

COMISSÃO DE DEFESA DO CONSUMIDOR

PROJETO DE LEI Nº 7.316, DE 2002

Dispõe sobre o uso de assinaturas eletrônicas e certificado digitais, a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, a prestação de serviços de certificação e dá outras providências.

AUTOR: PODER EXECUTIVO

RELATOR: DEPUTADO CELSO RUSSOMANO

I - RELATÓRIO

O projeto de lei em epígrafe foi apresentado pelo Poder Executivo em 7 de novembro de 2002, a fim de disciplinar o uso de assinaturas eletrônicas e a prestação de serviços de certificação digital, atualmente delineados pela MP 2.200-2, de 24 de agosto de 2001. Importante consignar que anteriormente houve a publicação do Decreto nº 3.587/00, que instituiu a ICP-Gov uma infraestrutura para a administração federal em sentido subjetivo, ou seja, apenas para as entidades integrantes do Poder Executivo, excludente, portanto, dos órgãos do Poder Legislativo, Judiciário e, principalmente, de toda a sociedade civil, que não poderia se valer de seus serviços.

A Medida Provisória 2.200-2/01, marco regulatório da ICP-Brasil, possui vigência diferida pela Emenda Constitucional 32/01¹, ou seja, até que revogada ou haja deliberação definitiva do Congresso sobre o tema, continuará plenamente vigente e aplicável. Merece, entretanto, ser renovada, algo alcançado pelo presente projeto de lei que incorpora os princípios esculpidos nas principais legislações alienígenas, mormente na Diretiva 1999/93, da Comunidade Européia. Uma primeira iniciativa em legislar sobre a assinatura eletrônica ocorreu nos Estados Unidos, mais precisamente no Estado de Utah, com o objetivo de permitir a autenticação dos documentos eletrônicos e facilitar o comércio e outras relações contratuais via Internet, seguindo o sistema de Criptografia, com a promulgação da "*Digital signature and electronic authentication law*" de 02/02/1998 que facilitou

¹ Art. 2º As medidas provisórias editadas em data anterior à da publicação desta emenda continuam em vigor até que medida provisória ulterior as revogue explicitamente ou até deliberação definitiva do Congresso Nacional.

sobremaneira o seu uso pelas Instituições financeiras, permitindo a autenticação dos documentos por meio da Criptologia. Na mesma esteira, a Alemanha já tem a sua "*Informations Und Kommunikationsdienste Gesetz Iukdg*", lei federal que estabelece condições gerais para o uso das assinaturas digitais e se baseia no mesmo sistema da Criptografia. A ONU, por meio de uma comissão chamada UNCITRAL (Comissão das Nações Unidas sobre o Direito do Comércio Internacional) já volta os seus olhos para essa questão da segurança nas relações cibernéticas e reconhece os certificados digitais emitidos por uma entidade certificadora digital de outro Estado membro da União Européia, se este possuir um grau de segurança equivalente ao dos países membros da ONU.

A proposição foi encaminhada, primeiramente, à Comissão de Ciência, Tecnologia, Comunicação e Informática, aprovada em 1º de dezembro de 2004, na forma de Substitutivo elaborado pelo Deputado Jorge Bittar, que a relatou. Posteriormente, foi encaminhada à Comissão de Constituição e Justiça e Cidadania, cujo relator, Deputado Maurício Rands, votou pela constitucionalidade, juridicidade e boa técnica legislativa. Antes, porém, da discussão da matéria nesta segunda Comissão, apresentamos, em novembro de 2007, requerimento ao Presidente da Casa para que este órgão técnico legislativo também apreciasse a proposição, já que tem por objeto regular os meios pelos quais se validará o comércio eletrônico no país, com indubitável ingerência sobre os consumidores brasileiros. O requerimento foi deferido com novo despacho, devendo esta Comissão se pronunciar antes da Comissão de Constituição e Justiça e Cidadania.

II – VOTO DO RELATOR

No presente projeto, é clara a preponderância de matéria técnica, como a definição de termos e requisitos para a prestação de serviços de certificação digital, uma vez que seu objetivo é garantir a segurança e a confiabilidade necessárias para que os documentos eletrônicos tenham autenticidade com mesmo valor jurídico das assinaturas manuscritas. A internet permite que indivíduos, empresas, governos e outras entidades realizem uma série de procedimentos e transações de maneira rápida e precisa. Graças a isso, é possível fechar negócios, emitir ou receber documentos, acessar ou disponibilizar informações sigilosas e economizar dinheiro evitando processos burocráticos. No entanto, da mesma forma que os computadores oferecem meios para tudo isso, podem também ser usados por fraudadores, o que significa que tais operações, quando realizadas por vias eletrônicas, precisam ser confiáveis e seguras, e a certificação digital é capaz de atender a essa necessidade.

A certificação digital nada mais é que um tipo de tecnologia de identificação que permite que transações eletrônicas dos mais diversos tipos sejam feitas considerando a sua integridade, autenticidade e confidencialidade, de forma a

evitar que adulterações, interceptações ou outros tipos de fraude ocorram. Importante salientar que a infraestrutura de chaves públicas não é apenas o aspecto formal, oriundo da lei, nem o material, plasmado nas mais diversas entidades prestadoras do serviço. Decorre, isso sim, de um conjunto de normas, procedimentos, regras técnicas que garantem tanto o fornecimento de certificados digitais como a sua utilização correta e com os atributos previstos. Tal característica é de fundamental importância em um mundo binário, onde não se conhece as pessoas com quem se está lidando ou, acaso conhecidas, não se tem certeza se aquela pessoa é a mesma em quem se acredita ser. O crescimento exponencial das redes e utilizadores da Internet constitui um fortíssimo elemento de pressão da procura no sentido do aumento dos investimentos em infraestruturas de redes de telecomunicações, bem como a necessidade de se normatizar as suas regras, porque se isso não for feito certamente haverá uma parada econômica frente à demanda cada vez maior pela segurança da informação.

Uma Infraestrutura de Chaves Públicas pode ser configurada basicamente em dois modelos: o hierárquico e o de confiança distribuída. O primeiro é estabelecido em forma vertical, metaforicamente na figura de uma árvore invertida, situando-se no topo uma entidade na qual todos os que vêm abaixo, inclusive os usuários, devem confiar. A confiança dissemina-se de cima para baixo: a entidade localizada no ápice da hierarquia, denominada Autoridade Certificadora Raiz, emite um certificado digital para uma autoridade certificadora subsequente, e esta emite um certificado digital para o usuário final. Já no modelo de confiança distribuída, por sua vez, cada autoridade certificadora constitui uma hierarquia independente, não havendo, a princípio, níveis intermediários. Estabelecem-se inúmeras hierarquias, que, para se comunicarem, deverão recorrer à certificação digital cruzada². A forma legal dada ao modelo brasileiro é a de uma estrutura hierarquizada e centralizada, com a previsão da existência de uma única AC-Raiz, que atua e opera com certificados digitais de uso geral em uma estrutura nacional. Nos Estados Unidos, a título de exemplo, diferentemente do modelo centralizado brasileiro, existem diversas espécies de infraestruturas, tanto públicas quanto privadas, de chaves públicas. Neste modelo, a interoperabilidade é um ponto central, com a formação de certificados digitais cruzados, denominados de pontes (“bridges”). Assim, tal modelo é policêntrico, pois inexistente uma estrutura principal de gerenciamento. Ciente das dificuldades apresentadas por este modelo difuso há alguns anos os americanos

“... promoveram a iniciativa do projeto federal Bridge Certification Authority, que tem por escopo fundamental viabilizar a intercomunicação entre os titulares de certificado digitais que adquiriram as suas chaves de Autoridades Certificadoras diversas. Em que pese os esforços, os próprios envolvidos no projeto têm reconhecido que a iniciativa se

²

MENKE, Fabiano. *Assinatura Eletrônica no Direito Brasileiro. Editora Revista dos Tribunais*. São Paulo, RT., 2005, p.

transformou numa empreitada que tem sido marcada pelo lento progresso.”³

Pelo exposto, o modelo brasileiro inspira-se no alemão, com basicamente duas vantagens frente ao norte-americano: a) a uniformidade de padrões técnicos e políticas facilita a interoperabilidade entre os usuários de certificados digitais e gera o aumento das possibilidades de acordos internacionais de reconhecimento recíproco de certificados digitais. Face essas características, é um sistema mais barato, pois não exige esforços para acreditação recíproca; b) o processo de credenciamento prévio imprime maior confiança e credibilidade ao sistema. Assim, é fácil identificar a origem segura do certificado digital.

Uma importante transformação para o direito decorre do aprofundamento das relações humanas pelos sistemas telemáticos via a desmaterialização. Fenômeno típico do desenvolvimento da tecnologia digital projeta-se tanto nas relações sociais quanto nas relações negociais estabelecidas por intermédio da internet. Na sociedade contemporânea, questionou o professor Newton de Lucca⁴, estamos progressivamente suprimindo a presença física das partes na celebração dos negócios e também nas formalidades a ela inerentes? A resposta é positiva, e o certificado digital nada mais é que a segurança dentro do avanço inerente aos sistemas tecnológicos, de acordo com o modelo adotado pela República Federativa do Brasil (CF/88, art. 1º), consubstanciado na Medida Provisória 2.200-2/01.

Pois bem. O substitutivo apresentado na Comissão de Constituição e Justiça e Cidadania pelo Deputado Maurício Rands aperfeiçoa significativamente os avanços já alcançados com o substitutivo aprovado pela Comissão de Ciência e Tecnologia, Comunicação e Informática desta Casa. Mas avanços pontuais devem ainda ser consignados. Assim, o presente projeto deve possuir um norte muito claro a ser seguido: estimular a competitividade ao facilitar o credenciamento do maior número possível de autoridades certificadoras, mas sem permitir, de forma alguma, qualquer fragilidade na segurança da informação assegurada pelos certificados digitais.

Nesse ponto da análise, impende verificar que ainda cabem alguns aprimoramentos no substitutivo já apresentado na Comissão de Constituição e Justiça e Cidadania pelo Deputado Maurício Rands, texto base no presente projeto, pelos quais passamos a expor detalhadamente:

1 – alterar a ementa e toda a estrutura do texto que se refira ao termo “*assinaturas eletrônicas*”, pois a expressão correta é “*assinaturas digitais*”. Isso

³ MENKE, Fabiano. *Assinaturas Digitais, Certificados Digitais, Infra-Estrutura de Chaves Públicas Brasileira e a ICP-Alemã*. Disponível em: <<http://www.buscalegis.ufsc.br/revistas/files/journals/2/.../4429-4422-1-PB.pdf>>. Acesso em: 13 Jan 2010.

⁴ LUCCA, Newton de. *Contratos pela Internet e via computador: requisitos de celebração, validade e eficácia*. Bauru: Edipro, 2001, p. 23.

porque sob a denominação de assinatura eletrônica inclui-se um sem número de métodos de comprovação de autoria empregados no meio virtual. A assinatura digital, portanto, consiste em espécie do gênero assinatura eletrônica, e representa um dos meios de associação do indivíduo a uma declaração de vontade veiculada eletronicamente, mais especificamente, ao procedimento de autenticação baseado na criptografia assimétrica⁵. Consta, inclusive, da definição do Glossário da Câmara Técnica de Documentos Eletrônicos – CTDE, órgão vinculado ao Conselho Nacional de Arquivos - CONARQ:

Assinatura digital

Modalidade de assinatura eletrônica, resultado de uma operação matemática que utiliza algoritmos de criptografia e permite aferir, com segurança, a origem e a integridade do documento. Os atributos da assinatura digital são: a) ser única para cada documento, mesmo que seja o mesmo signatário; b) comprovar a autoria do documento digital; c) possibilitar a verificação da integridade; d) assegurar ao destinatário o “não repúdio” do documento digital, uma vez que, a princípio, o emitente é a única pessoa que tem acesso à chave privada que gerou a assinatura.

Assinatura eletrônica

Geração, por computador, de qualquer símbolo ou série de símbolos executados, adotados ou autorizados por um indivíduo para ser o laço legalmente equivalente à assinatura manual do indivíduo.

2 – alterar a ementa e toda a estrutura do texto que se refira apenas às palavras “*certificação*” e “*certificado*”, pois as expressões corretas são “*certificação digital*” e “*certificados digitais*”. Consta, inclusive, da definição do Glossário da Câmara Técnica de Documentos Eletrônicos – CTDE, órgão vinculado ao Conselho Nacional de Arquivos - CONARQ:

Certificação digital

Atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um certificado digital por uma autoridade certificadora (INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, 2007).

3 – atualizar a definição de documento eletrônico constante no art. 2º, para adequá-la à definição do Glossário da Câmara Técnica de Documentos Eletrônicos – CTDE, órgão vinculado ao Conselho Nacional de Arquivos - CONARQ:

Documento eletrônico

Informação registrada, codificada em forma analógica ou em dígitos binários, acessível e interpretável por meio de um equipamento eletrônico.

⁵ MENKE, Fabiano. *Assinatura Eletrônica no Direito Brasileiro. Editora Revista dos Tribunais*. São Paulo, RT, 2005, p. 42.

4 – retirar a previsão da alínea “d” do inc. VI do art. 2º, pois imprópria, uma vez que a assinatura digital, em si mesma, não é passível de falsificação, mas apenas de utilização fraudulenta.

5 – alterar toda a estrutura do texto que preveja a utilização de “*carimbos de tempo*”, pela expressão “*carimbo do tempo*”, pois a preposição “do” é específica em relação à preposição “de”, que passa a idéia que o carimbo é de qualquer tempo, e não aquela determinada hora, dia, mês e ano. Não por outro motivo foi a expressão consagrada na DOC-ICP-11 (Comitê Gestor da ICP-Brasil) – versão 1.2, 05 de abril de 2010, que estabelece uma visão geral do sistema de carimbos do tempo no Brasil.

6 – inserir, na alínea XIII do art. 2º, o artigo “a”, após a palavra “autorizado” e antes do verbo “emitir”.

7 – substituir, no inciso XIV do mesmo artigo, bem como no art. 23, a palavra “validar” por “verificar”, expressão mais adequada para a atividade desempenhada pelas entidades de registro.

8 – alterar a redação, na alínea “a” do inciso XIX do art. 2º, para: “*a) gerem chaves de assinatura que permitam seu uso por um dispositivo seguro de assinatura*”.

9 – inserir a previsão, no parágrafo único do art. 2º, para que os serviços notariais e de registro também possam atuar como prestadores de serviço de suporte credenciados, com a seguinte redação: “*Equiparam-se a pessoa jurídica, para os fins dos incisos X, XIII, XV e XVII, os que exerçam os serviços notariais e de registro por delegação do poder público, nos termos do art. 236 da Constituição Federal, desde que observados todos os requisitos e as exigências previstas nesta lei*”.

10 – substituir o § 2º do art. 9º pela seguinte redação, contida nos termos de titularidade vigentes com a Resolução CG ICP-Brasil nº 73, de 24 de novembro de 2009: “*O certificado digital é um documento eletrônico de caráter público e seu uso pressupõe a disponibilização de todos os dados nele contidos*”.

11 – já no art. 10, deve-se excluir a expressão de pessoa jurídica, pois restritivo, ou seja, a atuação do Comitê regulamenta tanto os certificado digitais de pessoa jurídica quanto os de pessoa física. Assim, fica a seguinte redação: “*O Comitê Gestor regulamentará a utilização e a responsabilidade pelo uso do certificado digital tanto de pessoa física quanto jurídica*”.

12 – substituir a redação contida no art. 11, inc. II, pela seguinte, também constante nos termos de titularidade vigentes com a Resolução CG ICP-Brasil nº 73, de 24 de novembro de 2009: “*II - houver suspeita de comprometimento de sua chave privada, mídia ou senha, especialmente em caso de perda, furto, roubo, acesso indevido*”. Já no inc. III deve-se alterar a redação para seja prevista a revogação, inclusive de ofício, no caso da utilização por terceiro que não o titular do

certificado, previsão esta que, em conjunto com a disposição criminal desta lei, visa a reforçar o caráter de identificação do usuário do certificado digital. *Verbis*: III - “*caso constatada a sua emissão imprópria, defeituosa ou mesmo a sua utilização por terceiro, inclusive de ofício*”.

13 – no art. 12, alterar a redação para possibilitar a ampliação do aceite de outros tipos de certificado digital com mais segurança, definidos pelo Comitê Gestor da ICP-Brasil, na seguinte redação: “*As aplicações e os demais programas que admitirem o uso de certificado digital qualificado de um determinado tipo devem aceitar qualquer certificado digital qualificado de mesmo tipo ou de outro tipo com requisitos de segurança mais rigorosos, restringindo-se aos tipos de certificado digitais definidos pelo Comitê Gestor da ICP – Brasil*”.

14 – no art. 17, caput, substituir a preposição “de” por “das”, pois mais adequada. Ainda nesse mesmo artigo, incluir a previsão de três representantes dos prestadores de serviços de certificação digital na composição do Comitê Gestor, pois a contribuição desses profissionais, na prática, será valiosa do ponto de vista da segurança nas deliberações do colegiado. *Verbis*: Art. 17: “*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 uma das seguintes entidades, indicados por seus titulares*”. (...). XI - “*três representantes dos prestadores de serviços de certificação digital*”.

15 – no parágrafo primeiro do artigo 11, substituir a redação proposta pela seguinte, pois albergada no Decreto Nº 6.605, de 14 de Outubro de 2008, que dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva – COTEC: “*São convidados para participar das reuniões, em caráter permanente, dois representantes indicados pelo Conselho Nacional de Justiça – CNJ*”.

16 – já o § 5º do art. 17 deve trazer a expressa previsão que o Comitê Gestor é composto por uma Secretaria Executiva e uma Comissão Técnica Executiva – COTEC, *verbis*: “*O Comitê Gestor da ICP-Brasil será composto por Secretaria-Executiva e Comissão Técnica Executiva- COTEC, na forma do regulamento*”.

17 – o inc. VIII do art. 18 deve constar expressamente que compete ao Comitê regulamentar o processo de homologação, nos seguintes termos: VIII – “*regulamentar o processo de homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil*”.

18 – ainda no art. 18, prever expressamente como uma das atribuições do Comitê Gestor da ICP-Brasil: X – “*regulamentar o padrão de assinatura digital avançada*”.

19 – no art. 20, inc. I deve-se inserir o aditivo “e”, entre as palavras “*técnicas*” e “*operacionais*”; já no inciso II, deve-se prever a mesma redação para os carimbos do tempo, *verbis*: II - “*executar as políticas de certificação de carimbo do tempo e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, enquanto Entidade Auditora do Tempo (EAT)*”. Conseqüentemente, devem-se reenumerar todos os incisos subseqüentes.

20 – no art. 20, inserir o inc. VIII, com a seguinte previsão: VIII - “*gerenciar a sua lista de política de assinatura digital avançada*”; e inc. XIV, com a seguinte previsão: XIV - “*gerir processos de homologação de sistemas e equipamentos de certificação digital regulamentados pelo Comitê*”. Inserir, ainda, o seguinte inciso: XV – “*gerir o sistema de emissão de carimbos do tempo regulamentado pelo Comitê Gestor*”

21 – excluir os incisos originais XII e XIII do art. 20, com a conseqüente renumeração dos restantes, pois não afetos ao objeto do Instituto Nacional de Tecnologia da Informação – ITI.

22 – no caput do art. 25, evitar a repetição da palavra carimbo do tempo, substituindo-a pelo pronome “-los”, bem como, no parágrafo primeiro, que a hora a ser utilizada pelas entidades será aquela provida pela Entidade Auditora do Tempo, com a seguinte redação: “*Aos prestadores de serviço de carimbo do tempo credenciados compete emití-los, manter registros de suas operações bem como desempenhar outras atividades correlatas. § 1º A hora a ser utilizada pelos prestadores de serviço de carimbo do tempo credenciados na ICP-Brasil será aquela provida pela Entidade Auditora do Tempo (EAT)*”.

23 – suprimir os artigos 28, 31 e todo o capítulo V (art. 42 a 45) do Título III, pois as atividades de credenciamento, manutenção e encerramento das atividades dos prestadores de serviço de certificação digital, entidades de registro, prestadores de serviço de suporte e prestadores de serviço de carimbo do tempo se encontram inteiramente regulamentadas pelo Comitê Gestor da ICP-Brasil, por meio, entre outros, da Resolução nº 47, de 03 de dezembro de 2007, e não é interessante, do ponto de vista técnico e operacional, cristalizar a matéria com previsão em lei, pois extremamente mutável e requer sucessivas alterações pelo referido Comitê. Quanto ao parágrafo único do art. 34, deve ser suprimido, pois perdeu o objeto em face da inexistência de §1º no art. 40 (antiga remissão).

24 – no art. 30, modificar a redação para a seguinte: “*A assinatura de documentos eletrônicos, decorrente de certificados digitais qualificados, exige o uso de componentes de aplicação de assinatura homologada que indiquem a produção de uma assinatura digital avançada conforme padrão regulamentado pelo Comitê Gestor da ICP-Brasil*”.

25 – aprimorar a redação do art. 37, de modo a assegurar uma maior garantia aos consumidores. *Verbis*: Art. 37. “*Os prestadores de serviço de certificação digital respondem solidariamente com as entidades de registro e os prestadores de serviço de suporte a eles vinculados pelos danos a que derem causa*”.

26 – deve-se extirpar a previsão constante no § 2º do art. 47 e o art. 48 por inteiro, pois a lei não deve conter palavras inúteis, renumerando os artigos subsequentes.

27 – remodelar a previsão contida no art. 43 para estender a proteção do Código de Defesa do Consumidor à toda ICP-Brasil, *verbis*: “*À Certificação Digital aplicam-se as disposições normativas da ICP-Brasil estabelecidas por esta lei, pela AC Raiz – Instituto Nacional de Tecnologia da Informação (ITI) e pelo Comitê Gestor da ICP-Brasil, bem como o Código de Defesa do Consumidor – CDC*”.

28 – já o art. 50 deve ser inteiramente suprimido, pois adota conceitos que destoam da técnica mais avançada e, principalmente, vai ao encontro do PLC 11/07, atualmente em análise na Comissão de Constituição e Justiça do Senado Federal. Isso porque o citado PLC adota procedimentos semelhantes ao da microfilmagem de documentos, a qual dispensa autenticação cartorial, que já são reconhecidos pela sociedade e pela jurisprudência como tecnicamente eficazes e válidos para conferir aos documentos micro filmados os mesmos efeitos jurídicos dos documentos originais. Assim, submeter a validade da “cópia” em meio eletrônico à assinatura do tabelião é gerar custos e burocracia desnecessários, além de ser inviável, do ponto de vista operacional na medida em que estabelece providência para produção de documentos privados digitais não exigida para a produção de documentos privados em papel, perdendo-se a principal vantagem que se pretende com a digitalização. Como se não bastasse, a própria remissão ao art. 223 do código civil não se afigura adequada à espécie, pois mesmo no diploma civil, acaso contestada a autenticidade, o original deve ser exibido. Assim, a conferência pelo tabelião mostra-se, por tudo, despicienda, merecendo tal artigo ser excluído do presente projeto e renumerados os seguintes.

29 – inserir, dentro do Título III, o Capítulo VI (Da Disposição Criminal), para constar a seguinte previsão:

Falsa Identidade

Art. 42 - Usar, como próprio, certificado digital alheio ou ceder a outrem para que dele se utilize, documento dessa natureza, próprio ou de terceiro:

Pena - detenção, de quatro meses a dois anos, e multa, se o fato não constitui elemento de crime mais grave.

Justifica-se a criminalização de tal conduta, pois a atividade de certificação digital por si só já é considerada uma atividade de risco⁶. Por isso, todo cuidado no processo de identificação do titular de um certificado digital é necessário para garantir a lisura do sistema. Daí que um dos pilares da ICP-Brasil, e de qualquer Infra-Estrutura de Chaves Públicas que pretenda ser segura o suficiente⁷, é o requisito de identificação do interessado mediante a sua presença física perante a respectiva Autoridade de Registro⁸. Isso porque ao receber um certificado digital, o titular do certificado terá a possibilidade de concluir uma infinidade de negócios jurídicos que, via de regra, são de valores ilimitados. Assim, a impossibilidade da outorga de procuração convencional para a aquisição ou utilização do certificado digital deriva que a identificação é atributo próprio da personalidade da pessoa, jurídica ou física, intransmissível, por definição (Código Civil art. 11 c/c 52).

Considerando-se que para se obter uma carteira de identidade tradicional é indispensável o comparecimento presencial do cidadão perante o respectivo órgão da Secretaria de Segurança Pública⁹, conclui-se que o fornecimento do certificado digital não pode ter requisitos de segurança de identificação mais abrandados. Nas palavras do Prof. AUGUSTO TAVARES ROSA MARCACINI¹⁰, profissional respeitado da Comissão de Informática Jurídica da própria ORDEM DOS ADVOGADOS DO BRASIL, Seccional São Paulo, se alguém se apropriar da chave privada alheia, poderá ler todos os seus documentos sigilosos e poderá assinar documentos eletrônicos como se fosse o verdadeiro titular das chaves. O usuário é o único guardião da chave privada, a ninguém mais compete protegê-la e mantê-la distante de pessoas mal-intencionadas.

Em razão disso, e em função de não se poder mensurar as conseqüências de uma eventual extrapolação dos limites da atuação do usuário de um certificado digital, já que com um certificado há a possibilidade de se concretizar infindáveis negócios jurídicos, é juridicamente aceitável apenas a presença física do representante legal - como órgão da pessoa jurídica - e da pessoa física quando da solicitação e utilização do certificado digital. Assim, a sua utilização apenas cabe aos mesmos e não a quaisquer terceiros, prática essa infelizmente comum nos dias de hoje, onde os proprietários de pessoas jurídicas simplesmente entregam seus

⁶ Resolução CG ICP-Brasil nº 40, de 18 de abril de 2006, subitem 2.2.2.3.3: O ato de credenciamento da AC condicionará a emissão o do certificado digital pela AC Raiz ou pela AC de nível imediatamente superior, conforme o caso: "(...) b) à apresentação, pela AC credenciada à AC Raiz, no prazo máximo de 10 (dez) dias após o deferimento do credenciamento, de apólice de contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades;"

⁷ "Segurança é Fato, é o direito como factum visível, concreto, que se vê, como a pista de uma rodovia em que se transita, que dá firmeza ao caminhante, para que não se perca nem se saia dos limites traçados pela Autoridade competente." Segurança Jurídica e Jurisprudencial. Carlos Aurélio Mota de Souza. Ed. LTr, 1996, pág. 25.

⁸ O primeiro Projeto de Lei nacional que tentou regular o tema certificação digital foi o Projeto elaborado pela comissão de informática da Ordem dos Advogados do Brasil, seccional São Paulo (PL nº 1.589/99). Tal projeto em seu art. 25 também exigia a presença física do titular de um certificado digital ao estabelecer: "*o tabelião certificará a autenticidade de chaves públicas entregues pessoalmente pelo seu titular, devidamente identificado: o pedido de certificação será efetuado pelo requerente em ficha própria, em papel, por ele subscrita, onde constarão dados suficientes pra identificação da chave pública, a ser arquivada em cartório.*"

⁹ Lei nº 7.116, de 29 de agosto de 1983, regulamentada pelo Decreto nº 89.250, de 27 de dezembro de 1983.

¹⁰ Direito e Informática: Uma abordagem jurídica sobre a criptografia. Rio de Janeiro: Forense, 2002, pág. 51

certificados digitais, principalmente a contadores. Com tal previsão busca-se evitar a prática hoje comum e indubitavelmente desastrosa para a segurança do consumidor.

III – CONCLUSÃO

Por todo exposto, votamos, quanto ao mérito, pela aprovação do Projeto de Lei nº 7.316, de 2002, do Substitutivo da Comissão de Ciência e Tecnologia, Comunicação e Informática, na forma do Substitutivo anexo.

Sala da Comissão, em de de 2010

Deputado Celso Russomanno
Relator

COMISSÃO DE DEFESA DO CONSUMIDOR

SUBSTITUTIVO AO PROJETO DE LEI Nº 7.316, DE 2002

Dispõe sobre o uso de assinaturas digitais e certificados digitais, a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, a prestação de serviços de certificação digital e dá outras providências.

O CONGRESSO NACIONAL decreta:

TÍTULO I

DAS ASSINATURAS DIGITAIS E DOS CERTIFICADOS DIGITAIS

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Esta lei estabelece normas sobre o uso de assinaturas digitais e certificados digitais, a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, a prestação de serviços de certificação digital e dá outras providências.

Art. 2º Para os fins desta Lei entende-se por:

I – documento eletrônico, uma informação registrada, codificada em forma analógica ou em dígitos binários, acessível e interpretável por meio de um equipamento eletrônico;

II - assinatura digital, o conjunto de dados sob forma eletrônica, ligados ou logicamente associados a outros dados eletrônicos, utilizado como método de comprovação da autoria;

III – assinatura digital avançada, a assinatura digital que:

- a) esteja associada inequivocamente a um par de chaves criptográficas que permita identificar o signatário;
- b) seja produzida por dispositivo seguro de criação de assinatura;
- c) esteja vinculada ao documento eletrônico a que diz respeito, de tal modo que qualquer alteração subsequente neste seja plenamente detectável; e
- d) esteja baseada em um certificado digital qualificado e válido à época da sua aposição;

IV – chave de criação de assinatura, o conjunto único de dados eletrônicos, tal como chaves criptográficas privadas, utilizado para a criação de uma assinatura digital;

V – chave de verificação de assinatura, o conjunto de dados eletrônicos, tal como chaves criptográficas públicas, utilizado para a verificação de uma assinatura digital;

VI – dispositivo seguro de criação de assinaturas, o dispositivo físico (hardware) e lógico (software) destinado a viabilizar o uso da chave de criação de assinatura que, na forma do regulamento:

- a) assegure a confidencialidade desta;
- b) inviabilize a dedução desta a partir de outros dados;
- c) permita ao titular proteger a chave de criação de assinatura, de modo eficaz contra o seu uso por terceiros; e
- d) não modifique o documento eletrônico a ser assinado;

VII – certificado digital, o documento eletrônico que vincula uma chave de verificação de assinatura a uma pessoa, identificando-a;

VIII – certificado digital qualificado, o certificado emitido no âmbito da ICP-Brasil por prestador de serviços de certificação digital credenciado que contenha, ao menos:

- a) o seu número de série;
- b) o nome do seu titular e a sua respectiva chave de verificação de assinatura;
- c) a identificação e a assinatura digital avançada do prestador de serviços de certificação digital credenciado que o emitiu;
- d) a data de início e de fim de seu prazo de validade;
- e) as restrições ao âmbito de sua utilização se for o caso;
- f) as restrições ao valor das transações nas quais pode ser utilizado se for o caso;
- g) outros elementos definidos nas normas complementares a esta Lei, aprovadas pelo Comitê Gestor da ICP-Brasil;

IX – prestador de serviços de certificação digital, a pessoa jurídica que emite certificado e presta outros serviços relacionados com assinaturas digitais;

X – prestador de serviços de certificação digital credenciado, o prestador de serviço de certificação digital autorizado a emitir certificado digital no âmbito da ICP-Brasil;

XI – carimbo do tempo, documento eletrônico emitido por uma parte confiável, que serve como evidência que uma informação digital existia numa determinada data e hora;

XII – prestador de serviço de carimbo do tempo, a pessoa jurídica que atua como parte confiável para emissão de carimbos de tempo e presta outros serviços correlatos;

XIII - prestador de serviço de carimbo do tempo credenciado, o prestador de serviço de carimbo do tempo autorizado a emitir carimbos de tempo no âmbito da ICP-Brasil;

XIV - entidade de registro, a pessoa jurídica operacionalmente vinculada a um prestador de serviço de certificação digital, que processa as solicitações de emissão e de revogação de certificado digital, verifica a identidade dos usuários, e desempenha outras atividades correlatas;

XV - entidade de registro credenciada, aquela autorizada a desempenhar suas atividades no âmbito da ICP-Brasil;

XVI – prestador de serviço de suporte, a pessoa jurídica que disponibiliza recursos humanos especializados e/ou infra-estrutura física e lógica a um prestador de serviço de certificação digital, um prestador de serviço de carimbo do tempo ou a uma entidade de registro;

XVII – prestador de serviço de suporte credenciado, o prestador de serviço de suporte autorizado a funcionar no âmbito da ICP-Brasil;

XVIII - componentes de aplicação de assinatura, os produtos físicos (hardware) e lógicos (software) que:

- a) vinculem ao documento eletrônico processo de produção e verificação de assinaturas digitais; ou
- b) verifiquem assinaturas digitais e confirmem certificados digitais, disponibilizando os resultados;

XIX – componentes técnicos para serviços de certificação digital, os produtos físicos (hardware) e lógicos (software) que:

- a) gerem chaves de assinatura que permitam seu uso por um dispositivo seguro de assinatura digital; ou
- b) mantenham certificados digitais disponíveis ao público para verificação por rede de computadores.

Parágrafo único. Equiparam-se a pessoa jurídica, para os fins dos incisos X, XIII, XV e XVII, os que exerçam os serviços notariais e de registro por delegação do poder público, nos termos do art. 236 da Constituição Federal, desde que observados todos os requisitos e as exigências previstos nesta Lei.

CAPÍTULO II DAS ASSINATURAS DIGITAIS E DOS DOCUMENTOS ELETRÔNICOS

Art. 3º A aposição de uma assinatura digital deve referir-se inequivocamente a uma pessoa natural ou jurídica e ao documento eletrônico ao qual é aposta.

Art. 4º As assinaturas digitais avançadas têm o mesmo valor jurídico e probante das assinaturas manuscritas, na forma do art. 219 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil.

Art. 5º A assinatura digital avançada será reconhecida quando aposta durante o prazo de validade do certificado digital em que está baseada e respeitadas as restrições indicadas neste.

Parágrafo único. A assinatura digital avançada aposta após a expiração ou revogação do certificado digital em que está baseada ou que não respeite as restrições indicadas neste equivale à ausência de assinatura.

Art. 6º Não serão negados efeitos jurídicos ao documento eletrônico, desde que admitido como válido pelas partes ou aceito pela pessoa a quem seja oposto, pelo simples fato de sua assinatura digital não ser avançada.

Art. 7º Os carimbos do tempo emitidos por prestador de serviço de carimbo do tempo credenciado presumem-se verdadeiros e revestem-se de pleno valor jurídico e probatório em relação à data e hora neles apostas.

Art. 8º Não serão negados efeitos jurídicos ao carimbo do tempo emitido por prestador de serviço de carimbo do tempo não credenciado, desde que admitido como válido pelas partes ou aceito pela pessoa a quem seja oposto.

CAPÍTULO III

DOS CERTIFICADOS DIGITAIS

Art. 9º O certificado digital qualificado será emitido a um titular, pessoa natural ou jurídica.

§1º O titular do certificado digital gerará o par de chaves criptográficas e responderá pela guarda e pelo uso exclusivo da chave de criação de assinatura digital.

§2º O certificado digital é um documento eletrônico de caráter público e seu uso pressupõe a disponibilização de todos os dados nele contidos.

Art. 10º O Comitê Gestor regulamentará a utilização e a responsabilidade pelo uso do certificado digital tanto de pessoa física quanto jurídica.

Art. 11º O certificado digital qualificado será revogado:

I - por solicitação do titular;

II - houver suspeita de comprometimento de sua chave privada, mídia ou senha, especialmente em caso de perda, furto, roubo, acesso indevido;

III - caso constatada a sua emissão imprópria, defeituosa ou mesmo a sua utilização por terceiro, inclusive de ofício;

IV - caso seja constatada a inexatidão ou desatualização de qualquer dos dados nele constante;

V - por determinação judicial;

VI - em outros casos definidos pelo Comitê Gestor.

§1º A decisão de revogação do certificado digital qualificado com fundamento nos incisos III a V será sempre motivada pelo prestador de serviço de certificação digital credenciado e comunicada ao titular.

§2º Os certificados digitais revogados na forma dos incisos do caput deste artigo serão publicados imediatamente na lista de certificados digitais revogados pelo prestador de serviço de certificação digital que os emitiu.

§3º O titular de certificado digital qualificado deve comunicar ao prestador de serviços de certificação digital ou à entidade de registro a ele vinculado qualquer violação da confidencialidade de sua chave de criação de assinatura ou de sua mídia armazenadora, solicitando a revogação do correspondente certificado digital.

Art. 12. As aplicações e os demais programas que admitirem o uso de certificado digital qualificado de um determinado tipo devem aceitar qualquer certificado digital qualificado de mesmo tipo ou de outro tipo com requisitos de segurança mais rigorosos, restringindo-se aos tipos de certificado digitais definidos pelo Comitê Gestor da ICP – Brasil.

Art. 13. Fica assegurado ao certificado digital emitido no exterior os mesmos efeitos do certificado digital de que trata o inciso VII, do art. 2º.

Parágrafo Único. Tratados, acordos ou atos internacionais de certificação digital bilateral ou de certificação digital cruzada poderão atribuir aos certificados digitais emitidos no exterior os mesmos efeitos do certificado digital de que trata o inciso VIII do art. 2º.

TÍTULO II
DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA
CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 14. A certificação digital realizada no âmbito da ICP-Brasil se sujeitará aos preceitos desta Lei e ao que dispuser, ainda, o seu Comitê Gestor.

Art. 15. A ICP-Brasil tem como objetivo garantir a autenticidade, a integridade e validade jurídica das assinaturas digitais avançadas, para a segurança das transações eletrônicas, aplicações de suporte e aplicações habilitadas que utilizem certificados digitais qualificados.

Art. 16. A ICP-Brasil é composta por uma Autoridade Gestora de Políticas – Comitê Gestor, por uma Autoridade Certificadora Raiz – AC Raiz e, ainda, pelas seguintes entidades credenciadas:

- I - prestadores de serviço de certificação digital;
- II - entidades de registro;
- III - prestadores de serviço de suporte; e
- IV - prestadores de serviço de carimbo do tempo.

CAPÍTULO II
DO COMITÊ GESTOR

Art. 17. 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 das seguintes entidades, indicados por seus titulares:

- I - Ministério da Justiça;
- II - Ministério da Defesa;
- III - Ministério da Fazenda;
- IV - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

V - Ministério do Planejamento, Orçamento e Gestão;
VI - Ministério da Ciência e Tecnologia;
VII - Ministérios das Comunicações;
VIII - Casa Civil da Presidência da República;
IX - Gabinete de Segurança Institucional da Presidência da República; e
X - Advocacia-Geral da União;
XI - Três representantes dos prestadores de serviços de certificação digital.

§ 1o São convidados para participar das reuniões, em caráter permanente, dois representantes indicados pelo Conselho Nacional de Justiça – CNJ.

§ 2o A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 3o Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 4o A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 5o O Comitê Gestor da ICP-Brasil será composto por Secretaria-Executiva e Comissão Técnica Executiva - COTEC, na forma do regulamento.

Art. 18. Compete ao Comitê Gestor da ICP-Brasil:

- I – coordenar o funcionamento da ICP-Brasil;
- II – estabelecer a política, os critérios e as normas técnicas para o credenciamento dos prestadores de serviço de certificação digital, entidades de registro, prestadores de serviço de suporte e prestadores de serviço de carimbo do tempo, em todos os níveis da cadeia de certificação;
- III – estabelecer a política de certificação digital 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 digital e regras operacionais dos prestadores de serviço de certificação digital, entidades de registro, prestadores de serviço de suporte e prestadores de serviço de carimbo do tempo credenciados na ICP-Brasil;
- VI – identificar e avaliar as políticas de infra-estruturas de certificação digital externas, negociar acordos de certificação digital bilateral, de certificação digital 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.

VII – dispor sobre os tipos de certificados digitais no âmbito da ICP-Brasil;

VIII – regulamentar o processo de 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, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança;

X – regulamentar o padrão de assinatura digital avançada.

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

CAPÍTULO III DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

Art. 19. O Instituto Nacional de Tecnologia da Informação - ITI, autarquia federal vinculada à Casa Civil da Presidência da República, é a Autoridade Certificadora Raiz da ICP-Brasil.

Art. 20. Ao ITI compete:

I - executar as políticas de certificação digital e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil;

II - executar as políticas de certificação de carimbo do tempo e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, enquanto Entidade Auditora do Tempo (EAT);

III - propor a revisão e a atualização das normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil;

IV - credenciar e autorizar o funcionamento dos prestadores de serviço de certificação digital, entidades de registro, prestadores de serviço de suporte e prestadores de serviço de carimbo do tempo na ICP-Brasil;

V - aprovar políticas de certificado digital, práticas de certificação digital e regras operacionais dos prestadores de serviço de certificação digital, entidades de registro, prestadores de serviço de suporte e prestadores de serviço de carimbo do tempo credenciados na ICP-Brasil;

VI - gerenciar os certificados digitais dos prestadores de serviço de certificação digital de nível imediatamente subsequente ao seu,

incluindo a emissão, expedição, distribuição e revogação desses documentos eletrônicos;

VII - gerenciar a sua lista de certificados digitais revogados;

VIII - gerenciar a sua lista de política de assinatura digital avançada;

IX - executar as atividades de fiscalização e de auditoria dos prestadores de serviço de certificação digital, entidades de registro, prestadores de serviço de suporte e prestadores de serviço de carimbo do tempo credenciados na ICP-Brasil, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor;

X - aplicar sanções e penalidades na forma da Lei;

XI - promover o relacionamento com instituições congêneres no País e no exterior;

XII - celebrar e acompanhar a execução de convênios e acordos internacionais de cooperação, no campo das atividades de infraestrutura de chaves públicas e áreas afins;

XIII - estimular a participação de universidades, instituições de ensino e iniciativa privada em pesquisa e desenvolvimento, nas atividades de interesse da área da segurança da informação e da infra-estrutura de chaves públicas;

XIV - gerir os processos de homologação de sistemas e equipamentos de certificação digital regulamentados pelo Comitê;

XV - gerir o sistema de emissão de carimbos do tempo regulamentado pelo Comitê Gestor;

XVI - executar outras atribuições que lhe forem cometidas pelo Comitê Gestor da ICP-Brasil.

Parágrafo único. A AC Raiz não emite certificado digital para o usuário final.

Art. 21. Para a consecução dos seus objetivos, o ITI poderá, na forma da lei, contratar serviços de terceiros.

CAPÍTULO IV DAS ENTIDADES CREDENCIADAS NA ICP-BRASIL

Art. 22. Aos prestadores de serviço de certificação digital credenciados, compete emitir, expedir, distribuir, revogar e gerenciar os certificados digitais; manter registros de suas operações; bem como colocar à disposição dos usuários listas de certificados digitais revogados e outras informações pertinentes.

Parágrafo único. É vedado a qualquer prestador de serviço de certificação digital credenciado certificar nível diverso do imediatamente subsequente ao seu, exceto nos casos de acordos de certificação digital lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP Brasil.

Art. 23. Às entidades de registro credenciadas compete processar as solicitações de emissão de certificado digital, verificar a identidade do titular do certificado digital, bem como desempenhar outras atividades correlatas.

Art. 24. Aos prestadores de serviço de suporte credenciados compete, dentre outras atividades correlatas, disponibilizar recursos humanos especializados e/ou infraestrutura física e lógica.

Art. 25. Aos prestadores de serviço de carimbo do tempo credenciados compete emití-los, manter registros de suas operações bem como desempenhar outras atividades correlatas.

§ 1º A hora a ser utilizada pelos prestadores de serviço carimbo do tempo credenciados na ICP-Brasil será aquela provida pela Entidade Auditora do Tempo (EAT).

§ 2º A forma de distribuição dos sinais primários para sincronização de frequência e tempo será definida em normas complementares a esta Lei, aprovadas pelo Comitê Gestor da ICP-Brasil.

TÍTULO III

DA PRESTAÇÃO DE SERVIÇOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL

CAPÍTULO I

DO CREDENCIAMENTO

Art. 26. A prestação de serviço de certificação digital fora do âmbito da ICP-Brasil não se sujeita à prévia autorização do Poder Público, sendo facultativa a solicitação de credenciamento.

Art. 27. O processo de credenciamento dos prestadores de serviço de certificação digital, entidades de registro, prestadores de serviço de suporte e prestadores de serviço de carimbo do tempo será disciplinado pelo Comitê Gestor, além das regras descritas nesta Lei.

Art. 28. O credenciamento do prestador de serviço de certificação digital implicará a emissão de seu certificado digital pela AC Raiz ou por prestador de serviço de certificação digital já credenciado na ICP-Brasil, na forma do parágrafo único do art. 18.

Art. 29. O ato de credenciamento do prestador de serviço de certificação digital pela ICP-Brasil indicará quais os tipos de certificado digitais que este está autorizado a emitir.

§ 1º Caso o credenciamento limite a autorização a determinados tipos de certificados digitais, o prestador de serviço de certificação digital poderá, a qualquer tempo, solicitar nova autorização à emissão de outros tipos de certificados.

§ 2º O certificado digital emitido por prestador de serviço de certificação digital credenciado, e em conformidade à autorização de que trata o caput, conterá a informação de que é um “certificado digital qualificado”, sendo vedado o emprego desta expressão para designar quaisquer outros certificados digitais.

CAPÍTULO II DOS COMPONENTES DE APLICAÇÃO E DOS COMPONENTES TÉCNICOS

Art. 30. A assinatura de documentos eletrônicos, decorrente de certificados digitais qualificados, exige o uso de componentes de aplicação de assinatura homologada que indiquem a produção de uma assinatura digital avançada conforme padrão regulamentado pelo Comitê Gestor da ICP-Brasil.

Art. 31. Os componentes de aplicação de assinatura conterão, conforme dispuser o Comitê Gestor, mecanismos que demonstrem:

- I – a que documento a assinatura se refere;
- II – se o documento não foi modificado;
- III – a que titular de certificado digital está vinculado o documento; e
- IV – o conteúdo do certificado digital em que está baseada a assinatura.

Art. 32. Os componentes técnicos para serviços de certificação digital conterão, conforme dispuser o Comitê Gestor, mecanismos que:

- I – assegurem que as chaves de criação de assinatura produzidas e transferidas a dispositivo seguro de criação de assinatura sejam únicas e sigilosas; e
- II – protejam os certificados digitais que estejam disponíveis para verificação e obtenção na rede de alterações, cópias ou obtenções (download) não autorizadas.

CAPÍTULO III

DOS DEVERES DAS PRESTADORAS DE SERVIÇOS DE CERTIFICAÇÃO DIGITAL

Art. 33. O prestador de serviço de certificação digital credenciado deverá, no momento da solicitação de emissão de um certificado digital qualificado, informar o solicitante, prévia e adequadamente sobre:

- I – os efeitos jurídicos das assinaturas eletrônicas avançadas;
- II – a forma de geração do par de chaves criptográficas;
- III – as medidas necessárias para a proteção e segurança da chave de criação de assinatura;
- IV – as medidas necessárias para a verificação de assinaturas eletrônicas de maneira confiável; e
- V – os casos e as formas de revogação do certificado digital.

Parágrafo único. Os contratos de prestação de serviço de certificação digital serão redigidos em termos claros e com caracteres legíveis, de modo a facilitar a compreensão de suas cláusulas.

Art. 34. O prestador de serviço de certificação digital credenciado deverá informar os titulares de certificado digitais qualificados por ele emitidos do encerramento de suas atividades, para que estes possam:

- I – solicitar a revogação de seu certificado digital; ou
- II – autorizar a transferência de sua documentação a outro prestador de serviço de certificação digital credenciado para preservação do certificado digital.

Art. 35. O prestador de serviço de certificação digital credenciado é obrigado a manter confidencialidade sobre todas as informações obtidas do titular que não constem do certificado digital qualificado.

§ 1º Os dados pessoais não serão usados para outra finalidade que não a de certificação digital, salvo se consentido expressamente pelo requerente, por cláusula em destaque, que não vincule a prestação do serviço de certificação digital, ou se obtido por fonte diversa.

§ 2º A quebra da confidencialidade das informações de que trata o caput deste artigo, quando determinada pelo Poder Judiciário, respeitará os mesmos procedimentos previstos em lei para a quebra do sigilo bancário.

CAPÍTULO IV DA RESPONSABILIDADE PELA PRESTAÇÃO DO SERVIÇO DE CERTIFICAÇÃO DIGITAL

Art. 36. As entidades integrantes da ICP-Brasil, inclusive a AC Raiz, respondem diretamente pelos danos a que derem causa.

Art. 37. Os prestadores de serviço de certificação digital respondem solidariamente com as entidades de registro e os prestadores de serviço de suporte a eles vinculados pelos danos a que derem causa.

Art. 38. Os prestadores de serviço de carimbo do tempo respondem solidariamente pelos danos a que derem causa os prestadores de serviço de suporte a eles vinculados.

Art. 39. São nulos de pleno direito os itens das políticas de certificado digital e das práticas de certificação digital, bem como as cláusulas dos contratos de prestação de serviço de certificação digital, que impossibilitem, exonerem ou atenuem a responsabilidade do prestador de serviço de certificação digital por vícios de qualquer natureza dos serviços por eles prestados.

Parágrafo único. Em situações justificáveis, poderá ocorrer limitação da indenização quando o titular do certificado digital for pessoa jurídica.

CAPÍTULO V DA INFRAÇÃO E DAS PENALIDADES

Art. 40. A AC Raiz poderá tomar as medidas necessárias para prevenir ou coibir a prática de atos contrários a esta Lei ou às suas normas complementares, praticados pelos prestadores de serviço de certificação digital, entidades de registro, prestadores de serviço de suporte ou prestadores de serviço de carimbo do tempo credenciados na ICP-Brasil.

Art. 41. A infração por prestador de serviço de certificação digital credenciado a qualquer dispositivo desta Lei ou das normas complementares aprovadas pelo Comitê Gestor da ICP-Brasil, assim como as determinações exaradas pela AC Raiz da ICP-Brasil, implicará a aplicação das seguintes penalidades, conforme a gravidade da infração e na forma da Lei:

- I – advertência por escrito;
- II – multa simples ou diária de R\$ 100,00 (cem reais) a R\$ 1.000.000,00 (um milhão de reais);
- III – proibição de credenciamento de novas políticas de certificado digital;
- IV – suspensão da emissão de novos certificados digitais; e
- V – descredenciamento.

§1º As penalidades poderão ser aplicadas isoladas ou cumulativamente.

§2º A penalidade prevista no inciso V será aplicada, sem prejuízo de outras sanções cabíveis, quando:

I – o credenciamento for obtido por meio de declarações falsas ou outros meios ilícitos;

II - no exercício de atividade de prestação de serviço de certificação digital estiverem sendo praticados atos em desconformidade com esta lei ou com normas complementares aprovadas pelo Comitê Gestor da ICP-Brasil.

§3º Da decisão de descredenciamento caberá pedido de reconsideração e recurso com efeito suspensivo, na forma das normas complementares a esta lei, aprovadas pelo Comitê Gestor da ICP-Brasil.

CAPÍTULO VI DA DISPOSIÇÃO CRIMINAL

Crime de Falsa Identidade

Art. 42 - Usar, como próprio, certificado digital alheio ou ceder a outrem, para que dele se utilize, documento dessa natureza, próprio ou de terceiro:

Pena - detenção, de quatro meses a dois anos, e multa, se o fato não constitui elemento de crime mais grave, sem prejuízo do disposto no Código Penal e leis especiais.

TÍTULO IV DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 43. À Certificação Digital aplicam-se as disposições normativas da ICP-Brasil estabelecidas por esta lei, pela AC Raiz – Instituto Nacional de Tecnologia da Informação (ITI) e pelo Comitê Gestor da ICP-Brasil, bem como as da Lei nº 8.078, de 11 de setembro de 1990 - Código de Proteção e Defesa do Consumidor.

Art. 44. O Poder Executivo disporá sobre o uso de certificados digitais qualificados na emissão de passaportes, de documentos de identidade, de carteira nacional de habilitação, de certificados digitais de registros de veículos, bem como em outras aplicações.

