UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

FRANCISCO CÉSAR GONÇALVES DA SILVA FILHO

A CERTIFICAÇÃO DIGITAL COMO MECANISMO DE MANUTENÇÃO DA SEGURANÇA JURÍDICA NOS CONTRATOS FIRMADOS VIA INTERNET NO BRASIL

FORTALEZA
2012

FRANCISCO CÉSAR GONÇALVES DA SILVA FILHO

A CERTIFICAÇÃO DIGITAL COMO MECANISMO DE MANUTENÇÃO DA SEGURANÇA JURÍDICA NOS CONTRATOS FIRMADOS VIA INTERNET NO BRASIL

Trabalho de Conclusão de Curso submetido à Faculdade de Direito da Universidade Federal do Ceará, como requisito parcial para obtenção do grau de Bacharel em Direito.
Área de concentração: Direito Civil.
Orientador: Prof. Dr. Regnoberto Marques de Melo Júnior.

FORTALEZA

2012

FRANCISCO CÉSAR GONÇALVES DA SILVA FILHO

A CERTIFICAÇÃO DIGITAL COMO MECANISMO DE MANUTENÇÃO DA SEGURANÇA JURÍDICA NOS CONTRATOS FIRMADOS VIA INTERNET NO BRASIL

Trabalho de Conclusão de Curso submetido à Faculdade de Direito da Universidade Federal do Ceará, como requisito parcial para obtenção do grau de Bacharel em Direito em conformidade com os atos normativos do MEC e do Regulamento de Monografia Jurídica aprovado pelo Conselho Departamental da Faculdade de Direito da UFC. Área de concentração: Direito Civil.

Aprovada em: 08/06/2012

BANCA EXAMINADORA

_____

Prof. Dr. Regnoberto Marques de Melo Júnior (Orientador)
Universidade Federal do Ceará - UFC

_____

Prof. Dr. Hugo de Brito Machado Segundo
Universidade Federal do Ceará - UFC

_____

Eric de Moraes e Dantas
Mestrando em Direito da Universidade Federal do Ceará - UFC

“Nem só de pão vive o homem...”

“Trololololololololololo”
Eduard Khil

“Comece fazendo o que é necessário; depois, faça o que for preciso e, de repente, você estará fazendo o impossível.”
São Francisco de Assis

AGRADECIMENTOS

Primeiramente, agradeço a Deus pelo dom da vida, qualidades, virtudes e defeitos, pois acredito que existe um caminho traçado para todos e minha chegada a este momento representa o fim de uma jornada para o começo de outra, ainda mais desafiante.

Agradeço aos meus pais pelas excelentes oportunidades de estudo, pela dedicação investida em mim e pelo constante apoio para que eu pudesse extrair o máximo das oportunidades da vida.

Agradeço ao meu pai, Francisco César Gonçalves da Silva, pelo amor constante, confiança e conselhos sempre valiosos, mostrando que nunca estive sozinho nesta minha caminhada rumo ao sucesso.

Agradeço minha mãe, Antonia Paiva da Silva, pelo suporte, ajuda e auxílio sempre prestados, dando-me esperanças para prosseguir e confiar no meu potencial.

Agradeço às minhas irmãs, Tamara e Terezinha, que sempre me ajudaram no que foi preciso e sempre foram refúgios em conversas tranquilizantes, motivadoras e divertidas.

Aos meus colegas, inúmeros, José Lívio, Jonas Amster, Yuri Amorim, Pollyana Torres, Jéssica Teles, Rossana Wellyn, Mariana Holanda, Camila Gonçalves, Sarah Marinho e todos os demais que a limitação das linhas não me permite citar no momento, estou agradecido a Deus por tê-los colocados em meu caminho.

Aos meus colegas de Centro Acadêmico, gestão Edificando Conquistas (2008-2009), oportunidade única de crescimento e de trabalho em equipe, que rendeu, certamente, uma das gestões mais profissionais e vitoriosas da história do CACB.

À Livraria Fortlivros, na pessoa de Jothe Frota, pelos momentos de confraternização, estudo, pesquisa e, especialmente, pela oportunidade de conhecer inúmeras pessoas e fazer vários amigos.

Finalmente, ao Professor Dr. Regnoberto Marques de Melo Júnior, que sempre muito confiou neste trabalho e me incentivou com valiosas lições aqui empregadas.

RESUMO

Esta monografia visa tratar de um instrumento ainda pouco difundido academicamente, mas que, com o crescimento das relações contratuais via Internet, se torna cada vez mais necessário: a Certificação Digital. A popularização da Internet como meio de concretização de transações comerciais, especialmente através dos sítios de *e-commerce*, faz com que este instrumento seja cada vez mais necessário para garantir a legitimidade e veracidade das informações trocadas. Neste trabalho, busca-se demonstrar os benefícios da utilização da certificação digital como forma de legitimar a prova, adaptando-a aos moldes exigidos pelo Código Civil Brasileiro, protegendo ambas as partes contratantes, sobretudo em razão das fraudes tecnológicas e dos vícios do negócio jurídico, garantindo a necessária segurança jurídica que qualquer indivíduo precisa ter ao realizar uma negociação via Internet. Nesse diapasão é que se faz necessária a identificação eletrônica das partes negociantes, de modo a garantir que o indivíduo com quem se poderia realizar o negócio jurídico é realmente quem diz ser quem é, se possui endereço físico e se possui condições de arcar com a negociação entabulada, estabelecendo, por fim, caso necessário, elementos mínimos de identificação em caso de não cumprimento do negócio jurídico para o acionamento do Poder Judiciário para cobrar o adimplemento da obrigação contratual.

Palavras-chave: Internet. Certificação Digital. Contrato. Prova. Documento. Segurança Jurídica. Comércio Eletrônico.

ABSTRACT

This paper intends to deal with an academically low broadcasted instrument which due the growth of contractual negotiations over the Internet becomes essential: Digital Certification. The popularization of the Internet as a way of sealing commercial transactions, specially through e-commerce websites, make this instrument even more necessary to assure legitimacy and veracity of exchanged information. This paper also intends to demonstrate the benefits of the use of digital certification as way of legitimate judicial proof, bring it accordingly as demanded by the Brazilian Civil Code, protecting contracting parts, mostly due technological frauds and contentment and social defects, reassuring properly security which every individual must have when performing a virtual negotiation. In this line of thought, it is necessary the identification contractual parts allowing both of the to be sure that the individual with whom they negotiate is who he claims to be, if he has a physical address and if he has means of fulfill the contract. At least it is established, in case of need, minimum set of elements of identification to present a petition and go to Court requiring the due performance of the contract.

Keywords: Internet. Digital Certification. Contract. Proof. Documento. *E-commerce*.

SUMÁRIO

1. INTRODUÇÃO

O Brasil experimentou nos últimos anos um crescimento vertiginoso das conexões com a Internet, do número total de usuários e da qualidade e da velocidade da conexão. Sobre esse aspecto, abriu-se a um número exponencialmente grande de consumidores a possibilidade de realizar inúmeros serviços na comodidade de sua residência.

Uma pesquisa da empresa publicitária F/Nazca[1], realizada em 2010, apontou que 54% da população brasileira com mais de 12 anos de idade possuía acesso à Internet e que, desse total, correspondente a cerca de 81 milhões de pessoas, 23% costumavam fazer compras *online*, em média, 4,2 vezes ao ano. Por outro lado, os 77% dos internautas que não compravam via Internet não o faziam por receio de não receber a mercadoria ou de não receber o produto no prazo avençado.

Mesmo assim, o crescimento do vulto negociado pelos sítios de *e-commerce* cresce ano a ano. No ano de 2009, o crescimento do faturamento das lojas de venda via Internet cresceu 30%, ultrapassando a marca de R$ 10 bilhões de reais negociados[2]. A tendência se matinha para 2010, oportunidade em que o setor planejava crescer mais de 40% em relação ao ano anterior[3]. E a tendência é o crescimento ainda maior, posto que mais de 86% dos consumidores virtuais se dizem satisfeitos com o serviço, conforme pesquisa do "e-bit" em parceria com o Movimento Internet Segura (MIS)[4].

---

[1] Brasil tem 81,3 milhões de internautas em ação. **Portal da agência F/Nazca**. São Paulo, 29 nov. 2010. Disponível em http://www.fnazca.com.br/index.php/2010/11/29/brasil-tem-813-milhoes-de-internautas-em-acao/ Acesso em 08 set. 2011.

[2] Vendas pela internet movimentam R$ 10,6 bi em 2009 e crescem 30%. **Portal Folha Online.** São Paulo, 16 mar. 2010. Disponível em http://www1.folha.uol.com.br/folha/dinheiro/ult91u707493.shtml. Acesso em 08 set. 2011.

[3] Lojas online preveem crescer 40% e faturar R$ 2,2 bi no Natal. **Portal de Economia do IG.** São Paulo, 18 nov. 2010. Disponível em http://economia.ig.com.br/empresas/comercioservicos/lojas+online+preveem+crescer+40+e+faturar+r+22+bi+no+natal/n1237830083237.html. Acesso em 08 set. 2011.

[4] Aprovação de comércio eletrônico chega a 86,3% no Brasil **Portal da Revista Galileu.** Disponível em http://revistagalileu.globo.com/Revista/Common/0,,EMI119934-17770,00-APROVACAO+DE+COMERCIO+ELETRONICO+CHEGA+A+NO+BRASIL.html. Acesso em 08 set. 2011.

É como explica PINHEIRO (2009, p. 1), *in verbis:*

> O cotidiano do mundo jurídico resumia-se a papéis, burocracia e prazos. Com as mudanças ocorridas desde então, ingressamos na era do tempo real, do deslocamento virtual dos negócios, da quebra de paradigmas. (...) O direito também é influenciado por essa nova realidade. A dinâmica da era da informação exige uma mudança mais profunda na própria forma como o Direito é exercido e pensado em sua prática cotidiana.

Um campo tão propício ao crescimento fica também exposto ao risco das fraudes eletrônicas que não podem ser deixadas de lado pelo Direito. Se levarmos em consideração que os valores apontados acima se referem apenas às negociações virtuais concretizadas legalmente, com o pagamento de todos os tributos legalmente devidos, sem entrar na conta as negociações do mercado cinza, sites de leilões, compras coletivas e sites de intermediação fornecedor-consumidor também se pode observar que a Internet ainda tem muito o que melhorar em confiabilidade especialmente para os consumidores.

A certificação digital, instituída pela Medida Provisória nº 2.200-2 de 24 de agosto de 2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira, foi um marco importantíssimo para que o país passasse a contar com mecanismos mais eficientes para a identificação dos indivíduos eletronicamente, zelando pela segurança dos dados que trafegam pela Internet.

Percebe-se que a preocupação estatal com a veracidade das informações prestadas via Internet é crescente. A partir do ano de 2010, através da Instrução Normativa nº 969/2009, a Receita Federal do Brasil passou a exigir certificação digital para a entrega de declarações para as pessoas jurídicas não optantes do "Simples"[5].

Infelizmente, a certificação digital ou assinatura eletrônica[6] ainda não se incorporou ao cotidiano das pessoas. Entretanto, a vida de "pessoas comuns" sem o

---

[5] BRASIL. Receita Federal do Brasil. **Instrução Normativa 969/2009**. Disponível em http://www.receita.fazenda.gov.br/legislacao/ins/2009/in9692009.htm. Acesso em 08 set. 2011.

[6] A assinatura digital é o ato do usuário decorrente da obtenção do certificado digital, através do qual o portador deste certificado afirma que determinado documento é autêntico. O certificado digital é a "marca" concedida pela Autoridade Certificadora que permite que o usuário assine digitalmente documentos com fé pública. Trata-se de uma relação instrumento-ato: o instrumento é a certificação digital e o ato é a assinatura digital. Analogicamente explicando, é como o carimbo (certificado digital) e a estampa por ele produzida (assinatura digital). Apesar dessa diferença terminológica, neste

certificado digital pode estar nos seus últimos dias, pois a nova identidade pessoal de cada brasileiro terá a assinatura eletrônica e alguns municípios brasileiros iniciaram o projeto piloto em 2011[7]. Como se vê, é crescente a preocupação com a segurança dos dados transmitidos e, à longo prazo, a exigência será benéfica para os cidadãos, vez que as empresas não precisarão exigir o pagamento de valor tão alto de juros nem arcarão com tantos custos junto às seguradoras, pois terão uma mínima certeza de seu crédito, conforme se explicará neste trabalho.

O que se apercebe é que o panorama atual não poderia perdurar. Se não se resta dúvida de que as transações comerciais realizadas via Internet são regidas pela legislação já existente, como o Código de Defesa do Consumidor e o Código Civil, o mesmo não se poderia dizer dos documentos gerados *online*, comumente utilizados como meio de prova judicial e extrajudicialmente.

Tais documentos são facilmente adulteráveis, podendo servir como meio escuso para a obtenção de provimento judicial injusto. Todavia, até o momento, os documentos digitais possuem presunção *juris tantum* de sua veracidade (assim como qualquer outro), mas que, muitas vezes, não podem ter sua inalterabilidade comprovada[8], em caso de ser levantada sua falsidade, em razão de, por exemplo, o documento não estar mais disponível para exibição.

Neste ponto surge a insegurança jurídica das partes: o documento pode ter sido adulterado, mas não se pode comprovar que tal falsificação ocorreu; o comprador disse que era “X”, quando, na verdade, era “Y”; vendas pagas com cartões de crédito dos quais o comprador não é o titular e outras situações conhecidas do dia-a-dia dos operadores do Direito.

O certificado digital aqui se apresenta como ferramenta capaz de solucionar essa equação: a função de transformar um documento qualquer gerado na Internet, em um documento público, a favor do qual milita a presunção de

---

trabalho se usam os termos certificado digital e assinatura digital, bem como suas variações, como sinônimos para facilitação da compreensão do leitor.

[7] Nova identidade do brasileiro terá certificação digital. **Portal IDG Now!** São Paulo, 16 set. 2010. Disponível em http://idgnow.uol.com.br/seguranca/2010/09/16/nova-identidade-do-brasileiro-tera-certificacao-digital/. Acesso em 08 set. 2011.

[8] Se possível fosse a descoberta de alteração nos documentos gerados eletronicamente, estaríamos, em tese, diante de um caso do crime de falsidade ideológica ou material, capitulados no Código Penal Brasileiro.

veracidade, desde que assinado digitalmente, efetivando maior segurança jurídica para as partes intervenientes em dada relação jurídica.

Para tanto, trabalharemos os conceitos de documento, analisando-o especialmente sobre o aspecto do documento eletrônico e de certificação digital, suas implicações ao conceito de documento e ao princípio da segurança jurídica.

Através dessa demonstração, os contratos firmados via Internet, desde que certificados digitalmente, estariam resguardados das comuns fraudes nas relações virtuais, especialmente no que se refere à identificação das partes, às informações de pagamento e à execução forçada do pacto, quando necessário.

2. DO CONCEITO DE DOCUMENTO

Documento é toda coisa que possa representar a realização de um fato, ou seja, é todo instrumento que, com símbolos, imagens e outros caracteres representativos, possam demonstrar a ocorrência de fatos.

DIDIER JR. (*et alii*, 2009, p. 147) indicam como elementos constituintes do documento os seguintes aspectos: autoria, conteúdo e suporte.

A autoria deve ser analisada no enfoque material (quem produziu a representação de fato contida) e intelectual (sob ordens de quem o documento foi produzido); o conteúdo, como sendo exatamente a representação de algum fato; e o suporte, definido, simplificadamente, como o meio pelo qual a representação de um fato foi armazenada (papel, DVD, CD, *USB Flash Drive...)*

As formas que o documento pode assumir são inúmeras, apesar de, especialmente aqui no Brasil, a palavra “documento” ser imediatamente relacionada com papeis escritos. Na verdade, em razão da ampla gama de elementos que podem representar a realização de um fato, o documento pode assumir diversos aspectos, sem que se descaracterize seu núcleo fundamental (representação de um fato), como CDs, DVDs, fotos, vídeos, gravações sonoras, páginas impressas da Internet, e-mails...

O documento eletrônico, em tese, não se amolda ao conceito tradicional de documento, porém, mesmo não sendo “coisa”, não se pode negar seu elemento de registro de fatos em razão da atividade humana voluntária.

O documento gerado virtualmente, por poder ser armazenado em diversas fontes, com possibilidade de realização de *backups* preventivos, melhor serve à função de prova, como assevera DIDIER JR. (*et alii*, 2009, p. 145):

> Justamente por ter aptidão para representar um fato de modo permanente e duradouro, sem se perder nas armadilhas do tempo, o documento é considerado uma fonte segura de prova. Essa sua segurança se reflete na importância que se dá, normalmente, na experiência forense, à prova documental. Também se reflete na importância que o próprio legislador, até mesmo historicamente, passou a dar-lhe, sobretudo quando se tratasse de prova documental produzida por órgão público.

O próprio Código Civil, em seu artigo 225, garantiu ao documento gerado virtualmente validade como meio de prova em qualquer esfera probatória, *verbis*:

> Art. 225. As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão.

Ainda que com a redação claríssima[9], restava a alguns doutrinadores a dúvida sobre a aceitação dos documentos gerados eletronicamente, levando alguns pensadores à exegese conceitual, fazendo-os abstrair da verdadeira função do documento (registrar a existência de um fato), passando a entrar nos pormenores da informática, os quais são absolutamente dispensáveis para a compreensão (e aceitação) dos documentos eletrônicos como meio de prova, como lecionava GICO JR. (1999, p. 15):

> Não encontramos, em texto doutrinário algum, a preocupação de um jurista em saber como o cabeçote do aparelho de videocassete opera em transformação dos registros magnéticos daquela fita cassete em som e imagem. (...) Essas coisas são detalhes técnicos que ao jurista não interessam em sua atividade normal.

Bem caminhou o citado jurista ao fazer esta observação. Jamais os pensadores do Direito se preocuparam com a mecânica do sistema, de entender como um gravador ou como uma impressora funcionam, para verificar que os conteúdos produzidos por esses aparelhos eram verdadeiramente documentos, uma vez que realizavam a representação de fatos. Muito ao contrário, tais documentos foram e, provavelmente, sempre serão aceitos judicialmente, bem como qualquer outro meio de registro que corrobore para a verificação de um fato em juízo.

Nesta toada, bem caminhou o Conselho da Justiça Federal durante a IV Jornada de Direito Civil com o enunciado nº 298:

> Enunciado nº 298/CJF - Arts. 212 e 225: Os arquivos eletrônicos incluem-se no conceito de "reproduções eletrônicas de fatos ou de coisas" do art. 225 do Código Civil, aos quais deve ser aplicado o regime jurídico da prova documental.

[9] Lembra-se aqui do tradicional brocardo "in claris cessat interpretativo", absolutamente inaplicável ao Direito moderno. Tal afirmação encontra respaldo na própria dúvida arguida no corpo do texto referente os documentos eletrônicos.

O citado enunciado garantiu ao documento eletrônico devido valor probatório que lhe deverá ser atribuído, desde que respeite a ressalva trazida pelo enunciado nº 297, também da IV Jornada de Direito Civil, *verbis*:

> Enunciado nº 297/CJF – Art. 212: O documento eletrônico tem valor probante, desde que seja apto a conservar a integridade de seu conteúdo e idôneo a apontar sua
> autoria, independentemente da tecnologia empregada.

O documento eletrônico, dessa forma passa a ser definitivamente aceito juridicamente como fonte de prova, desde que respeite alguns dos caracteres da definição tradicional clássica, como a integridade do registro do fato e da autoria. Destaque-se, por outro lado, que as amarras doutrinárias existentes em relação ao documento eletrônico foram bastante aliviadas, pela leitura da parte final do enunciado nº 297, já citado, que diz “independentemente da tecnologia empregada”, o que já abre espaço para outras tecnologias futuras ainda não descobertas para o homem como meios de registro de fatos.

2.1 O problema do documento eletrônico

Como se viu, para se atribuir valor probatório ao conteúdo de um documento eletrônico, é preciso, nos termos do enunciado nº 297 do Conselho da Justiça Federal, que se possa conservar a integridade de seu conteúdo e garantir quem é o seu autor.

Eis que se gera um grave problema de insegurança jurídica neste ponto. É realmente possível garantir que o documento eletrônico não teve seu conteúdo alterado? É possível garantir de quem se diz autor de tal documento de fato o é? Existem mecanismos capazes de periciar devidamente um documento eletrônico?

A resposta para tais questionamentos é negativa. Não se pode assegurar com absoluta certeza que determinado documento eletrônico, produzido nos moldes atuais, é genuíno. Ele pode conter um vício ou adulteração imperceptível a um leigo, por já ter sido gerado com vícios (falsidade ideológica) ou por ter passado por um processo de falsificação (falsidade material), para que o documento registrasse aquilo que a parte que pretende utilizá-lo deseja ver registrado.

Infelizmente, os aspectos acima mencionados vem passando desapercebidos pelo Poder Judiciário brasileiro. Poucos são os operadores do Direito com um razoável conhecimento de informática que podem ter essas dúvidas em relação à autenticidade de documentos eletrônicos. E mesmo que as tenham, caso seja arguida a falsidade de um documento, quem são os pouquíssimos profissionais habilitados a fazer uma perícia em um documento eletrônico, sem mencionar o preço proibitivo de tal artifício processual?

O Judiciário do Brasil ainda não chegou a esse ponto de maturidade em relação aos documentos eletrônicos, fazendo com estes sejam, costumeira e indevidamente, aceitos indiscriminadamente na via judicial, à despeito do enunciado nº297 do Conselho da Justiça Federal e da segurança jurídica. Pior ainda, tais documentos, verdadeiros ou falsos, estão no limbo em relação ao poder-dever de apreciar livremente as provas do juiz, fazendo com que sejam considerados como autênticos, conforme se revistam da fumaça do bom direito, ou como forjados ou insuficientes, caso o juiz não se convença da verossimilhança das alegações.

Outros países já passaram pelas mudanças conceituais que o Brasil vem passando. Nos Estados Unidos, por vários anos, as provas obtidas por meio de documentos eletrônicos eram proibidas em razão das regras processuais *Hearsay Rule* e *Best Evidence Rule.* Pela primeira regra, um documento não pode ser aceito judicialmente se o autor dele não pode se fazer presente para prestar testemunho sobre seu conteúdo e autoria, nem para ser contraditado sobre os termos do documento[10]. Pela segunda, somente os documentos originais poderiam ser utilizados como prova - e como os documentos eletrônicos, para a mentalidade da época, eram cópias dos documentos de computador, não poderiam ser aceitos[11].

Na segunda fase, por assim dizer, do desenvolvimento da mentalidade americana de aceitação dos documentos eletrônicos se identificou pelo afastamento

[10] A *Hearsay Rule* inviabilizava a utilização de documentos eletrônicos cujos autores tivessem falecido ou desaparecido – por exemplo -, pois não poderiam prestar juramento perante o Tribunal sobre seu conteúdo. Inicialmente, a questão era ainda maior, pois afirmava-se que o autor pessoal de tais documentos não era o ser humano, mas uma máquina inanimada, incapaz comparecer em Juízo para ser questionada acerca do documento. Esta posição inicial foi superada rapidamente, em nome do que o Direito brasileiro chama “princípio da instrumentalidade das formas”.

[11] Evidente o problema da *Best Evidence Rule*, pois existem (e existiam) documentos eletrônicos gerados originariamente em meio virtual e a sua não aceitação implicava na não aceitação de prova fatal para o direito discutido no caso.

do *Hearsay Rule* e do *Best Evidence Rule* em relação a tais documentos, passando à sua aceitação indiscriminada. Verificou-se, porém, depois, que o afrouxamento das exigências em relação aos documentos eletrônicos provocou a cegueira das cortes americanas, que aceitavam quaisquer documentos virtualmente gerados como autênticos, apesar dos vários trabalhos científicos alertando o público sobre a possibilidade de adulteração. Hoje, porém, a questão está superada, desde que os documentos eletrônicos respeitem as regras de cada estado em relação da autenticação de documentos eletrônicos e do uso processual adequado[12].

O Brasil também procura resolver os problemas de credibilidade dos documentos eletrônicos. A Certificação Digital pessoal (ou assinatura digital) foi a solução encontrada pelo Governo Federal para garantir, a médio e longo prazos, a autenticidade e segurança jurídica relativa aos documentos eletrônicos.

[12] O Estado da Califórnia, por exemplo, no seu "Evidence Code", exige na seção 1401 que todos os documentos escritos, gerados eletronicamente ou não, antes de serem admitidos como evidência, devem ser autenticados ("1401. (a) Authentication of a writing is required before it may be received in evidence."). Disponível em http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=evid&codebody=&hits=20. Acesso em 08 set. 2011.

3. DO CONCEITO DE CERTIFICADO DIGITAL

Para que se possa entender o que é um certificado digital, primeiramente é preciso compreender o que é criptografia[13], no que nos auxilia a jurista PINHEIRO (2009, p. 161), *verbis*:

> A criptografia é uma ferramenta de codificação usado para envio de mensagens seguras em redes eletrônicas. (...) Na Internet, a tecnologia da criptografia utiliza o formato assimétrico, ou seja, codifica as informações utilizando dois códigos, chamados de chaves, sendo uma pública e outra privada para descodificação, que representa a assinatura digital do documento.

Complementando, pode-se dizer que criptografia é a ciência matemática que consiste em assegurar o sigilo das informações em determinado meio, através da conversão de algarismos em um código ininteligível, que somente pode ser decifrado com a utilização do algoritmo (função matemática) e da chave ("senha") corretos.

Em termos leigos, é possível definir a criptografia como o código embutido em alguma mensagem eletrônica para evitar sua leitura e/ou modificação por terceiros não autorizados, que desconhecem a chave criptográfica (espécie de "senha" do documento) e o algoritmo utilizados[14].

Qualquer pessoa pode gerar seu próprio certificado digital, existindo programas próprios no mercado, gratuitos inclusive, que permitem que cada pessoa gere um certificado digital pessoal para se comunicar com maior segurança. O documento gerado e assinado digitalmente por este certificado particular, somente pode ser lido por quem possuir a outra chave digital compatível com a assinatura emissora do documento e chave criptográfica para decodificação.

---

[13] DINIZ (2008, p.764-675) também nos auxilia a compreender o conceito: "Criptografia é um conjunto de técnicas matemáticas, que, mediante uso de algoritmos, possibilita a codificação da mensagem, resguardando a privacidade e a segurança do contrato eletrônico".

[14] VERONESE (2007, p.326-327): Existem dois tipos de criptografia: simétrica, utilizada nos certificados digitais privados ("O primeiro sistema é o de criptografia simétrica. Ela utiliza a mesma chave, gerada a partir de um algoritmo, para cifrar e decifrar a mensagem. Esta chave é compartilhada pelo remetente e destinatário. A mensagem original (chamada de texto simples), é transformada em um texto cifrado") e assimétrica, dos certificados públicos ("A criptografia assimétrica consiste na utilização de duas chaves, uma para cifrar e outra para decifrar. A partir do algoritmo serão geradas duas chaves, que formam um par único. Uma delas será pública e ficará disponível para o uso geral. A outra será privada, mantida pelo titular.")

Em suma, temos que: o indivíduo que gera uma assinatura digital, na verdade gera um certificado digital[15], contendo “senha” – chave privada - e “contrassenha” – chave pública. Um documento gerado por este indivíduo, digitalmente assinado, na verdade é como se fosse protegido por senha. Sua alteração, só é possível por outro indivíduo que possua a chave privada, enquanto que a leitura desse documento é possível para qualquer um possua a chave pública, se assim desejar o proprietário da assinatura digital.

Com esta explanação inicial, já nos é possível definir certificação digital como instrumento de identificação pessoal, gerado por particular ou por autoridade certificadora, que, por meio de criptografia, pode garantir a autenticidade de registros eletrônicos.

O problema do certificado digital gerado por particulares por meio de programas próprios consiste no fato de que da mesma forma que um documento eletrônico pode ser facilmente adulterado, os dados que o gerador da assinatura eletrônica inserem no *software* podem ser verdadeiros ou falsos, não existindo nenhum controle sobre a autenticidade dessas informações. Ou seja, o documento assinado digitalmente com o uso de um certificado particular, na verdade, não oferece nenhuma garantia ao receptor acerca da autenticidade daquele documento.

Para resolver essa situação, era preciso transferir a responsabilidade pela emissão de certificados digitais dos particulares para organismos públicos, que pudessem aferir a autenticidade das informações prestadas pelos interessados, gerando, finalmente a segurança da autenticidade dos documentos digitalmente assinados.

3.1 Legislação aplicável ao certificado digital

O processo de transferência para o Poder Público da responsabilidade na emissão de certificados digitais veio em 2001, com a edição da Medida Provisória (MP) nº 2.200-2, de 24 de agosto.

O referido instrumento normativo afirma em seu artigo 1º:

[15] Remetemos o leitor do presente trabalho à nota de rodapé n.º 6, onde é explicada a diferença entre certificado digital e assinatura digital e esclarecemos a relativa e proposital imprecisão terminológica deste trabalho.

> Art. 1º. Fica instituída a Infra-Estrutura (sic) de Chaves Públicas Brasileira – ICP – Brasil, para garantir a **autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica**, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. [grifo do autor]

Prima facie, a MP 2.200-2/2001 traçou os objetivos de um certificado digital (autenticidade, integridade e validade jurídica de documentos eletrônicos), bem como suas principais aplicações. Saliente-se que tais aplicações representam um rol meramente exemplificativo, não excluindo quaisquer outras possibilidades de novos usos para as assinaturas digitais.

A ICP-Brasil é organizada de forma hierárquica, organizada por regulamento, sendo composta por uma autoridade gestora de políticas e pela cadeira de autoridades certificadoras composta pela Autoridade Certificadora Raiz (AC-Raiz), pelas Autoridades Certificadoras (AC) e pelas Autoridades de Registro (AR) (art. 2º da MP 2.200-2/2001).

A Autoridade Certificadora Raiz (AC-Raiz) tem competência para emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível inferior ao seu, realizar atividades de fiscalização e auditoria das AC, das AR e dos prestadores de serviço habilitados na ICP-Brasil, sendo-lhe vedado, contudo, a emissão de certificados pela AC-Raiz diretamente ao usuário final (art. 5º da MP 2.200-2/2001). A função de AC-Raiz, no Brasil, é exercida pelo Instituto Nacional de Tecnologia da Informação – ITI, autarquia federal, vinculada ao Ministério de Ciência e Tecnologia (art. 12 c/c art. 13 da MP 2.200-2/2001).

Observa-se, portanto, que a AC-Raiz tem uma função precipuamente regulatória e fiscalizatória dos outros componentes da ICP-Brasil, como analisa VERONESE (2007, p. 330), *verbis*:

> O sistema criado é estruturado como uma pirâmide ou como uma cadeia de certificação digital, que tem no seu vértice o ITI [AC-Raiz]. O vértice não significa controle direto e sim fiscalização (auditoria técnica) e determinação de procedimentos padronizados (regulamentos) pelas entidades que, efetivamente, certificam os cidadãos.

Às Autoridades Certificadoras (AC) compete, através da emissão de certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, emitindo, expedindo, distribuindo, revogando e gerenciando certificados (art. 6º da MP 2.200-2/2001).

Às Autoridades de Registro (AR), que são vinculadas às AC existentes, compete identificar e cadastrar usuários, encaminhar solicitações de certificados às AC e manter registros de suas operações (art. 7º da MP 2.200-2/2001).

No interesse de melhor garantir a legitimidade das prestadas por órgãos da Administração Pública Federal, já a partir de 2000, inicialmente por meio do Decreto n.º 3.865 e, posteriormente, através do Decreto Presidencial n.º 3.996, de 31 de outubro de 2001, que regulamentara a prestação e contratação dos serviços de certificação digital por órgãos do governo federal, a União já havia se rendido à maior segurança proporcionada pelo certificado digital.

Dentre os particulares, somente com o Decreto presidencial n.º 6.605 de 14 de outubro de 2008 foi regulamentado o Comitê Gestor da Infra-Estrutura *(sic)* de Chaves Públicas Brasileira – CG ICP-Brasil, que exerce a função de autoridade gestora de políticas do ICP-Brasil para a emissão de certificados digitais ao público.

O art. 3º do Decreto n.º 6.605/2008 delineia a competência do CG ICP-Brasil:

> Art. 3o Compete ao CG da ICP-Brasil:
> I - coordenar o funcionamento da ICP-Brasil;
> II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das Autoridades Certificadoras - AC, Autoridades de Registro - AR, Autoridades de Carimbo de Tempo - ACT e demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;
> III - estabelecer a política de certificação e as regras operacionais da AC Raiz;
> IV - auditar e fiscalizar a AC Raiz e os seus prestadores de serviço de suporte;
> V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificado e regras operacionais das AC, AR e ACT e definir níveis da cadeia de certificação;

> VI - aprovar políticas de certificados e regras operacionais, credenciar e autorizar o funcionamento das AC, das AR, das ACT e demais prestadores de serviço de suporte, bem como autorizar a AC Raiz a emitir o correspondente certificado;
> VII - identificar e avaliar as políticas de infra-estruturas de certificação externas, negociar 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.
> VIII - aprovar as normas para homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil;
> IX - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, de modo a garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança; e
> X - aprovar seu regimento interno.

3.2 A certificação eletrônica pública como meio garantidor da autenticidade dos documentos eletrônicos

Como abordado anteriormente, os programas pessoais para geração de certificados digitais apresentam um sério problema de confiabilidade, uma vez que, como são gerados pelos particulares, as informações fornecidas para a criação de tais assinaturas digitais podem não ser autênticas.

Tal questão é fortemente mitigada pela criação da Infraestrutura de Chaves Públicas do Brasil – ICP-Brasil – e todas as autoridades certificadoras vinculadas à ela.

Na geração de um certificado digital "público"[16], o procedimento, apesar de bem mais burocrático, garante a necessária segurança jurídica que a sociedade deve receber dos poderes constituídos.

Neste procedimento, o usuário interessado em adquirir um certificado digital precisa se deslocar até uma Autoridade Certificadora ou Autoridade de

[16] O certificado digital é termo único, não importa se expedido pelo próprio particular ou pela Autoridade Certificadora. Todavia, para diferenciação científica e melhor compreensão do leitor, o termo "certificação digital pública" se refere às certificações digitais emitidas pelas ACs, por autorização da AC Raiz e determinação legal da MP 2.200-2/2001.

Registro, identificar-se e apresentar, no original, todos os documentos que o identifiquem. Esses documentos são conferidos pela autoridade pública e somente após essa verificação detalhada é emitido o certificado digital em favor do requerente.

Porém, não é somente essa verificação documental do requerente que traz segurança jurídica àqueles que se comunicam ou negociam por meio do certificado digital "público". Na verdade, o crivo da autenticidade é dado por um terceiro dado aposto no certificado digital diverso daqueles já mencionados anteriormente (chaves pública e privada): assinatura de um terceiro confiável[17] de todos os indivíduos certificados – a Autoridade Certificadora, por meio de autorização da Autoridade Certificadora Raiz.

Fazendo uma analogia de certo modo vulgar, a assinatura deste terceiro confiável em muito se assemelha a atividade do tabelião que autentica um documento ou reconhece a firma de um interveniente em uma relação jurídica, pois este ato do tabelião confere ao documento fé pública, de forma que tal documento possui presunção de autenticidade, como explica PEREIRA (2006, p. 596):

> Realizado perante o notário, faz a lei decorrer sua fé pública a autenticidade do ato, no que diz respeito às formalidade exigidas, e se alguém as nega, tem de dar prova cabal da postergação. No que diz respeito ao conteúdo da declaração, vigora a presunção de autenticidade, no sentido de que se tem como exata a circunstância de que o agente a fez, nos termos constantes do texto.

O mesmo deverá ser reconhecido aos documentos eletrônicos assinados digitalmente por um certificado "público": na medida em que a Autoridade Certificadora apõe a sua assinatura, o certificado digital induz àquele documento a marca da autenticidade.

---

[17] Conforme afirma GAVILANES (2005, p. 45-46): A aceitabilidade do certificado dependerá da confiança dos usuários nas práticas de trabalho da Autoridade Certificadora, para tanto as "AC´s" devem manter um elevado padrão de conduta na identificação dos usuários finais e nos procedimentos de emissão dos certificados. A Autoridade Certificadora é no final responsável pela identificação segura e confiável dos seus usuários finais.

Essa autenticidade do documento certificado digitalmente já vem sendo reconhecida pelos Tribunais brasileiros[18]:

> DESERÇÃO DO RECURSO ORDINÁRIO INTERPOSTO MEDIANTE DOCUMENTO ELETRÔNICO CERTIFICADO POR ASSINATURA ELETRÔNICA. NECESSIDADE DE COMPROVAÇÃO DO PREPARO.
> A internet é uma realidade que não pode mais ser contestada. Uma das vantagens, entre outras milhares, oferecidas pela rede mundial de informações é a interposição de recursos mediante documento eletrônico. **Para a segurança e confiabilidade das informações passadas eletronicamente pela rede, necessário se faz que os documentos obtenham certificação digital por parte do recebedor. O ICP-Brasil (Infra-Estrutura de Chaves Públicas Brasileira), criado pela Medida Provisória nº 2200/2001, é um dos sistemas de segurança existentes, elaborado - para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras** -[19]. (...) Recurso de revista conhecido e provido. [grifo nosso]
>
> EXECUÇÃO DE TÍTULO EXTRAJUDICIAL. Desnecessidade de apresentação do título original. Sem circulação. Cópia com microfilme registrado no Cartório de Registro de Títulos e Documentos. MP 2.200/01 - Certificado digital goza de presunção de veracidade. Agravo provido. [20]

Outro aspecto a ser invocado é a proteção de um documento certificado digitalmente contra alterações de terceiros e mesmo do próprio autor do documento sem a sua permanente inutilização[21].

Na medida em que os documentos certificados digitalmente não podem ser alterados por terceiros nem mesmo pelo próprio autor, a questão inicialmente

---

[18] Em sentido contrário, algumas Cortes ainda mantem entendimento retrógrado face às inovações da Certificação Digital. Contudo, a sua não aceitação não decorre da não-confiança no mecanismo e sim em seu caráter recentíssimo. É o que se observa neste julgado do Egrégio Tribunal de Justiça de Pernambuco: (...) A certificação digital ainda não se encontra completamente integrada à vivencia diária da sociedade, não podendo, ainda, ser tida como regra, não obstante seus evidentes benefícios à celeridade das relações horizontais interparticulares. Outrossim, o importante, para o caso, era saber se o réu foi notificado, e aí incide o argumento anterior: não está clara sua cientificação, ainda que o oficial do cartório tenha dado afirmação em sentido diverso. A Lei nº 11.419/06 ainda não pode, infelizmente, ser inteiramente aplicada. (TJPE – AGV 7100-75.2011.8.17.0000 – Rel. Des. Frederico Ricardo de Almeida Neves – Dje 09/02/2011)

[19] BRASIL. Tribunal Superior do Trabalho. Recurso de Revista n.º 6400-66.2006.5.04.0104 – Rel. Min. Lelio Bentes Corrêa – DJu 07/11/2008)

[20] BRASIL. Tribunal de Justiça de São Paulo. Agravo de Instrumento n.º 0028961-68.2011.8.26.0000 – Rel. Des. Silveira Paulilo – DJe 11/05/2011).

[21] Tal proteção é dada pela chave pública existente no certificado digital. A criptografia é medida pelo número de “bits” utilizadas para proteger tais chaves. Quanto maior o número de bits, maior o grau de criptografia e maior a dificuldade de adulteração.

posta, relacionada à relatividade do documento eletrônico nos tribunais resta, na grande maioria dos casos, igualmente superada.

Como afirmado anteriormente, a assinatura da Autoridade Certificadora em muito se assemelha a atuação de um tabelião cartorário. Assim sendo, inexistem empecilhos para que os documentos digitalmente certificados sejam aceitos irrestritamente nos tribunais como se documentos públicos fossem, na forma disposta pelo Código de Processo Civil:

> 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.
>
> Art. 365. Fazem a mesma prova que os originais:
> (...)
> III - as reproduções dos documentos públicos, desde que autenticadas por oficial público ou conferidas em cartório, com os respectivos originais.

O documento assinado digitalmente, caso aceito da forma que se desenha neste trabalho, ainda produz mais um efeito benéfico ao direito dos litigantes em ações judiciais: como é da natureza dos documentos eletrônicos serem facilmente copiados (*backup*)[22], o não reconhecimento de um direito em razão do perecimento de um meio de prova, seu extravio ou se, por algum outra razão, não puder ser utilizado em Corte, permite a reapresentação da prova por aquele que a originalmente apresentou, caso tenha feito tal cópia de segurança.

3.3 A certificação eletrônica pública nos contratos firmados via Internet

Os contratos celebrados via Internet, nos moldes atuais, são costumeiramente firmados através de *sites* de comércio eletrônico, onde um fornecedor coloca à disposição de um consumidor seus produtos e serviços, para que o possível comprador realize a avaliação das condições ofertadas e decida pela realização ou não da negociação.

---

[22] A importância do documento eletrônico vem sendo reconhecida, especialmente na inexistência de documento físico, como neste recurso de apelação: Tribunal de Justiça do Estado de São Paulo. Apelação Cível nº 990092501755. Relator: Kioitsi Chicuta. São Paulo, 04 de agosto de 2010.

Ocorre que, em geral, as partes dessa relação jurídica contratual não se conhecem pessoalmente e, possivelmente, jamais se conhecerão. Surge aqui uma questão relevante quanto à segurança das relações contratuais firmadas via Internet, como já analisava DINIZ (2008, p. 756):

> Como provar a veracidade e fidedignidade da mensagem ou contrato eletrônico ou até mesmo da ausência de fraudes? Como se poderia ter certeza de que se está contratando com a pessoa certa, que se encontra do outro lado da comunicação eletrônica?(...) Como proteger o consumidor via Internet e aprimorar a relação de consumo no fornecimento virtual de produtos e serviços?

Essa questão, na modalidade negocial vigente, permanece sem uma resposta cabal, que extirpe todas as dúvidas supraventiladas. Os fornecedores, como forma de atenuar a insegurança virtual, forçam seus possíveis consumidores a realizarem cadastros virtuais, indicando dados pessoais, bancários e criação de *logins* e senhas para a utilização dos mecanismos de compra.

Ocorre que este procedimento não se mostra completamente seguro ao fornecedor. Como assegurar a identidade dos adquirentes de seus produtos, pois a mera indicação de alguns dados pessoais não assegura a veracidade destes (mesmo problema atribuído ao certificado digital “particular”), podendo inclusive “ser um menor e até mesmo se passar por outra pessoa, dando nome ou apresentando número de cartão de crédito que não é seu” (DINIZ, 2008, p. 763), o que aniquila qualquer possibilidade de negócio jurídico válido na forma do art. 104 do Código Civil Brasileiro.

Ao consumidor também é semelhante a situação de insegurança, pois este, ao negociar via Internet, pode não ter conhecimento do histórico de determinado estabelecimento virtual, não ser informado sobre a sede do estabelecimento, sua situação jurídica e financeira... Ou seja, o consumidor, levado pela sua boa-fé, era levado a crer que uma loja virtual era confiável e, acreditando na informação, com ela vem a negociar.

A questão é tão tormentosa que o Estado de São Paulo editou a Lei Estadual n.º 14.516, de 31 de agosto de 2011, assegurando que “todas as empresas atuantes no Estado de São Paulo ficam obrigadas a encaminhar aos contratantes, por escrito, os contratos firmados verbalmente por meio de “call center” ou outras

formas de venda a distância" (art. 1º), como forma de assegurar uma proteção mínima ao consumidor[23].

A solução para a questão passa pela negociação via Internet com a utilização da certificação digital pública, emitida por uma Autoridade Certificadora autorizada pela AC-Raiz. A partir do momento em que o consumidor de determinada loja aceita a oferta do estabelecimento que se propõe a prestar um serviço ou entregar um produto ao cliente, ele deverá apresentar seu certificado digital público, o qual indica seu nome, endereço e outras informações pessoais, como número da carteira de identidade e do CPF (Cadastro de Pessoa Física). À loja, também, será possível realizar a "triangulação" de informações fornecidas pelo cliente em seu cadastro, com as informações contidas no certificado digital apresentado e com os dados bancários ou informações de cartão de crédito utilizadas para pagamento da obrigação assumida.

Concomitantemente, o estabelecimento virtual deverá fazer o mesmo: apresentará sua certificação digital pública, de forma que o cliente, igualmente, terá acesso aos seus dados cadastrais, especialmente, a localização de sua sede, o nome de seus responsáveis legais e de seus sócios.

Tal negociação comercial, uma vez apresentadas as certificações digitais dos intervenientes, garantirá a mínima segurança jurídica de que necessitam as partes. Ao mesmo tempo, tal documento, assinado digitalmente por ambos os contraentes, se instituirá em meio de prova – com força da fé pública do certificado digital, conforme defendemos[24] – a ser utilizada em caso de inexecução contratual por qualquer das partes.

A questão dos problemas referentes ao inadimplemento obrigacional restará também bastante mitigada. Por meio da apresentação da certificação digital mútua, as partes terão condições de obter os reais endereços físicos, de modo que uma persecução judicial se tornará bem mais fácil, tendo em vista que a prática

[23] Observe-se que a lei não se limita aos chamados "call centers", mas abrange também outras formas de venda à distância, como a venda via Internet, o que, em tese (não se sabe da real eficácia desta norma até o momento), faz incidir a norma em comento.

[24] A utilização do certificado digital nos documentos comprobatórios de contratos firmados via Internet garante a necessária integridade do arquivo e identifica a autoria, requisitos essenciais para a aceitação destes meios de prova nos tribunais.

demonstra que nem sempre os bancos de dados das Juntas Comerciais e da Receita Federal do Brasil, cujos endereços costumam servir de base para citações, estão atualizados.

Portanto, a certificação digital pública, utilizada nas negociações via Internet dá aos contratantes dupla proteção: a primeira obtida no momento de conclusão do contrato firmado e a segunda na hipótese de se recorrer ao Judiciário para obter o adimplemento da obrigação contratual assumida.

4. DO PRINCÍPIO DA SEGURANÇA JURÍDICA COMO MARCO DE TODAS AS RELAÇÕES CONTRATUAIS

O princípio da segurança jurídica é decorrência direta do Estado Democrático de Direito estabelecida pela Carta Magna vigente, estabelecida, implicitamente, logo em seu texto preambular:

> Nós, representantes do povo brasileiro, reunidos em Assembléia Nacional Constituinte para instituir um **Estado Democrático**, destinado a assegurar o exercício dos direitos sociais e individuais, a liberdade, a **segurança**, o bem-estar, o desenvolvimento, a igualdade e a justiça como valores supremos de uma sociedade fraterna, pluralista e sem preconceitos, fundada na harmonia social e comprometida, na ordem interna e internacional, com a solução pacífica das controvérsias, promulgamos, sob a proteção de Deus, a seguinte CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL. [grifo nosso]

Ademais, foi erigido ao nível de direito fundamental, insculpido no art. 5º, inciso XXXVI, i*n verbis:*

> Art. 5º (...)
> XXXVI - a lei não prejudicará o direito adquirido, o ato jurídico perfeito e a coisa julgada;

CANOTILHO (2003, p. 257) melhor explica a abrangência deste princípio constitucional:

> O princípio geral da segurança jurídica em sentido amplo (abrangendo, pois, a idéia de protecção da confiança) pode formular-se do seguinte modo: o indivíduo tem o direito de poder confiar em que aos seus actos às decisões públicas incidentes sobre os seus direitos, posições ou relações jurídicas alicerçadas em normas jurídicas vigentes e válidas por esses actos jurídicos deixados pelas autoridades com base nessas normas se ligam aos efeitos jurídicos previstos e prescritos no ordenamento jurídico.

CASALI (200-, p. 6281) apresenta sua conceituação de segurança jurídica, *verbis*:

> Portanto, colacionando os elementos aqui abordados pode-se conceituar segurança jurídica como a garantia da exigibilidade de direito certo estável e previsível, devidamente justificado e motivado com vistas à realização da justiça.

Como neste trabalho se trata da intersecção existente entre o princípio da segurança jurídica, o certificado digital e o direito contratual, direcionaremos a discussão ao princípio da segurança jurídica sob o enfoque do ato jurídico perfeito

(relações jurídicas, nas palavras de CANOTILHO), quando se pode falar em um direito certo estável e previsível.

A segurança jurídica tem o escopo de proteger o cidadão contra mudanças repentinas no direito que acreditava possuir, protegendo-o contra o Estado e contra os particulares que violarem as relações jurídicas entabuladas. Nas palavras de MOTTA (2008, p.32), “a segurança jurídica é, pois, um valor ético que antecede ao Estado e que este incorpora para gerar certeza, confiabilidade e estabilidade às relações sociais regidas pelo direito”.

Caso fosse valor meramente ético, não possuiria força vinculante aos indivíduos regidos pelo Estado; mas na medida em que é um valor incorporado ao Estado, transcende seu valor moral, se tornando regra jurídica vinculante.

CASALI *apud* CANOTILHO (200-, p.6276) afirma que o núcleo fundamento do princípio da segurança jurídica se desenvolve em torno de dois conceitos:

> (1) estabilidade ou eficácia ex post da segurança jurídica: uma vez adoptadas, na forma e procedimento legalmente exigidos, as decisões estatais não devem poder ser arbitrariamente modificadas, sendo apenas razoável alteração das mesmas quando ocorram pressupostos materiais particularmente relevantes.
>
> (2) previsibilidade ou eficácia ex ante do princípio da segurança jurídica que, fundamentalmente, se reconduz à exigência de certeza e calculabilidade, por parte dos cidadãos, em relação aos efeitos jurídicos dos actos normativos.

No aspecto individual, o princípio da segurança jurídica se caracteriza pela existência de mecanismos traçados pelo Estado (por lei) ou pelos particulares (por meio de negócio jurídico) que permite às partes buscar de meios que as permitam buscar a satisfação de seus direitos, ou melhor, das obrigações assumidas e não cumpridas pela outra parte. E mais, a confiança que, uma vez entabulado negócio jurídico, os termos acordados serão respeitados sob pena das sanções previstas na lei.

Para a segurança jurídica existir, é preciso, nas palavras de MOTTA (2008, p. 36-37) que o ordenamento possua as seguintes características: ser originário de um órgão oficial (“monopólio na exteriorização das fontes do direito, capaz de lhe conferir publicidade e autoridade, evidenciando o caráter obrigatório a

partir de sua origem"); ser escrito ("pois limita e identifica o sistema, que se constrói sobre bases mais democráticas"); ser legislado ("em contraposição ao um direito jurisprudencial[25] (...) a lei assumiu o papel de fonte principal do direito").

Observa-se, portanto, que, do ponto de vista legislativo, o ordenamento jurídico pátrio apresenta relativa segurança jurídica aos cidadãos, dispondo-os de mecanismos para persecução de seus direitos quando estes forem desrespeitados.

Acontece que a segurança jurídica não se pode ser aferida somente pela existência (ou não) de normais legais claras que disciplinem relações entre indivíduos, mas que se possa aplicá-las nos casos concretos e para isso veio a certificação digital, como adiante será explanado.

4.1 Ato jurídico perfeito

Como ato jurídico perfeito pode-se entender todas as relações jurídicas (CANOTILHO) que, sendo realizadas conforme as disposições legais vigentes, possui força cogente entre as partes, impedindo mudanças unilaterais e atribuindo-se de mecanismos capazes de proteger o indivíduo contra o descumprimento da relação jurídica dotada desta característica.

Se um ato jurídico é reputado como perfeito quando é realizado segundo as formalidades legais, não resta dúvida que as consequências desse ato perfeito podem (devem) ser perseguidas no âmbito do Poder Judiciário.

É fundamental a leitura do artigo 104 do Código Civil (CC) vigente para se analisar em que se constitui um negócio jurídico perfeito dentro do direito contratual:

> 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.

A plena capacidade do agente é atingida na maioridade (art.5º, CC), exceto nas exceções previstas em lei (art. 5º, parágrafo único, CC). A capacidade do

[25] Apenas uma discordância do autor quanto à este ponto. O direito jurisprudencial não é necessariamente menos estável do que o direito legislado. Os melhores exemplos são os Estados que utilizam da *common law* em que precedentes jurisprudenciais centenários são aplicados como se leis fossem, o que demonstra que a existência de lei tratando de determinado assunto não significa, em absoluto, a maior estabilidade do Direito.

agente pode ser relativa (hipóteses do art. 4º do CC), quando este deverá ser assistido nos atos da vida civil ou absolutamente incapaz (art. 3º, CC), quando deverá ser representado por seu tutor.

O objeto do negócio jurídico deve ser lícito (não proibido por lei, nem contrário à moral e aos bons costumes), possível (é necessário que exista, pelo menos, em potencial, no momento da celebração do pacto) e determinado ou determinável (é preciso que, no momento do adimplemento, seja possível se determinar quantidade, qualidade e espécie da obrigação assumida).

A forma do negócio jurídico, em nosso tema, não exige maiores questionamentos, pois, via de regra, os contratos firmados via Internet se referem à negociação de bens móveis e/ou prestação de serviços, razão pela qual não é comum a exigência legal de forma específica para o pacto.

Respeitados estes requisitos, pode-se dizer que o negócio entabulado se configura como ato jurídico perfeito, podendo produzir todas as consequências previstas em lei e em contrato.

Essas consequências jurídicas se configuram como direito adquirido daqueles se intervieram na celebração do contrato, conforme ensina BULOS (2008, p.490).

Como explanado no tópico anterior, o princípio da segurança jurídica pressupõe não só um prévio conhecimento das condições previstas (estabilidade) como também as consequências (previsibilidade) que advirão.

4.2 A certificação digital como mecanismo de manutenção da Segurança Jurídica nos contratos firmados via Internet

Não resta dúvida que a estabilidade das relações jurídicas existe. Mas a previsibilidade, nos contratos celebrados via Internet, pressupõe aspectos externos à lei, como a possibilidade de contatar a outra parte contratante, de conhecer seu endereço físico e de saber se possui condições técnicas, jurídicas e financeiras de honrar os compromissos assumidos.

Ou seja, apesar de o negócio jurídico celebrado via Internet ser reconhecido como um ato jurídico perfeito, devendo, portanto, ser albergado pelo princípio da segurança jurídica, a então inexistência de meios para responder as questões anteriormente formuladas punha “em cheque” meios mais eficazes de salvaguardar os direitos adquiridos advindos dos contratos firmados virtualmente.

Neste sentido, a certificação digital representou um importante passo, no contexto brasileiro, para a proteção das partes contratantes e para o oferecimento de mecanismos para a persecução dos direitos violados quando do não adimplemento contratual.

Por meio da certificação digital pública, os caracteres extrínsecos à relação contratual (que não impediam a formação de um negócio jurídico válido, mas prejudicam o potencial cumprimento da obrigação), passam a ser conhecidos. Além disso, tais informações possuem um acobertamento de legitimidade dado pela legislação (MP 2.200-2/2001).

Neste sentido, o que este trabalho procurou defender foi a manutenção da segurança jurídica nas relações entabuladas via Internet, o que significa que ela já existe no meio virtual, uma vez que existem empresas que tratam da negociação virtual como ramo principal da atividade, já possuindo a credibilidade necessária no mercado.

Por outro lado, existem empresas que estão iniciando no mercado e, como tal, não fornecem ao oblato, habituado a negociar somente com empresas que conhece no seu dia-a-dia, a necessária confiança de a elas confiar seus dados pessoais, seu número de cartão de crédito ou mesmo se receberá o objeto contratado.

O mesmo pode ser comentado em relação aos consumidores no olhar das empresas: na medida em que estes, costumeiramente, são clientes esporádicos e, muitas vezes, realizam poucas compras no mesmo estabelecimento, também a empresa policitante tem dificuldades em identificar a veracidade das informações

prestadas em seus cadastros virtuais, de forma que, também ela, não possui a necessária confiança que deve possuir com que está contratando[26].

A certificação digital certamente elimina os problemas acima apresentados, de forma que, tanto o consumidor como a empresa policitante, poderão aferir, de pronto, a legitimidade das informações prestadas pela parte adversa, sabendo de logo que são verdadeiras.

Ademais, terão acesso a dados pessoais fornecidos à AC, no momento da emissão do certificado digital público, como endereço físico, telefone válido, o que certamente facilitará uma persecução judicial no caso de descumprimento das obrigações contratuais entabuladas.

Assim se forma um direito contratual forte, eficiente e confiável, como exige o princípio da segurança jurídica, na medida em que os contratantes sabem com quem realmente estão contratando e podem ter certeza que as obrigações assumidas serão cumpridas, voluntária ou judicialmente.

A segurança jurídica dessas negociações com certificados digitais públicos, também decorre do documento por elas gerado (documento virtual assinado digitalmente) que, conforme anteriormente defendido, deve possuir a mesma fé e força jurídica de um documento público produzido por agente cartorário, de forma que garantir a previsibilidade (CANOTILHO) das relações jurídicas se torna uma atividade bem mais simplificada àquele que teve um direito prejudicado.

[26] Neste ponto uma digressão é necessária: uma das razões para as altas taxas de juros praticadas no mercado se dá em razão da insegurança que as empresas possuem acerca da “certeza” de seu crédito. Se tais informações pudessem ser comprovadas *prima facie,* seria possível uma redução dos juros ao consumidor.

5 CONCLUSÕES

Do exposto, pode-se concluir o seguinte:

a) O crescimento das negociações via Internet se apresenta forte e com possibilidades para um avanço ainda maior, visto que o número de pessoas que negocia de forma *on-line* ainda é incipiente, em razão das desconfianças relacionadas ao pagamento e do recebimento dos produtos e serviços avençados;

b) Mesmo incipiente, o mercado virtual vem apresentando crescentes montantes relacionados às negociações pela Internet;

c) Tais negociações ainda não são completamente seguras, posto que é (era) virtualmente impossível realizar a correta identificação dos contratantes, se possuíam meios para adimplir a obrigação ou mesmo sua credibilidade no mercado;

d) Certificação digital é um instrumento de identificação pessoal, gerado por particular ou por autoridade certificadora, que, por meio de criptografia, pode garantir a autenticidade de registros eletrônicos;

e) A certificação digital foi um instrumento que surgiu para propiciar a identificação das partes. Apresentava o problema de ser unicamente obtido de forma particular, de forma que as informações fornecidas para obtenção da assinatura digital eram prestadas conforme o bem-querer do solicitante, de forma que, igualmente, não poderia se ter certeza da veracidade das informações prestadas pelo solicitante do certificado digital particular;

f) Isso se encerrou com a edição da Medida Provisória n.º 2.200/2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), que criou uma autarquia federal para regulamentar a emissão de certificados digitais públicos no Brasil;

g) A estrutura orgânica do ICP-Brasil é formada pela Autoridade Certificadora Raiz (AC-Raiz), responsável pela coordenação,

fiscalização e emissão de diretrizes dos outros órgãos da cadeia; pelas Autoridades Certificadoras (AC), que mediante, autorização da AC-Raiz, certificam indivíduos que a elas requerem e pelas Autoridades de Registro (AR), que meramente cadastram os indivíduos e as encaminham às AC;

h) A grande inovação no mecanismo de emissão de certificados digitais públicos se encontra na burocracia, que, neste caso, é positiva. Deste trâmite mais “complicado”, é possível que as Autoridades Certificadoras façam uma verificação documental e das demais informações prestadas pelo solicitante do certificado digital, de forma que, uma vez expedida a assinatura digital pública, pode-se afirmar, com certeza, a veracidade das informações prestadas em meio virtual;

i) Outro mecanismo de segurança dos certificados digitais públicos advém da “marca” posto por um terceiro confiável, com fé pública provinda da Lei, que é a Autoridade Certificadora;

j) O grande problema dos documentos digitais (não assinados digitalmente) consiste na impossibilidade de se determinar a legitimidade das informações nem se aferir, com certeza, se os documentos sofreram algum tipo de adulteração em seu conteúdo, conforme a exigência do Enunciado n.º 297 do Conselho da Justiça Federal;

k) Com a adoção de uma certificação digital pública, todos os problemas em relação aos documentos virtuais se esvaziam, posto que o maior problema deles, que era assegurar a inalterabilidade do conteúdo, não mais representa um entrave à aceitação deles, uma vez que, uma vez assinados digitalmente, tais documentos são protegidos contra alteração, sob pena de inutilização de seu conteúdo;

l) Os contratos virtuais, na forma como são formalizados atualmente, não preenchem os requisitos necessários a dar segurança jurídica entre

as partes, vez que as informações prestadas não podem ser verificadas;

m) Desta insegurança dos documentos virtuais assinados digitalmente, decorre a grande ideia defendida neste trabalho, que consiste em que todas as negociações realizadas virtualmente sejam realizadas por meio da apresentação, por ambas as partes contratantes, de seus certificados digitais públicos, de forma que, no momento da conclusão do negócio, possam saber, de pronto, com quem realmente negociam e se as partes possuem meios para adimplir as obrigações assumidas;

n) Deste instrumento de negociação, advirá um documento virtual assinado digitalmente por ambas as partes, com presunção de legitimidade, por meio da MP n.º 2.200-2/2001 e por interpretação extensiva dos art. 364 e 365 do Código de Processo Civil, à semelhança de um documento público emitido por um agente cartorário;

o) O princípio da segurança jurídica é ferramenta cogente no ordenamento jurídico e direito fundamental dos indivíduos, conforme idealiza o preâmbulo constitucional e determina o art. 5º, XXXVI, da Carta Magna;

p) O princípio da segurança jurídica pode ser reduzido a dois elementos que são a estabilidade contra mudanças unilaterais e não previstas e a previsibilidade dos efeitos dos negócios jurídicos entabulados;

q) Discutiu-se também que os negócios jurídicos virtuais se constituem em atos jurídicos perfeitos, razão pela qual devem ser acobertados pelo princípio da segurança jurídica e que a certificação digital somente fornece um elemento extra, porém fundamental, para que este desígnio seja alcançado.

BIBLIOGRAFIA

BARBAGALO, Erica Brandini. **Contratos eletrônicos**. São Paulo: Saraiva, 2001.

BEHRENS, Fabiele. **A assinatura eletrônica como requisito de validade dos negócios jurídicos e a inclusão digital na sociedade brasileira.** Disponível em: < www.dominiopublico.gov.br/download/texto/cp008696.pdf> . Acesso em: 10 set.2011.

BETHONICO, Cátia Cristina de Oliveira. **O comércio eletrônico.** Disponível em: < http://biblioteca.unisantos.br/tede/tde_arquivos/1/TDE-2009-09-04T102420Z-219/Publico/Catia%20Bethonico.pdf> . Acesso em: 10 set.2011.

BULOS, Uadi Lâmmego. **Curso de Direito Constitucional**. 2ª Ed. São Paulo: Saraiva, 2008.

CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição.** 7 ed. Lisboa: Almedina, 2006.

CASALI, Guilherme Machado. **Sobre o conceito de segurança jurídica**. Disponível em: < http://www.conpedi.org.br/manaus/arquivos/anais/bh/guilherme_machado_casali.pdf > . Acesso em: 10 set.2011.

DIDIER JR, F.; BRAGA, P.S.; OLIVEIRA, R. **Curso de Direito Processual Civil**: teoria da prova, direito probatório, teoria do precedente, decisão judicial, coisa julgada e antecipação dos efeitos da tutela. 4 ed. Salvador: Juspodvm, 2009. V. 2

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro:** teoria das obrigações contratuais e extracontratuais. 24 ed. São Paulo: Saraiva, 2008. V.3

FERNANDES NETO, Guilherme. **O abuso do direito na internet**. Disponível em: <http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/24255/23818>. Acesso em: 16 out.2010.

GAVILANES, Juan Carlos Guede. **A certificação digital como instrumento de garantia da segurança e credibilidade da informação digital**: um estudo de caso brasileiro. Disponível em: < www.cipedya.com/web/FileDownload.aspx?IDFile=157000> . Acesso em: 10 set.2011.

GICO JUNIOR, Ivo Teixeira. **O documento eletrônico como meio de prova no Brasil**. Disponível em http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/gico.pdf. Acesso em 18 jul. 2010.

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.** Disponível em: <

http://www.teses.usp.br/teses/disponiveis/3/3142/tde-26072007-164132/publico/DissertacaoAirtonRobertoGuelfi.pdf> . Acesso em: 10 set.2011.

LAWAND, Jorge José. **Teoria geral dos contratos eletrônicos.** 1 ed. São Paulo: Editora Juarez de Oliveira, 2003

LUCCA, Newton de. *et al*. **Direito & Internet**: Aspectos jurídicos relevantes. 1 ed. Bauru: Edipro, 2000.

MARQUES, Cláudia Lima. **Confiança no Comércio Eletrônico e a Proteção do Consumidor:** (um estudo dos negócios jurídicos de consumo no comércio eletrônico). São Paulo: Editora Revista dos Tribunais, 2004.

MATTOS, Analice Castor de. **Aspectos relevantes dos contratos de consumo eletrônicos.** Disponível em: <http://www.biblioteca.pucpr.br/tede/tde_arquivos/1/TDE-2007-04-04T112911Z-528/Publico/Analice%20Dto.pdf>. Acesso em 04 out. 2010.

MILAGRE, José Antonio. **A difícil legislação sobre os contratos eletrônicos**. Disponível em: <http://webinsider.uol.com.br/2007/05/29/a-dificil-legislacao-sobre-os-contratos-eletronicos> . Acesso em: 16 out.2010.

MOTTA, Artur Alves da. **Segurança jurídica:** da crise ao resgate. Disponível em: < http://www.lume.ufrgs.br/bitstream/handle/10183/14804/000669425.pdf?sequence=1 > . Acesso em: 10 set.2011.

PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil**. 21 ed. Rio de Janeiro: Forense, 2006. v.1

PERRONI, Otávio Augusto Buzar. **O Contrato Eletrônico no Código Civil Brasileiro**. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

PINHEIRO, Patrícia Peck. **Direito Digital.** 3 ed. São Paulo: Saraiva, 2009.

PINHEIRO, Patrícia Peck. **Direito Digital**. 2 ed. São Paulo: Saraiva, 2007.

PROTEÇÃO DO CONSUMIDOR NO COMÉRCIO ELETRÔNICO SOB A ÓTICA DA TEORIA DA CONFIANÇA. Disponível em: <http://www.nucleodedireito.com/artigos/trabalhos-juridicos/direito-do-consumidor/protecao-do-consumidor-no-comercio-eletronico-sob-a-otica-da-teoria-da-confianca>. Acesso em 01 out. 2010.

RODRIGUES, Silvio. **Direito Civil:** dos contratos e das declarações unilaterais da vontade. 30 ed. São Paulo: Saraiva, 2007. V.3

SCHOUERI, Luís Eduardo. *et al*. **Internet**: O direito na era virtual. 2 ed. Rio de Janeiro: Forense, 2001.

VERONESE, Alexandre. **A política de certificação digital: processos eletrônicos e informatização judiciária**. Disponível em: <

www.conpedi.org.br/manaus/arquivos/anais/bh/alexandre_veronese.pdf> . Acesso em: 10 set.2011.

ANEXOS

ANEXO A – MEDIDA PROVISÓRIA N.º 2.200-2/2001

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

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

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

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

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

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Art. 5º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.

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

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

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

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

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

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

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

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

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

Art. 12. Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação - ITI, com sede e foro no Distrito Federal.

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

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

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

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

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

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

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

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

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

II - remanejar, transpor, transferir, ou utilizar, as dotações orçamentárias aprovadas na Lei Orçamentária de 2001, consignadas ao Ministério da Ciência e Tecnologia, referentes às atribuições do órgão ora transformado, mantida a mesma classificação orçamentária, expressa por categoria de programação em seu menor nível, observado o disposto no § 2o do art. 3o da Lei no 9.995, de 25 de julho de 2000, assim como o respectivo detalhamento por esfera orçamentária, grupos de despesa, fontes de recursos, modalidades de aplicação e identificadores de uso.

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

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

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

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

FERNANDO HENRIQUE CARDOSO
José Gregori
Martus Tavares
Ronaldo Mota Sardenberg
Pedro Parente

ANEXO B – DECRETO N.º 3.865/2000

Estabelece requisito para contratação de serviços de certificação digital pelos órgãos públicos federais, e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso das atribuições que lhe confere o art. 84, incisos IV e VI, da Constituição,

DECRETA:

Art. 1º Somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico, os órgãos da Administração Pública Federal, direta e indireta, e as entidades a eles vinculadas poderão contratar, para uso próprio ou de terceiros, quaisquer serviços de certificação digital de:

I - documentos em forma eletrônica;

II - aplicações de suporte; e

III - transações eletrônicas.

Parágrafo único. O Comitê Executivo do Governo Eletrônico poderá baixar normas complementares para cumprimento do disposto neste artigo e no art. 3º do Decreto de 18 de outubro de 2000, que o instituiu no âmbito do Conselho de Governo.

Art. 2º Este Decreto entra em vigor na data de sua publicação.

Brasília, 13 de julho de 2001; 180o da Independência e 113o da República.

FERNANDO HENRIQUE CARDOSO
Martus Tavares
Pedro Parente

ANEXO C – DECRETO N.º 3.996/2001

Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

O VICE-PRESIDENTE DA REPÚBLICA, no exercício do cargo de Presidente da República, usando das atribuições que lhe confere o art. 84, incisos II, IV e VI, alínea "a", da Constituição, e tendo em vista o disposto na Medida Provisória no 2.200-2, de 24 de agosto de 2001,

DECRETA:

Art. 1º A prestação de serviços de certificação digital no âmbito da Administração Pública Federal, direta e indireta, fica regulada por este Decreto.

Art. 2º Somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico, os órgãos e as entidades da Administração Pública Federal poderão prestar ou contratar serviços de certificação digital.

§ 1º Os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.

§ 2º Respeitado o disposto no § 1o, o Comitê Executivo do Governo Eletrônico poderá estabelecer padrões e requisitos administrativos para a instalação de Autoridades Certificadoras - AC e de Autoridades de Registro – AR próprias na esfera da Administração Pública Federal.

§ 3º As AR de que trata o § 2o serão, preferencialmente, os órgãos integrantes do Sistema de Administração do Pessoal Civil - SIPEC.

Art. 3º A tramitação de documentos eletrônicos para os quais seja necessária ou exigida a utilização de certificados digitais somente se fará mediante certificação disponibilizada por AC integrante da ICP-Brasil.

Art. 3º-A. As aplicações e demais programas utilizados no âmbito da Administração Pública Federal direta e indireta que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitido por qualquer AC integrante da ICP-Brasil.

Art. 4º Será atribuída, na Administração Pública Federal, aos diferentes tipos de certificados disponibilizados pela ICP-Brasil, a classificação de informações segundo o estabelecido na legislação específica.

Art. 5º Este Decreto entra em vigor na data de sua publicação.

Art. 6º Fica revogado o Decreto no 3.587, de 5 de setembro de 2000.

Brasília, 31 de outubro de 2001; 180o da Independência e 113o da República.

MARCO ANTONIO DE OLIVEIRA MACIEL
Martus Tavares
Silvano Gianni

ANEXO D – DECRETO N.º 6.605/2008

Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC.

O VICE-PRESIDENTE DA REPÚBLICA, no exercício do cargo de Presidente da República, usando das atribuições que lhe confere o art. 84, incisos IV e VI, alínea "a", da Constituição, e tendo em vista o disposto na Medida Provisória no 2.200-2, de 24 de agosto de 2001,

DECRETA:

Art. 1º O Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, instituído pela Medida Provisória no 2.200-2, de 24 de agosto de 2001, exerce a função de autoridade gestora de políticas da referida Infra-Estrutura.

Art. 2º O CG ICP-Brasil, vinculado à Casa Civil da Presidência da República, é composto por doze membros e respectivos suplentes, sendo cinco representantes da sociedade civil, integrantes de setores interessados, e representantes dos seguintes órgãos:

I - Casa Civil da Presidência da República, que o coordenará;

II - Gabinete de Segurança Institucional da Presidência da República;

III - Ministério da Justiça;

IV - Ministério da Fazenda;

V - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

VI - Ministério do Planejamento, Orçamento e Gestão; e

VII - Ministério da Ciência e Tecnologia.

§ 1º Os representantes da sociedade civil serão designados para período de dois anos, permitida a recondução.

§ 2º Os membros do CG ICP-Brasil serão designados pelo Presidente da República.

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

§ 4º As deliberações do CG ICP-Brasil serão aprovadas por meio de resoluções.

§ 5º O quórum de deliberação do CG ICP-Brasil é de sete representantes, e o quórum de aprovação de deliberações é de maioria simples.

§ 6º Na hipótese de ausência do Coordenador titular e do seu suplente, a coordenação será exercida pelo Secretário-Executivo do CG ICP-Brasil.

§ 7º São convidados para participar das reuniões, em caráter permanente, dois representantes indicados pelo Conselho Nacional de Justiça.

§ 8º Poderão ser convidados a participar das reuniões do CG ICP-Brasil, a juízo do seu Coordenador ou do próprio Comitê, técnicos e especialistas de áreas afins.

Art. 3º Compete ao CG da ICP-Brasil:

I - coordenar o funcionamento da ICP-Brasil;

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

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

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

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

VI - aprovar políticas de certificados e regras operacionais, credenciar e autorizar o funcionamento das AC, das AR, das ACT e demais prestadores de serviço de suporte, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de infra-estruturas de certificação externas, negociar 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.

VIII - aprovar as normas para homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil;

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

X - aprovar seu regimento interno.

Art. 4º O CG ICP-Brasil será assistido e receberá suporte técnico da Comissão Técnica Executiva - COTEC.

§ 1º A COTEC será integrada por representantes, titulares e suplentes, indicados pelos membros do CG ICP-Brasil.

§ 2º O Secretário-Executivo do CG ICP-Brasil será o Coordenador da COTEC, cabendo-lhe designar os membros da Comissão.

§ 3º Poderão ser convidados a participar das reuniões da COTEC, a juízo do seu Coordenador ou dela própria, técnicos e especialistas de áreas afins.

Art. 5º Compete à COTEC:

I - manifestar-se previamente sobre matérias de natureza técnica a serem apreciadas e decididas pelo CG ICP-Brasil;

II - preparar e encaminhar previamente aos membros do CG ICP-Brasil expediente contendo o posicionamento técnico dos órgãos e das entidades relacionados com as matérias que serão apreciadas e decididas; e

III - cumprir outras atribuições que lhe forem conferidas por delegação do CG ICP-Brasil.

Art. 6º O CG ICP-Brasil terá uma Secretaria-Executiva, chefiada pelo Diretor-Presidente do ITI.

Parágrafo único. O Secretário-Executivo receberá do ITI o apoio necessário ao exercício de suas funções, inclusive no que se refere aos cargos de assessoria e ao apoio técnico e administrativo.

Art. 7º Compete à Secretaria-Executiva:

I - prestar assistência direta e imediata ao Coordenador do CG ICP-Brasil;

II - preparar as reuniões do CG ICP-Brasil;

III - coordenar e acompanhar a implementação das deliberações e diretrizes fixadas pelo CG ICP-Brasil;

IV - coordenar os trabalhos da COTEC; e

V - cumprir outras atribuições que lhe forem conferidas por delegação do CG ICP-Brasil.

Art. 8º Este Decreto entra em vigor na data de sua publicação.

Art. 9º Fica revogado o Decreto no 3.872, de 18 de julho de 2001.

Brasília, 14 de outubro de 2008; 187o da Independência e 120o da República.

JOSÉ ALENCAR GOMES DA SILVA
Dilma Rousseff.