

A ICP-BRASIL E OS PODERES REGULATÓRIOS DO ITI e do CG

Demócrito Reinaldo Filho

Juiz de Direito em PE

1. Considerações iniciais

A finalidade do presente trabalho é a de comprovar, através da análise das atribuições conferidas ao ITI – Instituto Nacional de Tecnologia da Informação e ao Comitê Gestor da ICP-Brasil, que esses órgãos, em conjunto, atuam com características próprias das agências reguladoras, no que diz respeito às atividades de certificação digital no nosso país, já que têm o poder de direcionar as atividades dos fornecedores privados de chaves de assinatura e certificados digitais, de acordo com interesses públicos juridicamente definidos. Embora o ITI e o Comitê Gestor da ICP-Brasil não tenham recebido a denominação de “órgão regulador” ou “agência reguladora” nos textos normativos referentes à atividade de certificação digital, ou mesmo em qualquer outro documento legal, veremos que na prática funcionam com poderes próprios desses órgãos.

2. Introdução à idéia-conceito de Infra-Estrutura de Chaves Públicas

O comércio eletrônico e as comunicações por meio de redes telemáticas de um modo geral encontram nos problemas relacionados à segurança das transações o grande empecilho ao seu pleno desenvolvimento. As pessoas se sentem inseguras quando são instadas a transacionar e se comunicar em ambientes que não fornecem completas condições de proteção aos seus interesses, bens e privacidade de suas informações. Elas precisam ter confiança nas relações que mantêm entre si nas redes abertas de comunicação, e isso se consegue através do uso de sistemas e meios de autenticação, confidencialidade e integridade.

Várias tecnologias existem no mercado destinadas a assegurar essas funcionalidades, mas a mais disseminada é a do sistema de assinaturas e certificados digitais baseados na criptografia de chaves públicas. Funciona mais ou menos assim: o remetente usa a chave pública do destinatário para “assinar” (codificar) sua mensagem de dados, que transita codificada até chegar ao endereço do destinatário, o qual, valendo-se da sua chave privada fica habilitado a decodificá-la. Todo usuário do sistema tem duas chaves: uma pública e uma privada. A pública é de conhecimento de todas as outras pessoas, enquanto que a privada deve ser mantida sob seu uso e conhecimento exclusivo. Também nas relações em um *website* é possível a garantia de autenticidade por meio desse sistema. O internauta que acessa um *site* pode se assegurar que ele pertence realmente a uma determinada empresa através do certificado digital exibido. Esse certificado contém os dados de identificação da pessoa responsável pelo *site*.

A geração, distribuição e gerenciamento das chaves públicas e dos certificados digitais⁽¹⁾ é feita por meio de entidades conhecidas como **autoridades certificadoras** (AC's)⁽²⁾. São essas autoridades certificadoras que vão garantir, por exemplo, que uma chave pública ou certificado digital pertence realmente a uma determinada empresa ou pessoa. São elas que formam a cadeia de confiança que dá segurança ao sistema. Fazem o papel desempenhado pelos notários no sistema de certificação tradicional. Da mesma forma que os cartórios tradicionais, são organizadas segundo critérios legais e obedecem, na prestação dos seus serviços de certificação, a toda uma política de procedimentos, padrões e formatos técnicos estabelecidos em regimes normativos. Obedecem, portanto, a um modelo técnico de certificação e estrutura normativa, que define quem pode emitir certificado para quem e em quais condições.

O conjunto ou modelo formado de autoridades certificadoras, políticas de certificação e protocolos técnicos compõe o que se convencionou chamar de “Infra-Estrutura de Chaves Públicas” ou simplesmente ICP⁽³⁾. Uma infraestrutura de chaves públicas não é apenas um feixe de leis, mas todo um

conjunto de regimes normativos, procedimentos, padrões e formatos técnicos que viabilizam o uso em escala da criptografia de chaves públicas(4) em rede digital aberta. Estrutura o suporte para a tecnologia de chaves públicas, de forma a permitir o gerenciamento e controle do uso de chaves (assinaturas) e certificados digitais. A função primeira de uma ICP, portanto, é permitir, por meio das *autoridades certificadoras* (AC's), a distribuição e o uso de chaves públicas e certificados com garantia de segurança.

A construção da infra-estrutura de chaves públicas é indispensável ao estabelecimento da hierarquia ou cadeia de confiança, base em que se fundamenta todo o sistema de certificação digital. No ambiente da Internet, pessoas desconhecidas umas das outras realizam transações entre si e necessitam estabelecer algum tipo de relação de confiança, que pode ser alcançada através da implementação de uma ICP, que se utiliza da cadeia de autoridades certificadoras. A relação de confiança não é estabelecida diretamente entre as partes de uma transação eletrônica, mas através de uma AC (autoridade certificadora), na qual confiam mutuamente para verificar e confirmar a identidade de ambas. É uma relação de confiança idêntica a que se forma em outros sistemas baseados na emissão e certificação de documentos em formato não digital. Por exemplo, os comerciantes em geral confiam na validade de um cartão de crédito que lhes é apresentado por um cliente. Isto ocorre porque eles têm uma relação de confiança com a empresa administradora do cartão; confiam na forma pela qual ela emite esse documento. O mesmo vale para o sistema de certificação digital. Ambas as partes de uma transação eletrônica concordam em confiar em uma AC que emite e verifica a autenticidade seus documentos (certificados) digitais.

Na prática, o gerenciamento da confiança funciona através de aplicativo de *software* incorporado ao computador do usuário. Normalmente, o software que faz a verificação de um certificado digital tem algum mecanismo ou função para confiar em AC's. Por exemplo, o programa utilizado para navegar na Internet (conhecido como *browser*) contém uma lista das AC's em que confia. Quando o usuário visita um determinado *site* (por exemplo, de um *shopping on*

line ou de um banco) e é apresentado ao navegador um Certificado Digital, ele verifica a AC que emitiu o certificado. Se a AC estiver na lista de autoridades confiáveis, o navegador aceita a identidade do *site* e exibe a página da *Web*. Em não sendo o caso, o navegador exibe uma mensagem de aviso, perguntando ao usuário se deseja confiar na nova AC. Geralmente o programa navegador dá opções para confiar permanente ou temporariamente na AC ou não confiar em absoluto. O usuário, portanto, tem controle sobre quais AC(s) deseja confiar, porém o gerenciamento da confiança é feito pelo aplicativo de *software* (neste exemplo, pelo navegador).

3. A ICP-Brasil: seu modelo de arquitetura e origem normativa

Como definimos anteriormente, 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.

Dependendo do modelo de ICP escolhido, os certificados emitidos por uma autoridade certificadora (AC) têm um âmbito de utilização de maior ou menor alcance. Explica-se: as autoridades certificadoras desempenham um papel crucial na Infra-Estrutura de Chaves Públicas, pois são elas quem expede e controla o uso dos certificados digitais. As AC's são organizadas e funcionam com base em um predeterminado número de regras e convenções, que dão forma ao próprio modelo de ICP. Existem diferentes modelos de infra-estrutura de chaves públicas, que podem ser escolhidos de acordo com as várias necessidades. Em outras palavras, existem distintas alternativas mediante as quais as organizações podem criar relações de intercâmbio confiáveis, cuja complexidade é diretamente proporcional à quantidade de autoridades

certificadoras (AC's) envolvidas (e que podem se relacionar entre si). Dependendo do modelo escolhido, as autoridades certificadoras estarão aptas a gerar certificados limitados ou de uso geral. Por exemplo, num modelo de uma única AC, é muito mais simples a administração do intercâmbio de certificados entre ela e os usuários finais. Somente ela expede e controla os certificados, criando um universo de certificação limitado ao espaço das relações de seus associados. Os usuários encontram na AC única o "ponto de confiança" comum, e assim usam seus certificados para confirmar a validade das chaves e identificar um ao outro. O processo do "caminho da certificação" passa sempre pela mesma e única AC.

A administração de um sistema (modelo) assim é muito mais simples, mas em compensação os certificados emitidos são de uso restrito para identificação dos usuários vinculados à AC única. Forma-se uma rede de confiança de espectro bastante reduzido. A coisa se complica se houver necessidade de estabelecer relação com outras pessoas (usuários) que não possuem certificados emitidos pela mesma AC. Para superar essa limitação, ou seja, para se operar a "escalabilidade" e extensão da cadeia de certificação original, criando-se novas "cadeias de confiança", dois caminhos podem ser seguidos: o primeiro, é o da *certificação cruzada*. Por esse meio, diferentes AC's intercambiam certificados entre elas, é dizer, emitem *certificados cruzados*. Quando um certificado cruzado é emitido, ocorre a expansão da cadeia de confiança de uma AC. Um usuário vinculado a ela passa a confiar na validade de certificados emitidos pela outra AC objeto da certificação cruzada. Considerando que o seu usuário confia na validade dos certificados que expede, quando ele se depara com um certificado cruzado emitido por sua AC de origem, passa a confiar na outra AC e, conseqüentemente, nos certificados por esta expedidos para seus próprios usuários finais. Esse processo possibilita que um usuário filiado a uma determinada AC adquira confiança na validade de certificado de usuário vinculado à outra AC. O processo de certificação cruzada é um meio, como se disse, de produzir a extensão da cadeia de confiança necessária à funcionalidade em escala de uma ICP. Nesse caso, as AC's se

certificam umas às outras acima das estruturas de certificação originais.

Um outro meio de ampliar o raio de extensão da validade de certificados emitidos por uma AC é integrá-la a uma estrutura maior e mais complexa, regulada por uma autoridade central, a AC-Raiz. A estrutura hierárquica original, formada pela AC e seus usuários, passa a fazer parte de um sistema maior, capitaneada por uma autoridade central de certificação, em que todas as demais autoridades certificadoras devem confiar. Em outras palavras, todos os “caminhos de certificação” devem passar em última análise por essa autoridade central, responsável pela garantia da cadeia de confiança e pela definição das práticas e políticas gerais de certificação. Nesse modelo, as autoridades certificadoras inferiores se certificam umas às outras dentro e abaixo da estrutura central.

A Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil foi instituída pela Medida Provisória 2.200/01(5) mediante adoção desse modelo de raiz única (árvore única). Deu forma legal a uma estrutura hierarquizada e centralizada – vertical –, com a previsão da existência de uma única AC-Raiz (árvore única), inicialmente regulada para operar com certificados de uso geral. A MP pretendeu instituir uma grande cadeia ou estrutura de certificação nacional. Ao invés de incentivar a criação de pequenas e múltiplas estruturas de certificação, que atuariam de forma autônoma e cada qual com políticas e práticas de certificação distintas, a Medida Provisória instituiu uma grande estrutura hierárquica, com a previsão de uma autoridade certificadora Raiz.

A MP não proíbe qualquer organização ou empresa de criar sua própria ICP. Podem montar uma autoridade certificadora e, dependendo de requisitos técnicos e legais de operabilidade, podem requerer registro junto à ICP-Brasil. Se uma autoridade certificadora criada e mantida por uma instituição qualquer adequa suas práticas de certificação aos regulamentos gerais da ICP-Brasil, pode vir a fazer parte de sua infra-estrutura, passando a ser mais um membro da cadeia nacional de confiança, e ampliando assim o poder de validade de seus certificados. Uma autoridade certificadora credenciada na ICP-BR pode vender certificados que sirvam para verificar assinatura em qualquer tipo de

documento ou transação, com valor probante em todo o território nacional. Em outras palavras, para que os certificados emitidos por uma autoridade certificadora adquiram, em nosso país, validade jurídica de uso geral (força probante contra terceiros), é preciso que ela esteja incorporada à ICP-Brasil(6).

O art. 1º. da MP 2.200-2 se resume a proclamar que “fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras”. A MP não definiu em detalhes a organização da ICP-Brasil, deixando essa tarefa para o regulamento, mas previu que “será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro – AR” (art. 2º.).

4. Órgãos componentes da ICP-Brasil

A MP 2.200-2, embora sem definir a organização da ICP-Brasil, indicou antecipadamente os órgãos que a compõem (art. 2º.), na seguinte ordem:

- c) um **Comitê Gestor**, autoridade gestora das políticas de certificação;
- d) a **Autoridade Certificadora Raiz** (AC-Raiz);
- e) as **Autoridades Certificadoras** (AC's); e
- f) as **Autoridades de Registro**.

4.1. O Comitê Gestor

O Comitê Gestor é o órgão que exerce a função de autoridade gestora das políticas de certificação da ICP-Brasil (art. 3º. da MP 2.200-2), vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente

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

- a) Ministério da Justiça;
- b) Ministério da Fazenda;
- c) Ministério do Desenvolvimento, Indústria e Comércio Exterior;
- d) Ministério do Planejamento, Orçamento e Gestão;
- e) Ministério da Ciência e Tecnologia;
- f) Casa Civil da Presidência da República; e
- g) Gabinete de Segurança Institucional da Presidência da República.

A coordenação do Comitê Gestor da ICP-Brasil é exercida pelo representante da Casa Civil da Presidência da República (par. 1º. do art. 3º.). Os representantes (cinco) da sociedade civil são designados pelo Presidente da República para períodos de dois anos, permitida a recondução (par. 2º.).

A Medida Provisória também definiu a competência desse Comitê Gestor (art. 4º.), estabelecendo que cabe a ele:

- g) implantar e coordenar o funcionamento da ICP-Brasil;
- h) estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço;
- i) estabelecer a política de certificação e as regras operacionais da AC Raiz;
- j) homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;
- k) estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR;
- l) definir níveis da cadeia de certificação;
- m) aprovar políticas de certificados, práticas de certificação e regras operacionais das AC e das AR;
- n) credenciar e autorizar o funcionamento das AR;
- o) autorizar a AC-Raiz a emitir os certificados das AR's credenciadas;

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

Em que pese a previsão de todas essas atribuições, na prática o Comitê Gestor apenas atuará como órgão colegiado de cúpula da ICP-Brasil, definidor das políticas gerais de certificação. A execução dessas políticas, bem como as atividades práticas de credenciamento, supervisão e auditoria das atividades dos prestadores de serviço de certificação (as AC's e AR's) são desempenhadas pelo ITI-Instituto Nacional de Tecnologia da Informação, já que o parágrafo único do art. 4º. da MP permite que as funções nele definidas sejam delegadas à AC-Raiz(7). O próprio art. 5º. da MP, ao definir a função da AC-Raiz, a elege como autoridade “executora das políticas de certificados e normas técnicas operacionais aprovadas pelo Comitê Gestor.

O Decreto n. 3.872, de 18 de julho de 2001, dispõe sobre o Comitê Gestor da ICP-Brasil, sua Secretaria Executiva, sua Comissão Técnica Executiva e dá outras providências.

4.2. A Autoridade Certificadora Raiz (AC-Raiz)

A AC-Raiz, como se afirmou acima, é a “primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil” (art. 5º. da MP 2.200-2). A ela compete:

- r) emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de

nível imediatamente subsequente ao seu;

- s) gerenciar a lista de certificados emitidos, revogados e vencidos;
- t) 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;
- u) exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

O papel de Autoridade Certificadora Raiz da ICP-Brasil é desempenhado pelo ITI – Instituto Nacional de Tecnologia da Informação (art. 13 da MP), autarquia federal vinculada ao Ministério da Ciência e Tecnologia.

4.3. Autoridades certificadoras e de registro

As Autoridades Certificadoras (AC's) são as entidades componentes da cadeia de certificação responsáveis pela emissão de certificados digitais a usuários finais. Situam-se em nível inferior ao da AC-Raiz na cadeia de certificação, já que são credenciadas por esta última para emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular (usuário final). A essas autoridades certificadoras (as AC's), compete basicamente:

- v) emitir, expedir, distribuir, revogar e gerenciar os certificados;
- w) colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes;
- x) manter registro de suas operações.

As AC's não podem certificar nível diverso do imediatamente subsequente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil (art. 9º. da MP).

As AR's (Autoridades de Registro) são entidades operacionalmente vinculadas a uma determinada AC. Em outras palavras, cada AC opera através

de uma AR, para efeito de realizar a tarefa de identificação e cadastro dos usuários finais. Além de cadastrar e identificar usuários(8), as AR's encaminham solicitações de certificados às AC's e devem manter registros de suas operações (art. 7º.).

Qualquer pessoa, de direito público ou privado, desde que preenchendo os requisitos gerais da política de certificação da ICP-Brasil, pode requerer credenciamento com AC e AR (art. 8º. da MP).

5. Os poderes de fiscalização e auditoria do ITI como Autoridade Certificadora Raiz da ICP-Brasil

A AC-Raiz integra a cadeia de autoridades certificadoras, composta por ela própria e por todos os outros prestadores de serviços de certificação (as AC's e AR's), conforme já vimos. Está um nível acima de todos os demais prestadores de serviços da cadeia de certificação e, por isso, desempenha papel de órgão regulador (juntamente com o Comitê Gestor) da atividade de certificação digital.

Em razão da posição que ocupa na hierarquia da ICP-Brasil, como primeira autoridade da cadeia de certificação, sua função primordial não é a prestação de serviços de certificação para os usuários finais do sistema. Aliás, o parágrafo único do art. 5º. da MP 2.200-2 veda à AC-Raiz emitir certificados para o usuário final. Os certificados emitidos pela AC-Raiz têm como objetivo único identificar a própria AC Raiz ou as AC de nível imediatamente subsequente ao seu. Essa função certificadora, limitada às AC's que se situam no segundo nível da cadeia de certificação, é desempenhada em conjunto com outra, que é a de executar atividades de fiscalização e auditoria de todas as demais entidades integrantes da ICP-Brasil. Como executora das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê-Gestor, a AC-Raiz realiza tarefa de fiscalização e auditoria das AC's e AR's prestadoras de serviços de certificação (art. 5º. da MP 2.200-2). Nessa tarefa de fiscalização, o

ITI (que é a AC-Raiz da ICP-Brasil) pode inclusive aplicar sanções e penalidades, na forma da lei (art. 14 da MP).

As atribuições de fiscalização e auditoria do ITI, em relação às atividades dos prestadores de serviços de certificação credenciados à ICP-Brasil, são exercidas em conformidade com as normas e critérios estabelecidos pelo Comitê Gestor. As auditorias que realiza têm o objetivo de verificar se todos os processos, procedimentos e atividades das AC's integrantes da ICP-Brasil (e suas AR's) estão em conformidade com as suas respectivas DPC, suas Políticas de Certificado, a Política de Segurança e as demais normas e procedimentos estabelecidos para a ICP-Brasil. A frequência das auditorias é variável e podem ser feitas previamente ao credenciamento de uma AC na ICP-Brasil ou a qualquer tempo, sem aviso prévio. Adicionalmente, as AC's podem sofrer auditoria anualmente para fins da continuidade do credenciamento perante a ICP-Brasil.

As auditorias de conformidade verificam todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais, incluindo o controle dos processos de solicitação, identificação, autenticação, geração, publicação, distribuição, renovação e revogação de certificados. Os tópicos cobertos por uma auditoria de conformidade incluem, dentre outros: política de segurança, segurança física, avaliação de tecnologia, administração dos serviços; investigação de pessoal, PC e DPC utilizadas, contratos e considerações de sigilo.

O Comitê Gestor tem baixado várias resoluções que detalham como deve ser exercida a atividade de fiscalização pelo ITI. Dentre elas, merece destaque a Resolução n. 25, de 24 de outubro de 2003, que aprova procedimentos a serem obedecidos por este último órgão(9). Essa resolução regulamenta o art. 14 da Medida Provisória 2.200-2(10), estabelecendo que a atividade fiscalizadora do ITI tem por objetivo verificar a conformidade da atuação dos prestadores de serviços de certificação (AC's e AR's) com as Declarações de Práticas de Certificação (DPC's), Políticas de Certificado, Política de Segurança e as demais normas e procedimentos estabelecidos pela ICP-Brasil (art. 2º.). Portanto, o ITI,

no exercício de sua atividade de fiscalização, desenvolve procedimentos voltados a verificar o cumprimento, pelas entidades credenciadas (prestadores de serviços de certificação e prestadores de serviços de suporte), das normas e regulamentos que regem a ICP-Brasil.

A citada Resolução prevê que o procedimento de fiscalização alcançará o exame de documentos, instalações técnicas e ambiente lógico do prestador de serviço de certificação, bem como seu próprio pessoal, podendo acarretar a aplicação de uma ou mais penalidades (art. 4º). A Resolução ainda traz regras (arts. 12 a 16) sobre o processo administrativo de fiscalização, estabelecendo prazo (de 10 dias) para defesa ou justificativa do prestador de serviços de certificação, quando constatada alguma irregularidade. Também prevê as penalidades a que fica sujeito o prestador de serviços de certificação, por infração a qualquer disposição legal ou regulamentar da ICP-Brasil ou pelo não atendimento das exigências estabelecidas pelo ITI. As penalidades previstas são as seguintes: a) advertência; b) proibição de credenciamento de novas políticas de certificado; c) suspensão da emissão de novos certificados por prazo determinado; e d) descredenciamento (art. 17). Da decisão que impõe qualquer penalidade cabe recurso (art. 19).

6. Poderes normativos do Comitê Gestor

Além dos poderes de fiscalização que são conferidos ao ITI, outros poderes atribuídos a esse órgão e ao Comitê Gestor indicam que eles, reunidos, atuam com características próprias das agências reguladoras, já que têm o poder de direcionar as atividades privadas de certificação digital de acordo com interesses públicos juridicamente definidos.

As agências reguladoras não se limitam a uma atividade de fiscalização, como se sabe. Aliás, a atividade normativa é a que mais se costuma associar à função reguladora, mas também a ela não se limita, pois as agências reguladoras costumam despenhar um conjunto mais amplo de atribuições.

Como observa Luís Roberto Barroso, “embora a etimologia sugira a associação da função reguladora com o desempenho de competências normativas, seu conteúdo é mais amplo e variado. Ainda quando se aproxime, eventualmente, da idéia de poder de polícia administrativa – poder de direcionar as atividades privadas de acordo com interesses públicos juridicamente definidos–, a regulação contempla uma gama mais ampla de atribuições, relacionadas ao desempenho de atividades econômicas e à prestação de serviços públicos, incluindo sua disciplina, fiscalização, composição de conflitos e aplicação eventual de sanções(11).

Além da diversidade de atividades que as agências reguladoras desempenham, observa-se uma diversificação dessas tarefas entre cada uma delas, em função da diversidade de textos legais existentes, editados com a finalidade de normatizar diferentes setores da economia(12). Em outras palavras, o alcance e extensão das atribuições de uma agência reguladora vai depender do “marco regulatório” do respectivo setor da economia(13).

Em relação à certificação digital, a atividade de regulamentação, definindo a política de certificação e editando normas técnicas e regras operacionais sobre práticas de certificação, foi conferida de forma primária ao Comitê Gestor da ICP-Brasil (art. 4º. da MP 2.200-2). O Comitê Gestor tem, pois, uma atividade normativa no âmbito da ICP-Brasil, cumprindo ao ITI (na condição de AC-Raiz) a execução das normas e regulamentos editados pelo primeiro órgão. Mas, como existe previsão de que as funções do Comitê Gestor sejam delegadas à AC-Raiz (parágrafo único do art. 4º. da MP), mesmo essa função normativa pode ser exercida pelo ITI. Na prática, o que observa é que essa função normativa é repartida entre esses dois órgãos, editando o Comitê Gestor normas mais gerais sobre a política de certificação e de funcionamento da ICP-Brasil, enquanto que o ITI expede normas de alcance menos gerais (portarias, por exemplo)(14).

A tendência, no entanto, é que a atividade normativa fique como atribuição exclusiva do Comitê Gestor. O Projeto de Lei n. 7.316, de 2002, que dispõe sobre a prestação de serviços de certificação e define a Infra-Estrutura

de Chaves Públicas Brasileira - ICP-Brasil, proíbe o Comitê Gestor de delegar à AC-Raiz atribuições referentes à edição de atos de caráter normativo (par. único do art. 14).

7. A estrutura jurídica do ITI e do CG em comparação com a das agências reguladoras tradicionais

As agências reguladoras foram introduzidas no Brasil sob a forma de autarquias e, conseqüentemente, com personalidade jurídica de direito público, sujeitas ao mandamento do art. 37, XIX da Constituição e com criação dependente de lei específica.

Tal natureza é fundamental para que as agências reguladoras desempenhem com eficiência o seu papel, que consiste em intervir no domínio econômico e fiscalizar a prestação de serviços de interesse público. A natureza autárquica (como parte da administração pública indireta do Estado) confere autonomia e independência estrutural ao órgão para fins da realização de suas atribuições. As agências reguladoras, no entanto, têm um grau de autonomia em relação ao Poder central ainda maior do que as autarquias comuns. São espécies de *autarquias de regime especial*⁽¹⁵⁾, dotadas de prerrogativas próprias conferidas pelas leis que as instituíram, de forma a aumentar seu grau de autonomia em relação ao Poder Público central.

O ITI – Instituto Nacional de Tecnologia da Informação, a quem cabe desempenhar as atividades de fiscalização e auditoria dos prestadores credenciados de serviços de certificação da ICP-Brasil, também é uma autarquia, transformada em tal pelo art. 12 da MP 2.200-2⁽¹⁶⁾. Por ter natureza autárquica, o ITI pode ser dotado de todas as independências estruturais que costumam caracterizar as agências tradicionais. Embora a Medida Provisória não defina nenhum regime especial para ITI, sabe-se que ele é apenas órgão executor das políticas de certificação, que são definidas pelo Comitê Gestor da ICP-Brasil, este sim um órgão com peculiaridades na sua composição que

demonstram claramente o sentido de autonomia em relação ao poder político central. O art. 3º. da MP prevê que o CG, além de representantes de ministérios, é composto por cinco representantes da sociedade civil, integrantes de setores interessados na atividade de certificação digital. A participação de representantes da sociedade no Comitê Gestor da ICP-Brasil confere-lhe uma autonomia política e de gestão, com independência em relação aos interesses estatais específicos.

O Projeto de Lei n. 7.316, de 2002, que dispõe sobre a prestação de serviços de certificação e define a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil(17), e que irá substituir a MP 2.200 como “marco regulatório” dos serviços de certificação em nosso país – o projeto prevê a sua revogação -, atribui uma composição ainda mais heterogênea ao Comitê Gestor. Não somente amplia para 16 o número de representantes da sociedade civil (integrantes de setores interessados) como prevê a participação de representantes do Senado Federal, da Câmara dos Deputados, de tribunais superiores (um do STF, um do STJ, um do TST, um do TSE e um do STM), do Ministério Público Federal.

As agências reguladoras tradicionais adotaram o modelo de formar conselhos compostos por profissionais altamente especializados em sua área, com independência em relação ao Estado. A composição do Comitê Gestor, sobretudo a que lhe é dada pelo Projeto de Lei 7.316/02, parece concorrer para a mesma finalidade.

A forma autárquica conferida ao ITI, órgão executor das políticas de certificação, e a composição híbrida do Comitê Gestor, autoridade gestora das políticas de certificação, conferem a eles autonomia estrutural e política, características próprias das agências reguladoras tradicionais.

Conclusões:

1- O “marco regulatório” da atividade de certificação digital em nosso país

coincide com a edição da MP 2.200, o primeiro texto legal a disciplinar a estrutura da ICP-Brasil, mas que deverá em breve ser substituído (revogado) pelo Projeto de Lei 7.316/02, diploma de maior amplitude normativa.

2- O conjunto de atribuições que foram conferidos pela MP 2.200 ao Comitê Gestor e ao ITI demonstra que esses dois órgãos, em conjunto, desempenham tarefas que, a despeito das peculiaridades, se incluem como atividades típicas de uma agência reguladora, pois possuem poder gerencial (técnico) e de controle sobre os prestadores de serviços de certificação credenciados.

Embora o ITI e o Comitê Gestor da ICP-Brasil não tenham recebido a denominação de “órgão regulador” ou “agência reguladora”, nos textos legais que constituem o marco regulatório da atividade de certificação digital no país, na prática funcionam como tal, na medida em que a atuação desses órgãos (em conjunto ou isoladamente) revela intervenção estatal junto a um setor privado, para impor normas de conduta a particulares que visem obrigá-los a atingir o bem estar coletivo.

3- O Comitê Gestor e o ITI não têm atribuição de regular a atividade de certificação digital como um todo, pois esta é livre e independe de autorização específica, mas na medida em que o art. 10 (e seus parágrafos 1º. e 2º.) da MP 2.200-2 confere validade diferenciada (maior) aos certificados expedidos no âmbito da ICP-Brasil, qualquer prestador de serviços que tiver interesse em expedir certificados com validade jurídica contra terceiros, terá que se credenciar junto a ela e, conseqüentemente, se submeter aos poderes regulatórios do Comitê Gestor e do ITI. Qualquer outra pessoa pode desenvolver uma infraestrutura para certificação digital, mas o raio de aceitação dos certificados que expedir terão alcance e validade limitados. A ICP-Brasil é a única infraestrutura de chaves públicas cujos órgãos a ela vinculados podem emitir certificados de aceitação e validade jurídica dentro de todo território nacional⁽¹⁸⁾, o que na prática faz com que o seu Comitê Gestor e o ITI atuem como órgãos reguladores da certificação digital no país. Ademais disso, o Projeto de Lei 7.316/02 prevê

que o ITI poderá fiscalizar prestadores de serviços não credenciados à ICP-Brasil.

4- A atividade regulatória sobre a ICP-Brasil é dividida entre o Comitê Gestor e o ITI, sendo que as atribuições normativas, de delineamento das regras gerais e de funcionamento (da ICP-Brasil), ficam a cargo do primeiro órgão, competindo ao segundo dar execução aos atos normativos. Enquanto não aprovado o Projeto de Lei 7.316/02, o ITI, na condição de Autoridade Certificadora Raiz, permanece com uma atividade normativa residual, naquilo que não conflita as resoluções do Comitê Gestor.

Notas:

(1) certificado digital: o documento eletrônico que vincula uma chave de verificação de assinatura a uma pessoa, identificando

-a.

(2) autoridade certificadora: a pessoa que emite certificados e presta outros serviços relacionados com assinaturas e certificados digitais.

(3) No inglês, PKI (abreviatura da expressão *Public Key Infrastructure*).

(4) criptografia assimétrica de chaves públicas: método pelo qual se utilizam duas chaves matematicamente relacionadas, onde uma delas é pública e, a outra, privada, para criação de assinatura digital, com a qual é possível a realização de transações eletrônica seguras e a troca de informações sensíveis e classificadas

(5) A MP 2.200 foi editada originalmente em 29/06/2001, vigorando por 30 dias, sendo reeditada (MP 2.200-01) em 28/07/2001. Finalmente, foi reeditada mais uma vez (MP 2.200-2) em 27/08/2001, passando a vigorar como “medida permanente” por força da Emenda Constitucional n. 32.

(6) De acordo com o par. 1º. do art. 10 da MP, os documentos eletrônicos certificados segundo processo disponibilizado pela ICP-Brasil presumem-se verdadeiros. Os certificados emitidos por autoridades certificadoras não vinculados a ela somente têm validade se aceitos pelas partes ou pela pessoa a quem for oposto (par. 2º.).

(7) O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira (art. 13 da MP). (8) O art. 7º. da MP estabelece, como regra geral da política de certificação no âmbito da ICP-Brasil, que a identificação e cadastro dos usuários perante as AR's seja feita com a presença física destes.

(9) Cópia da Resolução pode ser encontrada no site da ICP-Brasil (www.icpbrasil.gov.br).

(10) O art. 14 da MP 2.200-2 estabelece que “no exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei”.

(11) “Agências reguladoras: Constituição, transformações do Estado e legitimidade democrática”, artigo de Luís Roberto Barroso, publicado no site Jus Navigandi (www.jus.com.br), visitado em 03.04.05.

(12) Confira-se Luís Roberto Barroso, artigo citado.

(13) O que se denomina “marco regulatório”, que pode ser definido como “o conjunto de regras, orientações, medidas de controle e valoração que possibilitam o exercício do controle social de atividades de serviços públicos, gerido por um ente regulador que deve poder operar todas as medidas e indicações necessárias ao ordenamento do mercado e à gestão eficiente do serviço

público concedido, mantendo, entretanto, um grau significativo de flexibilidade que permita a adequação às diferentes circunstâncias que se configuram" (Agências reguladoras, artigo de Cristiano Martins de Carvalho, publicado no site Jus Navigandi – www.jus.com.br, visitado em 03.04.05).

(14) O ITI tem editado normas específicas, como a Portaria n. 1, de 12 de dezembro de 2001, por meio da qual se tornou público a geração do par de chaves assimétricas e a emissão do certificado da AC-Raiz; Portaria n. 12, de 26 de março de 2002, que fixa valores da tarifa de credenciamento das AC's; e outras portarias que tornam público a emissão de certificados de AC's intermediárias. Além disso, o ITI editou a Instrução Normativa n. 1, de 16 de fevereiro de 2005, que implementa o controle de versões das Políticas de Segurança, das Políticas de Certificados e das Declarações de Práticas de Certificação das Autoridades Certificadoras no âmbito da ICP-Brasil. Cópias dessas portarias e instrução normativa podem ser obtidas no site do ITI (www.iti.gov.br).

(15) Como observa Hely Lopes Meirelles, "*autarquia de regime especial* é toda aquela a que a lei instituidora conferir privilégios específicos e aumentar sua autonomia comparativamente com as autarquias comuns, sem infringir os preceitos constitucionais pertinentes a essas entidades de personalidade pública" (*Direito administrativo brasileiro*, 1993, p. 315).

(16) O art. 12 da MP 2.200-2, de 24.08.01, tem a seguinte redação: "Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação - ITI, com sede e foro no Distrito Federal".

(17) A Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, foi instituída a partir da edição da Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Contudo, a Medida Provisória, embora de capital importância, consagrou texto normativo de escopo restrito. Limitou-se, em linhas gerais, a estabelecer estrutura administrativa adequada à prestação satisfatória desses serviços. Daí o Executivo ter apresentado um projeto que consagra uma previsão normativa mais abrangente para a ICP-Brasil e prestação dos serviços de certificação.

O Projeto de Lei foi apresentado em plenário da Câmara em 07.11.02. Enviado à Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI), recebeu parecer do relator, Dep. Jorge Bittar, pela aprovação com substitutivo, em 17.11.04. Até 29.11.04, foram apresentadas 25 emendas ao substitutivo. Em 30.11.04, a Comissão aprovou por unanimidade o parecer do relator às emendas ao substitutivo. O projeto foi enviado, em 02.12.04, à Comissão de Constituição e Justiça e de Cidadania (CCJC), onde atualmente se encontra.

(18) Os certificados emitidos pelas AC's ligadas à ICP-Brasil podem inclusive ter validade em outros países, dependendo de tratados e atos internacionais de cooperação que são celebrados pelo Comitê Gestor.