A POLÍTICA DE CERTIFICAÇÃO DIGITAL: PROCESSOS ELETRÔNICOS E A INFORMATIZAÇÃO JUDICIÁRIA

Alexandre Veronese[*]

RESUMO

O trabalho focaliza o dilema da implantação do sistema brasileiro de certificação digital (ICP-Brasil) e da informatização do judiciário. A ICP-Brasil foi constituída pelo Instituto Nacional de Tecnologia da Informação (ITI), em um contexto pleno de críticas. O Conselho Federal da Ordem dos Advogados do Brasil (OAB) criticou fortemente o sistema em defesa de suas prerrogativas, constituindo um modelo alternativo de certificação digital. O conflito culminou em diversas ações, inclusive processos judiciais. Mas não houve a solução do impasse. É descrita a implantação do sistema, bem como o funcionamento da tecnologia. Depois, são analisados o quadro normativo e as críticas. O trabalho deriva de uma pesquisa realizada por meio de entrevistas e questionários sobre o modelo de certificação digital. A conclusão é que a discussão técnica e jurídica expressa a disputa social que deve ser entendida a partir de uma cadeia relacionada com o uso social da tecnologia. Ainda, que a falta de disseminação de uma tecnologia de uso geral, para garantia das trocas de informações, atrasa a informatização do judiciário.

PALAVRAS CHAVES

CERTIFICAÇÃO DIGITAL; PROCESSO ELETRÔNICO; INFORMATIZAÇÃO; ADVOCACIA.

ABSTRACT

The paper depicts the dilemmas raised by the implementation of the Brazilian digital certificates' system (Brazil's PKI) and the process of informatization of its courts. The Brazil's PKI was established by the National Institute of Information Technology

[*] Professor do Departamento de Direito Público da Universidade Federal Fluminense (UFF), advogado, doutorando em sociologia (Iuperj), mestre em sociologia e direito (UFF). E-mail: **veronese@matrix.com.br**. A pesquisa contou com fomento do Departamento de Pesquisa e Documentação da Seccional Rio de Janeiro da Ordem dos Advogados do Brasil. A parte técnica foi estudada a partir de uma bolsa oferecida pela CertiSign S/A. O trabalho contou com o auxílio de Christiana Soares de Freitas (UnB).

(“Instituto Nacional de Tecnologia da Informação”, also know by its acronym “ITI”) among a context of political turmoil along with a lot of criticism. The Federal Council of the Bar Association (“Conselho Federal da Ordem dos Advogados do Brasil”) made especially harsh critics against the system. That was due to its interest in the defense on some corporative prerogatives, like the emission of lawyers IDs. Also, it had been planning to launch its own digital certificates’ system. The conflict grew in many actions, including constitutional and ordinary lawsuits, without any visible solution. The paper describes the Brazil PKI system’s implementation process, and the main concepts of the technology. Then it analyses the legal framework and the critics delivered upon it. The paper was build from a research made with interviews and a survey inquiry about the models of managing digital certificates’ systems. Therefore, it concludes that both the technical and the legal debate show a social dispute, which has to be assessed from the comprehension of the technology’s social use. Hereafter, the lack of diffusion of a general use technology to guarantee data interchanges obviously delays the judicial system informatization.

KEYWORDS

DIGITAL CERTIFICATES; E-JUSTICE; INFORMATIZATION; E-LAWYERS.

INTRODUÇÃO

O primeiro problema da relação entre as tecnologias da informação e da comunicação e os processos judiciários, está na dificuldade de garantir segurança informacional para os partícipes das lides. Os usuários visualizam a Internet como um meio de comunicação sem possuir a noção clara de que ela funciona como um canal aberto. Muitas vezes, desconhecem os riscos à privacidade ao qual estão submetidos. Uma analogia interessante pode ser feita ao se verificar que os aparelhos de telefonia celular, cuja operação se dá por meio de sinais no espectro radioelétrico, utilizam criptografia para embaralhar as emissões e garantir o sigilo das conversas telefônicas. Este complicador pode ser compreendido pela frase de Steven Levy, estudioso da história da tecnologia criptográfica na Internet: “we think we are whispering, but we are really broadcasting” (LEVY, 2000).

O problema da segurança nas trocas eletrônicas é uma questão técnica. O atual "estado da técnica" é a criptografia assimétrica. Ela se mostrou revolucionária ao modo anterior de embaralhar mensagens: a criptografia simétrica. A fraqueza dos sistemas simétricos residia na necessidade de transmissão da chave criptográfica entre as partes envolvidas. O ideal seria possuir uma fórmula matemática que usasse duas chaves diferentes, sem compartilhamento: uma para cifrar as mensagens e outra para decifrá-las. Resolvido o dilema do ponto de vista teórico, o desenvolvimento tecnológico da criptografia de chaves públicas constitui o novo paradigma para a garantia da segurança na informação.

Apesar da solução, estes novos sistemas criptográficos ainda não atendiam os requisitos simbólicos para que fossem considerados como soluções sociais para o dilema da segurança da informação. A percepção de segurança não é somente um problema técnico. Ela é um problema social. De nada adianta a existência de uma solução tecnológica que é vista com ampla desconfiança pelos usuários; apesar de ser reconhecida como excelente pelos especialistas. Assim, a questão central é entender como uma solução, que visa efetivar segurança técnica, pode produzir segurança jurídica. Para este tema, há que ser compreendido o uso social desta tecnologia. Assim, para que os práticos do direito possam ser beneficiados por estas soluções técnicas, na informatização do seu cotidiano, ela precisa estar na margem de confiança do operador médio. É somente desta forma que segurança jurídica poderá ser conferida aos futuros processos eletrônicos. O presente trabalho mostra a dificuldade de institucionalização da infra-estrutura de chaves públicas (ICP) no processo social da informatização do Poder Judiciário. A pesquisa que o subsidia foi composta por seis entrevistas de campo com técnicos das autoridades certificadoras (AC). Também foi realizada uma pesquisa por meio de questionários com funcionários de duas AC. Para chegar ao problema da institucionalização cotidiana dos processos judiciais eletrônicos, é descrito o funcionamento da criptografia de chaves públicas, que possibilita tanto a realização de assinaturas eletrônicas com certificação digital, quanto a cifração dos dados. Posteriormente, será detalhado como está estruturada a legislação brasileira que instituiu o sistema nacional certificação digital e as críticas da comunidade jurídica, com destaque para a Ordem dos Advogados do Brasil (OAB). Esta organização normativa foi acompanhada de algumas opções políticas e técnicas, na forma de um modelo

organizacional. Assim, o modelo brasileiro é contrastado com a proposta da OAB e com a pesquisa realizada junto aos operadores técnicos das AC. Do conjunto de respostas dos técnicos, será extraída a conclusão de que os riscos operacionais são sempre presentes. A solução reside em seu possível controle social, que exige difusão e conhecimento cotidiano da técnica. Por fim, será analisado o impasse vivido pela com sua proposta específica de política para certificação digital que, por contrapor-se ao modelo existente, não se tornou viável do ponto de vista social. O esgotamento do problema político se deu com a aceitação, por parte da OAB, do modelo geral do governo brasileiro. Uma versão, com a integralidade dos dados, deste trabalho em fase de publicação (VERONESE, 2007).

1 FUNCIONAMENTO DAS ASSINATURAS ELETRÔNICAS E USO SOCIAL

A possibilidade de envio de informações sigilosas de forma segura fez com que, durante muitos anos, a certificação digital fosse restrita às redes governamentais envolvidas com a segurança nacional ou militar. O campo de estudos de sistemas criptográficos possui um histórico de controle por parte dos governos. Com o advento de novos usos sociais para estas técnicas foi feita uma distinção, relacionada com a publicação de um padrão civil pelo governo americano na década de 70, entre a criptografia civil e a militar.

Assim, o artefato técnico da criptografia obteve um alcance mais amplo do que tinha no passado, com seu foco original no segredo. Em especial, ele tornou-se uma tecnologia central para a comunicação em redes abertas, ou seja, pela Internet. No próximo tópico serão apresentados os fundamentos e os objetivos associados à tecnologia.

1.1 Criptografia: inovação social e técnica

Os algoritmos de criptografia estão ligados à idéia primordial de segredo. Desde a sua origem, o objetivo era tornar uma mensagem ilegível para uma terceira parte. A criptografia se manteve restrita ao uso militar durante muitos anos. Ela não teve grande desenvolvimento mesmo como campo de estudos acadêmicos, tendo em vista que havia controle na difusão de informações sobre o tema. A sua entrada na vida civil só ocorreu a partir de 1948 e 1949, que foi o biênio da publicação de dois artigos

seminais de Claude Shannon na “Bell System Technical Journal”. Quase vinte anos se passariam até que houvesse o desenvolvimento teórico em prol da criptografia do tipo assimétrico. A segunda mudança radical ocorreu com a publicação do artigo de Diffie & Hellmann, “Novas Direções na Criptografia”, que serviu de base para o desenvolvimento tecnológico, efetivado por Rivest, Shamir e Adleman, de um sistema de criptografia de chaves públicas (BENSOUSSAN & LE ROUX, 1999, p. 14). Desta forma, sem que houvesse a mudança de perspectiva científica e tecnológica, seria impossível pensar em realizar transações bancárias em larga escala pela Internet, por exemplo. O problema da certificação digital era resolver a troca segura de informações pessoais, comerciais ou bancárias sem que houvesse a violação dos dados. Resolvê-lo favoreceria não só o comércio eletrônico, mas diversos outros intercâmbios pela Internet. Os tópicos seguintes estão baseados em Autret, Bellefin & Oble-Laffaire (2002).

Os algoritmos simétricos são baseados em chaves privadas. Assim, o emissor cifra a mensagem e o receptor a decifra. Para as duas operações é utilizada a mesma chave, gerada por um algoritmo simétrico. Assim, a operação matemática é idêntica no cifrar e no decifrar. Ela dura o mesmo tempo e requer os mesmos meios computacionais. O primeiro sistema é o de criptografia simétrica. Ela utiliza a mesma chave, gerada a partir de um algoritmo, para cifrar e decifrar a mensagem. Esta chave é compartilhada pelo remetente e destinatário. A mensagem original (chamada de texto simples), é transformada em um texto cifrado. O destinatário, por sua vez realiza a transformação reversa, do texto cifrado para o texto simples. A força de um algoritmo de criptografia simétrico reside tão somente no tamanho da chave utilizada.

O grande problema do sistema de chaves simétricas reside no compartilhamento de chaves. Pode-se imaginar a dificuldade de manter relações sigilosas dentre de uma empresa, por exemplo. Se existirem tantas chaves quantos funcionários, a gestão delas será uma tarefa complexa no cotidiano dos empregados. Da mesma forma, existirão muitas possibilidades de perda e de vazamento das chaves, na medida que elas forem compartilhadas entre os vários funcionários. Se elas tiverem que ser trocadas sempre, a possibilidade de perda dos dados aumenta, pois sem uma chave, não se abre a mensagem cifrada. Se a chave for única para a empresa toda, seu vazamento significará exposição total. Em algum momento terá que haver intercâmbio

da chave entre emissor e receptor. Se ela for interceptada por um terceiro, toda a comunicação é comprometida. Ainda, este terceiro poderá intervir como se fosse tanto o emissor quanto o receptor. Este problema se relaciona profundamente com a ambiente das novas tecnologias da informação, quando se verifica o largo uso de redes abertas. A criptografia simétrica ainda possui utilidade. Ela é aceitável para uma comunicação única, onde a chave pode ser descartada depois do uso. Ela serve também para comunicações com baixo risco de vazamento. Mas ela possui desvantagens quando aplicada em comunicação contínua. Ela também não permite o sistema de assinatura eletrônica, com autoridades de certificação porque não há como manter uma chave pública para comparação. Por conta destes problemas é que a criptografia assimétrica se afirmou como um sistema confiável. A diferença central do algoritmo assimétrico é que ele gera duas chaves (uma pública e outra privada). A operação de cifrar é muito rápida. Já a operação de decifrar é muito lenta. Agora será traçado o funcionamento dos sistemas de criptografia de informações e de assinaturas digitais, no sistema de chaves públicas.

A criptografia assimétrica consiste na utilização de duas chaves, uma para cifrar e outra para decifrar. A partir do algoritmo serão geradas duas chaves, que formam um par único. Uma delas será pública e ficará disponível para o uso geral. A outra será privada, mantida pelo titular. A técnica permitiu o aparecimento de um meio mais seguro para a cifração de informações e, principalmente, para a montagem de sistemas de certificação digital (infra-estruturas de chaves públicas), que gerem as chaves públicas em repositórios abertos, bem como emitem as chaves privadas e são passíveis de auditoria e controle técnico. A função nova é a produção de assinaturas eletrônicas, passíveis de conferência. Com esta função é resolvido o dilema do compartilhamento de chaves pelos canais de comunicação inseguros. Deste modo, ela tornou-se um meio central para a segurança nos tempos atuais da Internet. Em resumo, existem duas funções técnicas, que têm importante uso com a criptografia assimétrica: a cifração de conteúdos de mensagens (sigilo) e a utilização de certificados digitais, como garantia das assinaturas digitais. Os certificados, que permitem as assinaturas, são gerados com chaves criptográficas. A Resolução n. 07, de 12 set. 2001, expedida pelo Comitê Gestor da ICP-Brasil, admite quatro graus de certificados de assinatura (A) e de sigilo (S). A gradação de força (tamanho, em bits) é o fator lógico relevante para

diferenciação das chaves criptográficas. O armazenamento em mídias diferenciadas é um elemento central para definição da possibilidade de uso das duas funções técnicas, que serão descritas no próximo tópico.

1.2 Aplicações: cifração de mensagens e assinaturas digitais

O primeiro uso é a cifração de mensagens. Para cifrar uma mensagem sem que haja risco de interceptação em uma rede aberta, Alice utiliza a chave pública de Bob. Após a cifração, esta só poderá ser decifrada com o uso da chave privada dele. Para que ela possa ser colocada em prática, há a necessidade da existência das duas chaves (pública e privada), geradas pelo mesmo algoritmo assimétrico.

Há um modelo da operação com assinatura, cujo uso pressupõe um algoritmo de "hash" para garantir a integridade da mensagem. Esta é realizada com a utilização do par de chaves das duas partes, onde a chave privada, de conhecimento apenas do remetente (Alice), assina a mensagem. Esta é também cifrada usando a chave pública do destinatário (Bob). Gera-se, ainda, um resumo da mensagem ("hash"): um valor único criado a partir de uma operação matemática que permite comparação para checar a ausência de alteração do conteúdo. A mensagem é enviada juntamente com um certificado digital específico para o destinatário em um pacote. No recebimento, o destinatário (Bob) verifica a mensagem comparando o valor desse resumo recebido com o valor do resumo gerado pelo remetente. Além disso, ele checa a assinatura com a chave pública do remetente (Alice) e decifra a mensagem com a sua chave privada (Bob). Assim, a mensagem trafega com segurança e garantia de identificação do remetente (Alice).

Uma outra opção seria cifrar apenas o resumo da mensagem. A cifração do resumo resolve a dificuldade de decifrar mensagens muito extensas (capacidade computacional), quando são utilizados os algoritmos assimétricos. Uma outra solução seria remeter, junto com o pacote, uma chave simétrica cifrada por meio de criptografia assimétrica. Neste caso, usar-se-ia a chave pública de Bob para cifrá-la, tendo em vista que o texto só poderia ser acessado por ele, que possui a chave privada para decifrar a chave simétrica e, então, decifrar o texto.

A criptografia assimétrica possibilitou a emissão de certificados digitais para serem apostos junto com as mensagens e, desta forma, garantirem, por meio de uma

entidade de certificação (terceiro de confiança), que aquela assinatura digital é realmente do remetente. A analogia mais simples pode ser feita com uma carteira de identidade, cujo uso atesta – por meio de uma entidade terceira numa relação entre duas pessoas – que um dos partícipes é realmente quem diz ser. Para a realização desta operação, pressupõe-se a existência de uma entidade que emite o certificado digital padronizado. Este certificado funciona como a assinatura digital e é produzida em relação estrita com a chave privada do usuário.

Ainda, há a participação de um terceiro de confiança, envolvido na checagem das mensagens, que é uma autoridade de certificação (AC). Ela fornece os certificados, as chaves privadas e ainda mantém os repositórios. Neste sentido, o sistema de certificação digital funciona como uma pirâmide, que tem no seu vértice uma instituição que a audita do ponto de vista técnico (AC-Raiz).

2 A LEGISLAÇÃO E O MODELO DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI)

Para entender a institucionalização do sistema de certificação digital brasileiro, serão demonstrados os antecedentes da atual legislação, bem como as críticas dirigidas ao modelo. Estas críticas geraram a modificação da primeira legislação sobre o tema e permitiram o debate para redação de um projeto de lei que, até o presente momento, tramita no Congresso Nacional. Esta história setorial facilita a compreensão do dilema da OAB e da dificuldade de expansão da informatização dos processos judiciais no país. Estas dificuldades estão atingindo o seu momento final, tendo em vista a edição recente de um conjunto de leis que visam formar um arcabouço jurídico para a permissão processual da informatização.

2.1 O sistema brasileiro de certificação digital

É pouco lembrado que antes da Medida Provisória (MP) n. 2.200, de 2001, houve a publicação do Decreto n. 3.587, de 05 set. 2000, criando a ICP-Gov, que seria uma infra-estrutura de chaves públicas para todas as instituições da União. Entretanto, a ICP-Gov não abrangeria os órgãos do Poder Legislativo, do Judiciário e, muito menos, serviria para a certificação digital em relação às empresas privadas e à sociedade civil. Ela seria apenas uma infra-estrutura de chaves públicas para os órgãos do Poder

Executivo federal. Este Decreto foi revogado, por completo, pelo Decreto n. 3.396, de 05 nov. 2001, abrindo espaço para a constituição da ICP-Brasil. A origem do sistema brasileiro de certificação digital é a formação de um ponto central de uma rede que serviria ao Poder Executivo federal. Mas, depois, este ponto foi ampliado para atingir todo a federação (incluindo os estados e municípios), bem como toda a sociedade.

A MP n. 2.200 de 2001, em sua primeira versão, estruturou a infra-estrutura de chaves públicas, localizada no ITI como a única ICP que deveria ser reconhecida no Brasil, do ponto de vista jurídico. Houve uma certa polêmica com esta opção, haja vista que existiam dúvidas sobre a possibilidade do governo fixar o que valeria, ou não, no tocante à certificação digital por meio de lei. A crítica estava centrada na impossibilidade do Estado cassar a possibilidade de que os indivíduos contratantes pudessem eleger uma outra ICP e os certificados como válidos para uma relação econômica pela Internet. Ou, mesmo que não fosse uma imposição, que seria pouco razoável induzir que haveria um certificado "mais legal" do que outros. As reclamações mais fortes vieram da OAB e referiam-se não só aos negócios privados, mas aos atos processuais que caminham para serem realizados pelo Internet (protocolo de petições, por exemplo). Esta polêmica, no seu aspecto mais normativo, foi sendo pacificada aos poucos pela modificação do texto original pelas duas subseqüentes edições da MP, mas está longe de ter sido definitivamente resolvido (MARCACINI, 2002; KAMINSKI & VOLPI, 2004).

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

No Brasil optou-se por um modelo que centrou toda uma infra-estrutura sob o controle técnico do Poder Executivo federal, no âmbito do ITI. Ele foi criado em 2000, por meio de um desdobramento do Centro de Pesquisas Renato Archer (CenPRA) – antigo Centro de Tecnologia para Informática – sediado em Campinas. Inicialmente, o ITI, bem como o CenPRA, era vinculado ao Ministério da Ciência e Tecnologia, que havia concentrado, em 1999, todas as unidades de pesquisa em uma única secretaria. Antes, as unidades estavam divididas entre o Ministério e o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). Ao CenPRA foi atribuída a função

de empreender a infra-estrutura de chaves públicas (ICP-Brasil) com a edição da MP n. 2.200 de 2001. Esse contexto político de criação do ITI foi bastante polêmico. Em primeiro lugar, o Instituto foi criado a partir de uma MP, uma ação legislativa empreendida pelo Executivo. Vários atores sociais apresentaram, na época, posições políticas divergentes ao governo.

De um lado, havia aqueles que eram contrários à decisão de centrar o modelo no ITI porque se recusavam a se subordinar à fiscalização e ao traçado de diretrizes por qualquer órgão da administração pública, Era o caso do Conselho Federal da OAB. Ela visava constituir sua própria autoridade certificadora Raiz (AC-Raiz; no caso, a ICP-OAB) para a informatização dos atos processuais dos advogados. O seu alerta era orientado pela defesa das prerrogativas dos vários entes federados, mesclada com uma oposição aos equívocos jurídicos do texto legal (MARCACINI, 2007).

Outros críticos, do modo como estava sendo feita a institucionalização da ICP-Brasil, eram ligados à comunidade acadêmica. O seu argumento era que como foram os cientistas que desenvolveram todo o projeto desde o seu início, no âmbito do CenPRA, logo, eles deveriam ter levado o processo adiante (FREITAS & VERONESE, 2006).

Pode-se verificar que o tempo da tecnologia não é o mesmo tempo da política, ou seja, a implementação dos artefatos técnicos tem muitos empecilhos que não são apenas de natureza tecnológica. Os artefatos, além de socialmente construídos, são aplicados mediante a produção de redes políticas específicas visando à sua utilização. Uma vez pronta, a tecnologia conhece, além do espaço técnico de sua produção, o espaço jurídico e social. Adiante será tratado do processo de incorporação do espaço técnico da criptografia no cenário político nacional. Esse processo abrange mudanças e estratégias do espaço jurídico, sem as quais o artefato não é incorporado socialmente e não adquire visibilidade pública (LATOUR, 2000; LATOUR, 1994). Este problema decorre da certificação digital ter sido criada para um ambiente de uso restrito. Assim, o ITI tinha como sua única missão fomentá-la, tornando-se um espaço técnico especializado. A mudança recente é a percepção de que a fixação numa agenda restrita não ajudou a popularização da tecnologia. Apenas a sua ampliação nas políticas públicas servirá para produzir tal efeito, uma vez que ela precisa de usos sociais (aplicações) para ser conhecida. A informatização do Poder Judiciário é certamente uma

das políticas públicas que será utilizada para expandir a certificação digital e resolver vários impasses de sua difusão. É relevante analisar as críticas ao modelo brasileiro para entender como este impasse está estruturado.

2.2 Críticas dirigidas ao modelo brasileiro

No presente tópico serão compendiadas as críticas dirigidas à implantação do ITI. Será demonstrado como parte delas foi absorvida na reedição da MP que instituiu o Instituto, bem como no Projeto de Lei (PL) n. 7.316, de 2002, que ainda tramita no Congresso. A primeira versão da MP foi publicada em 28 jun. 2001. A segunda edição, com a correção de detalhes e pequenos ajustes, foi publicada em 27 jul. 2001. Por fim, a terceira versão, que marcou a transferência fática para a Casa Civil da Presidência, foi publicada em 24 ago. 2001.

Em relação à passagem da redação original para a primeira reedição (segunda versão da MP), cabe ressaltar que as únicas mudanças diziam respeito à composição do Comitê Gestor do ITI. Este era ligado à Presidência da República, apesar do ITI ser submetido ao Ministério da Ciência e Tecnologia. As críticas da OAB apenas aumentaram, culminando em diversas ações contra o modo de informatização do sistema de petições do Tribunal Regional do Trabalho da 4ª Região (Rio Grande do Sul) e do Tribunal Superior do Trabalho (TST). O centro da polêmica é a necessidade de subordinação técnica da OAB ao sistema do ITI. A notícia do "O Estado de São Paulo" relata a divergência em relação ao sistema oriundo da MP (CERTIFICAÇÃO, 2005).

A edição da MP não coletou somente críticas porque a OAB, por meio do Conselho Federal, organizou os serviços de seu sistema fora da estrutura da ICP-Brasil. A construção da ICP-OAB é a evidência da discórdia. Ela funciona com duas autoridades certificadoras, que são as seccionais de São Paulo e Minas Gerais. Ela pode ser acessada no endereço: http://cert.oab.org.br. Ainda constitui parte do imbróglio a gestão do cadastro nacional de advogados, que é o banco de dados da OAB.

A passagem da segunda para a terceira versão da MP foi marcada pela transferência do ITI para a Presidência e fica evidente com a análise dos textos legais. O art. 14, da segunda versão, foi modificado, na terceira MP, tendo sido renomeado como o art. 16. Neste dispositivo foram atribuídas ao Diretor-Presidente do ITI as mesmas competências de gestão que antes eram facultadas ao Ministro. A noção de que houve

uma migração do âmbito do MCT para um espaço fora daquele Ministério fica clara quando é analisado o art. 17 (que não existia na redação original da Medida Provisória), onde estão dois dispositivos de transferência de bens (inciso I, art. 17) e recursos (inciso II, art. 17).

Pouco tempo depois, um decreto acomodou o órgão do âmbito da Casa Civil da Presidência da República, ainda que ele formalmente estivesse no Ministério da Ciência e Tecnologia. Além desta mudança central, foram incluídos novos dispositivos, na MP, que buscavam estruturar a nova instituição. Eles diziam respeito tanto à formação das diretorias, como a montagem da procuradoria federal especializada do órgão, conforme exposto nos art. 15 e 18 da nova redação. No campo técnico, as mudanças diziam respeito às funções da ICP-Brasil. Como a modificação do "licenciamento" de autoridades certificadoras (AC) para "credenciamento". O mais significativo é notar que houve uma expansão da possibilidade de agendas para o órgão.

Outras modificações se relacionam com o interesse de ampliar as competências e ações do Instituto. Pode-se considerar que elas estão ligadas ao movimento de construção de uma política nacional para a área de tecnologia da informação. Este processo tomou corpo no âmbito do último Governo, com a retomada de incentivo às empresas e órgãos federais de processamento de dados. Além de investimentos neste campo, houve a construção de políticas públicas para inclusão digital e de incentivo ao uso do software livre. Na terceira versão, fica claro que houve a conceituação do documento eletrônico para atender às finalidades da Secretaria de Receita Federal e aos órgãos fazendários dos Estados e dos municípios.

As modificações consolidaram o sistema piramidal, onde o vértice é representado pelo ITI, alocado junto ao órgão máximo do Poder Executivo (Presidência da República) que é o espaço político com maior visibilidade do aparelho estatal. Neste modelo, existe uma quantidade de competências atribuída ao Instituto, incluindo desde o traçado das políticas públicas até sua fiscalização (com aplicação de sanções), conforme o novo art. 14 (não existente na versão anterior). Este modelo é condizente com a organização administrativa e jurídica clássica, onde a direção é exercida por poucos indivíduos, que enfeixam um grande eque de responsabilidades. Há pretensão de coesão e lógica em termos de sistema.

O modelo proposto pela OAB é distinto. Ele resulta da ausência de um único vértice. Assim, existiriam diversos órgãos com competência para gerir os vários sistemas de certificação. Um exemplo deste modelo é o caso americano, onde cada Estado possui uma entidade raiz. Neste modelo, a interoperabilidade é um ponto central, com a formação de certificações cruzadas ("bridges"). A competência é compartilhada e atribuída conforme o uso social dos certificados. Ele se aproxima do sistema de certificação do tipo PGP ("Pretty Good Privacy"), onde não há uma estrutura principal de gerenciamento. O modelo é policêntrico, ou seja, baseado em uma lógica de rede.

É importante mencionar que as críticas resultaram não só na redação de uma reedição modificada da mesma MP, como também na estruturação de um PL, que apararia todas as arestas normativas. O ponto central deste debate oscila, à primeira vista, entre as opções na definição de um modelo tecnicamente mais seguro. Para além das questões jurídicas da categoria dos advogados, concernentes às prerrogativas da OAB, existe uma questão de fundo sobre os riscos envolvidos nas escolhas sobre qual modelo deve ser montado para prestação dos serviços de certificação digital.

2.3 Políticas de certificação digital

A definição de uma política nacional para certificação digital decorre da percepção específica sobre o desenvolvimento da tecnologia da informação em relação ao setor público: há escassez de recursos para investir-se em várias frentes de trabalho. A formação de políticas públicas não é somente uma opção intra-estatal. Os atores do mercado e da sociedade civil são diretamente implicados pelas opções estatais. Em alguma medida, estes atores não-estatais podem determinar o fracasso ou o sucesso de uma política pública acerca do uso social da tecnologia da informação pública.

O Estado brasileiro não produz mais equipamentos em quantidade para poder produzir uma política pública de informática autárquica. A necessidade de interconexão entre os órgãos que compõe a administração pública federal requer que haja amplo uso de protocolos técnicos padronizados. O quadro se torna mais complexo pela importância de que os sistemas federais possam trocar dados com os sistemas estaduais e municipais de processamento. Desta maneira, a relação com os fornecedores de equipamentos e de programas, que são atores de mercado, demanda um funcionamento efetivo de políticas públicas. Elas não somente devem perseguir o estado

da técnica, mas devem lidar com os desníveis e as assimetrias das diversas administrações públicas do país.

A sociedade civil tem também possibilidade de intervir nos processos de formação de políticas públicas sobre as tecnologias da informação aplicadas ao Estado. O problema é a dificuldade de lidar com o discurso técnico e seu potencial de legitimar posições políticas e sociais. A forma de lidar com este problema está relacionada à democratização do conhecimento e à existência de espaços públicos de diálogo sobre estas políticas públicas. Este problema não é uma exclusividade da área tecnológica. Ele é compartilhado por todas as decisões políticas que possuem debates técnicos como pano de fundo. A formação de uma esfera pública ativa pode minorar o dilema, além de fortalecer as decisões do ponto de vista da sociedade. Logo, a ampliação dos atores envolvidos é desejável. Entretanto, para que haja debate, nenhum dos atores (seja estatal, de mercado ou da sociedade civil) pode atuar como um "veto player", ou seja, possuir a capacidade de inviabilizar as políticas públicas. Deve ser ressaltado que existe, em tramitação na Câmara dos Deputados, o Projeto de Lei n. 7.316, de 2002, para resolver diversos problemas. Breve análise dele foi realizada em Veronese (2007).

3 PONDERANDO OS RISCOS: CENTRALIZAÇÃO OU DESCENTRALIZAÇÃO?

Os dois modelos possuem vantagens e desvantagens. O problema é conseguir avaliar a melhor adequação de um ou de outro sistema à informatização do sistema judiciário. Se a questão é a utilização de certificados digitais para o uso em processos judiciais, o razoável é que estes sejam acreditados por meio de auditoria de um órgão público, tal como ocorre com os produtos perigosos que são avaliados pelo Instituto Nacional de Metrologia e Qualidade Industrial (INMETRO). Entretanto, é ponderado pela crítica da OAB que apenas ela pode certificar os advogados. Logo, a informatização do judiciário, cujos processos envolvem advogados, depende de seu aval.

Foi feita uma sondagem sobre a percepção de receios e de responsabilidade entre os funcionários de duas AC do sistema da ICP-Brasil. Os parâmetros metodológicos se orientaram pelo estudo de KRIMSKY & GOLDING (1992) Foram distribuídos cerca de quarenta questionários para cada AC, devolvidos respondidos.

Tanto a identidade das AC, quanto dos seus funcionários foi preservada. A sondagem estabeleceu uma escala sobre como os serviços de certificação digital são percebidos pelos técnicos implicados. A pressuposição principal é que um sistema é mais seguro, na medida em que existem mais esforços para garantir a segurança. As perguntas foram construídas para tratar da percepção de riscos internos e externos. O motivo para a escolha dos receios foi derivado da crítica, pretensamente técnica, de que o sistema da ICP-Brasil apresentaria mais riscos por ser hierárquico. Não é o desenho abstrato que produz, ou não, sistemas seguros. É o uso social das práticas de segurança que o garante.

A pesquisa focalizou na descrição de riscos na perspectiva interna, ou seja, da visão dos próprios prestadores em relação aos danos potenciais e às possibilidades de responsabilização individual e organizacional que poderiam advir de problemas na entrega dos serviços. Está sendo tomado como pressuposto que o ponto de vista mais acurado é o que se refere aos receios de danos percebidos no foco interno, mas partilhado socialmente. Ou seja, os riscos são entendidos como um produto socialmente construído. A crítica que poderia advir a esta concepção é de que os danos seriam, então, subjetivos. Ela não procede porque as perdas são mensuráveis, apesar dos receios possuírem um grau de subjetividade. Se os danos podem ser "objetivados", os medos – subjetivos e construídos no âmbito do grupo social – também o são. Esta concepção explica porque os receios quanto à responsabilização são maiores em relação às organizações do que aos indivíduos, de acordo com a figura abaixo. Quando imerso num grupo técnico qualificado, o indivíduo tem noção de que a instituição lhe servirá de proteção.

Quatro perguntas trataram dos receios de responsabilidade. Destas, as duas primeiras versaram sobre a dimensão organizacional, ou seja, da responsabilidade da instituição. As duas últimas eram sobre a perspectiva individual. Tanto no caso individual, quanto no caso da organização, as perguntas separaram um panorama do receio de responsabilização administrativa da possibilidade de atribuição judicial.

No caso da relação de danos possíveis com o sistema, não houve grande oscilação na percepção de riscos entre os funcionários das duas AC. A única distinção entre a opinião dos dois grupos se refere ao quesito "parceiros", ou seja, de relações de dependência de sua AC com instituições externas. Há uma diferença substantiva na

posição relativa em que a AC “a” possui em relação à AC “b”, que explica a diferença: maior necessidade de parcerias.

Das três questões feitas sobre as perdas possíveis no sistema, a primeira era acerca de problemas com “dados, quebra de confidencialidade e perda de equipamentos”. O objetivo era manter a percepção adstrita aos equipamentos e às operações usuais. A segunda questão tratava da expansão destes problemas hipotéticas para as relações entre a organização e os parceiros (outras empresas, instituições públicas, etc). Por fim, a terceira questão mencionava os problemas financeiros na perspectiva da perda de clientes atuais e potenciais.

Por fim, a diferença relatada em relação à posição diferenciada de uma AC para outra fica nítida a partir da percepção de responsabilidade solidária (figura 09). Pode-se entender que a AC “a” possui um grau de autonomia em relação ao resto do sistema que não existe na AC “b”. Desta forma, os funcionários da primeira AC não se sentem tão pressionados, na sua percepção de riscos, com a possibilidade de que sua instituição seja obrigada a ressarcir danos em larga escala solidariamente com o sistema nacional de certificação. A percepção de que os riscos existem é muito semelhante, entretanto, no âmbito dos funcionários das duas AC.

A conclusão que pode ser extraída desta sondagem é que os funcionários que lidam com o sistema nacional de certificação digital, independentemente da posição de suas instituições, têm clara visão sobre a responsabilidade da atividade. As instituições funcionam como um catalisador de proteção para o bom desempenho destas funções, sem que haja a possibilidade de meramente descarregar nos indivíduos a responsabilização possível pelo andamento dos serviços. A percepção externa é muito distinta. Como especialistas na operação de sistemas complexos, eles compreendem a importância do uso correto dos procedimentos técnicos. Entretanto, a visualização acurada de uma observação externa – que leve em consideração que os processos técnicos são, na verdade, relações sociais – pode aclarar alguns dilemas. A força de um sistema de segurança está baseada na sua fiscalização e controle permanente. O fato dos técnicos do sistema da ICP-Brasil terem clarividência da sua possível responsabilização demonstra o clima de preocupação com a segurança do sistema nacional de certificação digital. Na pesquisa não ocorreu uma postura irresponsável dos técnicos de atribuir que

o sistema é seguro por si mesmo, abstratamente. Enfim, houve a percepção clara de que a segurança é um arranjo social que envolve a fiscalização ininterrupta.

O primeiro dilema diz respeito aos processos complexos que devem ser compreensíveis além dos círculos técnicos. Para que tal compreensão ocorra, deve existir disseminação dos conceitos. Para que haja uma opção social legitimada sobre segurança, há que ampliar o debate para espaços além do âmbito estritamente técnico. É, enfim, necessário ampliar a disseminação da informação para que haja maior compreensão.

O segundo dilema é relativo à percepção social dos riscos. Também foi mencionado anteriormente que os riscos "objetivados" são distintos dos receios. Os últimos são carregados de subjetividade. Desta maneira, é importante ouvir os receios dos técnicos. Eles demonstrarão que os riscos existem, obviamente, tendo em vista que indicam a possibilidade de danos para suas instituições. Entretanto, a sua visão é marcada por elementos de quem trabalha com segurança técnica. Há preocupação com a responsabilização. Desta forma, pode-se depreender dos dados e das análises qualitativas o receio com a responsabilização, que é típica da fiscalização contínua. Ela decorre da existência de procedimentos padronizados e claros, conferidos por técnicos externos as AC, que possuam competência jurídica e técnica reconhecida. Enfim, o que resume a garantia de segurança são os procedimentos de auditoria.

O terceiro dilema se relaciona com a solução dos dois dilemas anteriores. É importante conjugar a democratização com uma isonomia – percebida socialmente – dos procedimentos de segurança (conferência e acreditação). Um termo para distinção do modelo de certificação do sistema nacional (ITI) foi relatado reiteradamente nas entrevistas: "qualificação". Este adjetivo visa indicar que o certificado digital utilizado pelo sistema nacional possui amparo legal e técnico diferenciado. Na prática, a montagem de um organismo emissor de certificados digitais é bastante simples. O que diferencia a emissão de um certificado de outro não é um dado técnico apenas. É uma questão de segurança organizacional e estruturação social. Desta maneira, a segurança "objetivada" se relaciona com os receios subjetivos. Para minorar os receios e aproximá-los dos riscos efetivamente existentes, é necessário pensar sobre o problema do funcionamento cotidiano e das práticas existentes no âmbito das instituições. É menos um problema de natureza legal do que um dilema social e técnico.

Os dois modelos descritos anteriormente – hierárquico e "em rede" – possuem riscos "objetiváveis". A questão central diz respeito à percepção dos riscos. O que diferencia o primeiro modelo do segundo é a possibilidade de interação e difusão de suas práticas para várias áreas da vida social com um sistema de auditoria que é geral. O modelo da ICP-OAB é proposto em si mesmo, ou seja, sem auditoria externa. O mesmo nível de segurança exigida da informatização do judiciário, por exemplo, será o adotado pelo sistema bancário nacional e pela Secretaria da Receita Federal, sem distinção. Assim, haverá difusão de informação sobre segurança em um sistema compartilhado por vários órgãos, ao invés de um sistema específico para a máquina judiciária. Com esta difusão, mais atores serão agregados ao debate sobre segurança, melhorando a qualidade do sistema de uso geral.

CONSIDERAÇÕES FINAIS: O DILEMA SOCIAL, POLÍTICO E TECNOLÓGICO IMPOSTO À OAB

O Conselho Federal da OAB sofreu um primeiro revés em sua luta por uma autoridade certificadora própria com a ativação da autoridade certificadora da Justiça Federal (http://www.acjus.gov.br). Foi criada a AC do Poder Judiciário federal, sob controle do Superior Tribunal de Justiça (STJ). Ela foi formada dentro do sistema nacional de certificação digital, com submissão às auditorias técnicas do ITI (ASSINATURA DIGITAL, 2005).

Em que pesem as ponderações da OAB, o mercado de certificação parece andar rápido. A Serasa, empresa que lida com cadastros bancários, por exemplo, oferece os seus préstimos como uma intermediária para o processamento judiciário por meio de "agilidade na comunicação com clientes, Judiciário e órgãos do Poder Público em geral". Outras diversas empresas, credenciadas e auditadas pelo ITI, podem prestar os serviços, mesmo sob controle cadastral da OAB.

Este primeiro revés veio acompanhado de outros. Após a criação da AC-Jus, foram promulgadas duas medidas legislativas que possuem o potencial de dificultar a pretensão da OAB de institucionalizar sua ICP fora do sistema da ICP-Brasil. A primeira foi à inserção de um parágrafo no Código de Processo Civil (CPC), prevendo que as comunicações judiciárias eletrônicas deverão estar em conformidade com o sistema da ICP-Brasil. A alteração se deu pela inclusão de um parágrafo único ao art.

154, da Lei n. 5.869, de 11 jan. 1973, por meio da Lei n. 11.280, de 16 fev. 2006. Assim, aquele parágrafo único do CPC obriga que todos os atos processuais digitais devem ser certificados conforme a ICP-Brasil.

A segunda medida que ampliou o dilema da OAB foi à aprovação do PL n. 5.828, de 2001. Este PL foi sancionado na forma da Lei n. 11.419, de 19 dez. 2006, que normalizou o processo eletrônico brasileiro. Deve ser mencionado que o parágrafo único do art. 154, do CPC, foi transformado em parágrafo primeiro pela Lei n. 11.419, que acresceu um segundo parágrafo ao art. 154. Este PL teve origem na Câmara dos Deputados e agregou diversas modificações. Ele constitui um passo necessário para implementação prática da ICP-Brasil, tendo em vista que os serviços judiciários englobam uma enorme quantidade de atos e procedimentos. Desta forma, a informatização – certificada digitalmente no sistema da ICP-Brasil – permitiria um ganho produtivo em escala que baratearia a tecnologia e o acesso aos seus produtos e serviços (leitoras, "smart cards" e gestão de certificados). O Presidente da Comissão de Tecnologia da Informação, do Conselho Federal da OAB, Alexandre Atheniense, admitiu que a entidade caminharia para o a convergência: "Como alguns tribunais não admitem outra certificação que não a da ICP-Brasil, a OAB decidiu não comprar a briga. A próxima carteira da OAB, que ainda não tem data para entrar em circulação, terá um chip com certificação digital da ICP-OAB e da ICP-Brasil, garantindo que advogado possa entrar de vez na era do processo virtual" (AGUIAR, 2006).

O imbróglio em relação ao modelo brasileiro de certificação digital parecia resolvido. Entretanto, a OAB ajuizou uma Ação Direta de Inconstitucionalidade (ADI n. 3869, de 2007) contra a nova redação do art. 154 do CPC, postergando o problema. Como consideração final, cabe ressaltar que a ampliação do uso social desta tecnologia somente aclarará o artefato técnico para a sociedade. Sem a generalização da certificação digital, haverá mais dificuldade de se institucionalizar políticas públicas para este setor. O problema do sistema da ICP-Brasil não é de risco técnico. É de uso social. A tendência é que a polêmica termine em breve, com a expansão da informatização judiciária. Mas, para que isto ocorra, deverá ser formado o difícil consenso sobre o uso social desta inovação científica e tecnológica.

REFERÊNCIAS

AGUIAR, A. Assinatura eletrônica: OAB oferece dupla certificação digital para advogados. O Estado de São Paulo. Consultor Jurídico. 31 jul. 2006. Disponível: http://conjur.estadao.com.br/static/text/46844,1. Acesso: 08 mar. 2006.

ASSINATURA DIGITAL. O Estado de São Paulo. Consultor Jurídico. 12 jan. 2005. Disponível: http://conjur.estadao.com.br/static/text/32378,1. Acesso: 08 mar. 2006.

AUTRET, T.; BELLEFIN, L.; OBLE-LAFFAIRE, M. *Sécuriser ses échanges életroniques avec une PKI: solutions techniques et aspects juridiques*. Paris: Eyrolles, 2002.

BENSOUSSAN, A.; LE ROUX, Y. *Cryptologie et signature életronique: aspects juridiques*. Paris: Hermes, 1999.

CERTIFICAÇÃO DIGITAL deve evitar fraudes. O Estado de São Paulo. Link Digital. 18 jul. 2005. Disponível: http://www.link.estadao.com.br/index.cfm?id_conteudo=4322. Acesso: 08 mar. 2006.

FREITAS, C.; VERONESE, A. Segredo e democracia: certificação digital e software livre. Revista Informática Pública. Belo Horizonte. ano 08. n. 02.

KAMINSKI, O. VOLPI, M. M. A evolução da certificação digital no Brasil. In: ROVER, A. J. (Org.). *Direito e informática*. Barueri: Manole, 2004.

KRIMSKY, S.; GOLDING, D. (Ed.). *Social theories of risk*. Westport, CT: Praeger, 1992.

LATOUR, B. *Ciência em ação: como seguir cientistas e engenheiros sociedade afora*. São Paulo: Editora Unesp, 2000.

_____. *Jamais fomos modernos: ensaio de antropologia simétrica*. São Paulo: Editora 34, 1994.

LEVY, S. *Crypto: secrecy and privacy in the new code war*. London: Allen Lane, The Penguin Press, 2000.

MARCARCINI, A. T. R. *Direito e informática: uma abordagem jurídica sobre criptografia*. Rio de Janeiro: Forense, 2002.

VERONESE, A. *A política de certificação digital e a advocacia: processos eletrônicos e informatização judiciária*. Revista de Direito da Informática e das Telecomunicações, n. 2. p. 09-40. Belo Horizonte: Ed. Fórum, 2007.