriundos do Comitê Gestor, que visam orientar a ICP-Brasil no desenvolvimento de sua função administrativa, também devem encontrar respaldo legal nos parâmetros da Medida Provisória 2.200-2/01.

2.1.1 Contexto Histórico

Dentro de um contexto histórico, a primeira versão da Medida Provisória, foi publicada no dia 28 de junho de 2001, composta por apenas 15 artigos e contendo graves equívocos que comprometiam a segurança jurídica do sistema de certificação digital no Brasil.

Dentre as principais críticas direcionadas à primeira versão (Costa e Marcacini, 2004), podemos destacar a obrigatoriedade da geração do par de chaves criptográficas nos próprios computadores das autoridades certificadoras, conforme era previsto no artigo 8°, e a presença de um órgão do serviço de inteligência do Governo Federal, conforme dispunha o artigo 4º da versão original, denominado de Centro de Pesquisa e Desenvolvimento para a Segurança das Informações – CEPESC - assessorando o Comitê Gestor da ICP-Brasil em relação à sua tarefa de fixar diretrizes.[9]

Nesta primeira versão, conforme fixava o artigo 11, certificados digitais emitidos por entidades certificadoras não credenciadas junto à ICP-Brasil não possuíam valor jurídico, salvo os casos de certificações cruzadas previamente aprovadas pelo próprio Comitê Gestor.

Na segunda versão da Medida Provisória, e correspondente à primeira reedição, datada de 27 de julho de 2001, foram inseridas importantes modificações no artigo 8º, no tocante à produção do par de chaves criptográfico. Especificamente, foi suprimido do “caput” do referido artigo a exigência segundo a qual o par de chaves criptográfico deveria ser gerado na própria autoridade

---

[9] **- COSTA, Marcos da. MARCACINI, Augusto Tavares Rosa.** Direito em Bits. São Paulo. Editora Fiuza. 2004. Pág. 101.

certificadora. Com isso, foi incorporado um parágrafo único ao artigo 8.º, determinando expressamente que o par de chaves criptográficas será gerado sempre pelo próprio titular, e sua chave privada para assinatura será de seu exclusivo controle, uso e conhecimento.

Todavia, a primeira reedição da referida Medida Provisória obteve o mesmo destino do texto inicial, qual seja, foi revogada por uma segunda reedição. Em 24 de Agosto de 2.001, a segunda reedição, introduzindo uma terceira versão do texto, foi publicada pelo Governo Federal.

Esta segunda reedição, cuja designação se expressa pelo número 2.200-2/01, contém 20 artigos e esta em vigor atualmente porque sua edição foi anterior à Emenda Constitucional 32/01 de setembro de 2.001 que restringiu o uso de reedições de medidas provisórias.

Nesta segunda reedição, duas importantes modificações foram realizadas no corpo legal da MP 2.200-2/01.

O primeiro destaque refere-se à exclusão do órgão de assessoramento do Comitê Gestor – CEPESC – conforme reclamava a doutrina especializada, ao referir-se ao órgão como um ente de inteligência do governo voltado para a obtenção de informações confidenciais.

A segunda importante modificação realizada versa sobre os artigos 10 e 11. Nesta última versão, a regra de exclusividade de certificação digital assegurada à ICP-Brasil foi excluída amoldando-se às exigências da UNCITRAL[10]. Com isto, foram incluídos dois parágrafos no artigo 10, conferindo expressamente a possibilidade de existência de certificações digitais válidas e emitidas fora do âmbito da ICP-Brasil.

O parágrafo primeiro do referido artigo 10, cuida da presunção de veracidade, em relação aos signatários, das declarações contidas em documento eletrônico assinado digitalmente com a utilização do processo eletrônico de

---

10 **-** A UNCITRAL corresponde a um organismo ligado as Nações Unidas, responsável pela harmonização e unificação de leis internacionais. Na própria definição da ONU: The United Nations Commission on International Trade Law (UNCITRAL) (established in 1966) is a subsidiary body of the General Assembly of the United Nations with the general mandate to further the progressive harmonization and unification of the law of international trade. UNCITRAL has since prepared a wide range of conventions, model laws and other instruments dealing with the substantive law that governs trade transactions or other aspects of business law which have an impact on international trade. UNCITRAL meets once a year, typically in summer, alternatively in New York and in Vienna.

certificação digital disponibilizado pela ICP-Brasil[11]. Por sua vez, o parágrafo segundo, objetivando calar as críticas referentes à condição monopolizante de validade jurídica aos documentos eletrônicos assinados digitalmente, utilizando certificação digital ligada a ICP-Brasil, conferiu, expressamente, validade jurídica e probatória aos certificados emitidos fora do âmbito da ICP-Brasil, desde que aceito pelas partes[12], seguindo as recomendações feitas pela UNCITRAL, em seu modelo de lei para o comércio eletrônico editado em 1.999.

2.1.2 O que é uma Medida Provisória

Na atualidade, como alhures discorrido, a principal fonte legal de respaldo dos documentos eletrônicos no Brasil é a Medida Provisória 2.200-2/01.

Sem dúvida, as atuais medidas provisórias, consideradas espécies normativas de natureza infraconstitucional, dotadas de força e eficácia legal[13], tendo em vista seu caráter impessoal e genérico, editadas pelo Poder Executivo, consoante o princípio da legalidade (Silva, 2001)[14], representam o mais claro legado dos antigos decretos-lei, instrumentos legislativos larga e abusivamente utilizados pelos Presidentes da República, sob o argumento da urgencialidade.

Todavia, o atual modelo foi baseado nos chamados *"decreti-legge in casi straordinarii di necessitá e d'urgenza"* previstos no artigo 77 da atual Constituição Italiana. Não obstante o desvirtuamento sofrido pelo exercício de legislar do Poder Executivo (Moraes, 2003) (via de regra, as Medidas Provisórias não tratam de objetos em caráter de urgência), o referido dispositivo demonstra sua

---

11 - § 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.

12 - A Medida Provisória 2.200-2/01 não faz referência expressa de como esta aceitação reciproca de certificado digital fora do âmbito da ICP-Brasil poderá ser a expressada no mundo jurídico, visando um caráter probatório. Defronte a esta condição, podemos sugerir a realização de um contrato entre as partes, respeitando os requisitos de validade do negócio jurídico constantes do Código Civil, expressando as características de cada certificado utilizado entre as partes, assinado por duas testemunhas, e registrado no Serviço Notarial competente.

13 - Conforme jurisprudência do STF: MS 22.649, Rel. Min. Moreira Alves, DJ 20/11/96).

14 - Conforme José Afonso da Silva: "*significa a submissão e o respeito à lei, ou a atuação dentro da esfera estabelecida pelo legislador."* Curso de Direito Constitucional Positivo. 19ª. edição. Editora Malheiros. São Paulo. 2001. Pág. 425.

importância diante de situações onde se exige realmente um ato normativo excepcional e célere, para situações de relevância e urgência.[15]

Com o escopo de reprimir este desvirtuamento sofrido pelo uso das medidas provisórias, pois o Governo Federal passou a assumir um papel legiferante, semelhante ao Congresso Nacional, foi promulgada a Emenda Constitucional n.º 32, em 11 de Setembro de 2.001, impondo uma validade de 60 dias para as medidas provisórias, a contar da data de promulgação, a fim de serem avaliadas pelo Poder Legislativo, sob pena de perder a validade.

Agregado a esta nova regra, a referida emenda constitucional proíbe ainda a reedição das medidas provisórias dentro de um mesmo exercício legislativo.

Por outro lado, a Medida Provisória 2.200-2/01 ainda possui eficácia em razão de sua promulgação haver ocorrido anteriormente a data de promulgação da referida Emenda Constitucional n.º 32/01.

2.2 A atividade notarial

A atividade notarial visa assegurar a publicidade, autenticidade, segurança e eficácia dos atos jurídicos preventivamente. Com isso, é possível conferir às relações jurídicas que se utilizam da atividade notarial uma confiabilidade que as destaca das demais relações.

Esta confiabilidade é alcançada por meio de três princípios que servem à atividade notarial. O primeiro princípio é o da “fé pública notarial”.

Consoante ensinamentos de Ceneviva (2002)[16]a fé pública notarial representa a confiança depositada pela lei ao Tabelião para que no desempenho de sua função afirme, com presunção de veracidade, a eficácia dos negócios jurídicos. Isto significa, conforme ensina Rezende (2006)[17] que o notário é uma autoridade da sociedade nesse setor, vindo a garantir a certeza e autenticidade naquilo que exara.

---

[15] - MORAES, Alexandre de. Direito Constitucional. 13.º edição. São Paulo. Editora Atlas, 2003. Pág. 551.

[16] - CENEVIVA. Walter. Lei dos notários e registradores comentada (Lei n.º 8.935/94). 4ª. Edição. Editora Saraiva. São Paulo, 2002. Pág. 30.

[17] - REZENDE, Afonso Celso F. Tabelionato de Notas e o notário perfeito. 4ª. Edição. Editora Millennium. Campinas (SP). 2006. Pág. 31.

O segundo diz respeito a forma dos atos notariais. Quando são fixadas formas para os atos notarias por meio da lei, em verdade se quer assegurar que os atos respeitam todos os requisitos legais exigidos para a confiabilidade depositada. O desrespeito à forma poderá levar a nulidade do ato.

O terceiro princípio atinente à atividade notarial é o da autenticação, segundo o qual existe a certeza da existência do fato ou ato jurídico. O Notário, ao exercer o seu poder sobre o ato ou fato jurídico distinto, confere-lhe e certeza de sua existência para o mundo jurídico (Ceneviva, 2002).

O serviço público notarial fica caracterizado quando se verifica que a Constituição Federal (artigo 236) determinou que a fé pública será delegada a um indivíduo que, agindo conforme as formas legalmente determinadas, satisfaça a segurança legal dos atos judiciais (Rezende, 2006)[18]

Pela análise do artigo 22, inciso XXV, da CF, a competência legislativa sobre os registros públicos e serviços notariais é privativa da União (Antunes, 2005)[19]. Conforme bem demonstra, a presente regra deve ser interpretada de acordo com o artigo 236 da CF.

De acordo com o citado artigo 236 da CF, os serviços notariais e de registro são exercidos em caráter privado, por delegação do Poder Público. Dessa forma, o ente federativo responsável pela delegação do poder ao Notário é o Estado. Consoante ensinamentos de Ceneviva (2002 p.09) "*em cada Estado a delegação é outorgada pelo Poder Executivo local, na forma da lei estadual."*

Sem dúvida, esse poder de delegação da atividade notarial conferida aos Estados da Federação encontra fundamento jurídico na interpretação conjunta dos artigos 236 e 25, parágrafo 1.º, ambos da CF, uma vez que, o Estado delegando o poder ao Notário, em verdade está atuando em conformidade com sua competência material exclusiva residual.

O Estado, ao delegar um poder público, age administrativamente no desenvolvimento de uma atividade pública. Essa ação, conforme a lei 8.935/94, é exclusiva dos Estados da Federação por não estar enumerada expressamente a outro ente federativo. Neste passo, a fiscalização quanto ao cumprimento dos

---

18 - REZENDE, Afonso Celso F. Tabelionato de Notas e o notário perfeito. 4ª. Edição. Editora Millennium. Campinas (SP). 2006. Pág.31.

19 - ANTUNES, Luciana Rodrigues. Introdução ao direito notarial e Registral. Jus Navegandi, Teresina, ano 9, n.º 691, 27 de maio de 2005. Disponível em <http://jus2.uol.com.br/doutrina/texto.asp?id=6765>. Acesso em 11 dez. 2006.

objetivos pelo Notário fica a cargo da magistratura estadual do respectivo Estado ou Distrito Federal, em virtude de regra expressa no artigo 236, par. 1º da CF.

Os Notários, segundo disserta Antunes (2005)[20] são considerados pela doutrina como agentes públicos[21], uma vez que servem ao Poder Público para o desenvolvimento de uma função pública. O artigo 3.º, da lei 8.935/94[22] disserta que os notários devem ser profissionais do direito, dotados de fé pública, a quem é delegado o exercício da atividade notarial. Neste passo, devem ser observados os princípios constitucionais da legalidade, impessoalidade, moralidade, publicidade e eficiência inscritos no artigo 37 da CF.

A remuneração dos agentes públicos notariais é feita por meio de emolumentos, que são considerados contra prestações dispensadas pelo usuário ao notário a fim de custear o serviço notarial prestado (Melo Jr. 2005). A competência para a fixação dos valores é feita em geral por lei federal, sendo complementada por lei estadual.

As principais características que permeiam a atividade notarial são: caráter jurídico, cautelar, imparcial, público, técnico e rogatório. (Antunes. 2005)[23]

O caráter jurídico é verificado quando o tabelião, orientando as partes envolvidas no ato, assegura os requisitos legais para a sua realização. Com isso, evita-se futuras controvérsias jurisdicionais a respeito daquele ato (caráter cautelar).

A imparcialidade aplica-se ao agente notarial, que se vê diante de regras que lhe impõem responsabilidades administrativas, civis e penais em sua atuação.

O caráter público é alcançado pela própria função notarial. Embora o agente notarial seja um particular que recebeu por delegação uma atividade pública, não se pode desconsiderar prejudicado o caráter público dessa atividade.

---

20 - ANTUNES, Luciana Rodrigues. Introdução ao Direito Notarial e Registral. Jus Navegandi, Teresina, ano 9, n.º 691, 27 de maio de 2005. Disponível em <http://jus2.uol.com.br/doutrina/texto.asp?id=6765>. Acesso em 11 dez. 2006. Pág. 01.

21 - *"Todos aqueles que, servidores públicos ou não, estão legalmente intitulados a exercer, em nível decisório, uma parcela do poder público, investidos de competência especificamente definida pela ordem jurídica.* **MOREIRA NETO. Diogo de Figueiredo.** Curso de Direito Administrativo. 14ª. edição. Rio de Janeiro. 2005. Editora Forense. Pág. 284.

22 - "Art. 3º Notário, ou tabelião, e oficial de registro, ou registrador, são profissionais do direito, dotados de fé pública, a quem é delegado o exercício da atividade notarial e de registro."

23 - ANTUNES, Luciana Rodrigues. Introdução ao Direito Notarial e Registral. Jus Navegandi, Teresina, ano 9, n.º 691, 27 de maio de 2005. Disponível em <http://jus2.uol.com.br/doutrina/texto.asp?id=6765>. Acesso em 11 dez. 2006. Pág. 03.

O caráter técnico é verificado quando o agente notarial se vê obrigado a respeitar todos os requisitos legais fixados por lei para a realização do ato.

E por fim, o agente notarial somente agirá após livre manifestação da parte interessada, conferindo o caráter rogatório à atividade notarial.

2.3 A certificação digital vista pelo mundo

Ao iniciarmos um estudo sistemático da certificação digital, importante ponto que deve ser levado em consideração corresponde à natureza jurídica que os países vêm utilizando para designar a certificação digital.

O exercício de uma análise comparativa entre as normas jurídicas de vários países referente à natureza jurídica da certificação digital é importante tendo em vista o caráter globalizante de sua aplicação. A principal seara de aplicação da certificação digital é representada pelo comércio eletrônico internacional. Dessa forma, uma comunhão entre as várias órbitas jurídicas sobre o modo como a certificação digital é encarada revela-se primordial.

Dessa forma, iremos analisar quais são as regras de certificação digital que mais se aplicam nos países em que existe legislação específica, podendo com isso, verificarmos a tendência da legislação brasileira.

2.3.1 A Diretiva Européia 1999/1993 da Comunidade Européia

O principal objetivo da Comunidade européia ao emitir a diretiva 1999/1993 consiste em derrubar as barreiras que a técnica normativa poderia criar ao tratar da certificação digital. O desenvolvimento do uso das assinaturas eletrônicas nas relações comerciais eletrônicas encontra grande obstáculo nas barreiras normativas que os vários ordenamentos podem trazer.

Em suas considerações[24] a Comunidade Européia reconhece que as comunicações e o comércio eletrônico necessitam das assinaturas eletrônicas para a autenticação de dados. Por outro lado, a mesma comunidade afirma que as regras divergentes quanto ao reconhecimento legal das certificações pelos Estados-Membros representa importante obstáculo à utilização dessas aplicações.

Conforme o artigo 5[25], os Estados-Membros deverão assegurar às assinaturas eletrônicas avançadas, cujo fundamento encontra-se em certificado expedido por entidade certificadora qualificada perante o órgão público responsável, a força probante em processos judiciais, assim como assegurar que foram expedidos de acordo com regras legais que impõem à assinatura eletrônica as mesmas exigências das assinaturas manuscritas.

Em suas considerações, a Comunidade Européia esclarece que suas intenções não devem ser entendidas no sentido de padronizar a prestação de serviços de certificação. O interesse do Poder Público sobre a confidencialidade das informações prestadas pelo requerente do certificado não devem ser abrangidas pelas normas emitidas pela referida diretiva.

No mesmo passo, as regras contratuais quanto á celebração e execução dos contratos também não representam o alvo das referidas normas legais. Em verdade, a utilização da assinatura digital no âmbito contratual representará mais uma forma de realização de transações e não uma nova categoria contratual.

A interpretação, por outro lado, das regras da diretiva européia referentes à certificação digital devem ser feitas no sentido de propiciar que todos os Estados-Membros ofereçam as mesmas garantias sobre a certificação, possibilitando que entidades certificadoras possam expandir seus serviços para além das linhas fronteiriças que seus países sedes asseguram.

---

24 - Diretiva 1999/1993/CE do Parlamento Europeu e do Conselho, de 13 de Dezembro do 1999, relativa a um quadro legal comunitário para as assinaturas eletrônicas. Item n.º 4.

25 - Artigo 5.º. Efeitos legais das assinaturas eletrônicas: 1. a)Obedecem os requisitos legais de uma assinatura no que se refere aos dados sob forma digital, do mesmo modo que uma assinatura manuscrita obedece àqueles requisitos em relação aos dados escritos; e b) São admissíveis como meio de prova para efeitos processuais.

2.3.2 UNCITRAL – Uniform rules on electronic signatures

A UNCITRAL é um organismo ligado às Nações Unidas, responsável pelo desenvolvimento do comércio mundial. Nesta linha, desenvolveu, a exemplo da Comunidade Européia, uma proposta de regras para a utilização das assinaturas eletrônicas nas relações de comércio exterior.

A certificação digital, segundo as referidas regras da UNCITRAL, somente poderá ser emitida pela Autoridade Certificadora competente, e o certificado destina-se a identificar as pessoas que se utilizam da assinatura digital. Conforme o próprio texto, as autoridades de certificação desenvolvem um trabalho de identificação nas relações eletrônicas.

A primeira intenção da UNCITRAL, com a emissão de suas regras sobre o uso das assinaturas eletrônicas, é viabilizar o comércio eletrônico mundial, proporcionando o desenvolvimento da certificação digital cruzada. Os países asseguram a validade jurídica dos certificados digitais emitidos em outros países, ao mesmo nível de validade que os certificados emitidos pelas autoridades certificadoras domésticas.

Anualmente, a UNCITRAL elabora uma relação dos países que adotaram o referido projeto de lei. Até julho de 2006 eram os seguintes países: Austrália (1999); China (2004); Colômbia (1999); República Dominicana (2002); Equador (2002); França (2000); Índia (2000); Irlanda (2000); Jordânia (2001); México (2000); Nova Zelândia (2002); Paquistão (2002); Panamá (2001); Filipinas (2000); República da Coréia (1999); Cingapura (1998); Eslovênia (2000); África do Sul (2002); Siri Lanka (2006) Tailândia (2002); Venezuela (2001); e Vietnã (2005).

2.3.3 Portugal

Consoante as considerações do Conselho de Ministros, sobre a Resolução n.º 115/1998, de sua própria autoria, as assinaturas eletrônicas em geral e as assinaturas digitais em particular, não provam necessariamente a identidade do signatário. Dessa forma, considerando a técnica internacional consagrada, resolve instituir uma entidade certificadora, incumbida de assegurar níveis de segurança

aceitáveis para a confirmação da identidade do usuário da assinatura eletrônica ou digital.

Neste contexto, a referida resolução do Conselho de Ministros, em seu artigo 2º, define o certificado como o documento eletrônico autenticado com assinatura digital e que certifique a titularidade de uma chave pública e o prazo de validade da mesma chave.

Por entidade certificadora, o mesmo artigo 2º confere ser a entidade ou pessoa singular ou coletiva credenciada que cria ou fornece meios para a criação das chaves, emite certificados de assinatura, assegura a respectiva publicidade e presta outros serviços relativos à assinatura digital.

A atividade de certificação é de livre acesso, desde que o interessado preencha os requisitos pré-determinados na própria resolução 115/1998 em seus artigos 13, 14, 15 e 17. Neste ponto, a norma é clara em afirmar que a realização de negócios jurídicos não pode ficar adstrita à escolha de determinada entidade certificadora.

O artigo 21 relata os casos de revogação do credenciamento concedido à entidade certificadora, assegurando o seu funcionamento. Os casos de revogação estão expressamente previstos no artigo e a atividade ficará a cargo da autoridade credenciadora. A autoridade credenciadora corresponde a um órgão público responsável por verificar a presença dos requisitos mínimos para o exercício da atividade de certificação pelas entidades certificadoras interessadas.

No artigo 25 são fixados os deveres das entidades certificadoras. De forma diferente daquela adotada pela legislação brasileira, as entidades certificadoras são responsáveis pela emissão dos pares de chaves ao signatário, ou fornecer os meios técnicos necessários para esse fim. Todavia, conjuntamente com este dever, obriga-se a entidade certificadora em abster-se de tomar conhecimento do conteúdo das chaves privadas.

Nesta linha, o artigo 27 fixa a responsabilidade civil das entidades certificadoras pelos danos sofridos pelos titulares dos certificados e quaisquer terceiros em razão do descumprimento dos referidos deveres pela entidade certificadora.

Em seqüência, nos artigos 29, 30, 31 e 32 são formalizadas regras de conteúdo, suspensão, revogação dos certificados digitais e fixação das obrigações do titular do certificado.

2.3.4 Colômbia

Em Colômbia, o uso das assinaturas digitais vem regulamentado pela lei 527, de 23 de Agosto de 1999. Por conseqüência, o estabelecimento de entidades de certificação, e sua regulamentação também vêm descritos pelo mesmo ato normativo.

A lei não traz uma definição literal do que seja um certificado digital, por outro lado em seu artigo 2º especifica a definição de entidade de certificação. Dessa forma, conforme o texto da lei "*é aquela pessoa que, autorizada conforme a presente lei, está facultada a emitir certificados em relação às assinaturas digitais das pessoas, oferecer ou facilitar os serviços de registro e estampilhamento cronológico da transmissão e recepção das mensagens de dados, assim como cumprir outras funções relativas às comunicações baseadas nas assinaturas eletrônicas*"[26]

Segundo o artigo 29, somente pessoas jurídicas poderão desenvolver a atividade de certificação, a exemplo do que ocorre no Brasil. Entretanto, a exploração dessa atividade fica condicionada a prévia autorização da Superintendência da Indústria e Comércio.

Além dos serviços típicos de emissão de certificação digital, as entidades de certificação também poderão explorar as atividades de geração de par de chaves, assim como a atividade de emissão de estampilhas temporais e registro, arquivo e conservação das mensagens eletrônicas.

Regra interessante sobre a exploração da atividade de certificação consta do artigo 31[27]. Segundo referida regra, o valor cobrado pela emissão dos certificados será livremente fixado pela entidade de certificação. Dessa forma, podemos concluir pelo caráter capitalista da atividade de certificação, uma vez que a concorrência é livre entre seus exploradores.

---

[26] - Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

[27] - Artículo 31. Renumeración por la prestación de servicios. La remuneración por los servicios de las entidades de certificación serán establecidos libremente por éstas.

Por fim, conforme regra do artigo 36[28], está garantida a aceitação dos certificados emitidos pelas entidades de certificação registradas junto a Superintendência da Indústria e Comércio na realização de negócios pelo meio eletrônico.

2.3.5 Peru

A lei n.º 27.269, de 26 de Maio de 2000 regulariza o uso e desenvolvimento da atividade de certificação digital no Peru, e a sua aplicação no uso de assinaturas digitais.

Seguindo a linha da legislação portuguesa alhures analisada, a lei peruana confere ao certificado digital um caráter de título. Em seu artigo 4º, de forma expressa, afirma que o certificado digital será emitido em favor do titular da assinatura digital (par de chaves). Sem dúvida, partindo desta colocação, podemos asseverar que o certificado digital representa um título de propriedade, emitido em favor do detentor do par de chaves, cuja finalidade é identificar o signatário em relação à mensagem assinada digitalmente.

Neste passo, o artigo 6[29] conceitua o certificado digital como sendo o documento eletrônico criado e assentido digitalmente por uma entidade de certificação, vinculando uma determinada pessoa a um par de chaves, tendo a confirmação de sua titularidade (identidade).

Assim como na Infra-estrutura de Chaves Públicas do Brasil, o pedido para a emissão de um certificado digital perante as Autoridades Certificadoras Peruanas, será iniciado perante uma Autoridade de Registro, que será responsável pela guarda e proteção das informações prestadas para o ato. O artigo 13 da referida lei peruana, descreve as funções da entidade de registro: I – levantamento dos dados; e II – comprovação da veracidade das informações prestadas pelo solicitante do certificado.

---

[28] - Artículo 36. Aceptación de un certificado. Salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando la entidad de certificación, a solicitud de éste o de una persona en nombre de éste, lo ha guardado en un repositorio.

[29] - Artículo 6º. El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

Outra importante colocação feita pela lei peruana corresponde à validade dos certificados emitidos por entidades de certificação estrangeiras. Segundo o artigo 11, da referida lei peruana, os certificados emitidos por entidades estrangeiras terão a mesma validade e eficácia jurídica dos certificados nacionais sempre que os certificados sejam reconhecidos (validados) por uma entidade de certificação nacional.

Por fim, caberá ao Poder Executivo a indicação, por Decreto Supremo, de entidade administrativa responsável por regulamentar e cadastrar as entidades de certificação que atuarão na exploração da atividade de certificação digital.

2.3.6 Espanha

A regulamentação do uso, atividade e desenvolvimento das assinaturas eletrônicas na Espanha ocorre através do Real Decreto-lei n.º 14/1999, de 17 de Setembro.

Diferente das legislações até aqui analisadas, o Real Decreto-lei espanhol, de forma expressa, qualifica a certificação digital como atividade inteiramente diversa daquelas existentes nos documentos tradicionais (em papel) ou da fé conferida às assinaturas manuscritas.

Segundo esta posição, o certificado digital não encontra um paralelo com o sistema de validação de documentos e assinaturas manuscritas existentes, hoje, no ordenamento jurídico. Dessa forma, seu caráter jurídico não pode ser extraído de nenhuma atividade preexistente desenvolvida na sistemática dos documentos e assinaturas manuscritas.

Seguindo nesta linha, o Real decreto-lei conceitua o certificado digital como aquele que contém as informações descritas no artigo 8 do mesmo diploma legal, e é expedido por um prestador de serviços de certificação que cumpre os requisitos enumerados no artigo 12.

A prestação do serviço de certificação é feita de forma livre pelas entidades de certificação. O artigo 7[30] estabelece a criação de um serviço de certificação responsável pelo Registro das entidades de certificação, junto ao Ministério da Justiça.

Em seqüência, o Real decreto-lei discorre os elementos de existência do certificado digital e as regras sobre o tempo de vigência dos certificados (Artigos 8 e 9).

A fiscalização das entidades de certificação será feita pelo Ministério do Desenvolvimento, que através da Secretaria Geral de Comunicações verificará se as regras estabelecidas pelo Real decreto-lei estão sendo cumpridas.

2.3.7 República Tcheca

A assinatura eletrônica e a atividade de certificação digital na República Tcheca foi regulamentada pela lei n.º 227, de 29 de Junho de 2000.

Assim como a maioria das legislações mundiais sobre assinatura eletrônica e certificados digitais, a referida lei, por meio de seu artigo 2º preleciona os conceitos utilizados na atividade de certificação.

Desta relação, destacamos a concepção de provedor de serviços de certificação, como uma entidade responsável pela emissão de certificados e a respectiva lista de certificados emitidos, podendo ainda propor outros serviços relacionados com a assinatura eletrônica.

Por sua vez, os certificados são conceituados como uma expressão de dados emitidos por um provedor, o qual, liga os dados de verificação de identidade com o signatário. O certificado opera seus efeitos num chamado processo de verificação de identidade. Os dados utilizados nesse processo são denominados pela própria lei como dados de verificação da assinatura eletrônica.

A referida lei, visando exaurir os temas pertinentes a utilização da assinatura eletrônica nas relações sociais, em seu artigo 6.º traz a relação de obrigações referentes aos provedores de serviços de certificação. Embora o rol seja

---

30 - "*Se crea, en el Ministerio da Justicia, el Registro de Prestadores de Servicios de Certificación, en el que deberán solicitar su inscripción, con carácter previo al inicio de su actividad, todos los establecidos en España. Su regulación se desarrollará por Real Decreto".*

extenso, cabe-nos realizar uma especial ponderação sobre a letra “b”, do parágrafo 1º. Consoante a referida regra cabe aos provedores de serviços de certificação assegurar que todos os dados especificados nos certificados emitidos são exatos, verdadeiros e completos.

Sem dúvida, fazendo um paralelo com a sistemática normativa para os documentos no direito brasileiro, o papel desenvolvido pelos provedores de serviço de certificação quanto à validade dos documentos apresentados para a emissão dos certificados, assim como as informações constantes dos certificados devem ser asseguradas pelo próprio provedor.

Por fim, os provedores de serviço de certificação, para atuarem no mercado, devem ser registrados junto ao Poder Público, no Ministério competente.

2.3.8 Estados Unidos da América

O estado de Utah, nos Estados Unidos da América, foi o primeiro ente político no mundo a editar uma lei a fim de regulamentar o uso de assinaturas eletrônicas, entrando em vigor em 1995. Muito extensa e extremamente detalhista, conforme observa Marcacini (2002)[31], a referida lei traz um rol de conceitos técnicos e jurídicos.

No mesmo ano, o Estado da Califórnia editou sua lei sobre a validade das assinaturas digitais no mundo jurídico. Mais enxuta que a lei anterior do Estado de Utah, trazia apenas o conceito de assinatura digital e regulamentava o uso das assinaturas digitais perante os órgãos públicos, conferindo a mesma força das assinaturas manuscritas.

Diversamente do que analisamos até agora sobre Infra-estrutura de Chaves Públicas, o sistema Norte-Americano apresenta mais de uma autoridade certificadora raiz, sendo que cada estado possui sua legislação específica para a certificação.

Os Estados Unidos da América vêm enfrentando sérios problemas com essa posição, e o principal deles é a variação de legislações sobre o mesmo

---

[31] - **MARCACINI, Augusto Tavares Rosa.** Direito e Informática. Uma abordagem jurídica sobre criptografia. 1ª. Edição. Rio de Janeiro. Editora Forense. 2002. Pág. 59.

tema, acabando por causar sérias divergências no momento de validar a certificação digital emitida por Estados diferentes.

3 A INFRA-ESTRUTURA DE CHAVES PÚBLICAS DO BRASIL

O Poder Público deve assegurar à sociedade a presença dos direitos constitucionais nas relações em meio eletrônico. Isto implica investimento em desenvolvimento de mecanismos capazes de proporcionar a total inclusão digital da sociedade. A criação de uma Infra-estrutura de Chaves Públicas do Brasil representa uma dentre as várias formas de desenvolvimento da inclusão digital da sociedade.

Diante do exposto, no presente capítulo, passaremos a analisar o funcionamento da Infra-estrutura de Chaves Públicas do Brasil, identificando sua posição hierárquica dentro da Administração Pública, apontando seus principais órgãos formadores, definindo suas respectivas competências e funções.

Quanto ao papel desempenhado pela ICP-Brasil na sistemática de validade jurídica dos documentos eletrônicos, assinaturas digitais e certificados digitais, destacaremos a importância da segurança das informações para o funcionamento de toda a estrutura tecnológica. A partir da discussão a respeito das formas que podem ser empregadas em uma infra-estrutura de chaves públicas (centralizada ou descentralizada), identificando os pontos principais que caracterizam a ICP-Brasil como uma infra-estrutura centralizada; discorreremos sobre os principais pontos convergentes que povoam a doutrina especializada.

3.1 A Infra-estrutura de chaves públicas do Brasil

A Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil - segundo Custódio[32] (2001) é um conjunto de técnicas, práticas e procedimentos com o objetivo de fornecer suporte à implementação e à operação de um sistema de certificação digital baseado em criptografia de chave pública.

---

[32] **- CUSTÓDIO, Ricardo Felipe.** Análise Crítica da ICP-Brasil : Resposta a Consulta Pública. Laboratório de Segurança da Computação (LABSEC), UFSC. Florianópolis, 2001. Pág. 27.

Os certificados digitais oriundos da ICP-Brasil são atribuídos individualmente aos membros de um universo de usuários, cabendo ainda a ICP-Brasil gerenciar o ciclo de vida de cada certificado emitido, posto que, a qualquer momento, poderá haver a necessidade de renovar ou revogar o certificado diante de determinadas circunstâncias, como no caso de vencimento ou quebra do segredo da chave privada.

A implantação da ICP-Brasil teve natureza administrativa, tendo como objetos reais a emissão e distribuição de certificados digitais e seu controle de qualidade, além dos objetivos legais de assegurar autenticidade, integridade e validade jurídica aos documentos eletrônicos, como também as transações eletrônicas seguras, conforme descrito no artigo 1.º da MP 2.200-2/01.

Neste passo, o objetivo fundamental que legitimou a implantação da ICP-Brasil consiste em estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública. A força e a complexidade deste sistema são importantes, ao passo que determinam a confiança pública no certificado.

Quando o Poder Executivo Federal se utilizou de uma Medida Provisória para instituir a Infra-estrutura de Chaves Públicas do Brasil, objetivou estabelecer meios e métodos pelos quais estivesse assegurada a validade jurídica dos documentos produzidos em formato eletrônico.

Conforme bem observou Silvestre (2003)[33], o governo usou uma Medida Provisória como fundamento para a instituição de uma ICP-Brasil. Normalizou um serviço ao cliente, voltado para a garantia de autenticidade, integridade e validade jurídica das informações armazenadas eletronicamente. A certificação estava inserida dentro de uma política do Governo Federal, surgida em 2000 de estudos desenvolvidos pela Casa Civil da Presidência da República para a implementação do chamado “Governo Eletrônico”. Por meio desta política, o Governo Federal objetivava assegurar a legalidade das atividades voltadas para a inserção do Governo na era digital.

---

[33] **- SILVESTRE, Fábio André Chedid**. A ilegitimidade constitucional crítica da Infra-estrutura de Chaves Públicas Brasileira. Uma Semiótica do Poder. 2003. P. 53. Dissertação de Mestrado. Universidade Federal de Santa Catarina. Programa de Pós-Graduação. Engenharia de Produção e Sistemas. Florianópolis (SC). 2003.

Na continuação de seu raciocínio, Silvestre (2003)[34] crítica diretamente a postura que o Governo Executivo Federal tomou frente à implantação da Infra-estrutura de Chaves Públicas do Brasil. Deixou transparecer suspeitas quanto aos interesses em jogo. O uso de uma Medida Provisória demonstra claramente o interesse político do Governo na atividade de Certificação.

Conforme previsto pelo artigo 2.º da Medida Provisória 2.200-2/01[35], a Infra-estrutura de Chaves Públicas Brasileira é formada pelos seguintes entes: Autoridade Gestora de Políticas, ou seja, o Comitê Gestor que possui características de organismo político[36]; por uma Autoridade Certificadora Raiz, o Instituto Nacional de Tecnologia da Informação, possuidor de características de organismo administrativo; por uma cadeia de Autoridades Certificadoras Subseqüentes; e, por fim, uma cadeia de Autoridades de Registro.

Em razão da atividade de certificação ser encarada pela MP 2.200-2/01 como serviço público é prestado pelo Instituto Nacional de Tecnologia da Informação, Autarquia Federal criada pela MP 2.200-2/01. Assim, deverão ser respeitados, como princípios gerais, aqueles aplicados à Administração Pública, e que vêm descritos no artigo 37 da Constituição Federal, a saber: legalidade, impessoalidade, moralidade, publicidade e eficiência. [37]

Por outro lado, existem princípios específicos[38] que também devem ser observados por todos os órgãos de composição da ICP-Brasil e são os seguintes:

---

[34] - SILVESTRE, Fábio André Chedid. A ilegitimidade constitucional crítica da Infra-estrutura de Chaves Públicas Brasileira. Uma Semiótica do Poder.2003. P. 60. Dissertação de Mestrado. Universidade Federal de Santa Catarina. Programa de Pós-Graduação. Engenharia de Produção e Sistemas. Florianópolis (SC). 2003.

[35] - 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.

[36] - Artigo 3 da MP.2.200-2/01: *"A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República..."*

[37] - "Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência..."

[38] - Termos de Referência. Comitê Gestor da ICP-Brasil. Presidência da República. Casa Civil da Presidência da República. Disponível em: **https://www.planalto.gov.br/ccivil_03/consulta_publica/PDF/termodereferencia.pdf** . Acessado em 03 de Fevereiro de 2007.

- Princípio da responsabilização – todas as regras e normas que devem ser observadas e exigidas pelos órgãos que compõem a ICP-Brasil, devem ser detalhadamente fixadas;
- Princípio do conhecimento – todas as pessoas envolvidas no processo de funcionamento da ICP-Brasil, devem se manter informadas das normas fixadas e pós-fixadas para a função certificadora;
- Princípio da Ética – todos os sistemas de informação, assim como toda a estrutura utilizada no desenvolvimento das funções da ICP-Brasil deverão ser utilizadas de maneira coerente e determinada ao fim proposto;
- Princípio da Multidisciplinariedade – todas as práticas relacionadas com a segurança da informação numa ICP-Brasil deverão obedecer aos parâmetros das normas técnicas, administrativas, organizacionais, operacionais, educacionais, comerciais e jurídicos;
- Princípio da Proporcionalidade – A ICP-Brasil deverá observar os níveis de importância das informações trabalhadas a fim de fixar o nível de segurança a ser aplicado aos casos específicos;
- Principio da Integração – As normas práticas relacionadas com a segurança dos sistemas de informação devem ser criadas de acordo com as necessidades existentes para a sociedade e para o Governo;
- Principio da Atualização – Os sistemas de segurança da informação integrantes da ICP-Brasil deverão ser reavaliados periodicamente, conforme a necessidade temporal dos sistemas de informação;
- Princípio da Escalabilidade – trabalhar sempre com perspectivas de crescimento do número de usuários;
- Princípio da Interoperabilidade – o sistema da ICP-Brasil deve funcionar da forma mais aberta possível, obedecendo a paradigmas de sistemas abertos, de modo a reduzir ao máximo as incertezas.

3.1.1 Comitê Gestor

O Comitê Gestor, vinculado à Casa Civil da Presidência da República (a presidência do comitê é exercida por membro da Casa Civil), é

responsável pelo desenvolvimento e emissão das normas técnicas que circundam a atividade certificadora. Todas as normas procedimentais e de fiscalização são oriundas do referido órgão, em vista de ser o responsável direto e legal por essas tarefas conforme determina expressamente a MP 2.200-2/01.

Conforme preceitua Custódio (2004)[39]:

> "O Comitê Gestor da ICP-Brasil (CG ICP-Brasil) é a entidade máxima, integrante da arquitetura da Infra-estrutura de Chaves Públicas Brasileira - ICP-Brasil, responsável pelo estabelecimento e administração das políticas a serem seguidas pelas Autoridades Certificadoras - AC integrantes desta estrutura."

Seu corpo de agentes é formado por 05 integrantes da sociedade civil, que integram setores interessados no desenvolvimento do comércio eletrônico, e sete membros integrantes do Governo Federal (um de cada Ministério: Ministério da Justiça; Ministério da Fazenda; Ministério do Desenvolvimento, Indústria e Comércio Exterior; Ministério do Planejamento, Orçamento e Gestão; Ministério da Ciência e Tecnologia; Casa Civil da Presidência da República; e Gabinete de Segurança Institucional da Presidência da República). Todos serão designados pelo Presidente da República, sendo que os membros do Comitê Gestor, representantes da sociedade civil, possuirão um mandato de 02 anos, podendo haver recondução.

Várias são as competências fixadas pela Medida Provisória 2.200-2/01, por meio de seu artigo 4.º, destinadas ao exercício pelo Comitê Gestor. Vamos analisá-las mais pormenorizadamente a seguir.

Conforme preceitua o artigo 4.º, I da MP 2.200-2/01, foi-lhe atribuída como função principal a coordenação da implementação e funcionamento da ICP-Brasil, definindo as normas técnicas que serão aplicadas para esse fim.

Seguindo nesta diretriz, o artigo 4.º, II da MP 2.200-2/01, determina que o Comitê Gestor deve indicar a política, os critérios e as normas técnicas que deverão ser observadas pela Autoridade Certificadora Raiz, e pelas Autoridades Certificadoras Subseqüentes e Autoridades de Registro que buscarem o credenciamento diante da ICP-Brasil.

---

[39] **- CUSTÓDIO, Ricardo Felipe.** Análise Crítica da ICP-Brasil : Resposta a Consulta Pública. Laboratório de Segurança da Computação (LABSEC), UFSC. Florianópolis, 2001. Pág. 27**.**

Compete ainda ao Comitê Gestor, conforme descreve o Artigo 4.º, III da MP 2.200-2/01, estabelecer a política de segurança e as regras operacionais que deverão ser observadas pela Autoridade Certificadora Raiz. Como também prevê o inciso IV do referido artigo, funcionar como órgão fiscalizador, auditando a Autoridade Certificadora Raiz e seus prestadores de serviços quanto ao cumprimento das regras fixadas nesta política de segurança.

Dentro desta linha de comandos de atuação do Comitê Gestor, o artigo 4.º, incisos V e IV, da MP 2.200-2/01, determina que competirá a este, a emissão de diretrizes de política de certificado e definir níveis da cadeia de certificação que deverão ser seguidas pelas Autoridades Certificadoras Subseqüentes e pelas Autoridades de Registro, bem como, aprovar as respectivas políticas internas criadas pelas Autoridades Certificadoras Credenciadas e autorizar a Autoridade Certificadora Raiz a emitir o corresponde certificado.

O âmbito de aplicação da ICP-Brasil é o território nacional. Entretanto, sua criação ocorreu, entre outras razões, para fortalecer a prática do comércio eletrônico nacional e internacional. O uso da Internet, nas transações comerciais eletrônicas, vai muito além das barreiras físicas encontradas no mundo físico, destarte, a validade dos certificados eletrônicos deve seguir a mesma linha de abrangência dessas atividades. Pensando nisso, o artigo 4.º VII da MP 2.200-2/01 encarrega o Comitê Gestor, como órgão de relações internacionais, de manter acordos bilaterais de certificação cruzada.

Por fim, como conseqüência lógica do papel desenvolvido pelo Comitê Gestor, o inciso VIII, do artigo 4.º da MP 2.200-2/01 prevê que as atualizações, ajustes e revisões dos procedimentos e das práticas fixadas à ICP-Brasil serão realizadas pelo próprio Comitê Gestor.

3.1.2 Autoridade Certificadora Raiz

Conforme o artigo 13[40] da Medida Provisória 2.200-2/01, a Autoridade Certificadora Raiz é a primeira na cadeia de certificação no Estado Brasileiro, operada pelo Instituto Nacional de Tecnologia da Informação - ITI - que

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

conforme o artigo 12 do referido ato normativo tornou-se Autarquia Federal vinculada à Casa Civil da Presidência da República.

Dentro de seu rol de competências, a Autoridade Certificadora Raiz, é responsável pela certificação das Autoridades Certificadoras Subseqüentes, desenvolvendo ainda atividades de fiscalização junto a essas Autoridades Certificadoras Subseqüentes e Autoridades de Registro, conforme previsto pelo artigo 14[41] da referida Medida Provisória.

A Autoridade Certificadora Raiz desenvolve seu papel em consonância com as regras determinadas pelo Comitê Gestor, ou seja, é o comitê normalizador ditando regras para o órgão administrativo da Infra-estrutura de Chaves Públicas do Brasil.

O procedimento de fiscalização está regulamentado na Resolução n.º 25, de 24 de Outubro de 2.003, do Comitê Gestor da ICP-Brasil. O principal objetivo da atividade de fiscalização desenvolvida consiste em verificar a conformidade dos processos, procedimentos e atividades das Autoridades Certificadoras Subseqüentes integrantes da ICP-Brasil, de suas Autoridades de Registro e de seus prestadores de serviço de suporte com as suas respectivas Declarações de Práticas de Certificação – DPC, a Política de Segurança e as demais normas e procedimentos estabelecidos pela ICP-Brasil.

O ITI é responsável por auditar a candidata ao credenciamento para atuar como Autoridade Certificadora Subseqüente, quanto a suas instalações, rotinas, documentos e práticas. De uma forma geral, a candidata deverá demonstrar sua capacidade de gerenciar a emissão de certificados eletrônicos, gerenciar a lista de certificados revogados, proteger os dados, e tantos outros requisitos exigidos para a instalação de uma Autoridade Certificadora Subseqüente, podendo assim, emitir certificados eletrônicos aos interessados.

O certificado de mais alto nível na cadeia de certificação é o da Autoridade Certificadora Raiz e contém a sua chave pública, conforme vem destacada na Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil[42].

---

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

42 - Resolução n.º 1 de 25 de Setembro de 2001, que aprova a Declaração de Práticas da Autoridade Certificadora Raiz da ICP- Brasil.

A chave-pública da Autoridade Certificadora Raiz destina-se a atestar os certificados emitidos em favor das Autoridades Certificadoras Subseqüentes e a atestar a lista de certificados revogados emitidos pela própria Autoridade Certificadora Raiz.

A integração do ITI, a fim de viabilizar o seu funcionamento e desenvolvimento de suas funções, vem descrita nos artigos 15[43] e 16[44] da já citada Medida Provisória. Dentre as principais prerrogativas inerentes ao ITI, destacamos a função que o Diretor–Presidente da Autoridade Certificadora Raiz possui para recrutar pessoal especializado vinculado à prestação de serviço público em outros órgãos da Administração Pública para o auxílio das funções desenvolvidas pela Autoridade Certificadora Raiz, com as mesmas garantias e vantagens do cargo anterior.

Freitas e Loebens (2004)[45] destacam as funções e competências da Autoridade Certificadora Raiz, descritas no artigo 5.º da Medida Provisória, podendo ser assim descritas: I - Emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu; II – Gerenciar a lista de certificados emitidos, revogados e vencidos; III – Realizar atividades de fiscalização e auditoria das Autoridades Certificadoras e Autoridades de Registro; IV – Exercer outras atribuições que forem fixadas pelo Comitê Gestor da ICP-Brasil; V – Fiscalizar e impor sanções e penalidades.

São ainda obrigações da AC-Raiz as descritas pela Declaração de Práticas de Certificação[46] da Autoridade Certificadora Raiz, emitido pelo Comitê

---

[43] - Art. 15. Integrarão à 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.

[44] - 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.

[45] **- FREITAS, Vinicius Pimentel de Freitas. LOEBENS, João Carlos.** Contratos eletrônicos e o Comércio Internacional. VIII Seminario Internacional de la Federación Internacional de antiguos alumnos del I.N.A.P. de España. Toledo. Agosto de 2004. Pág. 28.

[46] **- Resolução** n.º 1 de 25 de Setembro de 2001, que aprova a Declaração de Práticas da Autoridade Certificadora Raiz da ICP- Brasil.

Gestor nas seguintes condições: I – A geração e o gerenciamento do par de chaves da Autoridade Certificadora Raiz; II – A emissão e a distribuição do certificado da Autoridade Certificadora Raiz; III – A emissão, a expedição e a distribuição dos certificados das Autoridades Certificados Subseqüentes; IV- A publicação de certificados por ela emitidos; V- A revogação de certificados por ela emitidos; VI – A emissão, o gerenciamento e a publicação da Lista de Certificados Revogados; VII – A fiscalização e a auditoria das Autoridades Certificadoras Subseqüentes e das Autoridades de Registro, e dos prestadores de serviço habilitados em conformidade com os critérios fixados pelo Comitê Gestor da ICP-Brasil; VIII – A implementação de acordos de certificação cruzada, quando determinados pelo Comitê Gestor da ICP-Brasil.

Em suma, podemos entender que a competência exercida pela Autoridade Certificadora Raiz vem descrita inicialmente pela própria Medida Provisória (art. 5º) e subsidiariamente relatada na Declaração de Prática de Certificação e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.

3.1.2.1 Uma Autarquia para operar a certificação digital

As autarquias são entidades estatais da administração indireta, criada por lei, com personalidade de direito público, descentralizada funcionalmente, para desempenhar competências administrativas próprias e específicas, com autonomia patrimonial, administrativa e financeira. [47]

Consoante assevera Meirelles (1999)[48] em razão da autarquia ser forma descentralizada de administração, através da personificação de uma tarefa pertencente à administração centralizada, somente devem ser outorgados serviços públicos típicos.

A função de Autoridade Certificadora Raiz é foi conferida ao ITI, que corresponde ao ente administrativo da ICP-Brasil. Conforme verificamos alhures, a Autoridade Certificadora Raiz é a autoridade administrativa máxima dentro da cadeia

---

[47] - **MOREIRA NETO, Diogo de Figueiredo.** Curso de Direito Administrativo.14ª. edição. Rio de Janeiro. Editora Forense. 2005. Pág. 253.

[48] - **MEIRELLES, Hely Lopes.** Direito Administrativo Brasileiro. 24ª. edição. São Paulo. Editora Malheiros. 1999. Pág. 311.

de certificação digital no Brasil, cujas competências estão expressas na MP 2.200-2/01.

Na atualidade, o Instituto Nacional de Tecnologia da Informação, autarquia federal vinculada à Casa Civil da Presidência da República, exerce esta função. Dessa forma, entre os vários serviços públicos prestados sob a competência do referido Instituto encontramos o ofício de Autoridade Certificadora Raiz.

Todas as responsabilidades jurídicas provenientes do exercício da função de Autoridade Certificadora Raiz serão suportadas pelo Instituto Nacional de Tecnologia da Informação, e suas atividades são controladas pela Casa Civil da Presidência da República, entidade estatal a qual é vinculada. [49]

3.1.2.2 As auditorias e o processo de (re) credenciamento

Conforme determina a Resolução n.º 12, de 14 de Fevereiro de 2002, do Comitê Gestor da ICP-Brasil, o credenciamento das Autoridades Certificadoras Subseqüentes diante da Autoridade Certificado Raiz - AC-Raiz - requer a realização de auditoria e fiscalização por órgão interno da própria AC-Raiz, quando será verificado se estão atendidos todos os critérios e procedimentos para credenciamento das entidades integrantes da ICP-Brasil, aprovados na resolução n.º 6, de 22 de novembro de 2002.

Havendo constatação, durante a realização da auditoria, de que alguns desses critérios ou procedimentos não tenham sido observados, a própria Autoridade Certificadora Raiz – AC-Raiz - comunicará a candidata para que satisfaça as exigências, dentro de prazo suficiente fixado pela própria AC-Raiz (Art. 3. º da Res. 12 de 22 de Novembro de 2002).

Ao final, estando satisfeitas as exigências e depois de comunicado este fato à Autoridade Certificadora Raiz – AC-Raiz – esta se manifestará sobre o deferimento ou indeferimento do pedido de credenciamento, encaminhando parecer ao Comitê Gestor.

---

[49] - MEIRELLES, Hely Lopes. Direito Administrativo Brasileiro. 24ª. edição. São Paulo. Editora Malheiros. 1999. Pág. 310.

3.1.2.3 A competência fixada pela declaração de prática de certificação

Vimos alhures que a Medida Provisória 2.200-2/01 fixa em seu artigo 5.º quais são os atos de competência da Autoridade Certificadora Raiz – AC-Raiz – que deverão ser desenvolvidos em sua atuação como entidade máxima da cadeia de certificação digital no ordenamento jurídico brasileiro. A Medida Provisória consiste em um ato normativo equiparado a lei ordinária, quanto à sua força e alcance.

Na seqüência da fixação de competências da AC-Raiz, discorremos sobre a complementação desta lista pelo Comitê Gestor, quando responsável pela elaboração das Declarações de Práticas de Certificação e demais normas técnicas e operacionais.

A Resolução n.º 1, de 25 de Setembro de 2001 do Comitê Gestor da ICP-Brasil, aprovou a Declaração de Práticas de Certificação da Autoridade Certificadora Raiz. Sobre este aspecto cabe-nos realizar algumas críticas.

A matéria de competência tratada pela Medida Provisória, entre outras questões, trata do exercício da atividade de certificação digital, que corresponde à principal função exercida pela AC-Raiz.

Essas regras, em decorrência de sua natureza jurídica (lei federal, em virtude de a Medida Provisória ser encarada como tal) correspondem a normas de direito público, logo, devem ser seguidas à risca pelo legislador hierarquicamente inferior, não podendo sofrer nenhuma forma de excepcionalidade por ato normativo inferior, que não esteja prevista em seu texto.

Desta sorte, o artigo 5.º, "caput", "*in fine"* da Medida Provisória n.º 2.200-2/01 dita a seguinte regra de competência referente à AC-Raiz: *"Exercer outras atribuições que forem fixadas pelo Comitê Gestor da ICP-Brasil."*

De acordo com esta norma, o Comitê Gestor possui competência de fixar outras competências além daquelas descritas pela própria Medida Provisória, incorporando um papel exclusivo do legislador ordinário. A competência fixada pela Medida Provisória referente à AC-Raiz decorre de normas de direito público, logo não podem ser excepcionadas por entes legislativos hierarquicamente inferiores, como ocorre com o Comitê Gestor, ao receber referida incumbência.

Em verdade, perante este verdadeiro cheque assinado em branco, os membros do Comitê Gestor podem exercer diretamente uma função que a Medida Provisória 2.200-2/01 deveria resguardar exclusivamente ao legislador ordinário, devido o seu caráter de interesse público.

O Comitê Gestor, encarado como órgão normalizador é responsável pelo desenvolvimento e aplicação da tarefa de certificação digital no ordenamento jurídico brasileiro, deve restringir-se apenas a instrumentalizar as normas gerais sobre certificação fixadas na Medida Provisória 2.200-2/01. Neste ponto, o referido ato normativo exclusivo do Poder Executivo andou mal, fixando norma de interesses particulares incondizentes com o interesse público que deveria perseguir.

Ponto de relevante valor no estudo sobre as aplicações da certificação digital corresponde à regra de competência da AC-Raiz fixada pelo Comitê Gestor, quando da fixação pela resolução n.º 01/01, da Declaração de Práticas de Certificação.

Prevê a referida resolução como competência da AC-Raiz: *"A implementação de acordos de certificação cruzada, quando determinados pelo Comitê Gestor da ICP-Brasil."*

Andou bem o Comitê Gestor, ao fixar a competência para a Autoridade Certificadora Raiz, para implementar os acordos de certificação cruzada por ele aprovado.

Neste ponto, notamos que o Comitê Gestor respeitou a competência inicialmente fixada pela Medida Provisória 2.200-2/01, ao invocar ao próprio Comitê a aprovação de acordos de certificação cruzada.

O Comitê Gestor, por meio de resolução, apenas operacionaliza a realização de acordos de certificação cruzada.

Dessa forma, o inciso VII, do artigo 4.º, da M.P. 2.200-2/01, fixa literalmente ao Comitê Gestor a seguinte norma:

> *"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."*

A previsão especifica de que compete ao Comitê Gestor identificar, avaliar, negociar e aprovar os acordo de certificação digital foi respeitado, ficando a cargo da Autoridade Certificadora Raiz apenas o trabalho técnico de implementar as diretrizes do acordo, atuando verdadeiramente como órgão administrativo da Infra-estrutura de Chaves Públicas do Brasil

Diante de todo o exposto, vimos que a Medida Provisória deixou margem ao Comitê Gestor para a fixação de novas competências à Autoridade Certificadora Raiz além daquelas inicialmente descritas na própria norma. Isso, sem dúvida, representa uma grande arma para a prevalência de interesses particulares sobre interesses públicos.

Por outro lado, também andou bem o Comitê Gestor, quando operacionalizou regra de sua competência, fixada originariamente pela Medida Provisória 2.200-2/01, à Autoridade Certificadora Raiz, por meio de resolução.

3.1.3 Autoridades Certificadoras Subseqüentes.

As Autoridades Certificadoras Subseqüentes desempenham uma atividade de certificação semelhante àquela desempenhada pela Autoridade Certificadora Raiz, à qual geralmente é ligada. A diferença encontra-se justamente no nível de aplicação. Sua atividade aplica-se a um nível hierárquico inferior, destinando-se ao usuário final.

Vale lembrar que o artigo 10, parágrafo 2.º da Medida Provisória 2.200-2/01 possibilita a existência de Autoridades Certificadoras Independentes sem vínculo hierárquico com a Autoridade Certificadora Raiz.

Ao contrário da Autoridade Certificadora Raiz, a competência para certificar inerente às Autoridades Certificadoras Subseqüentes é exercida perante o usuário final, ou seja, ao agente, pessoa física ou jurídica, que utilizará o certificado com a finalidade de desenvolver suas atividades cotidianas, como assinar documentos, identificar-se e firmar contratos, ao passo que os certificados emitidos pela Autoridade Certificadora Raiz destinam-se exclusivamente a conferir poder às Autoridades Certificadoras Subseqüentes emitirem certificados para outras Autoridades Certificadoras Subseqüentes ou certificados digitais ao usuário final objetivando os fins mencionados.

Conseqüentemente, as Autoridades Certificadoras Subseqüentes podem ser encaradas como certificadoras responsáveis pela emissão de certificados digitais destinados ao usuário final. O certificado tem a função de vincular a chave pública ao respectivo titular do par de chaves(art. 6º da MP 2.200-2/01).

Diante dessa assertiva, a função desempenhada pelas Autoridades Certificadoras Subseqüentes pode ser encarada, conforme destaca Custódio (2004, p. 31), "*como a base material e técnica da confiança da ICP-Brasil, já que esta irá gerenciar os certificados de chave pública em todo o seu ciclo de vida.*"[50]

O artigo 6.º, caput, da MP 2.200-2/01[51] descreve as principais competências referentes às Autoridades Certificadoras Subseqüentes, que são: 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 registros de suas operações.

Ainda no texto do artigo supra citado, o parágrafo único[52] determina expressamente que o par de chaves será sempre gerado diretamente pelo próprio titular, sendo que a chave privada será de seu exclusivo controle e conhecimento.

Esta determinação não estava presente na primeira versão da MP 2.200-2/01. Todavia, diante das duras críticas dirigidas contra a previsão inicial de que o par de chaves deveria ser gerado pelas Autoridades Certificadoras Subseqüentes, o Governo Federal resolveu por bem alterar o texto nas reedições seguintes, conferindo esta função ao próprio titular do par de chaves. A razão fundamental para as críticas é verdadeiramente óbvia: se a chave privada é gerada por outro que não o próprio titular da chave, não se sustenta a presunção de que ela seja de conhecimento apenas do titular.

Como veremos a seguir, esta medida é essencial para a credibilidade do sistema de certificação digital imposto pela MP 2.200-2/01.

O artigo 9.º da MP 2.200-2/01[53], por sua vez, vem descrever uma regra de segurança na Infra-estrutura de Chaves Públicas Brasileira, fixando

---

50 - CUSTÓDIO, Ricardo Felipe. Análise Crítica da ICP-Brasil : Resposta a Consulta Pública. Laboratório de Segurança da Computação (LABSEC), UFSC. Florianópolis, 2001. Pág. 31.

51 - 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.

52 - 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.

expressa vedação às autoridades certificadoras de emitir certificado em favor de Autoridades Certificadoras Subseqüentes de mesmo nível, exceto nos casos de acordos de certificação cruzada. De acordo com a regra do referido artigo, as Autoridades Certificadoras Subseqüentes estão autorizadas a certificar outras Autoridades, entretanto, de nível hierárquico inferior.

Desta regra, podemos concluir que é vedado a qualquer autoridade, imediatamente subseqüente à Autoridade Certificadora Raiz, certificar outra autoridade certificadora imediatamente subseqüente à Autoridade Certificadora Raiz. Esta competência cabe exclusivamente à Autoridade Certificadora Raiz. Somente o Instituto Nacional de Tecnologia da Informação, enquanto Autoridade Certificadora Raiz da ICP-Brasil, tem o poder assegurado na norma de auto certificar-se.

Por fim, lembram Freitas e Loebens (2004)[54] que os titulares de certificados também possuem obrigações perante as Autoridades Certificadoras Subseqüentes, como fornecer de modo completo e preciso todas as informações necessárias à sua identificação; garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos; utilizar de forma apropriada os certificados e as chaves privadas; conhecer os seus direitos e obrigações contemplados pela Declaração de Praticas de Certificação, Política de Certificação e outros documentos da ICP-Brasil; e informar à autoridade certificadora competente qualquer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado.

3.1.4. Autoridades de Registro

As Autoridades de Registro, assim como as Autoridades Certificadoras Subseqüentes, são órgãos vinculados à Autoridade Certificadora Raiz com a finalidade de auxiliar a prestação e o desenvolvimento da certificação digital.

---

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

54 - **FREITAS, Vinicius Pimentel de Freitas. LOEBENS, João Carlos**. Contratos eletrônicos e o Comércio Internacional. VIII Seminario Internacional de la Federación Internacional de antiguos alumnos del I.N.A.P. de España. Toledo. Agosto de 2.004. Pág. 30/31.

O desdobramento de suas operações ocorre vinculadamente às Autoridades Certificadoras Subseqüentes.

Por outro lado, o que diferencia as Autoridades de Registro das Autoridades Certificadoras Subseqüentes é justamente a função que desempenham. Conforme o artigo 7.º, da Medida Provisória 2.200-2/01[55], compete às Autoridades de Registro – ARs. – identificar e cadastrar usuários na presença destes, encaminhando solicitações de certificados às Autoridades Certificadoras Subseqüentes e manter suas operações.

Assim como acontece com as Autoridades Certificadoras Subseqüentes, as normas técnicas e procedimentais para a homologação de uma autoridade de registro são fixadas pelo Comitê Gestor,[56] e tanto empresas da iniciativa pública como da iniciativa privada podem ser homologadas para desempenhar referida tarefa.

Via de regra, a tarefa primordial das Autoridades de Registro se limita a identificar o requerente para a emissão de um certificado digital. O sentido da palavra "identificar", empregado pelo texto da lei deve ser encarado como individualização perante a sociedade, a fim de resguardar a implicação de futuras obrigações admitidas por meio dos certificados digitais.

É importante ressaltar que a função desempenhada pela Autoridade de Registro equipara-se a uma verdadeira atividade de identificação e individualização baseado em documentos de identificação e no comparecimento pessoal do titular do certificado digital, ao passo que, após verificar que o requerente, que pleiteia a expedição de um certificado, realmente é a pessoa indicada nos documentos, emitirá uma ordem de solicitação para a Autoridade Certificadora Subseqüente, a fim de que seja emitido o competente certificado.

Via de regra, as Autoridades de Registro são aprovadas pela Autoridade Certificadora Raiz independente de interferências das Autoridades Certificadoras Subseqüentes, prestando serviço de emissão de solicitação de

---

55 - 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.

56 - 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.

certificados digitais à Autoridade Certificadora Subseqüente a qual é vinculada mediante contrato em favor do solicitante.

Mais adiante, verificaremos como ocorre este procedimento para a solicitação de certificados digitais perante a Autoridade Certificadora Raiz e Autoridades Certificadoras Subseqüentes.

3.2 Os dados do certificado e a segurança das chaves na ICP

No âmbito da ICP-Brasil, dois são os elementos que compõem o quadro de informações que devem ser asseguradas para o sucesso das operações de certificação digital e da chave privada: I – Dados pessoais que individualizam o proprietário do certificado digital perante os demais entes da sociedade, sendo armazenados no certificado digital juntamente com a chave pública certificada; e II – A chave privada do proprietário do certificado que é gerada de forma aleatória por este, é de seu exclusivo poder e conhecimento.

Embora ambos os elementos sejam essenciais para a viabilidade do sistema de assinatura digital em documentos eletrônicos, propostos pela ICP-Brasil, possuem um ponto que os distingue. Refere-se ao sujeito passivo da obrigação de garantia dessas informações.

Quando a proteção da informação refere-se aos dados cadastrais e individualizadores do indivíduo, temos que a responsabilidade compete ao Poder Público, através da ICP-Brasil. Quando a proteção da informação perfaz-se sobre a proteção e guarda da chave privada do indivíduo, temos que a responsabilidade compete privativamente ao proprietário do par de chaves.

Esta distinção, como veremos a seguir é importante na medida em que aponta o possível responsável pela reparação de danos causados à sociedade e a terceiros, diante de uma possível fraude, conforme veremos mais adiante.

Dessa forma, a segurança da informação no âmbito da ICP-Brasil possui caráter fundamental para a sistemática dos documentos eletrônicos assinados digitalmente.

3.2.1 Informações contidas nos certificados

O certificado digital é um documento eletrônico assinado digitalmente por uma terceira parte confiável vinculando a chave pública a uma determinada entidade (pessoa física ou jurídica).

No desenvolvimento desta tarefa, o certificado digital deve conter informações que visem individualizar o proprietário perante seus pares, com a finalidade de imputar-lhe as obrigações e direitos oriundos do uso do certificado eletrônico.

No exercício desta função, as informações contidas nos certificados digitais devem ser suficientes para associar uma determinada chave pública ao respectivo proprietário do certificado.

Destarte, conforme determinação de regras oriundas da Infra-estrutura de Chaves Públicas, para o desenvolvimento dessa função inerente ao certificado digital, as informações que devem compor o corpo do certificado digital são: Nome do titular do certificado; e-mail do titular; número no Cadastro de Pessoa Física – C.P.F. – do titular; Chave Pública pertencente ao titular; designação e assinatura digital da Autoridade Certificadora Subseqüente responsável pela emissão do certificado.

As referidas informações, conforme descreve a Declaração de Práticas de Certificação da ICP-Brasil[57], e a Resolução n.º 7 do Comitê Gestor da ICP-Brasil[58], que aprova os requisitos mínimos para política de certificação na ICP-Brasil, serão fornecidas sob a exclusiva responsabilidade do titular do certificado digital.

Conforme classifica a Declaração de Práticas da Autoridade Certificadora Raiz, o Certificado e as Listas de Certificados Revogados – LCR - e informações corporativas ou pessoais que necessariamente façam parte desses documentos ou diretórios públicos são consideradas informações não sigilosas, sendo livremente divulgadas à sociedade. Através de um conceito negativo, a

---

57 - Resolução n.º 1 de 25 de Setembro de 2001, que aprova a Declaração de Práticas da Autoridade Certificadora Raiz da ICP- Brasil.

58 - Resolução n.º 7 de 12 de Dezembro de 2.001, que aprova os requisitos mínimos para as políticas de certificado na ICP-Brasil.

mesma Declaração classifica como sigilosa todas as demais informações, prevendo para os casos de quebra de sigilo a necessidade de ordem judicial.[59]

3.2.2 A segurança das Chaves Privadas

A segurança da chave privada representa o outro ponto de informação que deve ser assegurada para a garantia dos sistemas de assinatura digital. A chave privada do signatário, ao contrário das informações contidas pelo certificado, não é entregue à Autoridade Certificadora, ficando sob a responsabilidade exclusiva do titular do par de chaves.

A segurança do sistema reside justamente na obrigação que o titular do par de chaves assume de não divulgar a chave privada, nem mesmo à Autoridade Certificadora Subseqüente que emitiu o certificado em seu favor, adotando regras e técnicas que previnam esta hipótese.

Conforme destaca Marcacini (2003)[60], a obrigação de armazenamento da chave privada de forma segura consiste num elemento novo na órbita jurídica, tendo em vista que esta hipótese não possui precedentes quanto às assinaturas convencionais, destacando a importância desta medida como sendo de aspecto fundamental da segurança das assinaturas digitais.

Se um terceiro tiver acesso à chave privada de alguém terá a possibilidade de realizar assinaturas digitais em nome deste e terá em suas mãos o poder suficiente para firmar obrigações perante terceiros, considerados possíveis contratantes, em nome do titular do par de chaves. A assinatura digital é gerada pela chave privada e conferida apenas pela chave pública. Assim, um agente mal intencionado poderia efetuar compras via Internet, utilizando-se de uma "personalidade em potencial", representada pela chave privada do agente, assinando contratos e adquirindo obrigações.

Diante desta responsabilidade do titular de par de chaves em manter a chave privada em total segurança contra ataques externos, algumas técnicas são

---

59 - Resolução n.º 1 de 25 de Setembro de 2001, que aprova a Declaração de Práticas da Autoridade Certificadora Raiz da ICP- Brasil.

60 - **MARCACINI. Augusto Tavares Rosa.** Certificação eletrônica, sem mitos e sem mistérios. Revista do Advogado. "Internet". Publicada pela Associação dos Advogados de São Paulo. Ano XXIII, n.º 69. Maio de 2003. Página 111.

propostas, como o uso de *smart-cards* e *tokens*, que possuem um chip interno à prova de invasão e somente podem ser utilizados através de uma senha ou algum tipo de biometria (por exemplo, impressão digital). Esses dispositivos são capazes de processamento interno e podem receber programas que usam a chave privada, protegendo-a contra qualquer tipo de invasão.[61]

Destarte, como a guarda da chave privada fica sob a responsabilidade do titular do certificado digital que garante o par de chaves, qualquer forma de dano ou violação à direito, de cunho material ou moral, ocasionado pela perda de forma culposa, ensejará a reparação, de acordo com as regras dos artigos 186 e 927 do Código Civil Brasileiro.

Neste caso, fica caracterizada a obrigação do próprio titular do certificado digital. Para melhor compreensão do tema, suponhamos um caso prático no qual o titular do par de chaves que ao proteger sua chave privada de forma negligente, confere a possibilidade de sua apropriação por um fraudador, que utilizando-se desta chave privada estabelece contratos com diversos "*Web sites"* em nome do titular e, de forma dolosa, realiza transações de somas vultosas a fim de apropriar-se desses valores e não realizar o pagamento. Neste fato tão comum no cotidiano, estando a empresa/terceira de boa-fé, terá o direito de ser ressarcida dos prejuízos que sofreu e este ressarcimento deverá ser promovido pelo titular do par de chaves, uma vez que, por sua culpa, foi responsável pelos danos experimentados.

3.3 Procedimento para requisição de certificado.

A requisição de um certificado digital no âmbito da ICP-Brasil possui um procedimento administrativo próprio, fixado por meio das resoluções emitidas pelo Comitê Gestor da ICP-Brasil.

O procedimento administrativo, conforme determina o Comitê Gestor é dividido em duas espécies: o procedimento para a certificação digital realizado

---

[61] **- FREITAS, Vinicius Pimentel de. LOEBENS, João Carlos.** Contratos eletrônicos e o Comércio Internacional. VIII Seminario Internacional de la Federación Internacional de antiguos alumnos del I.N.A.P. de España. Toledo. Agosto de 2.004. Páginas 23/24.

perante a Autoridade Certificadora Raiz; e o procedimento para a certificação digital realizado perante as Autoridades Certificadoras Subseqüentes.

Os atos procedimentais perante a Autoridade Certificadora Raiz, via de regra, são mais rigorosos que os determinados para os atos procedimentais perante as Autoridades Certificadoras Subseqüentes.

A razão que fundamenta esta disparidade encontra-se na própria finalidade dos certificados emitidos, uma vez que os certificados distribuídos pela AC-Raiz têm como finalidade permitir que as Autoridades Certificadoras Subseqüentes atuem no mercado, ou seja, autorização para que a autoridade certificadora subseqüente possa emitir certificados com o selo “ICP-Brasil”.

Por outro lado, os certificados emitidos pelas Autoridades Certificadoras Subseqüentes destinam-se às pessoas (entidade final) num contexto virtual-tecnológico, no qual o agente utiliza-se de seu par de chaves para as operações autorizadas como assinatura digital, autenticação, sigilo, etc.

3.3.1 Procedimentos perante a AC-Raiz

As regras estabelecidas para o credenciamento perante a AC-Raiz estão descritas nas resoluções n.º 6 de 22 de Novembro de 2001 e n.º 12 de 14 de Fevereiro de 2002, expedidas pelo Comitê Gestor da ICP-Brasil.

A solicitação de credenciamento perante a AC-Raiz será encaminhada ao protocolo geral da Presidência da República e será recebida dentro do prazo de 30 dias pela Entidade Raiz, mediante despacho fundamentado.

Existem duas espécies de critérios que são exigidos para os candidatos ao credenciamento perante a AC-Raiz. Existem os critérios gerais, que são exigidos tanto das candidatas a Autoridades Certificadoras Subseqüentes, como das candidatas a Autoridade de Registro, e também existem os critérios específicos para cada espécie de autoridade.

São quatro os critérios exigidos em comum:

I - Ser órgão ou entidade de direito público ou pessoa jurídica de direito privado.

Dentro deste primeiro critério podemos extrair que a Autoridade Certificadora nunca poderá ser entendida como pessoa física, enquanto ente individualizado capaz de certificar uma outra pessoa.

Em decorrência disto, tanto o órgão como a entidade pública ou privada deverão estar regularmente constituídos e instituídos como pessoa jurídica, com personalidade jurídica e capacidade de adquirir direitos e obrigações na órbita legal. O que basicamente diferencia as pessoas físicas e jurídicas corresponde a sua formação, entretanto ambas são consideradas entidades de direito passíveis de aplicação da lei.

II - Estar quites com todas as obrigações tributárias e os encargos sociais instituídos por lei.

Via de regra, esta é uma exigência contida nas principais relações existentes entre a Administração Pública e os entes privados. Muitas são as circunstâncias em que o Poder Público, no exercício de sua função de perseguir o desenvolvimento e o bem estar social, acaba por transmitir à iniciativa privada, total ou parcialmente, a realização das tarefas, mas para isso, exige do prestador a regularidade perante os cofres públicos, como ocorre nos casos de licitação, sendo um dos principais requisitos objetivos para que a entidade ou o agente possa ser contratado consiste em sua regularidade tributária.

III - Atender aos requisitos relativos à qualificação econômico-financeiro estabelecidos, conforme a atividade a ser desenvolvida (lista de documentos exigidos que comprovem os requisitos solicitados).

A principal finalidade deste requisito consiste em evidenciar concretamente ao Comitê Gestor, a regular qualidade financeira da pessoa jurídica candidata a Autoridade Certificadora Subseqüente ou Autoridade de Registro. Entre os principais documentos exigidos podemos destacar: balanço patrimonial do último exercício financeiro ou demonstrativo financeiro, certidão negativa de falência ou concordata;

IV - Atender às diretrizes e normas técnicas da ICP-Brasil relativas à qualificação técnica, constantes dos documentos relacionados à resolução n.º 6, aplicáveis aos serviços a serem prestados (lista de documentos exigidos que comprovem as diretrizes solicitadas).

A principal finalidade do presente requisito consiste em demonstrar que a pessoa jurídica candidata a Autoridade Certificadora Subseqüente possui

capacidade técnica de exercer a função. Dentre os documentos exigidos vale ressaltar: declaração de práticas de certificação, política de certificados, política de segurança, documento explicitando se pretende ou não emitir certificados às autoridades certificadoras inferiores ao seu nível.

São quatro os requisitos exigidos especificamente às candidatas ao credenciamento como Autoridades Certificadoras Subseqüentes:

I - Apresentar, no mínimo, uma entidade operacionalmente vinculada, candidata ao credenciamento para desenvolver as atividades de Autoridade de Registro - AR, ou solicitar o seu próprio credenciamento como AR.

A justificativa para o presente requisito encontra fundamento perante as normas operacionais que regem a expedição de certificados eletrônicos pelas Autoridades Certificadoras Subseqüentes. De acordo com o artigo 7º da Medida Provisória 2.200-2/01[62], às Autoridades de Registro compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às Autoridades Certificadoras Subseqüentes e manter registro de suas operações. Destarte, a Autoridade de Registro consiste no órgão competente para iniciar o processo de solicitação de certificados eletrônicos perante a ICP-Brasil.

II - Apresentar a relação de eventuais candidatos ao credenciamento para desenvolver as atividades de prestador de serviço de suporte.

III - Ter sede administrativa, instalações operacionais e recursos de segurança física e lógica, inclusive sala cofre, compatíveis com a atividade de certificação, todos localizados no território nacional.

A política de segurança aprovada pelo Comitê Gestor, através da Resolução n.º 2, de 25 de Setembro de 2001, fixa quais os parâmetros que devem ser seguidos para garantir a segurança física e lógica das instalações de uma autoridade certificadora subseqüente.

O ambiente físico das atividades de segurança, deve ser entendido como aquele composto por todo o ativo permanente das entidades integrantes da ICP-Brasil. Entre as principais atividades de segurança física das instalações das

---

62 - 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.

Autoridades Certificadoras Subseqüentes estão: o controle de acesso pessoal aos locais internos e o uso de salas cofre.

O ambiente lógico, assim como o anterior, também sofre regulamentação quanto à forma de proteção. Ele deve ser entendido como o composto por todo o ativo de informações da entidade. Entre as principais atividades desenvolvidas nesse sentido podemos destacar a classificação das informações, de acordo com o seu grau de importância para o sistema, sofrendo assim maior proteção quando mais importante e devem ser protegidas contra ataques externos, visando evitar a ocorrência de prejuízos aos usuários.

IV - Contratar seguro para cobertura de responsabilidade civil decorrentes da atividade de certificação digital e de registro, com cobertura suficiente e compatível com o risco.

Neste requisito duas são as ponderações que justificam a sua pertinência. Em primeiro lugar, a falha da atividade desenvolvida pelas autoridades certificadoras, assim como todo serviço, é passível de gerar danos a seus usuários diretos ou indiretos; Em segundo plano, a fim de resguardar o direito às indenizações pelos danos sofridos aos usuários em potencial, nasce para as candidatas à Autoridade Certificadora Subseqüente a necessidade de contratarem seguro para a cobertura de suas responsabilidades cíveis.

Após cumprido todos os requisitos alhures esboçados, diferentemente da solicitação de certificado perante as Autoridades Certificadoras Subseqüentes, o requerimento deverá ser encaminhado à própria Autoridade Certificadora Raiz. O requerimento deve vir acompanhado dos documentos alhures referidos.

Seguindo o recebimento da solicitação de credenciamento pela Autoridade Certificadora Raiz, inicia-se o processo de auditoria e fiscalização da Autoridade Certificadora Subseqüente. Finalizadas as referidas tarefas, a decisão fundamentada será comunicada à candidata. Esta decisão poderá ser pelo deferimento total ou parcial, ou pelo indeferimento da política de certificado apresentada pela candidata. A política de certificado é o documento competente para descrever as atuações da candidata. Dessa forma, se as conclusões da auditoria indicarem que certas atividades ali descritas não apresentam certas condições diante da realidade técnica encontrada nos equipamentos da candidata, a política de certificação será indeferida total ou parcialmente.

O credenciamento se exaure com a emissão do certificado à Autoridade Certificadora Subseqüente. Após o deferimento do credenciamento, a Autoridade Certificadora Raiz emitirá, no prazo de 10 dias, o certificado autorizando o inicio das atividades de certificação. A Autoridade Certificadora Subseqüente por sua vez, terá um prazo máximo de 60 (sessenta) dias para entrar em operação.

3.3.2 Procedimentos perante a Autoridade Certificadora Subseqüente

O procedimento para a emissão de um certificado digital para o usuário final inicia-se nas Autoridades de Registro vinculadas à Autoridade Certificadora Subseqüente escolhida pelo candidato ao certificado. O candidato inicia o procedimento enviando à Autoridade de Registro competente os documentos exigidos pela política de certificação da Autoridade Certificadora Subseqüente da qual pretende obter o certificado.

A Autoridade de Registro realizará as devidas verificações quanto à regularidade e legitimidade do requerente, conforme exigidos pela Política de Certificação da referida Autoridade Certificadora Subseqüente, e após verificar a conformidade do pedido às regras preestabelecidas, encaminhará à referida Autoridade Certificadora Subseqüente, escolhida pelo requerente, a devida solicitação para a emissão do certificado.

Os procedimentos técnicos relativos ao par de chaves e efetiva emissão do certificado devem ser descritos na própria política de certificado da Autoridade Certificadora, devendo ser observados como requisitos essenciais para a emissão do competente certificado digital.

Vale ressaltar que princípios gerais de certificação fixados por norma legal devem ser seguidos pelas políticas de certificado das Autoridades Certificadoras Subseqüentes. Tal é o caso da necessidade de o requerente gerar o seu par de chaves e informar apenas a chave pública à autoridade certificadora, com o propósito de vinculá-lo ao certificado, mantido o sigilo da chave privada, conforme regra geral aposta na Medida Provisória 2.200-2/01.[63]

---

[63] - 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

Com a finalidade de estudarmos empiricamente o procedimento para solicitação de certificado digital operado diante da autoridade certificadora subseqüente, no presente trabalho vamos tomar como parâmetro a política de certificação da SERPRO do tipo A1[64] (PC SERPROACFA1).

Após receber da Autoridade de Registro a solicitação de emissão de certificado, o primeiro passo realizado pela Autoridade Certificadora SERPRO consiste na verificação da posse da chave privada.

A mensagem enviada pela Autoridade de Registro contendo a solicitação de emissão de certificado deve obedecer ao padrão PKCS#10. Esta mensagem deverá incluir uma assinatura digital produzida através do uso da chave privada correspondente à chave pública que consta da referida solicitação. Assim que for recebida, o software de certificação verificará a assinatura digital anexa à solicitação utilizando-se da chave pública aposta também na solicitação. Uma vez validada, a solicitação é armazenada no banco de dados do próprio software de certificação, na qual ser-lhe-á atribuído um número de identificação. Este número é gravado no corpo do termo de responsabilidade ou de titularidade junto com os dados do solicitante. Todos os dados da solicitação são autenticados pela Autoridade de Registro através de documentos oficiais.

O segundo e derradeiro passo consiste na própria emissão do certificado em favor do solicitante, que poderá começar a utilizá-lo em suas transações civis ou comerciais, quando assinadas eletronicamente.

3.3.3 Procedimento perante a Autoridade de Registro

O principal papel desenvolvido pelas Autoridades de Registro corresponde à identificação e individualização dos candidatos, de forma a não restar dúvida quanto ao agente.

---

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.

[64] - São quatro os tipos de certificados utilizados em assinaturas digitais: A1, A2, A3, A4. Iremos defini-los e estuda-los no Cáitulo 6, quando estudaremos os certificados digitais.

A solicitação de um certificado eletrônico é feita junto à Autoridade de Registro credenciada para atuar junto a Autoridade Certificadora Subseqüente escolhida pelo requerente.

As resoluções do Comitê Gestor da ICP-Brasil fixam regras gerais para as atividades das Autoridades de Registro. Todavia, cada Autoridade de Registro possui a sua Política de Certificação especificada pela Autoridade Certificadora Subseqüente à qual é ligada, que deve ser seguida, em consonância com essas regras gerais.

Seguindo na proposta de análise do presente trabalho, iremos detalhar como se desenvolve o processo de identificação realizado pelas Autoridades de Registro credenciadas junto a Autoridade Certificado SERPRO.

De acordo com a política de certificação da SERPRO[65], o candidato a emissão de um certificado eletrônico deverá se submeter a um processo de autenticação de identidade dos Titulares de Certificados.

O candidato deverá comparecer fisicamente, apresentando os documentos de identificação exigidos: uma foto recente; cédula de identidade ou passaporte, se estrangeiro; Cadastro de Pessoa Física – C.P.F.; Comprovante de residência; Número de identificação Social-NIS (Cadastro do Programa de Integração Social-PIS, Cadastro do Programa de Formação do Patrimônio do Servidor Público-PASEP ou Cadastro de Contribuintes Individuais do INSS-CI), se aplicável; Cadastro Especifico do INSS-CEI, se aplicável; Titulo de eleitor, se aplicável; Serão exigidos os documentos acima relacionados do responsável, caso o solicitante seja incapaz.

---

[65] **- SERPRO** – Serviço Federal de Processamento de Dados. Política de Segurança. Declaração de Práticas de Certificação da Autoridade Certificadora do SERPRO. Brasília (DF). Disponível em: https://thor.serpro.gov.br/ACSERPRO , acessado em 28 de Novembro de 2005.

4 O DOCUMENTO ELETRÔNICO

No presente capítulo, analisaremos a concepção legal conferida aos documentos em geral. Esta análise corresponde à sua posição dentro do sistema jurídico brasileiro, e sua utilização como fonte de prova judicial.

Destarte, identificaremos os requisitos necessários para conferir validade às provas em geral, e especificamente, aos documentos manuscritos e eletrônicos.

Após verificado os requisitos de validade, passaremos a analisar os elementos que no ordenamento jurídico brasileiro consubstanciam a força probante dos documentos em geral, e com isso, faremos um paralelo na sistemática dos documentos eletrônicos.

Por fim, identificaremos as principais semelhanças e diferenças entre os documentos manuscritos e os documentos eletrônicos, quanto a suas formas e caminhos até atingir o fim em comum.

4.1 O Documento

A palavra documento encerra sua origem etimológica no verbo latino *"docere"* significando as ações de ensinar, fazer conhecer, dar ciência.

O documento, de uma forma geral, é um instrumento largamente utilizado pelo ordenamento jurídico brasileiro. Sua importância transcende à mera instrumentalidade dos processos judiciais. Dentre as principias utilidades que os documentos em geral apresentam na órbita jurídica podemos destacar a fixação dos delitos de falsificação de documento público (Art. 297[66]) e falsificação de documento particular (Art. 298[67]) previstos no Código Penal Brasileiro; a condição de

---

66 - "Art. 297 - Falsificar, no todo ou em parte, documento público, ou alterar documento público verdadeiro:
Pena - reclusão, de dois a seis anos, e multa."

67 "- Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
Pena - reclusão, de um a cinco anos, e multa."

formalização de negócios jurídicos no Direito Civil (Art. 108[68]); o uso do documento como prova processual pelo Direito Processual Civil (Art. 355[69] e Art. 364[70] do CPC); e Processual Penal (Art. 231[71] e 232[72] do CPP).

4.2 A força probatória do documento no direito brasileiro

Em matéria processual, com a adoção do princípio da persuasão racional ou do livre convencimento judicial pelo sistema jurídico-processual de avaliação de provas, o juiz é livre para apreciar a força probante das provas constantes do processo, desde que observadas as regras processuais, ou seja, nenhuma prova possui um valor preestabelecido por lei, cabendo ao juiz do caso a análise das circunstâncias que perfazem sua força probante.

Segundo o referido princípio, o juiz poderá fundamentar sua decisão baseado em provas testemunhais contrárias às provas documentais apresentadas nos autos, quando possuir plena convicção de que as provas testemunhais apresentaram maior segurança jurídica a seu entendimento, como também, poderá ocorrer o contrário.

Entrementes, no ordenamento jurídico brasileiro, não obstante a livre análise das provas apresentadas aos autos, para a validade das provas em geral, inclusive a documental, é imperioso que sua produção ocorra diante dos princípios Constitucionais do contraditório[73], da ampla defesa[74], duplo grau de jurisdição e do

---

[68] - "Art. 108. Não dispondo a lei em contrário, a escritura pública é essencial à validade dos negócios jurídicos que visem à constituição, transferência, modificação ou renúncia de direitos reais sobre imóveis de valor superior a trinta vezes o maior salário mínimo vigente no País."

[69] - "Art. 355. O juiz pode ordenar que a parte exiba documento ou coisa, que se ache em seu poder."

[70] -" Art. 364. O documento público faz prova não só da sua formação, mas também dos fatos que o escrivão, o tabelião, ou o funcionário declarar que ocorreram em sua presença."

[71] - "Art. 231. Salvo os casos expressos em lei, as partes poderão apresentar documentos em qualquer fase do processo."

[72] - "Art. 232. Consideram-se documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares.

[73] - Ao fazermos referência ao princípio do contraditório como elemento essencial para a validade da prova no processo penal, tomamos como parâmetro a possibilidade plena e efetiva que as partes possuem para ter acesso e contradizer todas as informações disponiveis no processo, em especial, as provas produzidas pela parte contrária. Neste sentido Joaquim Canuto Mendes de Almeida coloca que o contraditório consiste na: *"ciência bilateral dos atos e termos processuais e possibilidade de contrariá-los."*. **FERNANDES, Antonio Scarance.** Processo Penal Constitucional. Editora Revista dos Tribunais. 3ª. edição , revista, atualizada e ampliada. 2002. Pág. 58.

[74] - O princípio da ampla defesa, muitas vezes confundido com o contraditório, mas na verdade complementar àquele, consiste, conforme expõe Rosane Cima Capiotto, numa *"garantia*

devido processo legal (Marcacini, 2003)[75]. A prova, de qualquer espécie, que for produzida sem observância dos referidos princípios, será considerada ilícita.

Somente após a apreciação dessas condições, a prova documental em geral poderá ser questionada e avaliada pelo julgador quanto as condições que pressupõem sua força probante.

Este aspecto representa o último passo para o exercício de valoração das provas realizado pelo juiz, em virtude do princípio da persuasão racional. Dois sãos os elementos que devemos ter em consideração para essa avaliação: Autoria (ou autenticidade) e Integridade.

A identificação da autoria é considerada o primeiro requisito fundamental para a avaliação da força probante das provas documentais em geral. A melhor doutrina nacional e internacional[76] destaca que assegurar a autoria consiste em elemento fundamental para se conferir força probante aos documentos em geral.

Outro requisito básico para a verificação da força probatória em geral na esfera jurídica consiste na garantia da integridade do documento.

O julgador, ao receber as provas documentais, deverá se ater à verificação dos elementos que compõem os requisitos de autoria e integridade do documento. A força probante do documento variará de acordo com a maior intensidade que o julgador obtiver sobre a certeza da autoria e integridade do documento.

A corroboração dos documentos em geral no mundo jurídico depende primeiro da análise da validade diante dos princípios e garantias constitucionais e, num segundo plano, da análise da força probante por meio da verificação da existência de circunstâncias que assegurem a autoria e a integridade.

---

constitucional que assegura ao acusado a possibilidade de trazer ao processo todos os elementos necessários ao esclarecimento da verdade, e até mesmo a possibilidade de calar-se, caso entenda ser a medida adequada. **FERRARI, Eduardo Reale.** A Excepcionalidade da Prova Ilícita no Processo Penal Brasileiro. Dissertação apresentada a Pontifícia Universidade Católica de São Paulo para a obtenção do Título de Mestre em Direito. São Paulo. 2004. Pág 12.

[75] - O principio do contraditório e da ampla defesa são corolários do principio do devido processo legal. De acordo com este principio, que surgiu na Inglaterra, contra as peripécias do Rei João Sem Terra, qualquer indivíduo somente poderá ser privado de seus direitos diante de um devido processo desenvolvido diante dos preceitos legais. Aplicando o conceito ao tema específico de provas penais chegamos a conclusão de que somente com o respeito aos principios constitucionais que regem a produção de provas, o juiz poderá fundamentar sua decisão condenatória, privando uma das partes.

[76] **- MARCACINI. Augusto Tavares Rosa.**“ Certificação eletrônica, sem mitos e sem mistérios”. Revista do Advogado. “Internet”. Publicada pela Associação dos Advogados de São Paulo. Ano XXIII, n.º 69. Maio de 2003. Página 80.

4.3 Provas ilícitas

Conforme visto acima, antes de verificarmos a força probante das provas devemos verificar sua validade jurídica. Para tanto, é necessário verificarmos se sua produção (p. ex.: colheita) ocorreu de forma lícita. Ocorrendo a negativa quanto a essas circunstâncias, estaremos diante de uma prova ilícita, ou seja, sem validade para o direito brasileiro.

Diante disso, a prova ilícita é aquela obtida em discordância das garantias e normas fundamentais asseguradas pela Constituição Federal de 1.988 para a proteção das liberdades públicas, especialmente dos direitos de personalidade e daquela sua manifestação que é o direito à intimidade. De acordo com a teoria pátria, são totalmente repugnáveis no direito brasileiro as provas consideradas ilícitas, com exceção baseada no princípio da proporcionalidade, originário das teorias jusnaturalistas formuladas na Inglaterra nos séculos XII e XIII, e posteriormente aperfeiçoadas no Direito Alemão.

Segundo o princípio da proporcionalidade, quando a prova ilícita versar sobre a defesa do acusado, resguardando uma garantia maior que aquela defesa na proibição de utilização das provas ilícitas, o julgador deverá ponderar a aplicação de ambos os princípios em questão, alcançando a melhor solução apoiado na Hermenêutica Constitucional. Vejamos, quando estiver em confronto o direito constitucional da intimidade invadida, contra o garantia de liberdade do acusado, que somente poderá ser assegurada com fundamento em provas ilícitas, esta deverá prevalecer, uma vez que a garantia da liberdade pode ser considerada um bem de maior valor legal, que o direito à intimidade.

As provas ilícitas diferenciam-se das provas ilegítimas, ao passo que estas são consideradas provas obtidas com afronta ao direito processual e não com afronta aos direitos e garantias constitucionais.

Diversamente da prova ilícita, que não será descartada somente nas hipóteses em que o bem constitucional protegido em questão for maior que o bem constitucional protegido pela proibição do uso da prova ilícita, a prova ilegítima não será descartada se da sua adoção não advier prejuízos para a parte contrária, em decorrência de sua natureza processual, ou quando o bem protegido em questão for maior que o bem protegido pela proibição da prova ilegítima.

Neste caso, as provas ilegítimas não serão anuladas desde que não acarretem prejuízo para as partes ou quando o bem protegido em questão for maior que o bem protegido pela vedação da prova ilegítima. Incorrendo qualquer uma das hipóteses anteriores, a prova ilegítima deverá ser descartada do processo, entretanto, não acarretando responsabilidade penal ao seu autor, como ocorre nas provas ilícitas, onde o autor, via de regra, responderá por afronta a direitos fundamentais garantidos.

Somente com uma acurada interpretação das provas produzidas em processo de forma lícita e legítima caberá ao juiz prolatar sua sentença baseada na certeza de sua convicção, apoiada sobre as provas originadas em conformidade aos direitos e garantias constitucionais.

4.4 A autoria

A autoria representa o primeiro elemento essencial de força probante dos documentos em geral, e conforme as palavras de Santos (1997, p. 388) “por autenticidade se entende a certeza de que o documento provém do autor nele indicado.”[77]

O primeiro passo para o exame da força probatória de um documento para fins legais consiste na demonstração inequívoca de sua autoria, encontrando-se suficientemente esclarecida a ponto de proporcionar a não suscitação de dúvidas.

Conferir a autoria ou falsidade da autoria de um documento eletrônico simboliza a possibilidade de identificar proporcionalmente a confecção do documento e conseqüentemente atribuí-lo ao aludido autor originário.

Via de regra, a autoria dos documentos em geral é obtida por meio das assinaturas. A assinatura, vista como sinal característico e exclusivo de seu autor, consiste no elemento por excelência capaz de gerar autoria aos documentos.

Quando usamos a expressão, assinatura digital, para designar o elemento aposto aos documentos eletrônicos, subentendemos equivocadamente

---

[77] **- SANTOS. Moacyr Amaral.** Primeiras Linhas de Direito Processual Civil. Editora Saraiva. 18ª. Edição. São Paulo. 1997. Pág. 388

que este elemento assegura sua autoria. Em verdade, a verificação da autoria neste processo utiliza a chave pública do signatário. Vejamos, uma vez assegurado juridicamente o vínculo entre a chave pública e o signatário, por meio de um documento denominado certificado digital, o resultado positivo no processo de verificação de inalterabilidade do documento eletrônico com o uso desta chave pública certificada garante a autoria do documento eletrônico ao proprietário do certificado.

Ocorrendo repúdio sobre a autoria de uma assinatura manuscrita, o exame grafotécnico é o meio empregado para o direito a fim de dirimi-la. Nos documentos eletrônicos, a impossibilidade de realização de exames grafotécnicos não inviabiliza sua utilidade pelo ordenamento jurídico brasileiro, uma vez que o exame grafotécnico poderá ser substituído por exames sobre a validade ou invalidade do certificado digital. No capítulo seguinte analisaremos com maior profundidade a referida questão.

4.5 A integridade

A integridade corresponde a uma qualidade indicando que um dado elemento mantém seus componentes originais. A verificação da integridade ocorre partindo-se do princípio de que uma alteração ocorrida em qualquer componente do elemento deixe vestígios que possam ser percebidos.

Em arquivos eletrônicos desprovidos de um sistema para assegurar a integridade, não encontramos a integridade, uma vez que podem sofrer alterações em seu formato original sem deixar vestígios que possam ser percebidos.

Conforme Samsom apud Porto (2002)[78], o que determina ao documento a força probante é sua capacidade de relatar o fato ou relação factual de maneira perpétua, sem a possibilidade de alteração imperceptível, sob pena de denunciar a menor forma de alteração posterior ao documento, modificando sua estrutura original e válida.

---

[78] **- PORTO, Luiz Guilherme Moreira**. Tipicidade nos crimes de falsidade documental em face do bem jurídica protedigo. 2002. 203p. Dissertação de Mestrado. Faculdade de Direito. Universidade de São Paulo. Sào Paulo. 2002. Pág. 49.

Com a integridade, o documento passa a ter uma característica de continuidade temporal, ou como observa Porto (2002), ao versar sobre o tema, designa a integridade como função de perpetuidade *"consistente na capacidade do documento de reter a declaração nele inserida de forma duradoura."*[79]

Porto (2002) ainda dissertando sobre o tema, coloca a integridade como sendo a primeira função desempenhada pelo documento: *"A primeira função exercida pelo documento é a de perpetuidade, consistindo na capacidade de o documento reter a declaração nele inserida, por tempo relevante."*[80]

Com o documento eletrônico, esta propriedade pode ser obtida com a utilização do sistema de criptografia assimétrica. Com os fundamentos da matemática aplicada utilizados pela criptografia assimétrica, uma vez gerada a assinatura, o reverso deste processo torna-se praticamente impossível. Dessa forma, ocorrendo a mínima alteração posterior à realização da assinatura, esta será detectada na futura verificação de validade do documento eletrônico. Este processo será mais detalhadamente estudado em capítulo posterior.

4.6 A autoria e integridade via assinatura digital

Ao surgir a idéia de documentos em formato eletrônico, fundada nos avanços tecnológicos de meados dos anos 90, os estudos jurídico-cientifícos declaravam a total impossibilidade de sua consideração como meio de prova documental, destacando, entretanto que, tais cientistas jurídicos desconheciam a conceituação de assinatura digital, surgida gradativamente no meio social, desde 1.977.

Marcacini (2003, p. 109) relata sobre a época:

> *"...nos primeiros estudos de informática relacionados ao direito, desenvolvidos até a primeira metade da década de 90, era negado o valor de prova*

---

[79] - **PORTO, Luiz Guilherme Moreira**. Tipicidade nos crimes de falsidade documental em face do bem jurídica protedigo. 2002. 203p. Dissertação de Mestrado. Faculdade de Direito. Universidade de São Paulo. Sào Paulo. 2002. Pág 49.

[80] - **PORTO, Luiz Guilherme Moreira.** Tipicidade nos crimes de falsidade documental em face do bem jurídica protedigo. 2002. 203p. Dissertação de Mestrado. Faculdade de Direito. Universidade de São Paulo. Sào Paulo. 2002. Pág 89.

> *documental aos chamados 'documentos informáticos'. A impossibilidade de se lançar uma assinatura manuscrita que se apegasse exclusivamente a um único documento eletrônico, bem como a inexistência de vestígios deixados por posterior adulteração são realidades inafastáveis da forma eletrônica.*
>
> *Todavia, tais estudos desconheciam avanços científicos recentes, que, em 1.977, haviam descoberto o que hoje chamamos de assinatura digital."*[81]

Desta sorte, pouco importa qual o elemento utilizado para a exteriorização documental, se papel, madeira, osso, pedaços de pano, ou formas digitalizadas, interessando ao mundo de valor probatório apenas a capacidade de atingir seu fim jurídico ou seja, atingir os requisitos de autoria e integridade, responsáveis pela força probante do diploma eletrônico.

Poderá ocorrer que os juizes não detenham conhecimento científico apropriado a fim de emitirem juízos de valor sobre a força probante do documento eletrônico, dificultando assim o exercício de reconhecimento dos elementos informadores da força probante desses documentos em geral.

Neste passo, cabe-nos fazer a ressalva fixada por Mittermaier, quando expõe que ao se deparar com dificuldades na identificação de elementos essenciais para a força probante de um documento, deverá o juiz valer-se de seus auxiliares técnicos, ou peritos comumente conhecidos, a fim de dirimir suas dúvidas.[82]

Uma assinatura digital realizada sobre um documento apresenta as seguintes características:

- Confere autenticidade ao documento eletrônico, possibilitando a fixação de responsabilidade apoiado neste documento;
- A assinatura digital, atendendo aos requisitos de segurança, dificilmente poderá ser falsificada, em vista de ser chancelada de forma diferente em cada documento assinado digitalmente. É importante frisar a responsabilidade do proprietário do par de chaves quanto à segurança da chave privada, não

---

[81] - **MARCACINI. Augusto Tavares Rosa.** In Certificação eletrônica, sem mitos nem mistérios. Revista do Advogado. Internet. Associação dos Advogados de São Paulo. Ano XXIII, n.º 69. Maio/2003. Pág 109.

[82] **- MITTERMAIER, C.J.A.** Tratado da Prova em Matéria Criminal. 2.ed. Campinas: Bookseller, 1997. Pág 305.

podendo ser transferida a ninguém, sob pena de se haver documentos eletrônicos assinados originalmente, sem a sua concessão;

- Não há possibilidade de ser reutilizada, tendo em vista que se amolda às características do documento eletrônico, não podendo sofrer modificações posteriores sob pena de perecimento;
- Impede que haja modificações posteriores à realização da assinatura sob pena de invalidade;
- O documento presume-se verdadeiro, com a possibilidade de prova em contrário, quando, por exemplo, o agente for coagido a assinar determinado documento, visando beneficiar terceiro criminoso.

4.7 A existência da prova documental nos documentos eletrônicos

Partindo do adágio sobre os documentos eletrônicos serem formados por bits e bytes não havendo necessidade de sua concretização na celulose, vivemos periodicamente utilizando e firmando obrigações por meio desta via.

Um exemplo corriqueiro acontece quando realizamos um saque no caixa eletrônico de nosso banco, utilizando o sistema *on line*, o banco firma um documento eletrônico que comprovará a retirada para desconto em nossa conta corrente.

A chegada da Internet mudou o conceito de fornecimento de serviços (Arbex, apud Tucci, 2000), principalmente pelos bancos, que investiram pesado na modernização das agências e profissionalização de seus funcionários, buscando explorar essas facilidades na busca da redução de custos e satisfação de seus clientes.[83]

A composição dos documentos eletrônicos (Custódio, Dias e Rolt, 2003) deve ser encarada como uma sucessão de bits, sendo que para tanto o

---

[83] - TUCCI. José Rogério Cruz e. Direito e Internet. Texto: Eficácia Probatória dos Contratos celebrados pela Internet. Coordenadores: Newton de Lucca e Adalberto Simão Filho. Editora Edipro. 1.º edição. 2000. Bauru – SP. Pág. 273/274.

usuário deverá dispor de computador compatível para criar e futuramente ter acesso às informações contidas no arquivo eletrônico.[84]

Em verdade, podemos considerar o surgimento dos documentos eletrônicos como um novo tempo para o armazenamento de dados. Por meio deste instrumento, o papel poderá significar algo pertencente ao passado, tendo em vista que as informações passaram a ser armazenadas em suportes mecânicos, magnéticos, óticos e fotossensíveis.

A assinatura digital aposta em um documento eletrônico é encarada como uma das formas mais seguras, tecnicamente, de assegurar os elementos da autenticidade e integridade dos dados eletrônicos, tendo em vista, dificultar em muito, a possibilidade de adulteração ou modificação do conteúdo probatório, após o seu encerramento pelo autor originário legal, perfazendo os requisitos essenciais para a força probante de toda e qualquer forma de prova documental eletrônica.

A possibilidade de realização de fraude junto aos documentos eletrônicos assinados digitalmente pode ser considerada no mesmo nível dos documentos autógrafos convencionais utilizados como prova em procedimentos judiciais no atual ordenamento jurídico brasileiro.

A possibilidade dos documentos eletrônicos assinados digitalmente serem considerados meio de prova equiparado aos documentos tradicionais constitui fato tão marcante que Dinemar Zoccoli, Silvia Miccoli, Manoel J. Pereira dos Santos e Ângelo de Angelis apud Renato Opice Blum (2001, p. 52)), afirmam:

> *"Frise-se que a verificação positiva de uma assinatura digital enseja um elevado grau de certeza jurídica da autenticidade da autoria e da integridade da mensagem ou outro tipo de documento, pois se comprova, com certeza substancial, que o documento não foi alterado e que provem de seu emissor. Dessa forma não vemos óbices para que um documento assim assinado não seja equiparado desde já, independentemente de lei específica ou complementar, a*

---

[84] - CUSTÓDIO. Ricardo F.. DIAS. Júlio S.. ROLT. Carlos R.. Texto: Assinatura Confiável de Documentos Eletrônicos. in Confiança no uso de documentos eletrônicos. BRy Tecnologia S.A. Laboratório de Segurança em Computação – LABSEC – UFSC. Laboratório de Tecnologia de Gestão – LABGES – UDESC. Florianópolis. Agosto de 2003. Pág. 09.

> *um original escrito e assinado de forma autografa pelo seu subscritor."*[85]

Vencida a etapa de nivelação jurídica dos documentos eletrônicos e autógrafos, verificamos tecnicamente algumas diversidades entre os diplomas acima referidos.

O documento autógrafo, que expressa informação, por meio da folha de papel, fornece ao agente a possibilidade de captação direta da informação. Dessa forma, o indivíduo, com o papel em mãos, analisa seu conteúdo, sem o auxílio de instrumentos mecânicos. Contrariamente a tal posicionamento, encontramos os documentos eletrônicos, necessitando de equipamentos específicos (ex. computadores) para expressar a sua informação.

A relação se faz necessária tendo em vista a forma na qual o documento foi compactuado, ou seja, em forma de bits. No documento tradicional imposto sobre a celulose (Blum, 2001), o acesso às informações representadas em seu corpo ocorre de forma direta, sem o auxílio de outros equipamentos, contrariamente ao que ocorre com os documentos eletrônicos armazenados em forma de bits, que necessitam do auxílio externo dos computadores para tornar-se compreensíveis diante da inteligência humana.[86]

Em outras palavras, a existência jurídica de ambos os documentos, eletrônico e autógrafo, não esta atrelada da forma material pela qual o documento se exterioriza, mas do resultado que o documento expressa.

Existindo em ambos os casos os elementos da autoria e da integridade, o instrumento, tanto em formato eletrônico como no formato autógrafo, conterá força probante suficiente como documento para fins judiciais. A lei, via de regra, não exige forma para a confecção do diploma. O que vale, consiste na obediência aos preceitos legais quanto aos direitos de cada indivíduo no momento da expedição do documento e a presença de elementos que assegurem a autenticidade e integridade deste mesmo diploma.

---

[85] - BLUM. Renato M. S. Opice. Direito eletrônico. A Internet e os tribunais. Texto: O processo eletrônico: assinaturas, provas, documentos e instrumentos digitais. Coordenador: Renato M. S. Opice Blum. Editora Edipro. 1.º edição. 2001. Pág. 52.

[86] - BLUM. Renato M. S. Opice. Direito eletrônico. A Internet e os tribunais. Texto: O processo eletrônico: assinaturas, provas, documentos e instrumentos digitais. Coordenador: Renato M. S. Opice Blum. Editora Edipro. 1.º edição. 2001. Pág. 10.

Embora esta regra de liberalidade quanto a confecção do documento tenha suas raízes no direito processual civil, aplica-se também ao direito processual penal. Neste sentido, são lapidares as palavras de Navarrete apud Tucci (2001):

> *"o que afasta o contrato tradicional de um contrato eletrônico, sob a perspectiva estrutural, é apenas a formação do mesmo, quanto ao modo de manifestação do consentimento e de aperfeiçoamento do negócio, bem como de sua respectiva prova, tanto judicial como extrajudicial."*[87]

A força probante do documento eletrônico depende da obtenção dos requisitos de autoria e da integridade, e uma vez alcançados referidos requisitos, o documento deverá ser encarado como os documentos autógrafos são, tendo em vista, as garantias técnicas e legais que os documentos eletrônicos dispensam em relação aos documentos autógrafos.

O documento eletrônico surgiu para suprir um velho anseio de toda a sociedade, qual seja, a substituição dos obsoletos documentos de papel. Há muito se tentava por meio da microfilmagem e da digitalização de documentos a permuta dos instrumentos de celulose, não sendo possível, entretanto, esta dispensa, uma vez que os sistemas não conseguiam proporcionar autenticidade e integridade aos documentos eletrônicos conforme ocorria aos documentos de papel.

A realidade começou a se transformar quando se vislumbrou a possibilidade de criar um diploma seguro sem a utilização do papel, nascendo assim o documento eletrônico.

Por outro lado, existem casos na lei brasileira que expressamente proíbe o uso de documentos eletrônicos, relatando a necessidade do documento de papel. Exemplificando esta referência, Blum (2001, p.56) disserta que para a fiança ainda é necessário o uso de documentos autógrafos, não aceitando a lei o formato eletrônico de documento, mesmo que estejam garantidos os elementos da autenticidade e da integridade.[88]

---

[87] **- TUCCI. José Rogério Cruz e.** Direito e Internet. Texto: Eficácia Probatória dos Contratos celebrados pela Internet. Coordenadores: Newton de Lucca e Adalberto Simão Filho. Editora Edipro. 1.º edição. 2000. Bauru – SP. Pág. 273/274

[88] **- BLUM. Renato M. S. Opice.** Direito eletrônico. A Internet e os tribunais. Texto: O processo eletrônico: assinaturas, provas, documentos e instrumentos digitais. Coordenador: Renato M. S. Opice Blum. Editora Edipro. 1.º edição. 2001. Pág. 56.

Hoje, no Brasil, a Medida Provisória n.º 2.200-2/01 vem reforçar aquilo que a lei intrinsecamente reconhece: equipara o documento eletrônico ao documento convencional ou autógrafo relacionado em nosso Direito Brasileiro, desde que o mesmo apresente os requisitos relacionados com a assinatura digital descritos na MP 2.200-2/01.

Na corrida pela evolução social, pequenas disparidades não devem ser encaradas como obstáculos intransponíveis ao desenvolvimento. O acúmulo de material corpóreo com finalidade de assegurar a prova futura de fatos passados, consubstancia tantos problemas quanto a realidade telemática que a nós é proposta neste início de século. A milenar cultura concretualista deve ceder diante das novas perspectivas tecnológicas, e o ser humano deve buscar aperfeiçoar o uso dos documentos eletrônicos em contrapartida a sua simples negação em decorrência de sua crônica ignorância.

5 A ASSINATURA DIGITAL

No presente capitulo, analisaremos os aspectos legais que levam uma assinatura ser aceita como instrumento judicial caracterizador de direitos e obrigações no ordenamento jurídico brasileiro.

Apoiado nestas considerações, vamos caracterizar o processo de produção de uma assinatura digital, apontando para a finalidade de assegurar a autenticidade e a integridade aos documentos eletrônicos por meio do instrumento chamado de “assinatura digital”.

Faremos um paralelo entre a assinatura digital e a assinatura manuscrita, dando destaque às principais diferenças e correlações entre ambas.

Por fim, realizaremos um estudo da criptografia assimétrica, tendo em vista, ser reconhecida como a técnica utilizada nos processos de assinatura digital, objetivando obter o fim almejado de segurança na integridade e autenticidade dos documentos.

5.1 A assinatura digital e seus aspectos técnico-jurídicos

Consoante verificamos no capítulo antecedente, o primado da razoável admissibilidade da assinatura digital, em relações jurídicas, como elemento equivalente da assinatura autógrafa que encontra fundamento nas condições que o instrumento digital possui de identificar o autor do documento eletrônico e manter a integridade das informações, com níveis de segurança equiparados à assinatura tradicional.

5.1.1 Conceito

Podemos entender por assinatura digital (Blum, 2001) o sistema de segurança, utilizando a matemática aplicada por meio da criptografia, fixada ao documento eletrônico ou existente em arquivo independente, sendo considerada inválida diante da menor modificação sofrida após a geração da assinatura digital

por meio da chave privada do signatário, visando proporcionar a força probante do documento eletrônico.[89]

A primeira lei no mundo a regularizar legalmente o uso das assinaturas digitais é proveniente do estado de Utah, nos Estados Unidos da América do Norte. A supra citada legislação era considerada demasiadamente longa, tendo entrado em vigor em 1.995.

Conforme explana Bruno (2004, 1ª. Parte)

> *"Utah Digital Signature Act (Lei de Assinatura Digital do Estado de Utah), foi à primeira iniciativa de natureza legislativa, em 09 de março de 1995, destinada a viabilizar a autenticação segura de documentos eletrônicos, de sorte a incentivar a utilização segura das assinaturas digitais, facilitando e viabilizando a prática do e-commerce, seguindo o sistema de criptografia de documentos."*[90]

No Brasil, o primeiro ato normativo destinado à regulamentação e uso dos documentos eletrônicos e assinaturas digitais foi representado pela Instrução Normativa n.º 17, de 11 de dezembro de 1.996, editada pelo Ministério da Administração Federal e Reforma do Estado, onde fixava um prazo de 360 dias para serem implementadas aplicações que tratassem da utilização de documentos eletrônicos.

A última aplicação normativa brasileira sobre a regulamentação e uso dos documentos eletrônicos e assinatura digital é a Medida Provisória 2.200-2 de 24 de Agosto de 2.001, que é analisada durante o presente trabalho.

5.1.2 Aspectos técnicos

Com o uso das chaves pública e privada baseadas em operações matemáticas, a assinatura digital resgata um alto índice de confiabilidade,

---

[89] - **BLUM. Renato M. S. Opice.** Direito eletrônico. A Internet e os tribunais. Texto: O processo eletrônico: assinaturas, provas, documentos e instrumentos digitais. Coordenador: Renato M. S. Opice Blum. Editora Edipro. 1.º edição. 2001. Pág. 24.

[90] - **BRUNO. Gilberto Marques.** In O comerciante virtual e a tendência mundial de uniformização da legislação – II. Disponível em: http://www.direitonaweb.com.br/colunista.asp?l=gilberto&ctd=412 , acessado em 21 de abril de 2.004.

equiparando-se ontologicamente às assinaturas autógrafas quando conferidas ao documento manuscrito.

A integridade da assinatura digital é assegurada, dessa forma, pela tecnologia criptográfica. O liame, por sua vez, entre o signatário e a chave pública é obtido por meio do certificado digital. Dessa forma, temos que os dois primeiros requisitos para a realização de uma assinatura digital, no âmbito de uma Infra-estrutura de Chaves Públicas é possuir um par de chaves assimétricos e um certificado digital.

Um outro requisito que pode ser levado é a existência um software de assinatura digital. A característica peculiar que deve ser exigida do software consiste na capacidade de realizar operações criptográficas de assinatura digital e verificação de assinatura digital.

Dessa forma, com os referidos requisitos presentes, o signatário que estiver diante de um arquivo eletrônico (imagem, vídeo, texto, etc.) poderá perfeitamente realizar uma assinatura eletrônica.

A geração técnica da assinatura ocorre em dois ciclos, seguindo os seguintes passos:

- 1° ciclo: De posse de um arquivo eletrônico, o usuário gera um bloco *hash*. Para a geração deste bloco é necessário a utilização de um algoritmo criptográfico de função *hash* como MD2, MD4, MD5, SHA1 entre outros. O Bloco *hash* consiste num valor seqüencial de bits com tamanho fixo obtido a partir da mensagem original. Ocorrendo a mudança de um único bit que seja da mensagem original, o valor seqüencial de bits que se obterá será totalmente diverso daquele gerado anteriormente à modificação do arquivo;
- 2.º ciclo: A assinatura digital propriamente dita é engendrada, quando o bloco *hash* originalmente gerado a partir da mensagem é criptografado utilizando-se a chave privada do signatário. Os mais comuns são RSA (baseado na teoria dos números), DSA (baseado na teoria dos logaritmos discretos) e o ECDSA (baseado na teoria das curvas elípticas);

O documento eletrônico assinado digitalmente é formado pelo arquivo eletrônico e a assinatura digital, que juntos ou separadamente, seguem o seu caminho para seu destinatário.

Esta emissão poderá ser feita com a utilização de um “invólucro de documento e assinatura”. Em verdade, este artefato pode ser encarado como um envelope, onde ficam depositados os elementos eletrônicos para a emissão.

Conforme a necessidade, o invólucro poderá conter o bloco de assinatura, o certificado digital, a lista de certificados revogados e o documento eletrônico que foi assinado, ou poderá ser composto com a exclusão do documento eletrônico que foi assinado.

Hoje o formato mais comumente utilizado para o encapsulamento de documentos eletrônicos e assinaturas digitais é o PKCS#7 (FERNANDES. 2006)[91]. A mais nova versão utilizada deste formato corresponde ao CMS3 (*Cryptografic Message Syntax version 3)* (HOUSLEY, 2004). A descrição deste formatoé realizado através da linguagem *Abstract Syntax Notation 1* (ASN.1) e codificados em *Distinguished Encoding Rules* DER (ITU-T, 2002).

Este formato permite que elementos de segurança sejam inseridos nos envólucros, como carimbo de tempo e contra-assinaturas. Além disso, permite a inserção de certificados e listas de certificados revogados, permitindo que estejam presentes num mesmo local todos os elementos necessários para a verificação da assinatura.

Vale ressaltar que a formatação PKCS#7/CMS (FERNANDES. 2006)[92] aceita qualquer seqüência de bits como conteúdo, sem restringir qualquer tipo de formatação de documento. Não coloca, portanto, limitações quanto ao tipo de informações que podem estar contidas no documento.

Ao receber o arquivo assinado digitalmente, contido ou não no formato PKCS#7/CMS, o destinatário deverá observar os seguintes passos a fim de verificar a autoria e a integridade do arquivo:

- De início, o destinatário deverá obter a chave pública do signatário de uma forma confiável. Num contexto de Infra-estrutura de Chaves Públicas, conforme visto no presente trabalho, essa chave é extraída do certificado digital do signatário;

---

91 **- FERNANDES, Murilo Rivau**. SIPEX: Uma proposta de modelo de política de assinatura. 100p. (Dissertação de Mestrado). Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos. São Paulo. 2006. Pág. 53.

92 **- FERNANDES, Murilo Rivau.** SIPEX: Uma proposta de modelo de política de assinatura. 100p. (Dissertação de Mestrado). Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos. São Paulo. 2006. Pág. 53.

- Realizada referida tarefa, o destinatário promoverá a geração de um bloco *hash*. Este novo bloco *hash* gerado é denominado de "*hash corrente".* Esta geração ocorre somente sobre o arquivo original recebido, excluindo-se a assinatura digital. Para tanto, o destinatário deverá utilizar-se do mesmo algoritmo de *hash* utilizado pelo signatário quando da geração da assinatura;
- Em seguida, o destinatário decifrará a assinatura digital utilizando a chave pública certificada. O resultado obtido corresponderá ao bloco *hash* gerado pelo signatário quando da produção da assinatura;
- Como última ação de verificação realizada pelo destinatário, haverá a comparação entre os blocos *hashs* anteriormente citados. Ocorrendo a igualdade entre ambos, o destinatário terá a certeza de que a assinatura digital é válida e foi gerada pela chave privada correspondente a chave pública certificada, utilizada por ele na operação de verificação. Como resultado, terá assegurada a autenticidade e integridade da mensagem.

Vários são os fatores que podem determinar a invalidade de uma assinatura digital. Podemos ter que o instrumento eletrônico assinado digitalmente ou o arquivo contendo a assinatura digital sofra uma alteração por agentes maliciosos antes de atingir seu destino. Os agentes, com o intuito de praticar algum delito ou ilícito civil, modificam os dados dessas caixas de informações para preencher interesses próprios.

As caixas de informações adulteradas não atingirão seus objetivos, ao passo que o destinatário final identificará a alteração maliciosa no momento de conferir a assinatura digital utilizando-se da chave pública certificada de propriedade do signatário.

Ilustrando as referidas colocações técnicas, suponhamos que o professor "A", ao corrigir o trabalho final de seu aluno "B", resolva por bem, parabenizá-lo por ter atingido seu objetivo. O Professor "A" escreve um texto eletrônico original com a seguinte mensagem: "Seu trabalho estava ótimo". Gera o bloco *hash* original da mensagem e o criptografa (assinatura digital), utilizando sua respectiva chave privada. Após, envia a mensagem e a assinatura digital conjuntamente à secretaria do curso a fim de ser entregue a seu destinatário.

Uma vez a mensagem estando presente no suporte técnico da secretaria, um funcionário "C", com intuito malicioso, insere modificações no texto

original, dispondo a mensagem da seguinte forma: “Seu trabalho estava péssimo”. Após a modificação, a mensagem é enviada ao seu destinatário via Internet.

Ao receber a mensagem eletrônica, o aluno “B” iniciará o processo de verificação do texto assinado digitalmente pelo seu professor “A”. O aluno “B”, gerará um novo bloco *hash* corrente. Na seqüência, o aluno “B” obterá a chave pública certificada, atribuída ao professor “A”. Com a chave pública, o aluno “B” realizará a decifração da assinatura digital. Com isso, será obtido o bloco *hash* original gerado com a produção da assinatura digital pelo professor “A”. Comparando o bloco *hash* corrente com o bloco *hash* original, o aluno “B” terá plenas condições de verificar a autenticidade e a integridade do documento recebido.

Realizado o referido processo, o aluno “B” constatará que os *hashs* denominados original e corrente não são iguais, indicando que os requisitos estruturais foram violados em face de terem ocorrido modificações posteriores ao encerramento da mensagem por seu autor original chamado de “A”.

Dessa forma, podemos constatar que a utilização das assinaturas digitais não livra as relações humanas dos delitos e ilícitos em razão das explanações acima esboçadas, pois há a possibilidade de um indivíduo realizar alterações maliciosas em documentos eletrônicos, entretanto, sua alteração será detectada.

A falsidade documental não surgiu com o advento da era eletrônica, vindo desde os primórdios da era documental, e em nossos dias, pessoas fazem-se passar por outras para a obtenção de carteiras de identidade, Carteira Nacional de Habilitação, abertura de Contas Correntes, entre outras.

Dessa forma, temos que a grande maioria das fraudes inerentes aos documentos eletrônicos existem em virtude do documento autógrafo, sendo traspassado aos documentos eletrônicos por meio de adaptações, não surgindo da conduta com o novo instrumento tecnológico, vez que é apenas mais um meio disponível para a prática de ilícitos.

5.1.3 O certificado digital e a força probante das assinaturas digitais

A assinatura digital representa a condição essencial para a força probante do documento eletrônico, conforme estipula a norma processual legal, exigindo a plena correspondência dos requisitos da autoria e da integridade.

Conforme expõe Marcacini (2003), um simples e-mail não poderá guardar a força probante dada ao documento eletrônico, caso não apresente uma assinatura digital, pois pode ser facilmente modificado sem deixar vestígios[93].

Blum (2001, p.51), compartilhando da opinião sobre a necessidade de assinatura digital junto ao documento eletrônico com o fim de conferir-lhe força probante, expõe:

> *"Reforçamos o entendimento que para a equiparação do documento eletrônico ao documento físico escrito e assinado (art. 368, CPC), tal deve estar certificado digitalmente por meio da criptografia assimétrica, pois, caso contrário, teríamos um contrato cuja forma se assemelha à forma verbal (ou, mais próximos ainda, do contrato verbal firmado por telefone, em que os contratantes sequer se põem face a face."*[94]

> *"A assinatura digital, por chaves públicas, oferece um elevado nível de segurança, proporcionando uma presunção muito forte de que o documento onde se encontra foi criado pela pessoa que dela é titular e, assim, satisfaz o objetivo do legislador na exigência de assinatura para atribuição de valor probatório aos documentos escritos."*[95]

A assinatura digital representa o meio tecnologicamente hábil a assegurar a autoria e a integridade dos documentos eletrônicos, permitindo que os diplomas eletrônicos tenham força jurídica diante da sociedade.

---

93 - MARCACINI. Augusto Tavares Rosa. In Certificação eletrônica, sem mitos nem mistérios. Revista do Advogado. Internet. Associação dos Advogados de São Paulo. Ano XXIII, n.º 69. Maio/2003. Pág 108 e 109.

94 - BLUM. Renato M. S. Opice. Direito eletrônico. A Internet e os tribunais. Texto: O processo eletrônico: assinaturas, provas, documentos e instrumentos digitais. Coordenador: Renato M. S. Opice Blum. Editora Edipro. 1.º edição. 2001. Pág. 58.

95 - BLUM. Renato M. S. Opice. Direito eletrônico. A Internet e os tribunais. Texto: O processo eletrônico: assinaturas, provas, documentos e instrumentos digitais. Coordenador: Renato M. S. Opice Blum. Editora Edipro. 1.º edição. 2001. Pág. 51.

É justamente nesta análise da força probante que a assinatura digital confere ao documento eletrônico, que surge a importância do certificado digital no contexto jurídico.

Consoante verificamos ao longo de todo o trabalho, num primeiro momento o certificado digital corresponde ao documento eletrônico responsável por assegurar o vínculo legal entre a chave pública e o signatário, identificando este signatário de forma segura e individualizada.

Ao se analisar a validade legal e técnica de um certificado digital, no momento de verificação da assinatura digital, o destinatário deverá observar algumas regras.

A primeira delas diz respeito a finalidade sobre o qual o par de chaves foi gerado. A presente informação pode ser obtida no próprio certificado, na extensão *Digital Signature*, especificado no campo *Key usage* do certificado.

A segunda regra corresponde a verificação do prazo de validade do certificado, ou seja, verificar se o certificado não esteja revogado. A revogação poderá ocorrer tanto pelo decurso do prazo de validade do certificado, como por expressa vontade de seu proprietário.

Por fim, verificar se as normas técnicas referentes à emissão e distribuição de certificados digitais pelas Autoridades Certificadoras foram obedecidas.

5.2 A criptografia assimétrica

A criptografia, assimétrica é uma das técnicas utilizadas pela assinatura digital, a fim de resguardar sua confiabilidade. A criptografia é considerada a arte milenar de encriptar informações de forma que somente o remetente e o destinatário tenham acesso ao seu conteúdo, em virtude de conhecer ou possuir o sistema de decifração.

Etimologicamente, a palavra criptografia significa a arte de ocultar a escrita.

Dessa forma, podemos conceituar tecnicamente a criptografia utilizando as palavras de Lucena (2001, versão 3) da seguinte forma:

> *"Una de las mejores definiciones que he encontrado para la palabra criptografía, viene a decir que es el conjunto de técnicas que permiten transformar un trozo de información, de tal forma que quienes deseen recuperarlo sin estar en posesión de otra pieza de información (clave), se enfrentarán a un problema intratable."*[96]

Conforme pondera Costa (2002, p. 23), a técnica da criptografia que primeiro teve sucesso entre a sociedade mundial é conhecida como cifra de César, por ter sido sistematizada pelo imperador romano Júlio César:

> *"Exemplo tradicional é o de Júlio César, que codificava as mensagens que enviava aos seus comandados, atribuindo a cada letra, a sua correspondente três casas acima, na ordem alfabética."*[97]

Exemplificando a cifra de César, tomemos como exemplo a frase: "Ataque a meia-noite". Aplicando o sistema criptográfico desenvolvido por Júlio César teremos a seguinte expressão: "DXDTZH D PHMD-QRMXH."

O primeiro trabalho publicado tratando sobre o tema da criptografia ocorreu no ano de 1.510, por um abade alemão chamado Johannes Trithemius, sendo considerado hoje como o pai da criptografia moderna.

Conforme observa Marcacini (2003, p. 11), a ciência criptográfica teve grande valia na segunda guerra mundial:

> *"Os alemães cifravam suas mensagens por meio de uma máquina eletro-mecânica, conhecida por Enigma. Considerado o mais sofisticado engenho da codificação até então inventado', o apetrecho foi um dos fatores que sustentaram as vantagens militares nazistas ao início do conflito e, a julgar pelo número de softwares de*

---

96 - ROSA, José Manuel Lucena. Comercio electrónico. Seminario Escuela Superior de Cajas de Ahorros, 1.997, 24 y 25 Octubre. MADRID.1997**.**

97 - COSTA, Marcos da. In *"A ICP-Brasil e os documentos eletrônicos."* Caderno Jurídico da Escola Superior do Ministério Público de São Paulo. Direito e Internet. Ano II – n.º IV – Julho de 2002. Pág. 23.

simulação encontrados pela Internet afora, a Enigma ainda povoa o imaginário dos interessados pela criptografia."[98]

Os primeiros passos dos elementos informadores do sistema de criptografia assimétrico, hoje, utilizado nas operações de assinatura digital foram proferidos em 1.976, pelos matemáticos Whitfield Diffie e Martin Hellmam.

Neste ano, o algoritmo Diffie-Hellmam, batizado com este nome em homenagem aos criadores, mostrou o caminho para a definição do primeiro algoritmo de criptografia assimétrico.

Os criadores, por meio de texto intitulado "New directions in cryptography", mostraram ao mundo a possibilidade de cifrar e decifrar sem a necessidade de usar a mesma chave.

Um ano depois, em 1.977, três outros matemáticos, Rivest, Shamir e Adleman, conseguiram aperfeiçoar o algoritmo Diffie-Hellmam, possibilitando não apenas a cifração pela chave pública e decifração pela chave privada, sendo possível também a cifração com a chave privada e a decifração com a chave pública. Esta nova aplicação do algoritmo Diffie-Hellmam ficou conhecido pelas iniciais dos nomes dos três matemáticos – RSA.

Nos dias de hoje, a técnica criptográfica está presente em nosso dia-a-dia, e muitos não se dão conta deste uso. Em operações de *home banking*, transações eletrônicas por meio de cartões de crédito, *Webmail*, entre outros serviços, usufruem da criptografia para tentar manter a segurança de seus dados.

Muitos opositores ao desenvolvimento das técnicas referentes à criptografia assimétrica sustentam que o sistema assimétrico criptográfico adotado para a assinatura digital representa grande perigo à comunidade mundial, conferindo oportunidade às quadrilhas e grupos terroristas, e ao crime organizado em geral, de manterem contato pelo mundo sem sofrer qualquer perturbação.

Com a devida vênia, os benefícios produzidos pela assinatura digital são maiores que os malefícios apontados. A criptografia assimétrica, se de um lado serve aos vários grupos que praticam ilícitos, de outro serve também para os órgãos de repressão ao crime, que também podem trocar informações de forma sigilosa.

---

98 - MARCACINI. Augusto Tavares Rosa. In Certificação eletrônica, sem mitos nem mistérios. Revista do Advogado. Internet. Associação dos Advogados de São Paulo. Ano XXIII, n.º 69. Maio/2003. Pág 11.

Verificamos dessa forma, que os opositores da sistemática da assinatura digital com uso de criptográfica assimétrica não possuem razão em suas argumentações, e seus discursos representam puro retrocesso para o avanço tecnológico, social e mundial, já que em todos os institutos há mais ou menos possibilidade de produzir benefícios ou malefícios.

Diante de todo o exposto, concluímos o presente capítulo reconhecendo que as assinaturas digitais não encontram barreiras legais no ordenamento jurídico brasileiro, a fim de serem reconhecidas. O fundamental para tal reconhecimento encontra-se na própria técnica desenvolvida por meio da criptografia, conferindo a segurança necessária equivalente exigida das assinaturas autógrafas.

6 CERTIFICADO DIGITAL

No presente capítulo serão analisadas as questões jurídicas e suas conseqüências técnicas que envolvem o certificado digital e a atividade de certificação digital.

Para iniciarmos uma análise crítica a respeito da atividade de certificação digital, o primeiro ponto a ser encarado refere-se a seu aspecto funcional, diante das regras de força probante dos documentos em geral.

A prestação de quaisquer serviço público deve respeitar as regras de competência fixadas na Carta Magna.

Neste passo, abre-se a discussão sobre a competência material constitucional do Governo Federal, que por meio da Casa Civil da Presidência da República, vem desenvolvendo a atividade de certificação digital no Brasil pela ICP-Brasil.

Em suma, podemos destacar como alvos do presente capítulo, a fixação do objetivo e da natureza jurídica da certificação digital, e a observação das regras de competência material previstas na CF para a atividade relacionada à força probante dos documentos. Com isso, será possível o exame da constitucionalidade da MP 2.200-2/01, listando os requisitos legais mínimos que devem ser observados quando da propositura de uma ICP-Brasil.

6.1 Considerações

Assegurar a integridade do documento eletrônico, a criptografia consegue suportar. Entretanto, havia ainda a necessidade de um elo de confiança, chamado de autenticidade, existente em documentos com força probante.

Esse nexo de confiança, na atualidade, é proporcionado por um documento público denominado “certificado digital”. No Brasil, consoante determina a MP 2.200-2/01, a atividade de certificação digital pode ser desenvolvida como uma atividade tipicamente pública, por meio da ICP-Brasil, assim como uma atividade privada, com fundamento jurídico no artigo 10, par. 2.º da MP 2.200-2/01.

O ato administrativo[99] de emissão do certificado digital é realizado pelo Poder Executivo Federal, sob o comando da casa civil da Presidência da República, objetivando, entre outras funções, assegurar a autenticidade dos documentos eletrônicos que forem assinados digitalmente.

A ICP-Brasil, conjunto de regras e procedimentos técnicos, é responsável pela atividade de certificação digital no Brasil. Possui como órgão administrativo a Autoridade Certificadora Raiz – AC-Raiz – que hoje é incorporada por uma Autarquia Federal (o ITI), considerada Pessoa Jurídica de Direito Público Interno, e a emissão do certificado digital para o usuário final ocorre por meio de prévia habilitação conferida pelo ITI às Pessoas Jurídicas de Direito Público ou Privado – denominadas de Autoridades Certificadoras Subseqüentes (AC Sub) – e às Pessoas jurídicas de Direito Público ou Privado denominadas de Autoridades de Registro – AR.[100]

O certificado digital surgiu exclusivamente para completar a lacuna encontrada na tecnologia das assinaturas digitais. O uso da criptografia assimétrica, em si, assegura a integridade dos dados eletrônicos, entretanto, para assegurar força probante documental a esses dados, era preciso assegurar também a autenticidade. Para tanto, surgiu o certificado digital, completando os requisitos exigidos pelas normas legais para conferir aos dados eletrônicos a garantia documental.

De acordo com o Instituto Nacional de Tecnologia de Informação, Autoridade Certificadora Raiz na ICP-Brasil:

> *"O certificado digital é um documento eletrônico, assinado digitalmente por uma terceira parte confiável, que associa uma entidade (pessoa, processo ou servidor) a uma chave pública.*
>
> *.Na prática, o certificado digital funciona como uma carteira de identidade virtual, que permite a*

---

99 **-** *"Ato administrativo é toda manifestação unilateral de vontade da Administração Pública que, agindo nessa qualidade, tenha por fim imediato adquirir, resguardar, transferir, modificar, extinguir e declarar direitos, ou impor obrigações aos administrados ou a si própria."* **MEIRELLES. Hely Lopes.** Direito Administrativo Brasileiro. 24ª. edição. São Paulo. 1999. Editora Malheiros. Pág. 132.

100 **-** Conforme vimos acima, a Autoridade Certificadora Raiz – ITI – não emite certificados a usuários finais, mas tão somente às Autoridades Certificadoras Subseqüentes.

identificação segura de uma mensagem ou transação em rede de computadores."[101]

Por sua vez, a lei modelo da UNCITRAL define certificado "como uma mensagem ou outro registro de dados confirmando o vínculo entre um signatário e dados da criação da assinatura".[102]

Segundo a Associação dos Advogados Americana, o certificado digital "é um registro eletrônico, gerado por uma autoridade certificadora, contendo (entre outros) o nome do titular do certificado de uma chave pública e outras informações indicadas."

6.2 Objetivo do certificado

Quando se fala em objetivos dentro da seara jurídica, deve-se entendê-los como o fim ou alvo que se pretende atingir legalmente através do instituto em questão.

Com isso, para melhor compreender a natureza jurídica da certificação digital, devemos antes entender, sob o aspecto funcional, qual o objetivo legal perseguido, levando-se em consideração a previsão normativa da M.P. 2.200-2/01.

Como todo ato jurídico, o documento tem por objetivo, tanto no que diz respeito aos documentos públicos como os documentos privados, à demonstração incontroversa de fato pretérito que cria, altera, modifica ou extingue relações jurídicas.

No caso do certificado digital, enquanto documento, a Resolução n.º 7, de 12 de Dezembro de 2001, do Comitê Gestor da ICP-Brasil, dispõe que são oito os tipos de certificados inicialmente previstos para os usuários finais da ICP-Brasil. Esta classificação é dividida em duas grandes categorias, levando-se em consideração a funcionalidade dos certificados: 1. Certificados de Assinatura Digital; 2. Certificados de Sigilo.

---

101 - Disponível em http://www.iti.br/ , acessado em 09 de Novembro de 2005.

102 - UNCITRAL. Electronic Signatures Draft Guide to Enactment of the UNCITRAL. Model Law on Electronic Signatures. Thirty-eighth session, New York, março de 2001.

Os certificados de sigilo são utilizados em aplicações do tipo cifração de documentos, base de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu segredo.

Em razão desta espécie de certificado não representar o escopo do presente trabalho, nos restringimos a realizar apenas a simples menção acima.

Os certificados digitais aplicados para a assinatura digital são de quatro tipos: A1; A2; A3; e A4, de acordo com o grau crescente de segurança disponibilizado. O certificado digital para assinatura tem por objetivo principal vincular o proprietário/signatário à chave pública assegurando a autenticidade aos documentos eletrônicos assinados digitalmente a partir da correspondente chave privada. A certificação digital, nesta órbita, é uma atividade ligada à força probante dos documentos eletrônicos.

A identificação do tipo de certificado ocorre pela análise do campo *"key usage"* existente em cada documento digital certificatório. Qualquer pessoa será capaz de examinar qual a aplicação do certificado, como nos casos destinados às assinaturas digitais.

O certificado com aplicação em assinaturas digitais assume uma posição de confiança na autenticidade (condição relacionada a força probante) do documento eletrônico por meio da assinatura digital. Pode-se dizer, com isso, que a finalidade consiste em assegurar a autenticidade dos documentos eletrônicos assinados digitalmente, por meio da vinculação entre o signatário e sua chave pública. Vale lembrar que esta vinculação feita pelo certificado possui as características de legitimidade em razão de seu caráter público.

Neste passo, Marcacini (2003)[103], em publicação na Revista do Advogado, da Associação dos Advogados de São Paulo – AASP, coloca que o certificado digital nada mais é que um documento eletrônico assinado digitalmente, responsável por atribuir a titularidade de uma chave pública.

Com isso, identificamos o objetivo imediato dos certificados digitais de aplicação em assinaturas, qual seja, (a) vinculação do signatário à chave pública utilizada para conferir a assinatura digital (b) conferindo autenticidade aos documentos eletrônicos assinados digitalmente. A seguir, será realizada a analise da

---

[103] - **MARCACINI. Augusto Tavares Rosa**. "Certificação eletrônica, sem mitos e sem mistérios". Revista do Advogado. "Internet". Publicada pela Associação dos Advogados de São Paulo. Ano XXIII, n.º 69. Maio de 2003. Pág. 112.

natureza jurídica que se pode alcançar sobre a certificação digital levando em consideração seu objetivo.

6.3 Natureza jurídica

A natureza jurídica da atividade de certificação digital aplicada à assinatura digital dependerá do entendimento dado à lei referente à atividade de certificação digital.

Existem duas interpretações importantes para esta natureza: quando o documento eletrônico detiver presunção de legitimidade ou quando o documento eletrônico não detiver presunção de legitimidade.

Por legitimidade devemos entender aquilo que detém a qualidade de legal ou que possui legalidade. É a qualidade do documento legal ou que está conforme as formalidades prescritas em lei.

Quando analisamos um documento, vários são os aspectos atingidos pela verificação da legitimidade. Entre eles podemos citar os requisitos de validade de um negócio jurídico (art. 104 do Código Civil) e a autoria do documento.

Diante de certas condições impostas pela norma legal ocorrerá a presunção de legitimidade de alguns ou de todos os aspectos do documento. Nesta órbita, a concepção da presunção é encarada como suposição da legitimidade, ou seja, todos os aspectos de legitimidade do documento devem ser acreditados pelo receptor sem a concreta conferência junto ao responsável pela sua emissão.

Como a legitimidade de um documento, em tese, sempre pode ser questionada judicialmente, o real efeito da presunção de legitimidade corresponde à inversão do ônus da prova, uma vez que a qualidade de presunção de legitimidade não exclui a verificação dos aspectos desta mesma legitimidade junto ao Poder Judiciário.

Para melhor elucidar a questão, tomemos como exemplo a escritura pública. Sua confecção é responsabilidade do Tabelionato de Notas, dessa forma todos os seus aspectos legais possuem presunção de legitimidade, e devem ser acreditados independentemente do receptor dirigir-se ao Tabelionato para conferir sua validade.

Seguindo nos exemplos, tomemos agora o reconhecimento de firma, que embora obrigue ao Tabelião a verificação dos requisitos de validade do negócio jurídico (artigo 104 do Código Civil), não o obriga a verificar o conteúdo desse documento. Nesta hipótese, conforme bem afirma Resende[104] (2006) "*o reconhecimento somente certifica a assinatura".* Com isso, a presunção de legitimidade atinge somente o aspecto ligado a assinatura do documento, como por exemplo a autoria ou a aceitação de seu conteúdo pelo signatário, mas nunca a validade ou veracidade do conteúdo do documento.

Conduzindo essas idéias para os documentos eletrônicos temos que o objetivo do certificado digital de assinatura digital consiste em assegurar a titularidade da chave pública possibilitando conferir a autoria dos documentos eletrônicos assinados digitalmente.

Partindo deste ponto, devemos entender que o certificado digital para assinatura digital desempenha seu papel na seara da força probante dos documentos eletrônicos asseverando[105] sua autoria. A chave pública é o elemento utilizado para a verificação da regularidade do documento eletrônico assinado digitalmente. O certificado digital para assinatura digital vincula a chave pública ao signatário. Em suma, o certificado digital une uma determinada pessoa à sua assinatura digital, e esta assevera a autoria dos documentos eletrônicos no qual é aposta.

Diante disso, podemos concluir que o conceito de certificado digital de assinatura digital corresponde a um documento eletrônico assinado digitalmente por agente competente, que desempenha uma função de possibilitar asseverar a autoria de outros documentos eletrônicos assinados digitalmente por meio da vinculação entre o proprietário do certificado e sua respectiva chave pública (utilizada para conferir a regularidade da assinatura digital), identificando e individualizando este mesmo proprietário diante dos seus pares no mundo eletrônico.

---

[104] - REZENDE, Afonso Celso F. Tabelionato de Notas e o notário perfeito. 4ª. Edição. Editora Millennium. Campinas (SP). 2006. Pág. 91

[105] - Neste contexto, o verbo asseverar deve ser entendido como "afirmar", "assegurar" ou "confirmar", mas sem presunção de legitimidade.

6.3.1 Documento eletrônico com presunção de legitimidade

De acordo com o artigo 10, parágrafo 1.º da MP 2.200-2/01, 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".*

Com fundamento na regra legal supra citada, foi estabelecida a idéia de que o certificado digital de assinatura digital atesta com presunção de legitimidade a autoria do documento eletrônico assinado digitalmente. Levando em consideração o quadro exposto, devemos averiguar junto às normas constitucionais, quem possui competência material para o desenvolvimento da atividade de certificação digital quando confere presunção de legitimidade quanto a autoria do documento eletrônico.

Utilizando-se de um aspecto formal para discutir o papel jurídico do certificado digital, Menke (2005)[106] aponta que o certificado digital, "*embora possibilite com razoável segurança agregar os atributos de autoria"*, aos documentos eletrônicos assinados digitalmente, não poderá ser equiparado ao reconhecimento de firma uma vez que "*não autentica quaisquer fatos e nem formaliza a vontade das partes"*. Acrescenta ainda que a grande diferença entre a atividade de certificação e a reconhecimento de firma reside no fato de que a AC não intervém em cada assinatura digital realizada ao passo que o Tabelião deverá sempre intervir quando reconhece a firma.

Com razão, a certificação digital quando confere presunção de legitimidade de autoria em relação ao documento eletrônico não deve ser encarada como um reconhecimento de firma.

Com o desígnio de aclarar as idéias colocadas pelo citado autor, devemos notar que quando o notário produz o reconhecimento de firma, deve anteriormente, aferir o documento, através de sua leitura, confrontando-o com as regras de validade do negócio jurídico presentes no artigo 104 do Código Civil Brasileiro. Quem bem explica esta colocação é Rezende (2006):[107]

---

[106] - MENKE, Fabiano. Assinatura Eletrônica no Direito Brasileiro. Editora RT. São Paulo. 2005. Pág. 115.

[107] - REZENDE, Afonso Celso F. Tabelionato de Notas e o notário perfeito. 4ª. Edição. Editora Millennium. Campinas (SP). 2006. Pág. 93.

> *"O reconhecimento de firma, qualquer que seja o documento, estabelece uma autenticidade ao mesmo e, para que isto possa acontecer, necessário que o agente seja capaz, a forma esteja determinada e não proibida por lei e o objeto absolutamente permitido. Desta maneira, anteriormente ao reconhecimento de firma, o notário deve proceder a leitura do documento que lhe é apresentado, verificando se pode ser firmado pelos participantes, se o objeto é lícito e que se encontra dentro das formas dos atos jurídicos prescritos legalmente.*

Todavia, como se verá adiante, esta ordem não deve ser entendida em relação ao conteúdo do documento. O reconhecimento de firma certifica somente a assinatura e não o conteúdo narrado no diploma. Dessa forma, sob o sentido funcional do reconhecimento de firma realizado pelos Tabelionatos, preciosa é a lição de Rezende (2006):[108]

> *"O reconhecimento de firma em um documento particular declara, por escrito, que uma determinada assinatura foi levada a efeito por determinada pessoa, ou que confere com a assinatura depositada anteriormente nos arquivos do Tabelionato. O reconhecimento somente certifica a assinatura,* ***e em nenhum momento faz certificação do conteúdo apresentado pelo documento em que a mesma se encontra*** *(grifo nosso)."*

Embora o certificado digital, quando confere presunção de legitimidade quanto a autoria do documento eletrônico, não deva ser encarado como um reconhecimento de firma, pelas razões expostas, o mesmo não podemos dizer em relação ao gênero dos serviços notariais.

Consoante disserta Antunes[109] (2005) a função do serviço notarial "*visa garantir a publicidade,* ***autenticidade****, segurança e eficácia dos atos jurídicos preventivamente, desobstruindo o Judiciário do acúmulo de processos instaurados no intuito de restabelecer a Ordem Jurídica do país, e atuando como instrumento de pacificação social"(*grifo nosso*).*

---

[108] **- REZENDE, Afonso Celso F.** Tabelionato de Notas e o notário perfeito. 4ª. Edição. Editora Millennium. Campinas (SP). 2006. Pág. 91

[109] **- ANTUNES, Luciane Rodrigues.** Introdução ao Direito Notarial e Registral. Jus Navegandi, Teresina, ano 9, n. 691, 27 maio 2005. Disponível em: **http://jus2.uol.com.br/doutrina/texto.asp?id=6765** . Acesso em 11 de Dezembro de 2006.

O reconhecimento de firma é a espécie que o legislador infraconstitucional (Provimento 85/98 da Corregedoria Geral do Estado de São Paulo) encontrou para instrumentalizar a competência privativa dos Tabelionatos quanto ao gênero dos serviços notariais fixada no artigo 236 da Constituição Federal.

O certificado digital quando conferir presunção de legitimidade em relação a autoria do documento deve ser encarado mais como um serviço notarial e menos como um simples reconhecimento de firma.

Na explanação, tem-se que o certificado digital, quando conferir aos documentos eletrônicos presunção de legitimidade em relação à autoria, desempenha a mesma função ontologicamente desempenhada nos serviços notariais, qual seja, a presunção legal conferida aos documentos por terceiro garantidor de autoria, por meio da utilização de assinaturas.

Diante de todo o exposto na presente seção, sob o aspecto funcional, conclui-se que o certificado digital quando conferir presunção de legitimidade quanto a autoria do documento eletrônico possui natureza jurídica de serviço notarial, e como expressamente determina o artigo 236 da Constituição Federal, o serviço notarial será exercido em caráter privado pelos Tabelionatos.

Os principais opositores desta ordem alegam que nem todo documento necessitará de presunção de legitimidade quanto a autoria do documento a fim de vincular as partes envolvidas, condição que desqualificaria a natureza jurídica de serviço notarial ao certificado digital quando confere presunção de legitimidade quanto a autoria do documento eletrônico.

Todavia, para esses casos podemos utilizar a regra do artigo 10, parágrafo 2.º da MP 2.200-2/01. Quando o documento dispensa a utilização da garantia notarial de autoria do documento, a certificação poderá ser obtida de forma aleatória.

Diante disso, se tivermos em consideração que o certificado digital confere presunção legal quanto a autoria do documento eletrônico temos que aplaudir a regra encontrada no projeto de lei 1.589/99, cujo anteprojeto foi elaborado pela OAB de São Paulo, que trata sobre a atividade de certificação digital no Brasil e tramita no Congresso Nacional.

De posse da natureza jurídica do certificado digital quando confere presunção de legitimidade quanto a autoria do documento eletrônico cabe-nos prosseguir na análise da natureza jurídica do certificado digital sob outro prisma.

6.3.2 Documento eletrônico sem presunção de legitimidade

Caminho totalmente antagônico ao supra citado encontramos quando realizamos uma interpretação mais estrita da regra prevista no artigo 10, parágrafo 1º da MP2.200-2/01. De acordo com a referida regra "*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"*

Em particular, a parte final da referida regra determina que os documentos eletrônicos "*presumem-se verdadeiros em relação aos signatários"*. Esta presunção de veracidade nada tem haver com o significado jurídico de presunção de legitimidade.

Por presunção de legitimidade devemos entender a inversão do ônus da prova. Já a presunção de veracidade é regra aplicável somente aos documentos particulares, conforme regra do artigo 368 do CPC.

Dessa forma, se entendermos que o certificado digital utilizado para assinatura digital não confere presunção de legitimidade quanto à autoria do documento, mas apenas assevera esta condição uma vez que não está expressamente prevista tal regra no artigo 10, parágrafo 1º da MP2.200-2/01, podemos concluir pela não aplicação do artigo 236 da Constituição Federal à atividade de certificação digital.

6.4 Competência material quando o certificado assegura presunção de legitimidade

Após a discussão sobre a natureza jurídica da certificação digital, que oscilará de acordo com os atributos que forem vinculados ao certificado digital, passamos à verificação da observância das regras legais de competência constitucional pela Medida Provisória 2.200-2/01.

Se considerarmos que a atividade de certificação confere presunção de legitimidade quanto à autoria do documento eletrônicos, estaremos diante de típico serviço notarial, que deverá ser exercido privativamente pelos Tabelionatos, conforme a regra do artigo 236 da Constituição Federal.

Isso porque num primeiro momento, a prestação do serviço público de certificação digital não se encontra descrita no rol de competências da União presente da Constituição Federal. Qual letra da Constituição Federal conduz a atividade de certificação digital sob a competência e responsabilidade da União?

Num segundo momento, a prestação do serviço de certificação digital pelo Poder Executivo Federal vem ferir regra de competência privativa fixada no artigo 236 da CF. Devido ao aspecto funcional, conferindo natureza jurídica de serviço notarial, a certificação digital deve ser desenvolvida pelos Tabelionatos, sob a fiscalização do Estado da Federação.

Contudo, esta condição não implicaria numa total inércia do Poder Federal. Sua atuação poderia ser externada por meio de um órgão regulador, consoante verificamos na prática de vários países que desenvolvem a atividade certificatória (capítulo 2), regulando o funcionamento das Autoridades Certificadoras e fiscalizando o cumprimento das normas técnicas pelas mesmas.

Por outro lado, se desconsiderarmos a presunção de legitimidade quanto a autoria do documento eletrônico proporcionado pelo certificado digital de assinatura digital, não devemos falar em aplicação da regra de competência do artigo 236 da Constituição Federal à atividade de certificação digital de assinatura digital.

6.5 Requisitos legais para uma ICP.

Após discutirmos sobre as duas vertentes da natureza jurídico da certificação digital, é possível a listagem de três requisitos legais essenciais para o seu desenvolvimento.

A atitude se mostra valiosa diante da oportunidade que os tecnólogos, pessoas responsáveis pelo desenvolvimento da tecnologia, incluindo-se neste quadro os elementos técnicos de prestação do serviço de certificação digital, terão de conhecer os limites legais para o exercício desse poder. Esses profissionais da área tecnológica são responsáveis por pesquisas e trabalhos voltados à evolução tecnológica. Dessa forma, o prévio conhecimento dos limites legais para o exercício da atividade de certificação digital é muito proveitoso para esse fim.

Três são os requisitos que deverão ser observados na construção de uma ICP-Brasil independente se sua natureza jurídica. O primeiro se expressa pelo poder de exercer a atividade de certificação digital.

O segundo requisito que podemos apontar é uma decorrência do controle federal das AC-Subs. É preciso que haja uma padronização entre as formas de certificação digital, uma vez que o exame de eficácia do certificado deve ser realizado em todo o território nacional.

O terceiro dos requisitos diz respeito à segurança dos documentos assinados com certificados emitidos sob a ICP-Brasil. Assegurar a autenticidade e a integridade dos documentos com o decorrer dos anos representa uma exigência primária, diante do propósito de perpetuidade das informações contidas. É preciso que os documentos sejam reavaliados toda vez que a técnica utilizada para a realização da assinatura digital torne-se obsoleta. Este ponto será melhor explorado no capítulo seguinte.

6.6 Certificados digitais para assinaturas digitais

Toda a discussão sobre a natureza jurídica do certificado digital e a análise da prestação do serviço de certificação digital diante das regras de

competência material firmadas pela Constituição Federal aplica-se apenas aos casos de assinatura digital.

Consoante estudado, os certificados digitais não se aplicam somente aos casos de assinaturas digitais, mas também nos casos de sigilo. Vale lembrar que, as regras de competência material apreciadas no presente trabalho não se aplicam nos casos de certificados digitais de sigilo.

A fim de identificar quais certificados devem são emitidos para servir às assinaturas digitais é preciso conhecer o campo "*key usage"* dos certificados.

Por meio do referido campo, presente no corpo do certificado, é possível a verificação de qual o seu propósito, se voltado ao sigilo ou para assinaturas digitais.

Na atualidade, tanto os certificados digitais utilizados para sigilo quanto àqueles utilizados para assinatura digital exigem para as garantias propostas pela MP2.200-2/01, que sejam emitidos sob a ICP-Brasil.

6.7 Projetos de lei que tratam da certificação digital

No presente texto, iremos analisar o tratamento jurídico dado pelos principais projetos de lei em tramitação no Congresso Nacional para as assinaturas digitais e para os certificados digitais. A finalidade consiste em verificar a correlação desses projetos com as regras de competência material fixadas na Constituição Federal para o desenvolvimento do serviço público de certificação digital conforme explicitado no presente trabalho.

Os projetos de lei que atualmente tramitam pelo Poder Legislativo são: 672/99 (que dispõe sobre a regulamentação do comércio eletrônico); 1.483/99 (dispõe sobre a fatura e assinatura digital); 1589/99 (dispõe sobre comércio eletrônico, validade jurídica, documento eletrônico e assinatura digital).

Todos os projetos de lei referidos acima estão presentes no substitutivo de número 4.906/01, que dispõe sobre o comércio eletrônico em geral.

O projeto de lei 672/99 não trata diretamente da atividade de certificação digital. A única menção relativa à identificação do signatário está contida em seu artigo 7.º, exigindo apenas que seja reservado para as mensagens

eletrônicas um método que assegure a identificação da pessoa, indicando sua aprovação quanto a informação assinada.

Por sua vez, o projeto de lei 1.483/99, ao instituir a fatura eletrônica e a assinatura digital nas transações de comércio eletrônico apenas faz a referência de que a assinatura digital terá sua autenticação e reconhecimento certificados por órgão público que será regulamentado para esse fim.

Em seu tempo, o projeto de lei 1.589/99, que corrobora com os principais aspectos abordados no presente trabalho, em seus artigos 16 e 25, que tratam respectivamente dos documentos eletrônicos e dos certificados eletrônicos, expressamente fixam a competência para exercer o serviço público de certificação digital aos Tabelionatos. Vale observar que o referido projeto de lei, expressamente fixa que a atividade não é estritamente pública, possibilitando a atividade privada de certificação digital por pessoas jurídicas de direito privado.

O substitutivo n.º 4.906/01, considera a atividade de certificação digital, elemento essencial para atribuir validade jurídica aos documentos eletrônicos. Dessa forma, seguindo as condições impostas no projeto de lei n.º 1.589/99, institui um sistema de certificação, no qual poderão atuar entidades públicas e privadas, sendo que neste último caso não é necessário credenciamento da AC perante o Poder Público. Por outro lado, àquelas entidades certificadoras que desejarem o credenciamento, deverão fazê-lo perante um órgão indicado pelo Poder Público.

Como podemos observar nos referidos projetos de lei listados acima, não há inviabilização da atividade de certificação digital, tanto nos casos de considerar a atividade de certificação como capaz de conferir com presunção de legitimidade a autoria do documento, assim como nos casos de não considerar a atividade de certificação digital como capaz de conferir presunção de legitimidade quanto a autoria dos documentos.

Por fim, temos que o projeto de lei 1.589/99, no caso de considerarmos que a atividade de certificação digital possui o atributo de conferir presunção de legitimidade quanto a autoria do documento eletrônico, expressamente declara a competência dos Tabelionatos para o desenvolvimento do serviço público de certificação digital sob a fiscalização dos Estados da Federação.

6.8 A certificação digital sem vinculação à ICP-Brasil

A primeira versão da Medida Provisória 2.200-2/01, monopolizava o exercício da atividade certificadora à ICP-Brasil. A regra legal introduzida, vinculava a validade jurídica dos documentos públicos e particulares em formato eletrônico à certificação digital oriunda da ICP-Brasil.

Várias foram as críticas, da doutrina especializada, direcionadas a esta monopolização estatal. Organizações sociais, como a Ordem dos Advogados do Brasil, saíram contra a previsão legal. Diante das críticas recebidas, a Medida Provisória 2.200-2/01, em suas duas mini reformas promovidas pelo Poder Executivo Federal, acabou por alterar esta regra.

Dessa forma, hoje, de acordo com o artigo 10, parágrafo 2.º: "*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 utilizam certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.*"

Podemos extrair da referida norma legal que, uma vez aceita pelas partes a origem independente da ICP-Brasil dos certificados eletrônicos, os efeitos que esta certificação digital produzirá no mundo jurídico equivalerá àquela assegurada pela ICP-Brasil para os seus certificados.

Todavia, esta previsão legal acarreta algumas circunstâncias jurídicas que merecem nossa total atenção, em virtude das conseqüências que podemos extrair da norma legal.

6.8.1 Natureza jurídica

A lei não diferenciou expressamente o alcance normativo das certificações digitais oriundas de Autoridades Certificadoras independentes da ICP-Brasil.

Conferir o mesmo alcance para ambos os tipos de certificação seria demasiadamente controvertido, uma vez que estaríamos conferindo força probatória de documento público aos certificados estritamente privados, quando oriundos da

iniciativa privada, considerados dessa forma, como documentos privados. A Autoridade Certificadora Independente passaria a atuar como um verdadeiro órgão público, contudo, sob um regime estritamente comercial.

Estaríamos diante de uma situação em que a pessoa jurídica de direito privado (ente particular) desenvolveria uma função pública sem assegurar forma de delegação desse poder, na atividade de certificação digital, sem sofrer qualquer tipo de regulamentação ou controle pelo Estado.

Dessa forma, segundo ensinamentos de Rover e Veiga (2003)[110] a natureza jurídica deste tipo de certificado digital equivale a um acordo de vontades, ou seja, um contrato entre as partes.

Com a devida vênia, discordamos em parte dos autores acima citados em razão de que a relação jurídica existente entre as partes neste acordo de vontades não alcança necessariamente relações jurídicas bilaterais de natureza patrimonial.

De acordo com Kümpel (2005, p. 05), os contratos em geral podem ser conceituados como:

> *"a fonte das obrigações estabelecidas pela convergência de duas ou mais vontades (elemento fundamental), de acordo com a lei, auto regulamentando interesses entre as partes contratantes (elemento estrutural), e cuja finalidade é adquirir, modificar ou extinguir relações jurídicas de natureza patrimonial (elemento funcional)*[111]*.*

Sem dúvida, o acordo entre as partes sobre a validade de um dado certificado digital oriundo de Autoridade Certificadora sem vínculo à ICP-Brasil, embora detenha as duas primeiras características do conceito de contratos, não vislumbra o último elemento indicado pela doutrina, qual seja, o elemento funcional.

Não pode ser considerado um contrato, uma vez que, podendo ser usado para fins comerciais entre outros, não envolve necessariamente a transferência de patrimônio de uma pessoa para outra.

---

[110] **- ROVER, Aires José. Veiga, Luiz Adolfo Olsen da Veiga.** *Validade Jurídica de documentos eletrônicos assinados com infra-estrutura diferente da ICP-Brasil.*Artigo Publicado pela UFSC em Setembro de 2003. Pág. 03.

[111] **- KÜMPEL. Vitor Frederico.** Direito Civil 3. Direitos dos Contratos. Coleção Cursos e Concursos, coordenados por Edilson Mougenot Bonfim. Editora Saraiva. São Paulo. 2005. Pág. 05.

Diante disso, preferimos alojar a natureza jurídica da certificação digital oriunda de Autoridade Certificadora Independente da ICP-Brasil, nos moldes do artigo 17 do projeto de lei n.º 1.589/99, como uma declaração jurídica de vontade, como vem regulamentada no artigo 107 do Código Civil.[112]

Na Teoria Geral dos Contratos a declaração de vontade constitui um elemento de formação dos contratos, mas a declaração de vontade em si, não poderá ser considerada como um contrato.

A natureza jurídica das certificações digitais oriundas de Autoridades Certificadoras independentes da ICP-Brasil não recebe a mesma roupagem das certificações digitais oriundas de Autoridades Certificadoras Subseqüentes da ICP-Brasil, uma vez que tais certificados não podem ser considerados documentos públicos com força vinculativa e de identificação pessoal. Os certificados digitais independentes equiparam-se às declarações de vontade entre as partes, segundo as quais, uma delas reconhece como verdadeira a chave pública apresentada pela outra parte e vice e versa, produzindo efeitos no mundo jurídico, sem presunção de legitimidade.

6.8.2 Força Probatória da certificação digital independente

Quando falamos em força probatória no direito processual devemos tratar da capacidade inerente aos institutos em demonstrar as alegações feitas pelos sujeitos numa determinada relação processual.

Nosso direito processual, embora exclua da relação de provas aceitas em juízo, àquelas produzidas com afronta aos direitos e garantias materiais e processuais (provas ilícitas e ilegítimas respectivamente – artigo 5.º, inciso LVI da CF), traz em suas normas positivadas um rol exemplificativo das principais formas de provas aceitas em juízo. Dentro deste rol podemos conceder destaque às provas testemunhais, periciais e documentais, entre outras.

O certificado digital, considerado como documento eletrônico assinado digitalmente insere-se justamente na última espécie que citamos acima, ou seja, é considerado uma prova documental.

---

[112] - “Art. 107. A validade da declaração de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir.”

Os certificados eletrônicos assinados e emitidos sob a égide da ICP-Brasil, embora possam objetivar documentos particulares, em si próprios, são considerados documentos públicos, uma vez que são oriundos de Pessoa Jurídica de Direito Público.

Por sua vez, a certificação digital oriunda de Autoridades Certificadoras Independentes, sem qualquer vínculo hierárquico de competência com a ICP-Brasil, não pode ser considerado documento público.

Todavia como já vimos, a natureza jurídica de ambas divergem, logo, sua categorização como prova também diverge. Os certificados digitais nesses casos são considerados documentos particulares.

Dessa forma, a força probatória dos certificados digitais independentes é a mesma força probatória que os documentos particulares possuem, conforme as regras dos artigos 368[113], 372[114], entre outros, do Código de Processo Civil.

6.9 A regra do artigo 154, parágrafo único do Código de Processo Civil

Por meio da lei 11.280/06, foi introduzido junto ao Título V, intitulado "dos atos processuais", no capítulo I, denominado "Das formas dos atos processuais", constante do Código de Processo Civil, no artigo 154, parágrafo único, a seguinte regra: "*Os tribunais, no âmbito da respectiva jurisdição, poderão disciplinar a prática e a comunicação oficial dos atos processuais por meios eletrônicos, atendidos os requisitos de autenticidade, integridade, validade jurídica e interoperabilidade da Infra-estrutura de Chaves Públicas Brasileira - ICP - Brasil."*

---

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

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

114 - "Art. 372. Compete à parte, contra quem foi produzido documento particular, alegar no prazo estabelecido no art. 390, se lhe admite ou não a autenticidade da assinatura e a veracidade do contexto; presumindo-se, com o silêncio, que o tem por verdadeiro.

Parágrafo único. Cessa, todavia, a eficácia da admissão expressa ou tácita, se o documento houver sido obtido por erro, dolo ou coação".

Consoante aponta Bedaque (2005)[115] a forma dos atos processuais objetiva constituir um fator de segurança para o processo, contribuindo decisivamente para a justiça da decisão.

Respeitando-se as regras processuais de forma fixadas para os atos processuais, observamos como conseqüência a legitimidade da decisão judicial, sendo que a segurança e a finalidade do ato foram alcançados. As regras de forma são interpostas em leis processuais com o escopo de garantir o respeito aos princípios processuais constitucionais no exercício do Poder Jurisdicional.

Como vimos, todo o desenvolvimento processual é regido por formas. Com isso, todos os sujeitos processuais estão vinculados às formas processuais (Bedaque, 2005), em conseqüência, temos que os poderes, obrigações, ônus e faculdades devem ser praticados conforme preestabelecido em norma processual.[116]

A própria validade da relação processual depende do respeito às formas processuais, uma vez que cabe ao juiz, antes de adentrar ao mérito da questão, analisar os pressupostos de validade do processo, que são as formas processuais estabelecidas para a garantia da segurança e finalidade do ato.

A inclusão da norma processual do parágrafo único, do artigo 154, entre as regras de forma dos atos processuais leva-nos a concluir que a validade e a autenticidade dos atos processuais, quando realizados em formato eletrônico, dependerá da utilização de certificados digitais oriundos da ICP-Brasil.

Para os atos processuais realizados em processos tidos como eletrônicos, além das regras formais previamente fixadas para a validade dos atos em geral, temos ainda uma regra específica, qual seja, a utilização de certificados digitais emitidos sob a ICP-Brasil.

Todavia, desastrosa foi a atitude do legislador, ao incluir no artigo 154 do CPC a regra de utilização dos certificados da ICP-Brasil, alvejando a validade e a autenticidade dos atos processuais em formato eletrônico.

---

115 - **BEDAQUE, José Roberto dos Santos.** Efetividade do Processo e Técnica Processual: Tentativa de Compabilização. Tese apresentada ao Concurso para o cargo de Professor Titular de Direito Processual Civil da Faculdade de Direito da Universidade de São Paulo. 2005. Pág. 415.

116 - **BEDAQUE, José Roberto dos Santos**. Efetividade do Processo e Técnica Processual: Tentativa de Compabilização. Tese apresentada ao Concurso para o cargo de Professor Titular de Direito Processual Civil da Faculdade de Direito da Universidade de São Paulo. 2005. Pág. 89.

A primeira ponderação que se pode fazer, de ordem sistemática, é quanto à regra processual prevista no *caput* do artigo 154 [117]. Refere-se à regra de aplicação do princípio da instrumentalidade das formas no processo civil. Trata-se de uma regra de aproveitamento dos atos processuais quando, embora não realizados de acordo com as formas constantes na lei processual, a segurança jurídica e a finalidade do ato foram atingidos.

Dessa forma, nada tem de relação com a utilização de certificados digitais emitidos no âmbito da ICP-Brasil, como forma para a realização válida dos atos processuais.

A conseqüência desta previsão pode ser sentida na interpretação da norma, uma vez que podemos concluir que a não utilização de certificado digital oriundo da ICP-Brasil por si só não é suficiente para invalidar o ato, uma vez que a segurança e a finalidade poderão ser atingidos de outra forma. Esta assertiva ganha ainda mais realce quando a interpretação é feita diante da norma jurídica contida no art. 10, par. 2.º da MP 2.200-2/01, prevendo a validade jurídica e força probante dos certificados digitais independentes.

Para melhor corroborar o pensamento, vale lembrar que a regra do parágrafo único do artigo 154 do Código de Processo Civil deve ser interpretada sistematicamente em consonância com as regras dos artigos 244[118], 249[119] e 250[120]. São regras processuais de recuperação e aproveitamento dos atos processuais realizados em desconformidade com as formas legalmente previstas.

Vencida a primeira etapa quanto a utilização de certificados digitais oriundos da ICP-Brasil na produção de atos processuais eletrônicos, seguimos por uma segunda análise.

---

117 - Art. 154.*"Os atos e termos processuais não dependem de forma determinada senão quando a lei expressamente a exig*ir, *reputando-se válidos os que, realizados de outro modo, lhe preencham a finalidade essencial."*

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

119 *-" Art. 249. O juiz, ao pronunciar a nulidade, declarará que atos são atingidos, ordenando as providências necessárias, a fim de que sejam repetidos, ou retificados.*

§ 1º O ato não se repetirá nem se lhe suprirá a falta quando não prejudicar a parte.

§ 2º Quando puder decidir do mérito a favor da parte a quem aproveite a declaração da nulidade, o juiz não a pronunciará nem mandará repetir o ato, ou suprir-lhe a falta."

120 *- "Art. 250. O erro de forma do processo acarreta unicamente a anulação dos atos que não possam ser aproveitados, devendo praticar-se os que forem necessários, a fim de se observarem, quanto possível, as prescrições legais.*

Parágrafo único. Dar-se-á o aproveitamento dos atos praticados, desde que não resulte prejuízo à defesa."

As principais conseqüências processuais que podemos extrair da norma do parágrafo único do artigo 154 do Código de Processo Civil, para o desenvolvimento da atividade certificadora na produção e armazenamento dos atos processuais em formato eletrônico, consiste no uso de certificados digitais como pressuposto processual para a validade do processo judicial.

O juiz, ao receber cada ato processual em formato eletrônico, tais como a petição inicial ou a contestação, além de analisar as regras processuais previamente existentes para a validade do ato (análise dos pressupostos processuais) terá ainda a obrigação de verificar a validade do certificado digital.

Qualquer vício constante do certificado digital utilizado para assegurar a autenticidade do ato processual, por exemplo, sua revogação, poderá ter como conseqüência a extinção do processo.

Nos atos processuais em formato eletrônico, a autoria (autenticidade) do documento processual, será verificada por meio do certificado digital. Todas as informações necessárias a individualização do signatário estarão ali presentes. Dessa forma, o organismo responsável para emitir certificados digitais aos serventuários da justiça deverá ser o próprio Organismo Judiciário, pois atualmente, a autoria (autenticidade) dos atos judiciais em geral é de competência exclusiva do Poder Judiciário, como poder independente e soberano.

A utilização de certificados digitais assegurando força probante aos atos processuais eletrônicos é perfeitamente aceita. Para haver o respeito às regras de divisão de poder (e conseqüentemente de divisão de competência) mister que cada Poder (Executivo, Legislativo e Judiciário) exerça o poder de certificação digital de seus membros soberanamente. Isso poderá ser realizado por meio da AC-Sub que esteja de acordo com os requisitos mínimos de segurança fixados por um órgão regulador federal, e sejam contratadas para oferecer este serviço.

Cada Poder é soberano em suas funções, sendo assim, o Poder Judiciário, através da contratação de uma Autoridade Certificadora Subseqüente, emite um certificada para cada um de seus membros, a fim de exercer suas funções nos atos eletrônicos. Vale ressaltar que o exercício do poder de conferir autenticidade é feito pelo Poder Judiciário através de um Autoridade Certificadora Subseqüente e não diretamente pela Autoridade Certificadora Subseqüente.

7 ASPECTOS DOS PROBLEMAS ENCONTRADOS NOS ALGORÍTMOS CRIPTOGRÁFICOS DE FUNÇÃO *HASH*.

Dentre os vários elementos técnicos envolvendo a segurança que a assinatura digital confere aos documentos eletrônicos, destacamos a utilização dos algoritmos criptográficos assimétricos, como o RSA e os algoritmos de função *hash,* como o MD5 e o SHA-1. O escopo do presente capítulo são os algoritmos de função *hash*, sendo encarados como fonte de integridade das informações em formato eletrônico.

Um algoritmo de criptografia pode ser entendido como uma função matemática usada no processo de cifração e decifração de informações. Um algoritmo é considerado assimétrico ou, como também é denominado, algoritmo de criptografia de chaves públicas, porque opera usando um par de números (duas chaves), de modo que a mensagem cifrada por uma das chaves somente será decifrada com a outra chave e vice e versa. Entretanto, os números que compõem as chaves não são derivados um do outro, dessa forma, uma das chaves poderá ser divulgada sem restrições (chave pública) sem representar perigo para a outra chave que deverá ficar sob o conhecimento exclusivo do signatário (chave privada).

O RSA é um algoritmo criptográfico de cifração de dados e tem como base de sua construção a teoria clássica dos números. Representa um dos algoritmos criptográficos assimétricos mais populares no meio cientifico brasileiro. Foi inventado por Ron Rivest, Adi Shamir e Len Adleman. É considerado como primeiro algoritmo criptográfico assimétrico a ser utilizado em assinaturas digitais.

Um algoritmo de função *hash* é um método matemático de mapeamento de valores de um conjunto infinito em um conjunto finito, utilizado para assegurar a integridade dos dados. Isso significa que os algoritmos de função *hash* baseiam-se num processo unidirecional, impossibilitando a descoberta da informação original partindo-se do bloco gerado. Se um único bit da mensagem original for alterado, um novo bloco hash totalmente diferente é gerado.

A função *hash* recebe um valor (seqüência de bits) e retorna um outro valor (seqüência de bits com tamanho fixo) denominado código *hash* ou resumo criptográfico.

A força do algoritmo de função *hash* é mensurada pelo grau de dificuldade de se encontrar colisões. As colisões ocorrem quando duas mensagens eletrônicas distintas, aplicando o mesmo algoritmo de hash, geram o mesmo resumo. Para melhor elucidação da assertiva acima, um exemplo pode ser verificado na figura 1:

Como exemplo tomemos o seguinte texto:

1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111

O resume *hash* do texto utilizando SHA-1, é: "e93d2b15501fee757c4cfce88af338c5088adf66"

Se trocarmos o número 1 inicial pelo número 2
2111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111

O resumo *hash* do texto utilizando SHA-1 será: "7a291e85bfd89446ffe55a43fcaaa3de09c23cf2"

Como pode ser observado a simples mudança de um número alterou completamente o resultado do cálculo do SHA-1.

Figura 1 – Exemplo de bloco *hash* gerado a partir de uma dada informação. [121]

7.1 Os algoritmos adotados pela ICP-Brasil.

Vimos que a assinatura digital é gerada a partir da conjugação de dois algoritmos criptográficos: o algoritmo de criptografia assimétrico, cuja principal característica é a presença de um par de chaves; e o algoritmo criptográfico de função *hash*, cuja principal característica consiste no seu processo unidirecional (sentido único).

Do arquivo que deverá ser assinado, calculamos o resumo criptográfico, por meio da utilização de um algoritmo de função *hash*. Sobre o resumo *hash* aplicamos a criptografia assimétrica, utilizando a chave privada.

Assim, temos a concepção de que a geração da assinatura depende de dois algoritmos criptográficos com características diferentes. Um denominado de criptografia assimétrica, composto por um par de chaves, responsável pela geração

[121] **Observatório Nacional.** Base de Dados. 2007. Disponível em **http://pcdsh01.on.br/** . Acesso em 01 de Fevereiro de 2007.

da assinatura; e outro denominado de função de *hash*, reduzindo o arquivo num pequeno bloco de informações irreversível.

Em linhas gerais, a escolha do algoritmo de criptografia assimétrico e do algoritmo criptográfico de função de *hash* é muito importante, pois estão intrinsecamente relacionados à integridade do documento.

A ICP-Brasil, com o objetivo de assegurar a integridade dos documentos eletrônicos assinados digitalmente aponta, por meio de atos normativos, quais os algoritmos que deverão ser usados. Consoante disserta a Declaração de Práticas de Certificação da AC-Raiz (Resolução n.º 1, do C.G.), em seu item 7.1.3, o certificado digital da AC-Raiz é assinado com um algoritmo criptográfico assimétrico RSA, utilizando-se do SHA-1 como algoritmo criptográfico de função de *hash.*

Seguindo nesta linha, a resolução n.º 7, de 12 de Dezembro de 2001, do C.G., aprovando os requisitos mínimos para políticas de certificado, no item 7.1.3 determina que serão admitidos no âmbito da ICP-Brasil, como algoritmos criptográficos utilizados para assinar os certificados emitidos ao usuário final os seguintes: RSA[122]; SHA-1[123] com RSA; MD5[124] com RSA; e SHA-1 com DSA[125].

Todavia, em 18 de maio de 2006, através do DOC ICP-01.01 – V 1.0, do Instituto Nacional de Tecnologia da Informação, ficou estabelecido que os algoritmos criptográficos que deverão ser utilizados para a assinatura de certificados de AC deverão ser necessariamente o SHA-1 com RSA, e os algoritmos criptográficos que deverão ser utilizados para assinar certificados de usuário final deverão ser o SHA 1 com RSA ou o SHA 1 com DSA.

---

122 - O RSA vem descrito na RFC 2313. Os RFC constituem uma categoria de documentos que descreve padrões da Internet. É proveniente do IETF (*Internet Engineering Task Force*) que é uma comunidade internacional composta por membros de vários setores interessados, preocupados com a evolução da arquitetura da Internet e seu perfeito funcionamento.

123 - O SHA-1 vem descrito no FIPS 180-1. É um documento de Publicação Federal de Padrões de Processamento de Informações emitido pelo NIST (National Institute of Standards and Technology).

124 - O MD5 vem descrito na RFC 1321.

125 - O DSA é um algoritmo criptográfico assimétrico, assim como o RSA, usado apenas para gerar a assinatura digital sobre o resumo da função de hash, não servindo para ser usado como criptografia de dados.

7.2 Algoritmo de função hash MD5.

O MD5, corresponde à abreviatura da expressão *"Message-Digest Algorithm 5,* consistindo num algoritmo de *hash*, com tamanho de 128 bits. Foi criado em 1992, por Ron Rivest, que o desenvolveu através da empresa RSA, localizada em *Bedford*, em *Massachusetts*, nos Estados Unidos da América, utilizado largamente como ferramenta para assegurar integridade de informações em formato eletrônico.

Todavia, já em 1993 (Xiaoyan, 2004)[126] , Bert den Boer e Antoon Bosselaus encontraram pseudo colisões no MD5, consistindo numa mesma mensagem com 02 diferentes grupos de valores iniciais. De acordo com a pesquisa, os ataques demonstraram uma grande fragilidade no bit do MD5 mais significativo.

Foi permitida a utilização do MD5, como função de *hash*, pelos órgãos públicos brasileiros desde a criação da atual ICP-Brasil, conforme podemos verificar pela Resolução nº 7 do Comitê Gestor da ICP-Brasil[127].

Em linhas gerais, conforme explica Xiaoyan (2004)[128], o algoritmo MD5 é compreendido pela função matemática de X=f(Z). Podemos compreender que "z" representa os bits existentes em uma mensagem, e "x" representa o valor de *hash* obtido através do algoritmo de hash.

Esse ataque, denominado de "ataque diferencial modular" tem como base um bloco codificado, no qual através de uma função XOR (ou exclusivo) parte-se de dois blocos diferentes de informação, obtendo-se o mesmo resumo criptográfico.

---

126 - XIAOYAN, Wang. DENGGUO, Feng. XUEJIA, Lai. HONGBO, Yu. Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. The School of Mathematics and System Science, Shandong University, Jinan250100, China. Institute of Software, Chinese Academy of Sciences, Beijing100080, China. Dept. of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai, China. 17 de Agosto de 2004.

127 - Comitê Gestor. Infra-estrutura de Chaves Públicas. Aprova os requisitos mínimos para políticas de certificado na ICP-Brasil. Resolução n.º 7, 12 de Dezembro de 2001. Brasília (DF). 29 p.

128 - XIAOYAN, Wang. DENGGUO, Feng. XUEJIA, Lai. HONGBO, Yu. Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. The School of Mathematics and System Science, Shandong University, Jinan250100, China. Institute of Software, Chinese Academy of Sciences, Beijing100080, China. Dept. of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai, China. 17 de Agosto de 2004.

Para a realização desses testes, foi utilizado um supercomputador IBM P690, e os testes durarão algumas horas até a obtenção dos primeiros resultados.

Klima (2005)[129], propondo um método aperfeiçoado a partir daquele construído pela equipe chinesa, conseguiu melhores resultados, utilizando-se daquilo que se denominou de inicialização de vetores. Consoante bem descreve o autor, a contribuição de sua pesquisa está na diminuição do tempo utilizado para o encontro de colisões, ocorrendo em no máximo 2 minutos, utilizando-se um simples *notebook* de 1.6 Ghz, enquanto que a equipe chinesa levou algumas horas para conseguir os mesmos resultados, com a utilização de um supercomputador. Todavia, o ganho de tempo com o método proposto pelo autor somente é atingido na primeira colisão, sendo que numa segunda colisão, o método proposto pela equipe chinesa é mais eficiente.

Nesta linha, a equipe chinesa demonstrou dois pares de colisão de mensagens, enquanto que no trabalho de Klima (2005)[130] foram apresentados 04 pares de colisão de mensagem, suficiente para a realização de ataques bem sucedidos de falsificação contra documentos eletrônicos.

A fragilidade do MD5 fica ainda mais evidente quando analisamos os trabalhos de Kim (2005)[131] e Stevens (2006)[132].

No primeiro trabalho, foram exploradas propostas em "*related-key rectangle and boomerang"* utilizando técnicas não randômicas de MD5 distinguindo-o de uma cifra aleatória escolhida.

No segundo trabalho, Stevens (2006)[133] apresenta um aperfeiçoamento dos ataques ao algoritmo *hash* MD5 para encontrar dois blocos de colisão, utilizando-se das mesmas condições e caminhos propostos pelo grupo de pesquisa chinês. A nova técnica baseia-se no cumprimento de determinadas

---

[129] **- KLIMA, Vlastimil**. Finding MD5 Collisions – a Toy For a Notebook. Prague, Czech Republic. 05 de Março de 2005.

[130] **- KLIMA, Vlastimil**. Finding MD5 Collisions – a Toy for a Notebook. Prague, Czech Republic. 05 de Março de 2005.

[131] **- KIM, Jongsung. BIRYUKOV, Alex. PRENEEL, Bart. LEE, Sangjin.** On the Security of Encryption Modes of MD4, MD5 and HAVAL.Katholieke Universiteit Leuven. ESAT/SCD-COSIC Kasteelpark Arenberg 10, B-3001 (Belgium). Center for Information Security Technologies (CIST) (Korea).

[132] **- STEVENS, Marc.** Fast Collision Attack on MD5. Department of Mathematics and Computer Science, Eindhoven University of Technology. The Netherlends.

[133] **- STEVENS, Marc.** Fast Collision Attack on MD5. Department of Mathematics and Computer Science, Eindhoven University of Technology. The Netherlends.

limitações, possibilitando a mudança dos diferenciais do primeiro ciclo. Para o segundo ciclo, Stevens utiliza o método empregado alhures por Klima.

Como bem destaca Klima (2005)[134], a comunidade científica não deve mais usar o MD5 como função *hash*, uma vez que ele não mais consegue assegurar seu principal propósito, a integridade dos dados.

7.3 Algoritmo de função hash SHA-1

O *National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia) – NIST – é um organismo do governo norte americano com responsabilidade de emitir padrões criptográficos na realização de assinaturas digitais.

Em primeiro de agosto de 2002, o NIST editou o documento *Federal Information Processing Standards Publication (*Publicação Federal dos Padrões de Processamento de Informações) sob o n.º 180-2. Neste documento restou acordado que o algoritmo de *hash* SHA-1 é suficientemente seguro para condensar representações computacionais eletrônicas, ou seja, é seguro para ser utilizado na realização de assinaturas digitais.

O SHA-1 (*Secure Hash Algorithm)* foi criado pelo NIST em 1994, como um avanço do SHA-0, sendo hoje considerado um algoritmo de hash confiável dado que a realização de ataques é computacionalmente inviável.

São características de código *hash* viável: a) resistência a primeira inversão, onde dado o bloco de *hash* é computacionalmente improvável a obtenção da mensagem original; b) resistência à segunda inversão, sendo computacionalmente improvável que se encontre uma outra mensagem que utilizando-se da mesma função de *hash* encontre o mesmo bloco; e c) resistência a colisões, sendo improvável que duas mensagens distintas gerem o mesmo resumo. (NIST 2000)

O SHA-1 utiliza uma seqüência de funções lógicas (f0, f1.....f79. Cada função ft, onde 0 <= t < 79, opera em três códigos “x”, “y” e “z”, gerando um

---

[134] - KLIMA, Vlastimil. Finding MD5 Collisions – a Toy For a Notebook. Prague, Czech Republic. 05 de Março de 2005.

código de saída de 32 bits de constante 2^{80}. Em linhas gerais, temos como entrada um arquivo qualquer em formato digital com um tamanho de até 2^{80} bits, obtendo na saída um resumo criptográfico de 160 bits.

Atualmente (Padrões e Algoritmos Criptográficos da ICP-Brasil – DOC ICP-01.01 – 2006), o algoritmo criptográfico adotado pela ICP-Brasil para a realização das assinaturas digitais é o SHA-1

Todavia, a segurança deste algoritmo está sendo abalada. A mesma equipe chinesa liderada por Xiaoyun (2005), responsável pela primeira quebra do MD5, desenvolveu novas técnicas capazes de encontrar colisões na função de *hash* SHA-1.

A base do ataque aplicado ao SHA-1 é encontrada no ataque diferencial original aplicado ao SHA-0, assim como na busca de colisão do MD5.

Sua resistência foi reduzida de 2^{80} para 2^{63}. Com isso conseguiram reduzir o tempo de quebra do SHA-1 pela força bruta em 2000 vezes.

Entretanto, esta redução não representa atualmente um perigo em potencial, a ponto de ser afastado o uso do SHA-1, mas demonstra que o SHA-1 é vulnerável, tendo seu tempo de vida útil reduzido.

Assim como para o MD5, a vulnerabilidade do SHA-1 foi possível por meio da utilização de um supercomputador. Vale ressaltar que na primeira quebra do MD5, pela equipe chinesa, também foi utilizado um supercomputador, e com base nessas pesquisas iniciais, outros pesquisadores conseguiram reduzir o tempo de quebra do MD5 em prazos desconsiderados, como 2 minutos, utilizando-se de um simples *notebook* de 1.6 Ghz. Quanto tempo mais o SHA-1 conseguirá resistir aos ataques?

O NIST prevê que o SHA-1 será definitivamente abandonado em 2.012, conforme prevê a FIPS 180-2 do NIST. Com isso, a tecnologia deverá se preocupar em continuar a conferir força valorativa aos documentos eletrônicos assinados digitalmente com o SHA-1 como técnica de função de *hash*.

7.4 Conseqüências da quebra do MD5 e SHA-1 para a ICP-Brasil

Vimos que, dentre os vários elementos tecnológicos utilizados para a realização de uma assinatura digital destacamos o algoritmo criptográfico de função

hash. Consoante bem disserta Xiaoyun (2005)[135] a segurança das assinaturas digitais depende, entre outras coisas, da força do algoritmo criptográfico de função *hash*.

Dessa forma, quando encontramos colisões nos algoritmos criptográficos de função *hash*, isso significa que podemos ter fraudes em assinaturas digitais. Klima (2005)[136] ressalta que o seu método de ataque ao MD5 é perfeitamente hábil a produzir assinaturas digitais forjadas.

Em 2001, conforme vimos na resolução n.º 7, do Comitê Gestor da ICP-Brasil, para as assinaturas digitais os algoritmos criptográficos assimétricos adotados eram o RSA e o DSA, e como algoritmos criptográficos de função de *hash* eram adotados o MD5 e o SHA-1.

Todavia, em Maio de 2006, o MD5 deixou de ser adotado pela ICP-Brasil como algoritmo criptográfico de função de *hash* consoante o DOC ICP 0101 – V1.0 visto acima, em razão de sua aparente fragilidade reconhecida pelo mundo científico. O MD5 não resistiu aos ataques de colisão produzidos contra ele, e conforme vimos nos trabalhos analisados nos textos anteriores, foi possível encontrar colisões com um tempo de até 2 minutos.

Ficou aparente, com isso, a possibilidade de se fraudar documentos eletrônicos por meio de assinaturas digitais forjadas. Esta condição é possivelmente encontrada na ICP-Brasil, uma vez que o algoritmo criptográfico de função *hash* MD5 somente deixou de constar nas regras da ICP-Brasil em maio de 2006, todavia, sua quebra foi anunciada em 2004. Assim, os certificados digitais assinados digitalmente com MD5 sob esse período possuem todas as características oriundas da MP2.200-2/01 (p. Ex.: conferir presunção de veracidade), mas por outro lado, podem estar vulneráveis.

De acordo com a nova posição adotada pela ICP-Brasil, restou o SHA-1 como algoritmo criptográfico de função *hash.*

Entretanto, de acordo com as recentes pesquisas apresentadas, cientistas chineses afirmam que a força do SHA-1 foi inicialmente fragilizada. Em

---

[135] **- XIAOYUN, Wang. HONGBO, Yu.** How to break MD5 and other hash functions. Shandong University, Jinan 250100, China.

[136] **- KLIMA, Vlastimil**. Finding MD5 Collisions – a Toy For a Notebook. Prague, Czech Republic. 05 de Março de 2005.

linhas gerais, podemos dizer que o SHA-1 sofreu um ferimento (fragilidade), mas não suficiente para ocasionar a sua morte.

Referido acontecimento não representa na atualidade um fator de insegurança, uma vez que mesmo com o encontro das fragilidades o SHA-1 ainda preenche os requisitos de força exigidos mundialmente dos algoritmos criptográficos de função *hash*.

Por outro lado, isso representa um aviso, uma vez que algumas técnicas de ataque já foram encontradas, apontando o caminho a ser seguido pelos cientistas para o encontro de outras, comprometendo a vida útil do SHA-1.

Com a natural evolução científica, a segurança técnica oferecida pelos algoritmos criptográficos de função *hash* não é duradoura, aniquilando assim a idéia de perpétua confiança dos documentos eletrônicos assinados digitalmente.

7.5 Criticas quanto a expressa adoção de algoritmos pela ICP-Brasil.

A lei, enquanto regra escrita, deve traçar todos os elementos que serão observados pelo seu destinatário no momento em que se cumprirá teleologicamente a norma jurídica (preceito abstrato existente em cada regra).

Corresponde numa praxe, a fixação pelas regras, tanto jurídicas como técnicas, do caminho que o destinatário deve guiar-se para a realização do fim proposto. O respeito a esses parâmetros garante a validade de seus atos.

Seguindo nesta linha, o Comitê Gestor da ICP-Brasil resolveu fixar, por meio de seus atos, os algoritmos criptográficos de função *hash* que deverão ser utilizados para a realização das assinaturas digitais. Consoante vimos acima, atualmente o SHA-1 representa o único algoritmo de função *hash* utilizado na ICP-Brasil.

Sob uma visão hermenêutica, consoante estabelece a resolução n.º 7, de 12 de Dezembro de 2001, do C.G., em seu item 1.1, os requisitos mínimos e obrigatórios que devem ser observados pelas AC-Sub para o exercício da atividade de certificação digital estão ali descritos.

As garantias oferecidas pela ICP-Brasil às assinaturas digitais produzidas com certificados emitidos sob a sua égide, dependem da observância desses requisitos técnicos, como a utilização do SHA-1 para a geração do resumo *hash*.

Aparentemente, esta previsão não apresenta maiores problemas, entretanto, se aplicarmos uma perspectiva tecnológica evolutiva teremos alguns problemas a enfrentar.

O MD5 é um algoritmo de função *hash* que foi utilizado pela ICP-Brasil para a realização de assinaturas digitais até maio de 2006, todavia, teve sua fragilidade completamente provada em 2005.

Desta sorte, como já vimos, a ICP-Brasil assegura força valorativa de assinaturas digitais e documentos eletrônicos gerados com o MD5 após a sua quebra ser determinada pelo mundo científico. Com isso, foi dada margem à existência de assinaturas digitais forjadas e documentos eletrônicos adulterados com todos os elementos de força valorativa garantidos pela ICP-Brasil.

A razão dessa situação encontra imediato alicerce na principal característica oriunda da fixação de regras, qual seja, conferir legitimidade aos atos que são produzidos de acordo com suas diretrizes.

Neste ponto, poderíamos concluir então que a expressa previsão dos algoritmos de função *hash,* pela regra, representaria um mal desnecessário, uma vez que os próprios órgãos técnicos envolvidos na prestação do serviço público de assinatura digital, como por exemplo as Autoridades Certificadoras Subseqüentes, poderiam alterar as opções de acordo com a evolução tecnológica.

Cabe-nos realizar algumas críticas a este quadro. Na atual cadeia de certificação, o ITI (AC-Raiz) representa o organismo máximo de garantia das assinaturas digitais produzidas sob a ICP-Brasil, responsabilizando-se por eventuais fraudes ocorridas em seu domínio.

Quando o Comitê Gestor, órgão político da ICP-Brasil responsável pela emissão de diretrizes, fixa determinados algoritmos de função *hash* para a geração das assinaturas digitais, além de outros objetivos, quer assegurar a responsabilidade da AC-Raiz quanto a confiança das assinaturas digitais geradas com certificados digitais emitidos sob a ICP-Brasil.

A liberdade de escolha quanto a utilização de algoritmos de função *hash* pelos organismos técnicos envolvidos na geração da assinatura digital, como

as AC-Sub, criaria em potencial a utilização de algoritmos de função *hash* considerados obsoletos, condição que por muitas vezes pode ser desconhecida pelo usuário final (signatário).

Essa condição poderia gerar, de alguma forma, responsabilidades à AC-Raiz, uma vez que desempenha um papel de órgão máximo na cadeia de certificação digital no Brasil.

Dessa forma, a expressa descrição dos algoritmos de função *hash* pela regra, assegura, pelo menos teoricamente, que os organismos envolvidos na prestação do serviço de assinatura digital não utilizarão elementos técnicos considerados inseguros pela ICP-Brasil.

Diante das críticas expostas, acreditamos que a melhor posição encontra-se na expressa previsão dos elementos técnicos que devem ser adotados para a atividade de geração da assinatura digital, uma vez que, a responsabilidade da AC-Raiz estará teoricamente assegurada.

7.6 A integridade dos documentos diante da evolução tecnológica.

Ao estudarmos os aspectos dos problemas enfrentados pelos algoritmos criptográficos de função *hash* na geração das assinaturas digitais verificamos que não há segurança técnica perpétua.

Esta condição desencadeia uma relação de limite de tempo para a força probante dos documentos eletrônicos. Todavia, este período não condiz com o período de vida útil do documento, uma vez que, como observamos em capitulo anterior, os documentos são criados para assegurar valor perpétuo às informações neles contidas.

Recomendação pouco proveitosa refere-se a utilização das assinaturas digitais em documentos eletrônicos com temporalidade baixa. Todavia referida técnica limitaria em muito a utilização das assinaturas digitais, a começar pelo processo judicial.

O problema oriundo desta natural evolução não deve ser enfrentado pela norma jurídica, mas cabe preponderantemente às regras técnicas, que deverão desenvolver mecanismos capazes de gerar a integridade aos documentos

eletrônicos pelo passar dos anos, da mesma forma que são encontrados no momento de sua produção.

8 CONSIDERAÇÕES FINAIS

Após o exame de todas as considerações referentes ao ponto de convergência entre a ciência jurídica e a ciência tecnológica, chega-se a conclusão de que ambas devem caminhar paralelamente para o desenvolvimento social. Dessa forma, sobre o específico tema proposto inicialmente, pode-se traçar as seguintes considerações.

8.1 Cumprimento dos objetivos

Ao inicio do presente trabalho, foi proposto atingir um objetivo dicotômico. Isso ocorre em virtude do caráter multidisciplinar apresentado pela matéria analisada. A primeira vertente, de cunho jurídico, concernente ao estudo do papel desenvolvido pela certificação digital no mundo jurídico sob o aspecto funcional de conferir ou não presunção de legitimidade de autoria ao documento eletrônico, chegando-se assim às possíveis naturezas jurídicas da certificação digital. A partir da análise das possíveis naturezas jurídicas do certificado digital foi possível a realização da análise crítica da competência material, fixada pela Constituição Federal para esses casos. Foi possível referendar os requisitos jurídicos necessários para o desenvolvimento de uma ICP-Brasil caracterizada pela legitimidade jurídica. Em suma, é a tecnologia se desenvolvendo de acordo com as regras legais que defendem nosso Estado Democrático de Direito.

O objetivo jurídico foi alcançado quando verificamos que o certificado digital para assinatura digital terá natureza jurídica de serviço notarial quando conferir presunção de legitimidade quanto a autoria do documento eletrônico. Neste passo, a regra de competência privativa material fixada no artigo 236 da CF, quanto à prestação do serviço notarial, deve ser a aplicada a atividade de certificação digital para assinatura digital. Por outro, se verificarmos que o certificado digital para assinatura digital apenas assevera a autoria do documento eletrônico, sem conferir presunção de legitimidade, a natureza jurídica de serviço notarial da atividade de certificação digital para assinatura digital fica excluída, e a aplicação da norma do artigo 236 da CF é inadequada.

Dessa forma, foi possível averiguar que a competência material para o desenvolvimento da atividade de certificação digital dependerá da função do certificado: conferindo presunção de legitimidade quanto a autoria do documento eletrônico ou não. A aplicação das regras de competência previstas no artigo 236 da CF dependerá diretamente desta questão. Os Tabelionatos serão competentes para desenvolver a atividade de certificação digital quando o certificado digital assegurar presunção de legitimidade quanto a autoria do documento eletrônico por meio da assinatura digital. Caso esta condição não esteja presente, a norma de competência fixada no artigo 236 da CF não se aplica ao caso.

A segunda vertente, de caráter tecnológico, consistiu na análise dos principais aspectos dos problemas enfrentados pela tecnologia utilizada na realização da assinatura digital. Entre outros recursos técnicos, a realização de uma assinatura digital requer a utilização do algoritmo criptográfico de função *hash*. Com a evolução tecnológica, tais recursos podem perder sua confiabilidade.

O objetivo tecnológico foi alcançado quando foi verificado que os algoritmos de função *hash* adotados pela ICP-Brasil na realização das assinaturas digitais sofreram ataques computacionais bem sucedidos que comprometeram sua segurança

A principal funcionalidade dos algoritmos de função *hash* consiste em manter a integridade do documento assinado digitalmente. A ICP-Brasil expressamente adotou dois tipos de algoritmos de função *hash*, o MD5 e o SHA-1. Em 2004, foram encontradas colisões no MD5 capazes de produzir assinaturas digitais forjadas, inviabilizando com isso o seu uso para fins de assinatura digital, o que levou a ICP-Brasil, em 2006, abandoná-lo. Ao mesmo tempo, foram encontradas colisões também no SHA-1, todavia, tais colisões ainda não foram consideradas suficientes para inviabilizar o seu uso.

Com isso, os documentos eletrônicos assinados digitalmente não podem ser considerados instrumentos totalmente seguros com o passar dos tempos, ainda mais quando se faz uma análise diante de uma das principais características dos documentos em geral, qual seja, a integridade segura da informação. Esta é uma falha que deve ser corrigida com o trabalho paralelo entre a Tecnologia e o Direito.

8.2 Contribuições

O desenvolvimento das relações humanas através dos novos canais de informação, como a Internet, representa um grande passo para a interação social.

Entretanto, a maioria das relações sociais dependem de regras legais para se desenvolverem. Entre essas relações podemos citar o uso de documentos eletrônicos. A força jurídica probante dos documentos eletrônicos depende da utilização de técnicas que lhe garantam a integridade e a autenticidade. Uma das técnicas mais utilizadas pelo mundo, para a obtenção da autenticidade dos documentos eletrônicos denomina-se certificação digital.

Desta sorte, temos que a tecnologia também trabalha para que as normas jurídicas de bem estar social estejam presentes nos novos canais de informação.

A contribuição apresentada para a ciência jurídica consiste no desenvolvimento dos estudos jurídicos da certificação digital, uma vez que, na atualidade, este trabalho é pouco realizado. A fixação da natureza jurídica da certificação digital para assinaturas digitais segundo seu aspecto funcional de conferir ou não presunção de legitimidade aos documentos eletrônicos, contribui para a legitimação de suas regras e procedimentos técnicos. Diante disso, a MP2.200-2/01 será considerada inconstitucional e a atual ICP-Brasil será considerada ilegítima se considerarmos que o certificado digital para assinaturas digitais confere presunção de legitimidade quanto a autoria do documento eletrônico, por não respeitar a regra do artigo 236 da CF. Caso o certificado digital para assinatura digital apenas asseverar a autoria do documento eletrônico sem presunção de legitimidade não teremos a inconstitucionalidade da MP 2.200-2/01, assim como não teremos a ilegitimidade da atual ICP-Brasil diante da regra do artigo 236 da CF.

Para a ciência tecnológica, a contribuição apresentada corresponde na análise dos principais aspectos dos problemas encontrados com a quebra dos algoritmos de função *hash* utilizados para a realização das assinaturas digitais. Tem-se que a ICP-Brasil adotando algoritmos de função de *hash* que já foram quebrados, acaba por assegurar valor jurídico a um documento eletrônico que pode ser forjado sem deixar evidências.

8.3 Conclusões

Diante de todo o exposto, podemos concluir que:
Sob o aspecto jurídico

- A Infra-estrutura de Chaves Públicas do Brasil consiste num conjunto de regras e procedimentos técnicos voltados à atividade pública de certificação digital. A Autoridade Certificadora Raiz consiste no órgão administrativo máximo na atual ICP-Brasil. Esta função é desenvolvida pelo Instituto Nacional de Tecnologia da Informação, autarquia federal vinculada à Casa Civil da Presidência da República. O órgão político máximo da ICP-Brasil é o Comitê Gestor, também vinculado a Casa Civil da Presidência da República, responsável pelo emissão das regras técnicas voltadas a prestação do serviço público de certificação digital. A ICP-Brasil ainda é formada pelas Autoridades Certificadoras Subseqüentes e pelas Autoridades de Registro, responsáveis pela emissão do certificado digital ao usuário final.;
- No atual ordenamento jurídico brasileiro, a aceitação dos documentos eletrônicos como fonte de relações sócio-jurídicas depende da garantia de autenticidade e integridade;
- A assinatura digital consegue assegurar a integridade, todavia para assegurar a autenticidade dos documentos eletrônicos na sistemática jurídica, depende intrinsecamente dos certificados digitais;
- A certificação digital consiste numa atividade pública ou privada prestada por uma terceira pessoa, cuja finalidade é de asseverar a autoria dos documentos eletrônicos por meio da assinatura digital certificada digitalmente;
- A natureza jurídica da atividade de certificação digital para assinatura digital variará de acordo com a funcionalidade do certificado digital: se o certificado digital conferir presunção de legitimidade quanto a autoria do documento eletrônico assinado digitalmente, a atividade de certificação digital será considerada serviço notarial e deverá respeitar as regras de competência determinadas no artigo 236 da CF; por outro lado, se o certificado digital apenas asseverar a autoria do documento eletrônico assinado digitalmente,

sem conferir presunção de legitimidade, não deverá ser aplicada a regra de competência do artigo 236 da CF à atividade de certificação digital;

- A Medida Provisória 2.200-2/01 será considerada inconstitucional, e a ICP-Brasil será considerada ilegítima, se a atividade de certificação digital possuir natureza jurídica de serviço notarial.

Sob o aspecto tecnológico:

- Os algoritmos de função *hash*, como por exemplo, o MD5 e o SHA-1, são utilizados na assinatura digital para assegurar a integridade dos documentos eletrônicos;
- Em 2004, o MD5 foi quebrado, possibilitando a realização de assinaturas digitais forjadas;
- Em 2004, algumas fragilidades foram encontradas no SHA-1, entretanto não eram suficientes para inviabilizar o seu uso para assinaturas digitais;
- A ICP-Brasil, adotou até maio de 2006 dois algoritmos de função *hash*, o MD5 e o SHA-1. Todavia após essa data, somente o SHA-1 é expressamente adotado;
- No Brasil, em razão da expressa previsão da ICP-Brasil, as assinaturas digitais realizadas com o algoritmo de função *hash* MD5 até maio de 2006 possuem valor jurídico, entretanto, com a quebra desse algoritmo em 2004, essas assinaturas podem ser perfeitamente forjadas sem deixar vestígios e continuando a ter valor jurídico.

8.4 Trabalhos Futuros

Vários são os trabalhos futuros que podem acrescer do presente estudo.

Inicialmente temos o estudo jurídico da certificação digital partindo-se de um aspecto formal.

Um outro trabalho consiste no estudo das várias formas que uma Infra-estrutura de Chaves Pública poderá tomar diante das ponderações sobre a natureza jurídica da certificação digital para assinaturas digitais.

Temos ainda a proposta técnico-jurídica de um sistema capaz de assegurar a integridade perpétua dos documentos eletrônicos assinados digitalmente diante da quebra dos algoritmos criptográficos de função *hash* ocorrido diante da evolução da sociedade.

Vale ressaltar, por fim, que a atual Infra-estrutura de Chaves Públicas do Brasil deve ser totalmente aproveitada quando da realização destes futuros estudos, tendo em vista os investimentos já realizados.

Bibliografia

ALMEIDA. Fernanda Dias Menezes. Competências na Constituição de 1988. 3ª. edição. São Paulo. Editora Atlas. 2005.

ANTUNES, Luciana Rodrigues. Introdução ao direito notarial e Registral. Jus Navegandi, Teresina, ano 9, n.º 691, 27 de maio de 2005. Disponível em <http://jus2.uol.com.br/doutrina/texto.asp?id=6765>. Acesso em 11 dez. 2006.

ARAÚJO, Edmir Netto de. Curso de Direito Administrativo. Editora Saraiva. São Paulo. 2005.

BEDAQUE, José Roberto dos Santos. Efetividade do Processo e Técnica Processual: Tentativa de Compatibilização. Tese apresentada ao Concurso para o cargo de Professor Titular de Direito Processual Civil da Faculdade de Direito da Universidade de São Paulo. 2005

BARRETO, Paulo S. L. M. *A Crise das Funções de HASH*. In: Simpósio de Segurança em Informática (SSI2005) – Palestrante Convidado. ITA/CTA, São José dos Campos: 2005.

BARRETO, **Paulo S. L. M**. *The Hashing Function Lounge*. Disponível em http://paginas.terra.com.br/informatica/paulobarreto/hflounge.html. Acessado em 21/11/2006.

BLUM. Renato M. S. Opice. Direito eletrônico. A Internet e os tribunais. Texto: O processo eletrônico: assinaturas, provas, documentos e instrumentos digitais. Coordenador: Renato M. S. Opice Blum. Editora Edipro. 1.º edição. 2001

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasilia. DF.: Senado 1988.

BRASIL. Decreto-lei 2.848, de 12 de Julho de 1940. Código Penal. Ministério da Justiça. Diário Oficial de 31 de dezembro de 1940. P. 2391.

BRASIL. Decreto-lei 3.689, de 10 de março de 1941. Código de Processo Penal. Ministério da Justiça. Diário Oficial de 13 de Outubro de 1941. P 19699.

BRASIL. Instituto Nacional de Tecnologia da Informação – ITI. Padrões e Algoritmos criptográficos. DOC-ICP 01.01, de 18 de Maio de 2006.

BRASIL. Lei Ordinária 10.406, de 01 de Outubro de 2002. Código Civil. Ministério da Justiça. Diário Oficial da União de 11 de Janeiro de 2003. P 1.

BRASIL. Lei Ordinária n.º 5.869 de 01 de Novembro de 1973. Código de Processo Civil. Ministério da Justiça. Diário Oficial de 17 de Janeiro de 1.973. P1.

BRASIL. Medida Provisória 2.200-2/01. 24 de Agosto de 2001. Institui a Infra-estrutura de Chaves P~ublicas do Brasil – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em Autarquia e dá outras providências. Diário Oficial da União. Poder Executivo. Brasilia, DF, 27 de Agosto de 2001.

BRASIL. Projeto de lei 1.483, de 12 de Agosto de 1999. Instituti a Fatura eletrônica e a assinatura digital nas transações de comércio eletrônico. Câmara dos Deputados Federal. Brasilia. DF 1999.

BRASIL. Projeto de lei 1.589/99, de 31 de Agosto de 1999. Dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital e dá outras providências. Câmara dos Deputados Federal. Brasília. DF. 1999.

BRUNO. Gilberto Marques. In O comerciante virtual e a tendência mundial de uniformização da legislação – II. Disponível em: http://www.direitonaweb.com.br/colunista.asp?l=gilberto&ctd=412 , acessado em 21 de abril de 2.004.

CASTRO, Aldemário Araújo. "*O documento eletrônico e a assinatura digital. Uma visão Geral.*" Revista de Direito Eletrônico. Publicação Oficial do Instituto de Direito Eletrônico. Ano I. Número 1. Junho à Agosto de 2.003. Pág. 06. Disponível em: http://www.ibde.org.br/revista/index_archivos/rede_ix.pdf . Acesso em 18 de Outubro de 2006.

CARVALHO FILHO; José dos Santos. Manual de Direito Administrativo. Editora Freitas Bastos. Rio de Janeiro. 1997.

CENEVIVA. Walter. Lei dos notários e registradores comentada (Lei n.º 8.935/94). 4ª. Edição. Editora Saraiva. São Paulo, 2002

COLÔMBIA. Lei 527, de 18 de Agosto de 1999. Por meio do qual se define e regulamenta o acesso e uso das mensagens de dados, do comércio eletrônico e das assinaturas digitais, e se estabelecem entidades de certificação e dá outras disposições. Congresso Colombiano.

Comitê Gestor. Infra-estrutura de Chaves Públicas. Aprova a Declaração de Práticas de Certificação da AC-Raiz da ICP-Brasil. Resolução n.º 1, 25 de Setembro de 2001. Brasília (DF).

Comitê Gestor. Infra-estrutura de Chaves Públicas. Aprova os requisitos mínimos para políticas de certificado na ICP-Brasil. Resolução n.º 7, 12 de Dezembro de 2001. Brasília (DF). 29 p.

COSTA, Marcos da. In *"A ICP-Brasil e os documentos eletrônicos."* Caderno Jurídico da Escola Superior do Ministério Público de São Paulo. Direito e Internet. Ano II – n.º IV – Julho de 2002.

COSTA, Marcos da. MARCACINI, Augusto Tavares Rosa. Direito em Bits. São Paulo. Editora Fiúza. 2004.

CRETELLA JUNIOR, José. Administração indireta brasileira: autarquias, concessionárias, subconcessionárias. 1ª. edição. Rio de Janeiro. Editora Forense. 1980. Pág. 50.

CRETELLA JUNIOR, José. Do Ato administrativo. São Paulo. Editora Bushatsky, 1977.

CUSTÓDIO, Ricardo Felipe. Análise Crítica da ICP-Brasil: Resposta a Consulta Pública. Laboratório de Segurança da Computação (LABSEC), UFSC. Florianópolis, 2001.

CUSTÓDIO. Ricardo F.. DIAS. Júlio S.. ROLT. Carlos R.. Texto: Assinatura Confiável de Documentos Eletrônicos. in Confiança no uso de documentos eletrônicos. BRy Tecnologia S.A. Laboratório de Segurança em Computação – LABSEC – UFSC. Laboratório de Tecnologia de Gestão – LABGES – UDESC. Florianópolis. Agosto de 2003.

Diretiva 1999/1993/CE do Parlamento Europeu e do Conselho, de 13 de Dezembro do 1999, relativa a um quadro legal comunitário para as assinaturas eletrônicas.

FERNANDES, Antonio Scarance. Processo Penal Constitucional. 3ª edição. São Paulo: Ed. Revista dos Tribunais, 2002.

FERNANDES, Murilo Rivau. SIPEX: Uma proposta de modelo de política de assinatura. 2006. 100p. (Dissertação de Mestrado). Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos. São Paulo. 2006.

FERRARI, Eduardo Reale. A Excepcionalidade da Prova Ilícita no Processo Penal Brasileiro. Dissertação apresentada a Pontifícia Universidade Católica de São Paulo para a obtenção do Título de Mestre em Direito. São Paulo. 2004. Pág 12.

FREITAS, Vinícius Pimentel de Freitas. LOEBENS, João Carlos. Contratos eletrônicos e o Comércio Internacional. VIII Seminário Internacional de la Federación Internacional de antiguos alumnos del I.N.A.P. de España. Toledo. Agosto de 2004

KELSEN, Hans. Teoria Geral do Direito e do Estado. 3ª. edição. São Paulo. Editora Martins Fontes. 2000.

KIM, Jongsung. BIRYUKOV, Alex. PRENEEL, Bart. LEE, Sangjin. On the Security of Encryption Modes of MD4, MD5 and HAVAL.Katholieke Universiteit Leuven. ESAT/SCD-COSIC Kasteelpark Arenberg 10, B-3001 (Belgium). Center for Information Security Technologies (CIST) (Korea).

KLIMA, Vlastimil. Finding MD5 Collisions – a Toy For a Notebook. Prague, Czech Republic. 05 de Março de 2005.

KÜMPEL.Vitor Frederico. Direito Civil 3. Direito dos Contratos. Coleção Cursos e Concursos. Editora Saraiva. São Paulo. 2005.

MARCACINI, Augusto Tavares Rosa. Direito e Informática. Uma abordagem jurídica sobre criptografia. 1ª. Edição. Rio de Janeiro. Editora Forense. 2002.

MARCACINI. Augusto Tavares Rosa. "Certificação eletrônica, sem mitos e sem mistérios". Revista do Advogado. "Internet". Publicada pela Associação dos Advogados de São Paulo. Ano XXIII, n.º 69. Maio de 2003.

MEDAUAR. Odete. Direito Administrativo Moderno. 10ª. Edição. Editora RT. São Paulo. 2006. Pág. 2006.

MEIRELLES, Hely Lopes. Direito Administrativo Brasileiro. 24ª. edição. São Paulo. Editora Malheiros. 1999

MELLO, Celso Antônio Bandeira de. Curso de Direito Administrativo. 17ª. edição. São Paulo. Editora Malheiros. 2004.

MENKE, Fabiano. Assinatura Eletrônica no Direito Brasileiro. Editora RT. São Paulo. 2005.

MITTERMAIER, C.J.A. Tratado da Prova em Matéria Criminal. 2.ed. Campinas: Bookseller, 1997.

MORAES, Alexandre de. Direito Constitucional. 13.º edição. São Paulo. Editora Atlas, 2003.

MORAES, Alexandre. Et al. Agências Reguladoras. Editora Atlas. São Paulo. 2002.

MOREIRA NETO. Diogo de Figueiredo. Curso de Direito Administrativo. 14ª. edição. Rio de Janeiro. Editora Forense. 2005.

PERU. Lei 27.269, de 26 de Maio de 2000. Lei de Assinaturas e certificados digitais. Congresso da República.

PIETRO, Maria Sylvia Zanella Di. Direito Administrativo. 13ª. edição. São Paulo. Editora Atlas. 2001.

PORTO, Luiz Guilherme Moreira. Tipicidade nos crimes de falsidade documental em face do bem jurídica protegido. 2002. 203p. Dissertação de Mestrado. Faculdade de Direito. Universidade de São Paulo. São Paulo. 2002.

RANGEL. Paulo. Direito Processual Penal. 6ª. Edição. Rio de Janeiro. Editora Lumen Júris. 2002.

REALE, Miguel. Filosofia do direito. 20ª. edição. São Paulo. Editora Saraiva. 2002.

REZENDE, Afonso Celso F. Tabelionato de Notas e o notário perfeito. 4ª. Edição. Editora Millennium. Campinas (SP). 2006.

ROSA, **José Manuel**.**Lucena** Comercio electrónico. Seminario Escuela Superior de Cajas de Ahorros, 1997, 24 y 25 Octubre. MADRID.1997.

ROVER, Aires José; VEIGA, Luiz Adolfo Olsen da. In *"Validade jurídica de documentos eletrônicos assinados com infra-estruturas diferentes da ICP-Brasil.*

2003. Disponível em: http://www.buscalegis.ufsc.br/arquivos/artigoairesolsenbuscalegis.pdf . Acessado em 18 de Outubro de 2006.

SANTOS. Moacyr Amaral. Primeiras Linhas de Direito Processual Civil. Editora Saraiva. 18ª. Edição. São Paulo. 1997.

SERPRO – Serviço Federal de Processamento de Dados. Política de Segurança. Declaração de Práticas de Certificação da Autoridade Certificadora do SERPRO. Brasília (DF). Disponível em: https://thor.serpro.gov.br/ACSERPRO , acessado em 28 de Novembro de 2005.

SILVA, José Afonso. Curso de Direito Constitucional Positivo. 19ª. edição. São Paulo. Editora Malheiros. 2000.

SILVESTRE, Fábio André Chedid. A ilegitimidade constitucional crítica da Infra-estrutura de Chaves Públicas Brasileira. Uma Semiótica do Poder.2003. 111 p. Dissertação de Mestrado. Universidade Federal de Santa Catarina. Programa de Pós-Graduação. Engenharia de Produção e Sistemas. Florianópolis (SC). 2003.

STEVENS, Marc. Fast Collision Attack on MD5. Department of Mathematics and Computer Science, Eindhoven University of Technology. The Netherlends.

TUCCI. José Rogério Cruz e. Direito e Internet. Texto: Eficácia Probatória dos Contratos celebrados pela Internet. Coordenadores: Newton de Lucca e Adalberto Simão Filho. Editora Edipro. 1.º edição. 2000. Bauru – SP.

UNCITRAL. Electronic Signatures Draft Guide to Enactment of the UNCITRAL. Model Law on Electronic Signatures. Thirty-eighth session, New York, março de 2001.

VALLE. J. Rodrigues. Curso de Direito Administrativo. 2ª. Edição. A. Coelho Branco Fº (editor). Rio de Janeiro. 1941

VASCONCELLOS, José Mattos de. Direito Administrativo. Vol. I. Imprensa Oficial. Rio de Janeiro. 1936.

XIAOYAN, Wang. DENGGUO, Feng. XUEJIA, Lai. HONGBO, Yu. Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. The School of Mathematics and System Science, Shandong University, Jinan250100, China. Institute of Software, Chinese Academy of Sciences, Beijing100080, China. Dept. of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai, China. 17 de Agosto de 2004.

XIAOYUN, Wang. HONGBO, Yu. How to break MD5 and other hash functions. Shandong University, Jinan 250100, China.