O FEDERALISMO NORTE-AMERICANO E O MODELO DE CERTIFICAÇAO DIGITAL: COMPRARAÇAO COM O MODELO BRASILEIRO

THE AMERICAN FEDERALISM AND DIGITAL CERTIFICATION MODEL: COMPARISON WITH THE BRAZILIAN MODEL

Paulo Ronaldo Ceo de Carvalho
Procurador Federal em exercício na Procuradoria Federal Especializada do Instituto Nacional de Tecnologia da Informação – ITI.
Especialista em Direito Público pela Universidade de Brasília – UNB

SUMARIO: Introdução; 1 O federalismo norte-americano; 2 A atividade de certificação digital e uma infra-estrutura de chaves públicas – PKI; 2.1 Proteção dos dados no meio eletrônico: certificação digital como solução; 2.2 A infra-estrutura de chaves públicas; 3 A Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil; 4 O modelo norte-americano de certificação digital; 5 Conclusão; Referências.

RESUMO: O peculiar federalismo norte-americano tem direta relação com o modelo de certificação digital adotado nos Estados Unidos. A grande autonomia dos estados membros, os quais estão autorizados a legislar sobre matérias relacionadas ao direito civil, possibilitou o surgimento de um quadro em que coexistem diversas leis tratando de assinaturas digitais e eletrônicas, bem como diversas infra-estruturas de chaves públicas (ICPs) de iniciativas tanto públicas quanto privadas. Para permitir a interoperabilidade entre as ICPs existentes no modelo norte-americanode, de confiança compartilhada, foi criada a figura da Autoridade Certificadora Ponte, inexistente em modelos de confiança hierárquicos.

PALAVRAS-CHAVE: Federalismo. Autonomia. Certificação digital. Infra-Estrutura de Chaves Públicas - ICP. Confiança Compartilhada. Interoperabilidade. Autoridade Certificadora Ponte.

ABSTRACT: The peculiar American federalism has direct relationship with the digital certification model adopted in the United States. The wide discretion of the member states, which are allowed to legislate on matters related to civil law, enabled the emergence of a framework in which there are several laws dealing with digital and electronic signatures and various public key infrastructure (PKIs) initiative both public and private. To enable interoperability between existing PKIs in American model, shared trust, was created the figure of the Bridge Certification Authority, noneexistent in hierarchical models.

KEYWORDS: Federalism. Autonomy. Digital Certification. Public Key Infrastucture – PKI. Shared Trust or Mesh PKI. Interoperability. Bridge Certification Authority.

INTRODUÇAO

Com o crescimento exponencial do uso do meio eletrônico para a satisfação das diversas necessidades do nosso cotidiano, fez-se necessário o uso da tecnologia para tornar esse uso mais seguro e eficaz. Atualmente, a certificação digital, baseada na criptografia assimétrica, é a tecnologia mais avançada para a segura comunicação no meio eletrônico, contornando o problema da atribuição de autoria e integridade dos documentos produzidos neste meio.

Uma infra-estrutura de chaves públicas, cadeia de confiança que viabiliza a emissão de cetificados digitais, pode ser configurada em modelos distintos, a saber, o hierárquico e o de confiança distribuída.

Os Estados Unidos da América adotaram em seu sitema jurídico de certificação digital o modelo de confiança distribuída, distanciando-se do modelo adotado no Brasil e na Europa.

O presente estudo pretende expor, simplificadamente, a relação entre o federalismo norte-americano e o modelo de certificação digital adotado nos Estados Unidos, comparando o mesmo com o modelo adotado no Brasil na Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil.

Para tanto, serão feitos alguns registros sobre o federalismo norte-americano e a sua influência sobre o sistema jurídico local, e sobre certificação digital e infra-estrutura de chaves públicas; a análise do modelo adotado no Brasil e, por fim, nos Estados Unidos.

1 O FEDERALISMO NORTE-AMERICANO

O federalismo, que tem as suas primeiras origens nos Estados Unidos, surgiu como resposta à necessidade de um governo eficiente em um grande território, que, ao mesmo tempo, assegurasse os ideais republicanos que vingaram com a revolução de 1776[1].

O Estado federal é aquele no qual existe uma distribuição de poder entre um ente dotado de soberania e outros dotados de autonomia. Diferentemente do que ocorre com a confederação, que nasce através de um tratado ou acordo entre as partes[2], já que cada um tem soberania e sua própria constituição, a federação tem início por meio de uma

1 MENDES, Gilmar Ferreira. *Curso de direito constitucional*. São Paulo: Saraiva, 2007. p. 753

2 Segundo MENDES, "para garantir a independência então conquistada, as antigas colônias britânicas firmaram um tratado de direito internacional, criando uma confederação, que tinha como objetivo básico preservar a soberania de cada antigo território colonial". Cf. MENDES, op. cit., p. 753

constituição, que prevê que um ente será soberano e todos os demais serão autônomos. Por isso, não há direito de secessão no Estado federal.

Deve ser mencionado, ainda, que no Estado federal todos os estados membros são dotados de poder constituinte decorrente, o que não ocorre no Estado unitário, que não possue tal poder.

Existem, entretanto, tipos de Estados federais diferentes, analisando-se a concentração de poder dentro de cada federação. Percebe-se claramente tal diferença na comparação da nossa federação com a federação norte-americana. É que o nosso federalismo, originalmente, é centrífugo ou por segregação, ao passo que o deles é centrípeto ou por agregação.

Por centrifugo ou por segregação entende-se aquelas federações que tinham um forte e único poder central, divididas, posteriormente em unidades autônomas. Nasce do centro para a periferia. É um federalismo de cunho centralizador. O pólo central tem diversas competências. É o caso do Brasil, que era um Estado unitário em 1824.

A federação centripeta ou por agregação, nasce de uma comunhão de forças direcionadas da periferia para o centro. Os Estados Unidos antes eram uma confederação, com diversos estados soberanos, transformado, posteriormente, em uma federação. Para MENDES:

> Cada entidade componente da confederação retinha a sua soberania, o que enfraquecia o pacto. As deliberações dos Estados Unidos em Congresso nem sempre eram cumpridas, e havia dificuldades na obtenção de recursos financeiros e humanos para as atividades comuns. Além disso, a confederação não podia legislar para os cidadãos, dispondo, apenas, para os Estados. Com isso não podia impor tributos, ficando na dependência da intermediação dos Estados confederados. As deliberações do Congresso, na prática, acabavam por ter eficácia de meras recomendações. Não havia, tampouco, um tribunal supremo, que unificasse a interpretação do direito comum aos Estados ou que resolvesse juridicamente diferenças entre eles.
>
> A confederação estava debilitada e não atendia às necessidades de governo eficiente comum do vasto território recém-libertado. O propósito de aprimorar a união entre os Estados redundou na original fórmula federativa, inscrita pela Convenção de Filadélfia de 1787 na Constituição elaborada, conforme se vê do próprio preâmbulo da carta, em que se lê: 'nós, o povo do Estados Unidos, a fim de formarmos uma União mais perfeita[...]'.

> Os antigos Estados soberanos confederados deixaram de ser soberanos, mas conservaram a sua autonomia, entregando a uma nova entidade, a União, poderes bastantes para exercer tarefas necessárias ao bem comum de todos os Estados reunidos. Passaram, por outro lado, a compor a vontade da União, por meio de representantes do Senado.[3]

Não existia um governo central criado. Antes da formação dos Estados Unidos eram 13 colônias separadas, regradas pela Inglaterra. Cada uma possuía seu próprio governo, sua própria cultura. Elas se uniram em 4 de julho de 1776 em uma tentativa de se libertarem dos ingleses. Para REINHART:

> Before the United States became a sovereign nation, it consisted of thirteen colonies belonging to Great Britain. On July 4, 1776, the colonies proclaimed independece from Great Britain, and that year representatives from each colony met in Philadelphia to sign the Declaration of Independence. The colonists recognized the need for a confederation of states to gain and maintain their independence from Great Britain and to strengthen their economic power. Together they wrote the Articles of Confederation, which were adopted by Congress in 1777 but not ratified by the states until 1781. The Articles provided for national protection of the colonies but did not give adequate power to the national governement. Great Britain relinquished its claim to the former colonies in 1782.
>
> The U.S. Constitution, intented to replace the Artices of Confederation, was completed in 1787 and ratified in 1789. Beforethe Constitution was written, lengthy arguments occurred over how much power the national (federal) government and stat governments would have. The Constitution reflects a compromise in qhich both share power. It outlines the powers given to the federal government and leaves other powers to the states.[4]

Com sua libertação da Inglaterra, passou-se a ter 13 países separados. Mas eles precisaram permanecer atrelados, para manter uma organização. Deve ser mencionado que o legislativo da confederação

3 MENDES, op. cit., p. 753.

4 REINHART, Susan M.. *Strategies for legal case Reading and vocabular development.* University of Michigan. 2007. p. 146

tinha poderes muito limitados. Mesmo para aprovar uma lei, fazia-se necessária a aprovação de pelo menos 9 Estados. Havia um grande receio quanto à formação de uma autoridade central.

Percebe-se, então, que enquanto as 13 colônias da América do Norte, que se reuniram em uma confederação, constituíam uma porção minima desse território, o Brasil já era um país de dimensões continentais quando a constituição de 1891 instituiu a federação como união indissolúvel e perpétua de suas antigas províncias. Desde a sua origem os Estados Unidos já eram federalistas, enquanto que o nosso país nasceu unitário. Para REALE:

> É que, no caso da república do Norte passa-se de uma multiplicidade de Estados, já constituídos,para um pacto federativo (donde a denominação de Estados Unidos da América) enquanto que no Brasil evoluímos de um Estado unitário para uma descentralização administrativa com a outorga de plena autonomia às antigas provícias do império.
>
> Essa distinção histórica importa em consequencias de vulto que não podem ser esquecidas. É que a federação norteamericana surgiu de um entendimento entre entidades políticas já constituídas, com seus quadros jurídico-políticos delineados de maneira independente, enquanto que no Brasil ocorria processo inverso, mantendo-se a unidade do Direito não constitucional.
>
> Isso explica por qual razão o federalismo norteamericano desenvolveu-se sem afetar as várias estruturas jurídicas estaduais, no tocante, por exemplo, aos direitos civil, mercantil e penal, cada Estado preservando, em suma, o que lhe era próprio, a sua organização jurídica. Basta lembrar o caso extremo da Luisiana, que continuou subordinado a um código moldado no francês de Napoleão, enquanto os demais estados preservavam sua experiência peculiar de *common law*, de natureza não legislativa, mas judicial-costumeira. Daí a estranheza com que vemos, por exemplo, a adoção lá de pena de morte ou a resposnabilidade penal dos menosres em uns Estados federativos e em outros não, com contrastes impressionantes no ordenamento jurídico do país.[5]

5 REALE, Miguel. *O Nosso Federalismo*. Disponível em: <http://www.miguelreale.com.br/artigos/nosfed.htm>. Acesso em: 19 set. 2011.

Continua, o autor supracitado, discorrendo que, por sua vez, no Brasil, as disposições jurídicas infra-constitucionais continuaram sendo as mesmas, herdadas de Portugal, em todo o País, permanencendo em pleno vigor o Código Filipino e demais legislações do império[6]. Arremata afirmando que "*nosso federalismo não foi, pois, integral, mas limitado ao plano político-constitucional*"[7].

Entretanto, observa-se que poucos dentre os novos estados norte-americanos independentes votariam para a ratificação de qualquer Constituição que não contivesse a previsão de um papel vigoroso e significativo para os estados signatarios[8].

Percebe-se que os estados norte-americanos não foram criados pela Constituição. Não existiu a necessidade de criá-los, já que os mesmo já existiam em 1787. Ressalte-se que tais estados escreveram e ratificaram aquela constituição[9]. Segundo BURNHAM:

> This fact of states 'aboriginal' existence makes the nature of the power of states significantly different from that of the federal government. The thirteen colonies emerged form the War of Independence as separate sovereign nation-states. Their status as such was modified only to the extent that they gave up certain rights in the Constitution of 1789 and later amendments to it. Thus, states need not search the federal Constitution for some positive grant of power to act or to make law: they have the power and inherent competence of separate, independent and sovereign nations and may pass legislation on any subject they choose, except as limited by the federal Constitution or their own constitutions. The text of the Tenth Amendment delineates this principle: 'The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people'.[10]

Ainda, deve ser mencionado que, em linhas gerais, a estrutura governamental de muitos estados americanos é semelhante à estrutura de poder do governo federal. Muitos conceitos foram emprestados das

6 REALE, op. cit.

7 REALE, op. cit.

8 BURNHAM, William. *Introduction to the law and legal system of the United States.* St. Paul: Thomson/West, 2006. p. 18.

9 BURNHAM, op. cit., p. 19.

10 BURNHAM, op. cit. p 19.

constituições estaduais e colocados na Constituição federal de 1789. Também, como os estados americanos conceberam, periodicamente, novas constituições, após a ratificação da constituição federal, eles copiaram da mesma alguns pontos[11]. Para BURNHAM:

> Executive power in most states is more diffused than federal executive power. On the federal level, the President appoints the members of his cabinet and other high-level executive official with the advice and consent of the Senate. By contrast, in many states, the heads of some major divisions of state government, such as the Attorney General or the Secretary of State or the Auditor General, are directly elected by the people. As such, they neither owe their office to the Governor nor can they be dismissed by the Governor. In many states, these officials are members of a different political party from the governor. It is even the case in some states that the Lieutenant Governor of the state is from a different political party than the Governor.[12]

É comum que os estados copiem a estrutura federal. Entretanto, não há uma regra. Como visto acima, ainda existem estados que não seguem o modelo federal americano em coisas básicas, como a forma de escolha de membros do alto escalão. Além disso, existem estados com legislativo unicameral, em detrimento da maioria, que possui legislativo bicameral, a exemplo do que ocorre no plano federal. Percebe-se, então, que os estados, em geral, copiam a estrutura do executivo federal. Mas não só. Copiam, em geral, o modelo de judiciário federal, com a alteração da nomenclatura das cortes. Entretanto, não observa-se uma obrigatória simetria.

Resta evidente que o federalismo americano difere do federalismo brasileiro. Mas não só. Difere também de outras formas de federalismo. Em outros federalismos, há a criação das divisões e dos entes federativos. Nos Estados Unidos os estados eram independentes e decidiram, abrindo mão de parte dos seus poderes e de sua soberania, formar uma união de estados federados.

Entretanto, levando-se em consideração que antes eram dotados de soberania, e ante a grande resistência de ceder os seus poderes ao governo central, observa-se que os estados possuem um nível de autonomia, em relação ao poder central, muito mais elevado que o de outras entidades federativas de outras federações, a exemplo do Brasil,

11 BURNHAM, op. cit. p. 19.

12 BURNHAM, op. cit. p. 20.

ainda que, venha sendo observado um crescimento progressivo do poder federal em relação ao poder dos estados.

A relação entre o poder federal e os estados, denominada de federalismo vertical, assim como o federalismo horizontal, que se refere ao relacionamento dos estados entre si, desde 1789, tem sofrido consideráveis mudanças. Observa-se o crescimento do primeiro e uma diminuição do segundo[13]. GODOY, ao tratar do federalismo vertical, afirma que:

> Essa relação é historicamente o resultado de conflitos políticos, de compromissos de consenso. O pacto federalista limita o poder entre as unidades da federação mesmo quando o governo central regula relações entre os estados, a exemplo do comércio interestadual. Três cláusulas orientam o pacto federativo norte-americano, a saber; a) os estados foram preservados como fontes de poder, com autoridade e natureza de órgãos da administração; b) aos estados foram reservados importantes poderes quanto à composição do governo central e os governos estaduais; e c) os poderes governamentais foram divididos entre o governo central e os governos estaduais.[14]

Nos Estados Unidos, levando-se em consideração os fatos históricos antes narrados, os estados mantiveram uma parcela significativa de poder e podem, inclusive, legislar sobre matérias relacionadas ao direito civil, comercial e penal. No Brasil, por força do que dispõe o art. 22, inc. I, da nossa Constituição Federal, tais matérias são de competência privativa da União. Só uma lei complementar poderia autorizar os estados a legislar sobre questões específicas relacionados a essas matérias.

E é sob esse prisma, das diferentes características entre o federalismo americano e o brasileiro, que será analisada a certificação digital nos Estados Unidos, bem como o sistema de certificação digital brasileiro.

2 A ATIVIDADE DE CERTIFICAÇAO DIGITAL E UMA INFRA-ESTRUTURA DE CHAVES PUBLICAS - PKI

2.1 PROTEÇAO DOS DADOS NO MEIO ELETRONICO: CERTIFICAÇAO DIGITAL COMO SOLUÇAO

É certo que alguns espaços e algumas relações no meio virtual exigem um ambiente seguro, com a correta identificação dos usuários.

13 BURNHAM, op. cit. p. 18. (tradução livre)

14 GODOY, Arnaldo Sampaio de Moraes. *Direito nos Estados Unidos*. Barueri, São Paulo: Manole, 2004. p. 73.

É que nestes meios são firmados contratos eletrônicos, movimentadas contas bancárias, enviadas informações sigilosas de uma filial para uma matriz da empresa, por exemplo.

Com o exponencial crescimento da *internet*, bem como com a expansão dos demais espaços virtuais, observa-se que a individualidade e a proteção das informações, enviadas pelo meio virtual, ficaram vulneráveis e suscetíveis a um excesso de transparência[15]. A *internet*, considerada uma rede aberta, apesar de possibilitar um incremento nas possibilidades de relações sociais, torna arriscada a realização de trocas comerciais e transferências de dados sensíveis[16].

A proteção de dados pessoais e a identificação com segurança do usuário constituem premissas básicas para a segurança da informação no meio digital. Para tanto, são desenvolvidas técnicas que tentam garantir o sigilo das informações circulantes, a integridade dos dados e a precisa identificação dos usuários do meio digital.

No meio digital, a segurança da informação circulante relaciona-se com conceitos de privacidade e integridade. Quer dizer, a informação, caso deseje o emissário ou destinatário da informação, poderá ser resguardada, impedindo violações e a alteração dos dados que a compõe.

De modo a garantir os pilares fundamentais de um ambiente seguro, é utilizada a criptografia. A criptografia é um processo pelo qual uma mensagem é transformada em outra mensagem usando uma função matemática e uma senha especial de criptografia, chamada chave.

Com efeito, "*as declarações de vontade com escopo de contrair obrigações, ou de alguma forma produzir efeito jurídico na esfera alheia, não podem dispensar a sua autoria e integridade*"[17]. Busca-se assim, ao proteger os dados pessoais e ao identificar o usuário, diminuir o fundado temor de ocorrência de fraudes.

Para VERONESE, "*o problema da segurança nas trocas eletrônicas é uma questão técnica bastante ampla*"[18]. Segundo o autor, o atual "*estado da técnica*" é revolucionária criptografia assimétrica, que se mostrou revolucionária em relação ao modo anterior de embaralhar mensagens (criptografia simétrica)[19]. É que a fraqueza dos sistemas simétricos residia na necessidade de transmitir a chave criptográfica entre as partes envolvidas.

---

15 VERONESE, Alexandre et al. *Segredo e democracia: certificação digital e software livre. Informática pública*, vol. 8 (2): 09-26, 2007, p. 9.

16 VERONESE, op. cit, p. 9-10.

17 MENKE, Fabiano. *Assinatura eletrônica:* aspectos jurídicos no direito brasileiro. São Paulo: RT, 2005, p. 37.

18 VERONESE, op. cit, p. 11.

19 VERONESE, op. cit, p. 11.

A realidade atual pede que nos negócios, a segurança seja componente crítico com o fito de proteger informações sensíveis da corporação. É que, como se verá adiante, a capacidade da Infra-Estrutura de Chaves Públicas oferece a possibilidade de que o individuo seja autenticado, criptografando e assinando digitalmente com privacidade, acessando de maneira segura a rede corporativa da empresa, protegendo os arquivos pessoais, possibilitando operações de *e-commerce*, remotamente, e assinando e-mails com proteção forte.

A certificação digital visa garantir a autenticidade das informações enviadas pelo meio virtual, identificando o emissor ao receptor das informações, possibilitando o trânsito de mensagens criptografadas, permitindo, conseqüentemente, o sigilo na comunicação[20].

Deve ser mencionado que o certificado digital constitui-se em um documento eletrônico que identifica pessoas, cuja validade é garantida por uma terceira parte de confiança. "*É uma estrutura de dados sob a forma eletrônica, assinado digitalmente por uma terceira parte de confiável que associa o nome e atributos de uma pessoa a uma chave pública*"[21]. Tem-se que:

> O fornecimento de um certificado digital é um serviço semelhante ao de identificação para a expedição de carteiras de identidade, só que o certificado é emitido com prazo de validade determinado. O interessado é identificado mediante a sua presença física pelo terceiro de confiança – com a apresentação dos documentos necessários – e este lhe emite o certificado digital.[22]

Dessa maneira, quando uma mensagem é assinada digitalmente, geralmente estará acompanhada do certificado digital do remetente, onde constará a chave pública do mesmo, entre outros dados. É que um software do destinatário aplicará a chave pública do emissor na mensagem e confirmará a autoria e a integridade do documento eletrônico[23].

2.2 A INFRA-ESTRUTURA DE CHAVES PUBLICAS

Uma infra-estrutura tem como princípio ser uma instalação estrutural posta à disposição da sociedade para prover determinado

20 VERONESE, op. cit. p. 11.

21 MENKE, op. cit., p. 49.

22 MENKE, op. cit., p. 49.

23 MENKE, op. cit., p. 50.

serviço, que poderá ser usufruído por qualquer interessado[24], objetivando a comunicação entre os envolvidos, ou o mero acoplamento, e, ao mesmo tempo, evitando a aplicação de soluções diferentes por cada interessado.

Busca-se a interoperabilidade com uma infra-estrutura. Ou seja, evita-se que soluções diferentes sejam aplicadas por qualquer um, e, com isso, venha a contribuir com a insegurança e o caos de dado sistema estrutural. Faz-se necessário, assim, que os equipamentos que compõem a infra-estrutura comuniquem-se, independentemente do fornecedor ou da marca do produto.

Tem-se, dessa maneira, que *"a infra-estrutura existe para que qualquer usuário possa simplesmente acoplar-se a ela e dela fazer uso quando necessário"*[25]. Tal raciocínio deve ser aplicado a uma infra-estrutura de chaves públicas, já que não seria coerente que indivíduos não pudessem se comunicar, transacionar ou mesmo acessar bancos de dados e contas correntes por terem certificados digitais de procedências diversas, por exemplo. Percebe-se, portanto, que a interoperabilidade tem como finalidade atingir toda a coletividade.

A expressão "infra-estrutura de chaves públicas" decorre da tradução do inglês de *public-key infrastructure (PKI)*. Uma Infra-estrutura de Chaves Públicas (ICP) ou Public Key Infraestruture (PKI) constitui-se em uma organização (sistema) que dispõe e abastece um serviço de certificação pública e serviços relacionados, que efetuam essa confiança por meio de tecnologia, infra-estrutura, práticas e procedimentos previamente determinados e periodicamente auditados. Para MENKE:

> Uma infra-estrutura de chaves públicas (ICP) poderia ser conceituada como um sistema que tem por finalidade precípua, mas não exclusiva, atribuir certificados digitais (e conseqüentemente assinaturas digitais) a um universo de usuários. Em realidade, além de fornecerem estes documentos eletrônicos às pessoas naturais, aos órgãos e às entidades públicas e privadas, os entes que compõem uma ICP – os terceiros de confiança – desempenham a tarefa de gerenciar o ciclo de vida dos certificados, uma vez que, a qualquer momento, pode haver necessidade de revogar e emitir novos certificados, como no caso de comprometimento da chave privada de determinado titular de um certificado digital em virtude de roubo ou de fraude.[26]

24 MENKE, op. cit., p. 56-57 e 58.

25 MENKE, Op. cit., p. 57.

26 MENKE, op. cit., p. 56.

REINALDO FILHO entende que:

> [...] uma Infra-Estrutura de Chaves Públicas (ICP) é um conjunto de regimes normativos, procedimentos, padrões e formatos técnicos que viabilizam o uso em escala da criptografia de chaves públicas; constitui um modelo formado por *autoridades certificadoras* responsáveis pela geração e gerenciamento de chaves e certificados públicos, utilizados (como método ou tecnologia viável) para garantir a autenticidade, a integridade e a validade jurídica de documentos e transações eletrônicas.[27]

Finalmente, registre-se que uma infra-estrutura de chaves públicas pode ser configurada basicamente em dois modelos: o hierárquico e o de confiança distribuída.

O primeiro é configurado numa hierarquia, na forma de uma árvore invertida, situando-se no topo uma entidade na qual todos os que vêm abaixo, inclusive os usuários, devem confiar. A confiança se dissemina de cima para baixo. A entidade localizada no ápice da hierarquia, denominada Autoridade Certificadora Raiz, emite um certificado para uma autoridade certificadora de segundo nível, e esta emite um certificado para o usuário final.

No modelo de confiança distribuída, 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 cruzada.[28]

3 A INFRA-ESTRUTURA DE CHAVES PUBLICAS BRASILEIRA - ICP-BRASIL

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 de uso geral em uma estrutura nacional. Para VERONESE:

> O sistema criado é estruturado como uma pirâmide ou como uma cadeia de certificação digital, que tem no seu vértice o ITI. O vértice

27 REINALDO FILHO, Demócrito. A ICP-Brasil e os poderes regulatórios do ITI e do CG . *Jus Navigandi*, Teresina, ano 10, n. 869, 19 nov. 2005. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=7576>. Acesso em: 08 fev. 2010.

REINHART, Susan M. *Strategies for legal case Reading and vocabular development.* University of Michigan. 2007.

28 MENKE, op. cit., p. 58.

> não significa controle direto e sim fiscalização (auditoria técnica) e determinação de procedimentos padronizados (regulamentos) pelas entidades que, efetivamente, certificam cidadãos.[29]

A Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil é o Sistema Nacional de Certificação Digital, que foi instituído pela Medida Provisória nº 2.200-2/01[30], 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. 1º).

MARTINI trata a Infra-Estrutura de Chaves Públicas Brasileira como um sistema. Para ele:

> Trata-se de um sistema composto de subsistemas fundamentais e constitutivos. Há um subsistema de *acreditação*, que visa a auditoria de conformidade aos padrões de interoperabilidade e de segurança das ACs e ARs integrantes e seu credenciamento.
>
> É ladeado por um subsistema de segurança física e lógica, bastante exigente e rigoroso para ambientes computacionais. Um subsistema para homologação de sistemas e equipamentos, que é o nosso Laboratório de Ensaios e Auditoria, já tratado de forma específica em diversas ocasiões. E, por fim, um subsistema de datação eletrônica, todavia ainda em vivo debate no Comitê Gestor da ICP-Brasil. Pode-se, sem dúvida, observar a presença de um "sistema auxiliar" jurídico e de normalização – pois todas as regras do sistema ICP-Brasil são públicas e bem definidas.[31]

Percebe-se que a ICP-Brasil busca realizar critérios objetivos de confiança. Segundo MARTINI, "*o sistema ICP-Brasil é um sistema de confiança*"[32]. Para o autor:

---

29 VERONESE, op. cit, p. 22.

30 A referida Medida Provisória permanece em vigor, tendo em vista o disposto no § 3º do art. 62 da Constituição Federal, na redação dada pela Emenda Constitucional n. 32, de 11 de setembro de 2001. As novas dispoisições constitucionais, decorrente da precitada E.C., são aplicáveis apenas às medidas provisorias editadas após a sua entrada em vigor, ou seja, após 11 de setembro de 2001. Ocorre que a Medida Provisória 2.200-2, de 24 de agosto de 2001, é anterior à E.C. 32. Portanto, não foi atingida por esta.

31 MARTINI, Renato. *Tecnologia e cidadania digital: ensaio sobre tecnologia, sociedade e segurança*. Rio de Janeiro: Brasport, 2008. p. 36.

32 MARTINI, op. cit., p. 37

> Portanto, só podemos desenvolver modelos de confiança reais e objetivos (os *"real-world models of trust"*, com quer Gerk) para sistemas de comunicação, no mundo da infra-estrutura da informação, quando dermos estruturas objetivas a todos estes modelos[33].

O sistema de confiança da ICP-Brasil é uma infra-estrutura integrada por uma Autoridade Gestora de Políticas (o Comitê Gestor da ICP-Brasil), uma Autoridade Certificadora Raiz (ITI), as Autoridades Certificadoras de nível subseqüente ao da Raiz, as Autoridades de Registro, as entidades que prestam serviços a essas autoridades e, logicamente, os usuários de todo esse Sistema; ou seja, aqueles que se utilizam dos certificados, e aqueles que confiam nos certificados digitais emitidos no âmbito da ICP-Brasil, conforme dispõe o art. 2 o da MP n o 2.200-2/01.

O Instituto Nacional de Tecnologia da Informação - ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira. É, portanto, a primeira autoridade da cadeia de certificação, responsável pelo credenciamento, auditoria e fiscalização das Autoridades Certificadoras de nível subseqüente, das Autoridades de Registro e Prestadores de Serviço de Suporte, nos termos do art. 5º da MP nº 2.200-2/01:

> 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. (Grifo nosso)

A ICP-Brasil é uma Estrutura técnica, mas se destina à produção de jurídicos de suma importância, tendo papel fundamental no que tange ao aperfeiçoamento das instituições democráticas e ao desenvolvimento econômico, social, cultural, político e tecnológico da sociedade brasileira.

---

33 MARTINI, op. cit., p. 37.

No âmbito técnico, podemos descrever sinteticamente a ICP-Brasil como uma cadeia de confiança que tem por objetivo precípuo o de permitir a comprovação da autenticidade e da integridade das manifestações de vontade dos indivíduos (pessoas naturais) e grupamentos coletivos (pessoas jurídicas).

Um certificado é um documento eletrônico emitido por uma Autoridade Certificadora que assevera a vinculação entre uma chave pública e o titular dessa mesma chave pública. A Autoridade Certificadora é o que se chama de um terceiro de confiança (*a trusted third part*) entre o signatário e o destinatário do arquivo de dados. Vale dizer, o destinatário confiará, acreditará no certificado emitido, ou seja, confiará que uma determinada chave pública realmente se refere à pessoa física ou jurídica à qual a Autoridade Certificadora diz pertencer.

Pois bem, é comum que em alguns sistemas seja estabelecido um *plus* para os certificados emitidos por aquelas Autoridades Certificadoras que atendam a determinados requisitos, normalmente aferidos por meio de um processo formal de acreditação. Esse *plus*, conforme será explicado a seguir, é essencialmente jurídico. Mas não se impede que algumas Autoridades Certificadoras continuem a atuar à margem do sistema institucionalizado pelo Estado.

Tal modelo foi o adotado pela União Européia, por meio da Directiva 1999/93/CE do Parlamento Europeu e do Conselho, em 13 de dezembro de 1999. Em seu art. 3º, dispõe esse diploma comunitário o seguinte:

> 1. Os Estados-Membros não devem sujeitar a prestação de serviços de certificação a autorização prévia.
>
> 2. Sem prejuízo do disposto no nº 1, os Estados-Membros podem introduzir ou manter regimes de acreditação facultativa que se destinem a obter níveis mais elevados na oferta dos serviços de certificação. [...]
>
> 3. Os Estados-Membros assegurarão a criação de um sistema adequado de controlo de prestadores de serviços de certificação estabelecidos no seu território que procedem à emissão de certificados qualificados destinados ao público.

Segundo MENKE:

> Tendo em vista a superveniência da Diretiva Européia 1999/93 – que, conforme mencionado, estipulou que a atividade de certificação

> digital independeria da concessão de autorização prévia pelo poder público, excepcionados os casos dos procedimentos de credenciamento voluntário, a serem implantados pelos Estados Membros para a obtenção de níveis de segurança mais avançados – o legislador alemão aboliu a exigência de autorização prévia estatal para todo e qualquer prestador de serviços de certificação.
>
> Isso foi levado a cabo com a edição da segunda *Signaturgesetz*, de 16.05.2001, que, todavia, manteve e conferiu ainda maior importância aos procedimentos de certificação credenciados (*akkreditierte Signaturverfahren*), ou seja, àqueles em que os interessados em atingir níveis mais altos de segurança na prestação de seus serviços, se submetem ao processo de credenciamento (*Akkreditierung*) perante o órgão regulador alemão, a Regulierrungsbehörde für Telekommunikation und Post (RegTP), que desempenha papel idêntico ao do Instituto Nacional de Tecnologia da Informação no Brasil.[34]

O *plus*, a que foi feito referência anteriormente, está em que certificados emitidos por um prestador de serviços de certificação que atenda a determinados requisitos (normalmente aferidos na acreditação) estarão vinculados a uma assinatura eletrônica com maior poder, é o de fazer com o que o arquivo de dados com ela subscrito seja automaticamente admitido como meio de prova para efeitos processuais. ocorre em razão de que a assinatura eletrônica passa a ter, por lei, o mesmo valor jurídico de uma assinatura manuscrita.

Não obstante, permite que assinaturas eletrônicas não consideradas avançadas possam também gerar efeitos jurídicos, como meio de prova, embora não atribua diretamente um valor probatório às mesmas. Vale dizer, no que tange a uma assinatura eletrônica ligada a um certificado emitido por um prestador de serviços de certificação não acreditado (ou que não cumpra os requisitos mínimos normalmente aferidos por meio da acreditação), cabe à parte que invoca o valor probatório do arquivo subscrito o ônus de demonstrar a validade probatória desse arquivo. Para tanto, a Diretiva diz somente que não serão negados efeitos legais e a admissibilidade como meio de prova a esse arquivo, sem dizer cabalmente, como faz quanto à assinatura eletrônica avançada e ao certificado qualificado, que o arquivo será admitido como meio de prova para efeitos processuais.

---

34 MENKE, Fabiano. Assinaturas digitais, certificados digitais, infra-estrutura de chaves públicas brasileira e a ICP alemã. *Revista de Direito do Consumidor*. v. 48, out – dez/2003.

Este foi o direcionamento adotado pela legislação pátria, isto é, pelo Poder Executivo no exercício de função legislativa atípica, porquanto a matéria hoje se encontra integralmente regulada pela medida Medida Provisória nº 2.200-2, de 24 de agosto de 2001, cujos efeitos se protraem com força de lei em razão do art. 2º da Emenda Constitucional nº 32, de 11 de setembro de 2001.

Como foi dito mais acima, a ICP-Brasil é um Infra-Estrutura técnica, mas se destina à produção de jurídicos. Efeitos, esses, que estão descritos no art. 10 da Medida Provisória, que dispõe:

> 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 verdadeiras em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 – Código Civil.

Os certificados emitidos no âmbito da ICP-Brasil atestam a equivalência entre a assinatura digital e a manuscrita, conduzindo à presunção de identificação entre um arquivo de dados e o seu autor, que já não poderá impugná-lo perante quem quer que contra ele pretenda fazer valer os efeitos do conteúdo desse arquivo.

Vale dizer, a assinatura digital vinculada a um certificado emitido no âmbito da ICP-Brasil conduz à presunção de autenticidade do documento subscrito, certo que é, como afirma Humberto Theodoro Júnior, que o "*código não subordina a validade do instrumento particular a que a firma do signatário seja reconhecido por tabelião ou qualquer oficial público. O que lhe dá autenticidade é a própria assinatura, ou seja, a escrita do nome do declarante, feita pessoalmente (de forma autógrafa*)".[35]

Já se afirmou acima que a ICP-Brasil é o Sistema Nacional de Certificação Digital e que, como tal, envolve prestadores de serviços de natureza distinta, ligados ao segmento de certificação, e os usuários desses serviços. Em posição destacada nesse sistema figuram as Autoridades Certificadoras, as emissoras de certificados digitais que estabelecem entre si uma cadeia hierárquica de confiança. Repita-se: no

---

35 THEODORO JUNIOR, HUMBERTO. *Comentários ao Novo Código Civil*. v. III. Tomo II. RJ: Forense, 2003. p. 480.

patamar mais elevado dessa cadeia está a Autoridade Certificadora Raiz da ICP-Brasil.

Deve ser mencionado que o modelo adotado no Brasil é semelhante ao adotado na Alemanha, onde a presença do Estado é muito forte. Mas tal presença não deve, e não pode, necessariamente indicar a existência de prestação de serviço público. Ao comentar o assunto, MENKE afirma que na Alemanha a presença do Estado é ainda mais forte "[...] *especialmente com vistas à interoperabilidade dos métodos de comprovação de autoria no meio virtual*"[36].

A legislação alemã sobre o assunto, pioneira na Europa, elegeu por política legislativa a intervenção estatal no controle e supervisão da atividade dos prestadores de serviço de certificação[37]. Na Alemanha, o órgão regulador responsável por tais atribuições é o RegTP. Segundo MENKE:

> [...] assim como no ordenamento jurídico alemão, *o texto legal brasileiro elegeu a política legislativa de intervenção estatal no controle e supervisão da atividade dos prestadores de serviço de certificação*, designando uma autarquia federal como responsável por tais atribuições[38]. (Grifo nosso)

O ITI é a AC Raiz da ICP-Brasil. É a primeira autoridade da cadeia de certificação e executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Compete à AC Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciando a lista de certificados emitidos, revogados e vencidos. Além disso, cabe à AC Raiz auditar e atuar como fiscalizadora das AC e das AR e dos prestadores de serviço habilitados na ICP-Brasil. Não deve ser esquecido que a ICP-Brasil é uma cadeia de confiança hierárquica.

E num sistema hierárquico de confiança, a hipótese mais comum é a de que o Estado posicione sua atividade regulatória para estabelecer

36 MENKE, op. cit., p. 74. Para o autor, *"o que caracteriza o modelo alemão de infra-estrutura de chaves públicas é o aspecto de ter optado pela configuração hierárquica e o de apresentar no ápice da cadeia de certificaçãoo uma entidade de direito público, a RegTP, que, além de credenciar, supervisionar e fiscalizar as atividades dos credenciados, emite certificados digitais para estes operarem. Desta forma, tem aplicação, não o modelo de diversas cadeias isoladas, tal qual o modelo de confiança distribuída, mas sim o de uma cadeia escalonada composta pela autoridade certificadora raiz no topo e os demais prestadores de certificaçãoo abaixo dela".* (MENKE, op. cit., p. 73-74)

37 MENKE, op. cit., p. 76.

38 MENKE, op. cit., p. 99

algum controle sobre os prestadores de serviços de certificação que se proponham a emitir certificados para o público, ainda que não se elimine o aspecto concorrencial, da livre iniciativa, que continua a ser a imagem diretora da ordem econômica no setor de certificação (inciso IV, do art. 170, da CF). Em sistemas como esse, normalmente se estabelece um processo de credenciamento, ou acreditação facultativo.

Em suma, o ITI é responsável pela administração direta da ICP-Brasil, fazendo o papel de AC Raiz, credenciando, auditando e fiscalizando as AC credenciadas, fomentando a certificação digital, e apoiando a Secretaria-Executiva do Comitê-Gestor da ICP-Brasil no que for necessário ao exercício das funções. Ou seja, típica atividade estatal de intervenção na atividade privada.

4 O MODELO NORTE-AMERICANO DE CERTIFICAÇAO DIGITAL

Como já visto anteriormente, uma infra-estrutura de chaves públicas pode ser configurada basicamente em dois modelos: o hierárquico e o de confiança distribuída. Deve ser mencionado que o modelo adotado nos Estados Unidos é diferente do modelo brasileiro, hierárquico. No modelo americano, 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 cruzada.

Observe-se que, os Estados Unidos são pioneiros em matéria legislativa sobre o assunto. Desde 1995 existe legislação tratando das assinaturas digitais. Mas, diferentemente do ocorrido no Brasil, tal legislação não foi editada no âmbito federal. O Estado de Utha foi o primeiro, com a completa Utah Digital Signature Act (UDSA).

A UDSA trata das definições, conceitos, efeitos das assinaturas digitais, certificados digitais e autoridades certificadoras. A referida lei surgiu para facilitar o comércio por meio de mensagens confiáveis, minimizando a incidência de assinaturas digitais forjadas e de fraudes no comércio eletrônico[39]. Em suma, buscou-se mais segurança para as relações travadas no meio virtual. Mas, para tanto, a lei previu uma série de exigências, trazendo o conceito de autoridade certificadora licenciada, a saber, *"[...] aquela que dispõe de uma licença válida expedida pela Divisio of Corporations and Commercial Code, do Departamento de Comércio de Utah"*. De outra banda:

39 MENKE, 2003.

> [...] às exigências previstas na lei e nos regulamentos, as autoridades certificadoras licenciadas desfrutam de certas vantagens. A principal delas é a do *status* jurídico-probatório das mensagens assinadas digitalmente. Consoante o previsto na seção 403, item 1, b. I, somente serão equiparadas aos documentos escritos aquelas mensagens eletrônicas assinadas digitalmente que forem conferidas mediante o emprego de chave pública inserida em certificado digital emitido por autoridade certificadora licenciada. Apenas neste caso a mensagem sera válida, exigível e produzirá efeitos tal qual se tivesse sido escrita sobre o suporte de papel.[40]

Para LORENZETTI, juntamente com a Uncitral, europeia, a lei de assinatura digital do Estado de Utah tem sido o modelo mais seguido e citado[41].

Ainda no ano de 1995, o Estado da Califórnia editou lei tratando do uso e das aplicações de assinaturas eletrônicas. Tal lei não possui o alcance e a abrangência da lei do Estado de Utah, dirigindo-se, especificamente, ao uso perante órgãos públicos[42]. Em 1999, o Estado de Nova York editou a *Eletronic Signature Record Act*, que definiu a assinatura eletrônica como *"[...] um meio eletrônico de identificação, que inclui a assinatura digital, única para aquela pessoa, associada com dados de uma maneira tal que garantam a autenticidades e a integridade, e é empregada por seu titular para que tenha a mesma força da assinatura manual."*[43]

É certo que, sendo o direito civil o regulador da formação dos contratos eletrônicos e das assinaturas digitais, atualmente, quase todos os cinquenta estados americanos já possuem legislação sobre o assunto. Entretanto, esses diversos estados, não raro, tratam a matéria de modo diferente uns dos outros. Segundo REZENDE:

> Tais leis se enquadram em 3 modelos. Há o modelo 'prescritivo', como o da lei de Utah, que regula o uso de assinaturas digitais e o funcionamento de PKIs. Há o modelo 'de critérios', como o da Califórnia, que estabelece parâmetros de funcionalidade e confiabilidade para o reconhecimento legal de de mecanismos

40 MENKE, 2003.

41 LORENZETTI, Ricardo L. *Comércio eletrônico*. Tradução de Fabiano Menke; com notas de Cláudia Lima Marques.- São Paulo: RT, 2004, p. 117.

42 MARCACINI, Augusto Tavares Rosa. O documento eletrônico como meio de prova. *Revista de Direito Imobiliário*, v. 47, p. 70, jul. 1999. DTR, 1999, 311.

43 LORENZETTI, op. cit., p 118.

> eletrônicos autenticatórios. E há, finalmente, o modelo de 'outorga', como o de Massachussets, que não aborda critérios ou mecanismos, mas delega às partes envolvidas o poder de decidir qual mecanismo pode substituir eletronicamente a assinatura de punho. Das 76 leis, apenas 36 em 20 Estados mencionam chaves assimétricas e PKIs.[44]

Percebe-se, portanto, que no meio de tantas leis, o tratamento dado por cada uma delas tende a ser diferente, observando-se as peculiaridades econômicas, culturais, sociais e tecnológicas de cada Estado. Entretanto, como já dito em outro momento, uma infra-estrutura pressupõe a perfeita comunicação entre os componentes integrantes. Deve haver a interoperabilidade, facilmente observada em modelos hierárquicos de certificação digital. Essa é uma das grandes diferenças entre o modelo adotado no Brasil e o modelo americano. Para MENKE:

> [...] não obstante o pioneirismo da Lei de Utah e os esforços de iniciativas legislativas de outras unidades federativas estadunidenses, há que se ressaltar que, curiosamente, nos Estados Unidos da América o desenvolvimento e a expansão das infra-estruturas de chaves públicas se deram de forma bastante desorganizada, de sorte que hoje em dia são diversas as ICPs em funcionamento naquele país, com base tanto em iniciativas governamentais quanto em iniciativas privadas.[45]

Continua, o precitado autor, afirmando que, dentre as diversas razões para o fenômeno transcrito acima, tem-se, principalmente, o fato de que a autonomia dos estados federados proporcionou a cada entidade federativa a edição de sua própria lei sobre assinaturas digitais e matérias afins, deixando-se de lado qualquer harmonia principiológica entre esses diplomas.[46]

Com elevado grau de autonomia legislativa, advindo do seu tipo de federalismo, notadamente em questões relacionadas ao direito civil, a legislação de cada estado criou critérios e procedimentos diferentes. A necessidade de harmonia entre os mesmos restou patente.

---

44 REZENDE. Pedro Antonio Dourado de. Certificados digitais, chaves públicas e assinaturas o que são, como funcionam e como não funcionam. *Revista de Direito Imobiliário*, v. 49, p. 129, Jul 2000 DTR, 2000, 357.

45 MENKE, 2005.

46 Ibid..

Entretanto, as empresas sediadas em solo americano começaram a implantar suas próprias infra-estruturas, com o fito de proteger dados sensíveis e gerir seus negócios. Mas, neste momento, também começaram a surgir problemas, já que as empresas possuem parcerias com outras empresas e entidades que também possuem sua própria ICP. Fez-se necessário, então, a conexão entre ICPs corporativas.

Além disso, tais ICPs corporativas, não raras vezes, possuem estruturas e políticas de certificação diferentes. A solução aplicada foi a utilização de uma ligação flexível entre as ICPs, encontrada na *Bridge Certification Authority – BCA* (Autoridade Certificadora Ponte), projetada para vincular ICPs de diferentes arquiteturas.

Tal figura não existe na ICP-Brasil, e não é encontrada como componente de uma ICP hierárquica. Pode, entretanto, fazer a ligação de uma ICP hierárquica com uma outra ICP do mesmo modelo ou de modelo diferente. Essa ponte não pode emitir certificados digitais para o usuário final, mas serve como ponte de confiança entre usuários de diferentes ICPs.

Ainda, deve ser mencionado que Governo Americano promoveu, há alguns anos, "*a iniciativa do projeto Federal Bridge Certification Autority, que tem o objetivo de viabilizar a intercomunicação entre os titulares de pares de chaves cujos respectivos certificados sejam provenientes de autoridades certificadoras diversas.*"[47]

A ICP do Governo Federal americano é um exemplo de uma ICP baseada no conceito de Autoridade Certificadora Ponte. Frise-se que, inicialmente, as ICPs do Governo Federal foram projetadas para funcionar na forma do modelo hierárquico. Para Hastings:

> However, these initial PKI plans ran into several obstacles. There was no clear organization within the government that could be identified and agreed upon to run a governmental "root" CA. While the search for an appropriate organization dragged on, federal agencies began to deploy autonomous PKIs to enable their electronic processes. The search for a "root" CA for a hierarchical federal PKI was abandoned, due to the difficulties of imposing a hierarchy after the fact. Instead, plans were developed to integrate the agency PKIs into a unified federal mesh PKI.
>
> The number and complexity of trust relationships required for the new federal mesh PKI was daunting. Government agencies began to

47 MENKE, 2005.

> search for a solution that would represent their trust relationships in a more manageable fashion. The concept of the BCA was developed and was chosen as the vehicle for a unified federal PKI. A prototype Federal BCA (FBCA) has been implemented and demonstrated. The prototype FBCA links five trust domains representing three federal departments, one state government, and one foreign government. The five trust domains include both hierarchical and mesh PKIs. In the FBCA demonstration, users from different trust domains were able to communicate with each other in a trusted fashion using secure electronic mail.[48]

Percebe-se aqui, mais uma razão para a adoção do modelo de confiança compartilhada pelos Estados Unidos. A demora para a escolha de uma entidade governamental, que funciona-se como AC-Raiz da ICP hierárquica, propiciou uma difusão de ICPs autônomas no seio do Governo Federal americano. Assim, fica claro que o conceito de Autoridade Certificadra Ponte foi o escolhido como condutor para uma futura lei federal unificada de ICP.

Atualmente, existe uma espécie de Comitê Gestor Federal da ICP que fornece orientações e direções aos órgãos federais americanos, sobre o estabelecimento de uma ICP federal[49]. O *National Institute of Standards and Technology – NIST* [50], uma agência do Departamento de Comércio dos Estados Unidos, tem um papel importante no desenvolvimento de uma ICP federal, já que, além de chefiar a implantação, serve como conselheiro do sistema.

A arquitetura da atual ICP federal apresenta a *Federal Bridge Certification Authority*, que propicia a interoperabilidade entre domínios de ICPs diferentes, que possuem políticas de certificação diferentes. Ressalte-se que a *Federal Bridge Certification Authority* está operacional desde o ano de 2001, e foi conceituada como uma ICP *hug* para fornecer a ligação entre os componentes.

A tecnologia utilizada nas *PKIs* norte-americans é a mesma utilizada no Brasil e em países europeus. Diferem, entretanto, quanto ao modelo e, consequentemente, procedimentos de segurança. No Brasil existe uma única infra-estrutura de chaves públicas, criada

48 HASTINGS, Nelson E. and POLK, William T. Bridge Certification Authorities: Connecting B2B Public Key Infrastructures. Disponível em: <http://csrc.nist.gov/groups/ST/crypto_apps_infra/pki/pkiresearch.html>. Acesso em: 25 set. 2011.

49 Informações sobre tal Comitê podem ser encontradas no sítio: <http://gits-sec.treas.gov/>

50 Ver: <http:www.nist.gov/>

por um instrumento normativo com amplitude nacional. Nenhum outro ente da federação brasileira, ou organismo ou entidade privada, podem criar a sua própria ICP pretendendo colher os mesmos efeitos constantes na MP 2.220-2. Além disso, como já dito, percebe-se uma forte presença do Estado no sistema. Uma autarquia federal é a Autoridade Certificadora Raiz responsável por emitir o certificado digital para as Autoridades Certificadoras, credenciando, auditando e fiscalizando as mesmas.

O procedimentos de credenciamento de uma AC é o mesmo em todo o nosso território nacional. Da mesma maneira, o procedimento de identificação do usuário final também é único, não sofrendo variação de acordo com o local.

No sistema americano de certificação digital não existe a figura da AC Raiz. Também, são diversas as ICPs, privadas ou governamentais, verificando-se uma fraca intervenção do Estado. O mercado tem uma maior liberdade de atuação.

Nos Estados Unidos é possível que as leis de uma estado exijam, por exemplo, a presença física do interessado em adquirir o certificado digital, com toda a sua documentação, utilizando-se da tecnologia de coleta de dados biométricos, enquanto que as leis de outro estado exijam apenas que o solicitante preencha um requerimento *on line*, sem precisar comprovar, com a máxima efetividade, que ele é quem diz ser. Diversidade de procedimentos e de políticas dificultam a comunicação entre as ICPs existentes, sendo necessária a criação de uma figura inexistente em nosso sistema, a saber, a já mencionada AC Ponte.

Deve ser mencionado que, por outro lado, o modelo hierárquico não apresenta grandes problemas de interoperabilidade. É um sistema com estrutura mais simples, com procedimentos únicos para qualquer interessado em participar do sistema de certificação, e para aqueles interessados em adquirir um certificado digital. Aponta-se como desvantagem a confiança concentrada em um único ponto, a AC Raiz. Alega-se que problemas de segurança na AC Raiz, que está no ápice, poderia comprometer todo o sistema escalonado e hierárquizado.

Já no modelo de confiança compartilhada, como existem múltiplos pontos confiança, entende-se que o comprometimento de uma AC não comprometeria todo o sistema, já que este poderia ser isolado. Entretanto apresenta problemas de interoperabilidade, fazendo-se necessária a certificação cruzada e a existência de uma AC Ponte. Além disso, possui estrutura mais complexa.

Frise-se, entretanto, que esta análise não pretende apontar qual dos modelos é o melhor. Pretende-se, entretanto, discutir a origem dessas

diferenças, reconhecendo a existência de vantagens e desvantagens em cada um dos modelos abordados.

Oportunamente, mencione-se que, embora cada Estado possua pelo menos uma lei relativa à assinatura eletrônica, é a lei federal que estabelece as diretrizes para o comércio entre os Estados.

Antes da operacionalização da *Federal Bridge Certifications Authority*, em 30 de junho de 2000, foi assinada pelo Presidente americano, à época, a *Electronic Signatures in Global and National Commerce Act – ESIGN*, estabelecendo a validade das assinaturas eletrônicas para o comércio interestadual e internacional. E foi neste período que diversos estados lançaram suas leis com conteúdo semelhantes ou mais específicos. Uns anos antes e outros anos depois. Mas essa foi a primeira grande intervenção do Governo Federal relacionada ao assunto.

A mencionada lei prevê a legalidade da assinatura eletrônica, sem dizer o método ou a tecnologia específica. Pelo contrário, ela veda que qualquer entidade exija uma tecnologia específica para transações eletrônicas.

Observa-se, portanto, um ambiente no qual praticamente todos os estados possuem sua própria legislação sobre o assunto, dando tratamento, muitas vezes, diversos umas das outras, em conjunto com a legislação federal que trata do gênero assinatura eletrônica, sem tratar especificamente da espécie assinatura digital e, por consequência, de uma infra-estrutura de chaves públicas.

5 CONCLUSÃO

No peculiar federalismo norte-americano os estados membros eram independentes e decidiram, abrindo mão de parte dos seus poderes e de sua soberania, formar uma união de estados federados. Assim, levando-se em consideração que antes eram dotados de soberania, e ante a grande resistência de ceder os seus poderes ao governo central, observa-se que os estados possuem um nível de autonomia, em relação ao poder central, muito mais elevado que o de outras entidades federativas de outras federações, a exemplo do Brasil.

Percebeu-se que os estados norte-americanos mantiveram uma parcela significativa de poder e podem, inclusive, legislar sobre matérias relacionadas ao direito civil, comercial e penal. No Brasil, por força do que dispõe o art. 22, inc. I, da nossa Constituição Federal, tais matérias são de competência privativa da União.

A infra-estrutura de chaves públicas, entendida como uma organização que dispõe e abastece um serviço de certificação digital

e assinatura digital em favor dos usuários, tanto pode ser configurado numa hierarquia, na forma de uma árvore invertida, situando-se no topo uma entidade na qual todos os que vêm abaixo, inclusive os usuários, devem confiar, como pode ser configurada no modelo de confiança distribuída, onde cada autoridade certificadora constitui uma hierarquia independente, não havendo, a princípio, níveis intermediários.

Portanto, 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 de uso geral em uma estrutura nacional. No modelo americano, cada autoridade certificadora constitui uma hierarquia independente, não havendo, a princípio, níveis intermediários. Lá existem diversas legislações, em cada estado e no âmbito federal, tratando do assunto e das diversas ICPs. Aqui, um ato normativo federal trata do assunto, tendo criado a única ICP, que possui âmbito nacional.

Assim, no meio de tantas leis, nada mais normal que o tratamento dado por cada uma delas seja diferente, observando-se as peculiaridades de cada entidade legiferante. Isso tende a afetar a interoperabilidade, comumente observada em modelos hierárquicos. Essa é uma das grandes diferenças entre o modelo adotado no Brasil e o modelo americano.

Concluiu-se que a grande autonomia dos estados federados proporcionou a cada entidade federativa a edição de sua própria lei sobre assinaturas digitais e matérias afins. Assim, com elevado grau de autonomia legislativa, advindo do seu tipo de federalismo, notadamente em questões relacionadas ao direito civil, a legislação de cada estado criou critérios e procedimentos diferentes. A solução, para driblar os problemas relacionados à falta de interoperabilidade, foi a criação das Autoridades Certificadora Pontes, entidade inexistentes em modelos hierárquicos de certificação digital, cuja finalidade cingi-se, tão somente, a propiciar a comunicação entre ICPs de domínios diferentes.

REFERENCIAS

BURNHAM, William. *Introduction to the law and legal system of the United States*. St. Paul: Thomson/West, 2006.

GODOY, Arnaldo Sampaio de Moraes. *Direito nos Estados Unidos*. Barueri, São Paulo: Manole, 2004.

HASTINGS, Nelson E. and POLK, William T.. *Bridge Certification Authorities: Connecting B2B Public Key Infrastructures*. Disponível em: <http://

csrc.nist.gov/groups/ST/crypto_apps_infra/pki/pkiresearch.html>. Acesso em: 25 set. 2011.

LORENZETTI, Ricardo L. *Comércio eletrônico.* Tradução de Fabiano Menke; com notas de Cláudia Lima Marques. São Paulo: RT, 2004.

MARCACINI, Augusto Tavares Rosa**.** *O documento eletrônico como meio de prova. Revista de Direito Imobiliário*, v. 47, p. 70, Jul 1999, DTR, 311.

MARTINI, Renato. *Tecnologia e cidadania digital:* ensaio sobre tecnologia, sociedade e segurança. Rio de Janeiro: Brasport, 2008.

MENDES, Gilmar Ferreira. *Curso de direito constitucional.* São Paulo: Saraiva, 2007.

MENKE, Fabiano. Assinaturas digitais, certificados digitais, infra-estrutura de chaves públicas brasileira e a ICP alemã. *Revista de Direito do Consumidor*, v. 48, out-dez 2003.

_____. *Assinatura eletrônica:* aspectos jurídicos no direito brasileiro. São Paulo: RT, 2005.

REALE, Miguel. *O nosso federalismo.* Disponível em <http://www.miguelreale.com.br/artigos/nosfed.htm>. Acesso em : 19 set. 2011.

REINALDO FILHO, Demócrito. A ICP-Brasil e os poderes regulatórios do ITI e do CG. *Jus Navigandi*, Teresina, ano 10, n. 869, 19 nov. 2005. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=7576>. Acesso em: 08 fev. 2010.

REINHART, Susan M. *Strategies for legal case Reading and vocabular development.* University of Michigan. 2007.

REZENDE. Pedro Antonio Dourado de. Certificados digitais, chaves públicas e assinaturas o que são, como funcionam e como não funcionam. *Revista de Direito Imobiliário.* v. 49, p. 129, jul 2000, DTR, 357.

THEODORO JUNIOR, HUMBERTO. *Comentários ao Novo Código Civil.* v. III. Tomo II. RJ: Forense, 2003.

VERONESE, Alexandre et al. Segredo e democracia: certificação digital e software livre. *Informática pública*, v. 8 (2): 09-26, 2007.