1

Segredo e democracia: certificação digital e *software* livre

Christiana Soares de Freitas

Alexandre Veronese

Palavras-Chave

Políticas Públicas – Certificação Digital – *Software* Livre

Resumo

O Instituto Nacional de Tecnologia da Informação (ITI) foi criado em 2000 com o intuito de desenvolver o sistema de certificação digital no Brasil, erigindo a Infra-estrutura Nacional de Chaves Públicas (ICP-Brasil). Desde então, tornou-se responsável por vários programas governamentais, entre eles o de certificação digital e o de *software* livre. Pondera-se, neste artigo, que a noção de segredo (aliada à criptografia e, conseqüentemente, à certificação digital) e a ampliação da democracia (exemplificada pelos esforços na expansão do *software* livre), são elementos complementares e não antagônicos. A pergunta central que norteia o trabalho refere-se à convergência – ou não – dos dois programas em destaque. Será que integram, de fato, um grupo de estratégias comuns voltadas para a elaboração e implementação de políticas públicas? A hipótese central a ser discutida é a de que a tensão constante entre programas estimulados pela conjuntura democrática atual (como o do *software* livre) e programas que não apresentam características que os favoreçam nesse contexto político (como o de certificação digital), não impede a existência de complementaridades entre tais programas. Em um primeiro momento, o artigo trata da criptografia no panorama internacional: do segredo de Estado à garantia de comunicação livre. Posteriormente, apresenta a formação do Instituto e a construção de agenda política de certificação digital. Concluindo, discute-se a posição do Instituto como aquele que se encontra no centro dos dilemas que norteiam as políticas públicas de inclusão digital no Brasil.

1. Introdução: demanda social, não apenas governamental[1]

Um historiador do campo científico e da técnica criptográfica, Steven Levy, afirma que, ao usarmos a *Internet*, acreditamos estar sussurrando quando, na verdade, estamos transmitindo a todos ("broadcasting") [Levy00]. É óbvio que as outras pessoas não têm acesso imediato às informações que trocamos pelo ciberespaço. Mas, se alguma delas quisesse conhecê-las, não seria difícil. Com o avanço da *Internet* e a expansão dos demais espaços virtuais, a individualidade e a proteção das informações enviadas por meio do ciberespaço ficaram vulneráveis, suscetíveis ao que se poderia considerar um "excesso de transparência". Pode-se pensar, ainda, em uma janela aberta para a violação da privacidade. Com isso, associados à expansão para o cotidiano do mercado e da sociedade, determinados problemas tornaram-se prementes. Um dos mais basilares está associado à insegurança no que diz respeito ao tráfego de informações que a *Internet*, considerada uma rede aberta[2], possibilita. Permite um incremento nas

[1] Uma versão preliminar deste artigo foi apresentada no XII Congresso Brasileiro de Sociologia (Belo Horizonte, 2005). Os autores agradecem os comentários dos pareceristas anônimos da revista pela substantiva melhora que seus argumentos proporcionaram. A responsabilidade pelas opiniões aqui expressas, entretanto, mantém-se conosco.

[2] A diferença entre uma rede de troca de informações fechada para uma aberta é simples. Enquanto na primeira os dois lados utilizam um canal dedicado que só pode, ordinariamente, ser acessado pelo emissor e pelo receptor, na rede aberta o canal é compartilhado com outras trocas comunicacionais. O primeiro exemplo é o telefone; os dois lados sabem quais são os números (e, logo, podem presumir com quem estão falando) e a linha só é usada por eles. Tal linha é, inclusive, protegida legalmente contra "invasão"

possibilidades de relações sociais, mas tem a contrapartida de tornar arriscada a realização de trocas comerciais e transferências de dados sensíveis. Como resolver esse problema de forma a congregar soluções técnicas e socialmente viáveis? Duas questões centrais são apresentadas na introdução. A primeira diz respeito à importância da criptografia[3] e da certificação digital como tema que interessa a todos os cidadãos e não somente ao Estado. A segunda refere-se às possibilidades de expansão das agendas de políticas públicas relativas às tecnologias da informação e comunicação, nas quais se inclui a expansão do *software* livre, como difusão da liberdade de acesso ao conhecimento. Dessa maneira, a noção de segredo e a de democracia apresentam-se de forma complementar e não dicotômica, se geridas em uma pauta comum.

A primeira questão decorre da expansão do uso social da *Internet*[4]. Com tal incremento, as questões de segurança nas transferências começaram a ser percebidas como centrais pelos usuários [Schn00; Schn03]. Nesse contexto, a criptografia surgiu como uma resposta técnica viável para garantir a confidencialidade das informações que o indivíduo escolhe manter como tal.

---

não autorizada (i.e. escuta). O segundo exemplo é a I*nternet*, onde não existe tal consolidação no que diz respeito à proteção legal [GiCa00].

[3] Existe uma diferença entre criptografia e criptologia. A primeira refere-se à aplicação prática, criada a partir da segunda, que pode ser encarada como um ramo da matemática, ou seja, um ramo de estudos

A análise do período de gestão governamental federal brasileira, encerrado em 2002, permite avaliar que o uso da criptografia manteve-se restrito ao uso estatal ou de interesse do Estado. O motivo para isso pode ter sido tanto a sua localização como um objetivo tecnicamente estratégico, quanto a dificuldade para desenvolver essa empreitada. Assim, por que democratização da informação seria incompatível com a noção de segredo que a certificação digital, no interesse estatal, suscita? Em um sistema de governo democrático – ou especialmente nele – há que existir direito à privacidade. Dito de outra forma, há que existir o direito a ter segredos.

A pesquisa que fundamenta o artigo baseou-se na leitura de documentos da área de certificação digital e de *software* livre, bem como na análise das políticas públicas dos dois períodos em questão. Além disso, foram realizadas cinco entrevistas com técnicos do setor de certificação digital[5].

A tese central do estudo afirma que o segredo gerado pelo uso da certificação digital não ataca os princípios democráticos que regem as sociedades contemporâneas, já que a confidencialidade a ela associada diz respeito ao direito do indivíduo (ou grupo) de exercer sua liberdade civil

---

[4] Uma boa quantidade de dados, acompanhados de interessante problematização sobre esta expansão podem ser acessados em [KaRi02]. Um quadro brasileiro pode ser conferido em [Sorj03].

[5] Essas entrevistas não foram incluídas no artigo, literalmente, visando à preservação dos laços de confiabilidade entre os entrevistados e os pesquisadores. Os pontos de vista enunciados no artigo são de inteira responsabilidade dos pesquisadores envolvidos.

(individual ou coletiva). As noções de democracia e segredo entrelaçam-se e não se contrapõem.

Alguns críticos, entretanto, apresentam a criptografia como um campo propício ao desenvolvimento de atividades criminosas tendo, por isso, impacto pernicioso na vida social [Grab03; Koop99]. Essa idéia é a expressão da dicotomia entre segurança do Estado e o direito à privacidade dos indivíduos possibilitado pela criptografia. Pode-se inferir que há um espaço para ponderação de valores entre um direito geral (proteção, segurança) e um direito individual (privacidade). Contudo, não se pode afirmar a existência de contraposição efetiva entre segredo e democracia na construção de políticas públicas relativas às tecnologias da informação e comunicação. A pressuposição de tal dicotomia, de forma preliminar, tende ao estabelecimento de políticas restritas, que não expandem a democratização do conhecimento e da cidadania.

Para minimizar os riscos, as políticas públicas devem integrar diversas demandas que possibilitem expandir o foco das instituições envolvidas. Dessa forma, para que as tecnologias da informação e da comunicação tenham uso democrático, precisam estar incluídas em contexto mais amplo do que o desenvolvimento de um produto ou aplicação apenas. O pressuposto de democracia é que haja uso social amplo da tecnologia, ou seja, que ela seja útil e disponível para todos.

7

Em um primeiro momento, este artigo apresenta a criptografia de forma histórica e conceitual. Posteriormente, descreve a infra-estrutura brasileira de chaves públicas. São analisados, também, a criação do Instituto Nacional de Tecnologia da Informação e seu contexto inicial de demandas até o período de 2002. Será feita uma comparação desse momento inicial com a expansão da agenda do Instituto, demonstrando que a contradição aparente entre democracia e segredo decorreu de um objetivo restrito no uso da tecnologia.

2. O que é a certificação digital

Certificação digital é um tema pouco conhecido até por aqueles que lidam constantemente com as diversas tecnologias presentes na contemporaneidade. No Brasil, a certificação digital vem, aos poucos, permeando várias práticas sociais e políticas em um contexto em que as tecnologias da informação são cada vez mais presentes. Em 06 fevereiro de 2005, foi publicada a notícia abaixo em um jornal de grande circulação[6]:

> Estímulo ao uso de e-CPF e e-CNPJ ganha força com parceria com bancos. Para popularizar o certificado digital entre pessoas físicas e jurídicas, a Receita Federal firmou parceria com a Federação Brasileira de Bancos (Febraban) para que instituições bancárias emitam smart cards reconhecidos pelo ICP-Brasil [Infra-estrutura de chaves públicas]: o e-CPF e o e-CNPJ. A ICP-Brasil é um conjunto de técnicas e procedimentos que garante autenticidade e validade jurídica a documentos eletrônicos. Até agora, Banco do Brasil e Caixa Econômica Federal eram as únicas

[6] O diário citado é o Jornal do Brasil, em circulação em todo o país.

8

> instituições bancárias que podiam emitir os *smart cards*. Depois da parceria com a Febraban, o Bradesco já manifestou interesse e deve ser habilitado. Serasa, Serpro, CertiSign e a própria Receita também emitem a certificação.

De alguma forma, a sigla ICP parece estar se aproximando do cidadão brasileiro. É interessante perceber que esse sistema de certificação digital, mesmo afetando significativamente a população, utiliza-se de nomenclaturas e processos amplamente desconhecidos pela sociedade civil, apesar da recente política de popularização da tecnologia em questão.

Poucos sabem que o sistema de certificação digital procura garantir a autenticidade das informações enviadas pelo ciberespaço, identificando ao receptor quem é o emissor daquelas informações. Também possibilita o trânsito de mensagens criptografadas (não visualizáveis facilmente, embaralhadas), que permitem sigilo na comunicação. O sistema assegura, do ponto de vista técnico, basicamente:

- autenticação, ou seja, identificação pública de quem é o emissor daquela mensagem, passível de conferência ou confirmação;
- confidencialidade, que vem a ser a possibilidade técnica de que a mensagem seja criptografada, ou seja, não passível de ser lida por outrem que não o destinatário pretendido;

9

- integridade, isto é, a possibilidade de utilização de um algoritmo para garantir que a mensagem não seja alterada em seu conteúdo; e
- não-repúdio, ou a produção de um elemento técnico de prova – mantido e colocado como disponível por um serviço – de que um determinado evento ou ação ocorreu; seria um modo de identificar, por exemplo, uma mensagem remetida com aquela pessoa que a assinou, de tal forma que não pudesse haver rompimento de tal vínculo entre usuário e mensagem; enfim, é um ponto polêmico, porque apesar do não-repúdio ser possível do ponto de vista técnico, não há garantias de que será assim considerado pelos tribunais [ABO02].

A possibilidade de envio de informações de forma segura, sem que haja o risco de que outra pessoa, que não a destinatária, abra a mensagem contendo as informações enviadas, fez com que, durante muitos anos, a criptografia fosse restrita às redes estatais. Essas redes utilizam tais recursos como forma de garantir a segurança e a inviolabilidade de informações secretas transmitidas e armazenadas, no interesse do Estado.

Faz-se, atualmente, distinção entre criptografia civil e estatal, oriunda da publicação, pelo governo americano, de um padrão civil de criptografia

na década de 1970, abrindo o campo às aplicações diversas. Enquanto a criptografia estatal depende do desconhecimento do público (segredo), a criptografia civil é voltada para esse público, com ampla difusão de seus parâmetros. Ela tem uma área de aplicação ampla, englobando vários setores da sociedade civil.

2.1. Criptografia: tecnologia em prol da democracia?

Os algoritmos de criptografia estão ligados à idéia primordial de segredo. Desde a origem, seu objetivo era tornar uma mensagem ilegível para uma terceira parte. Existem diversos mitos sobre o uso militar dos algoritmos que poderiam ser traçados até o imperador romano Júlio César, por volta de um século antes de Cristo [BeLe99]. A criptografia manteve-se restrita ao uso estatal até muito recentemente, por volta dos anos setenta do século vinte.

O uso de algoritmos criptográficos sempre foi controlado por órgãos de Estado, dedicados às questões militares ou de interesse estatal. Nos Estados Unidos, era atribuição exclusiva da “National Security Agency” (NSA). Em princípio, o uso da criptografia sem ser com finalidades estatais era considerado atitude suspeita. Poderia ser o indício de espionagem, por exemplo. Ao mesmo tempo, poderia apresentar-se como a solução para um problema que ficaria evidente com a *Internet*: como possibilitar o uso

maciço de trocas de dados, em redes abertas, sem que houvesse uma garantia de inviolabilidade das comunicações?

Visando à solução desse problema, vários autores dedicaram-se ao tema, em uma interseção entre a teoria da comunicação e a matemática. A partir dos anos de 1948 e 1949 (data da publicação de dois artigos seminais de Claude Shannon no "Bell Systems Technical Journal"), a comunidade científica pôde elaborar e desenvolver as bases de uma "nova criptografia"[7]. O desenvolvimento foi lento porque, como mencionam Bensoussan & Le Roux, "até 1967, o conhecimento em criptografia estava confinado a alguns organismos estatais especializados, dado o uso estritamente limitado às aplicações militares e diplomáticas" [BeLe99]. A mudança radical ocorreu com a publicação do artigo de Diffie e Hellmann, "Novas Direções na Criptografia", propiciando o desenvolvimento tecnológico de um sistema de criptografia de chaves públicas elaborado por Rivest, Shamir e Adleman, [BeLe99][8]. Os autores fundaram uma empresa, ainda hoje importante na área de segurança da *Internet*, com a sigla "RSA Inc.". Sem esse sistema, seria impossível pensar em realizar uma enorme quantidade de tráfego de forma segura na rede.

---

[7] Para detalhes sobre a obra de Shannon, cf. http://mit.edu/6.933/www/Fall2001/Shannon1.pdf

[8] Essa história é bem documentada em [Levy00]. Há uma exposição mais ampla e aprofundada sobre criptografia e signos em [Sing02] e [Ster98].

Atualmente, as linhas telefônicas convencionais são mantidas por empresas operadoras tecnicamente subordinadas a órgãos estatais (à Agência Nacional de Telecomunicações e ao Poder Judiciário, no caso brasileiro). Uma violação de comunicação telefônica não autorizada judicialmente, por exemplo, pode ser identificada e punida com razoável facilidade. No caso da *Internet* (e dos diversos provedores envolvidos), essa tarefa é mais complexa [Lemo05] pelo fato da comunicação se dar em uma rede aberta sem centrais controladas. A questão reside em garantir a troca segura de informações comerciais e bancárias (números de cartão de crédito, por exemplo), diminuindo a potencial violabilidade dos dados. Tal sistema tem o condão de favorecer não apenas a esfera comercial, mas também as outras da sociedade.

A solução decorreu da criação de novo conceito de algoritmo – o de chaves criptográficas públicas – a partir do citado desenvolvimento teórico de Diffie e Helmann e das aplicações técnicas de Rivest, Shamir e Adleman. Os algoritmos matemáticos tradicionais são baseados em uma única chave compartilhada que tanto cifra quanto decifra. A operação matemática é idêntica no cifrar e no decifrar. Ela dura o mesmo tempo e requer os mesmos meios computacionais, mensuráveis em velocidade ou capacidade de processamento. No algoritmo de chaves públicas, torna-se mais simples, rápido e econômico cifrar a mensagem do que decifrá-la. Para decifrá-la,

são necessários mais recursos computacionais. Este é o motivo porque os algoritmos tradicionais são denominados simétricos: o caminho de ida é igual ao de volta. No caso dos algoritmos assimétricos, usados em chaves públicas, o caminho de volta é distinto daquele de ida. Para compreender a aplicação dos conceitos matemáticos em termos de técnicas, foi elaborado um resumo simplificado, apresentado a seguir.

2.2. A segurança em três possibilidades: ser, ter ou saber

Imagine a necessidade de abrir uma porta. Existem três meios técnicos de garantir que somente uma determinada pessoa realize a tarefa. O primeiro meio afere que esta pessoa é aquela que diz ser. Ou seja, o mecanismo de abertura da porta reagirá positivamente a partir de alguma característica física ou psicológica apresentada pela pessoa. Exemplos vão desde o reconhecimento de comandos de voz, análises da retina até exames dos formatos das mãos – são os meios psicométricos ou biométricos. O segundo meio ocorre pelo fato de a pessoa possuir algo, ou seja, ter uma chave que seja lida pelo mecanismo, esteja ela na forma tradicional, de um cartão magnético ou de um chip. O terceiro meio, enfim, realiza-se pelo conhecimento de uma senha ou combinação [Sche04]. Todos pressupõem um engenho, ou seja, a existência de um mecanismo que leia ou codifique a tranca da porta.

A certificação digital pode ser entendida como um mecanismo, em princípio, mas é mais que isso; configura um engenho técnico e social que é redutível apenas ao sistema criptográfico. É um mecanismo social e técnico de gerenciamento de segurança que pode ter diversos usos.

Assim, o nível de investimento para a construção de um sistema que evite o acesso à porta (podem ser os dados bancários do indivíduo ou dados pessoais, por exemplo) pressupõe-se proporcional à importância do que está depois dela. Mas a segurança e as suas implicações representam um sistema social e técnico que envolve uma pluralidade de fatores humanos e não-humanos (computadores, leitoras, políticas, etc). Revela-se fundamental que o gerenciamento da segurança e a administração desse sistema complexo de elementos coordenados sejam realizados em um contexto que potencialize seus usos sociais em prol de toda a sociedade. Isso se torna ainda mais premente quando se considera seu alto custo de construção e manutenção.

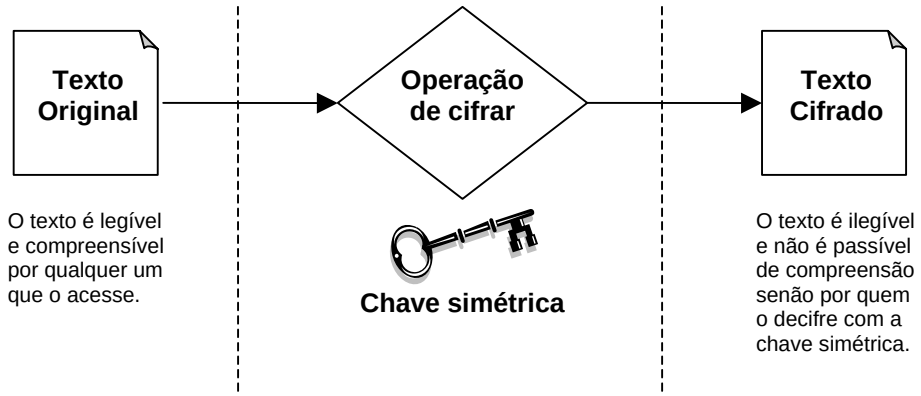
Para perceber as demais questões tratadas no artigo, faz-se necessário tratar da técnica da certificação digital e da evidência de sua utilidade, compreendendo, inclusive, um sistema baseado no uso de chaves compartilhadas, ou seja, de criptografia simétrica.

2.2.1. Criptografia simétrica

A criptografia simétrica – ou de chave secreta – utiliza a mesma chave para encriptar e decriptar a mensagem. Essa chave é compartilhada pelo

remetente e pelo destinatário. A mensagem inicial, chamada de texto original, é transformada para o texto cifrado. O destinatário, por sua vez, realiza a transformação reversa (do texto cifrado para o texto original), como mostra a figura a seguir.

Fig. 1. Simplificação da operação de cifração por algoritmo simétrico



Fonte: Adaptado de [ABO02]

A força de um algoritmo de criptografia reside no tamanho da chave utilizada. Existem vários algoritmos de chaves simétricas. Entretanto, alguns são mais comuns: o “Data Encryption Standard” (DES), o “Triple DES” (3DES) e o “Advanced Encryption Standard” (AES). O primeiro, DES, é o algoritmo simétrico mais utilizado. Ele foi desenvolvido pela IBM e adotado pelo governo americano na década de 1970. Possui uma chave de 56 bits, pequena em termos atuais. Apresenta-se, por isso, bastante vulnerável a ataques de força bruta (busca exaustiva de todas as chaves possíveis). Já o segundo, 3DES, é uma evolução do primeiro, ou seja, foi projetado para

melhorar o DES. Ele criptografa os dados, com a mesma chave de 56 bits, três vezes seguidas. O terceiro algoritmo, AES, é resultado de um concurso organizado pelo "National Institute of Standards and Technology" (NIST)[9] para selecionar um cifrador simétrico que substituísse oficialmente o DES. Embora feito primariamente para uso pelo governo americano, certamente terá aplicação geral. Foi selecionado após dois anos de análise rigorosa de 15 propostas diferentes, finalizada em 2000. O algoritmo AES foi desenvolvido por Joan Daemen e Vicent Rijmen e possui tamanho de chave variável em três formatos: 128, 192 ou 256 bits [Faus01].

Existem dois problemas com sistemas de cifração simétrica. O primeiro é sua aplicação em relação à *Internet*. Uma mensagem cifrada pressupõe o compartilhamento de chaves idênticas entre os dois envolvidos. O compartilhamento da chave envolve um canal de transmissão diferente da *Internet*, sabidamente insegura. Os canais seguros são caros e de difícil gerenciamento. Imagine o envio, de tempos em tempos, de chaves em mídias físicas, como CDs, pelo correio. Há de se considerar, inclusive, a possibilidade de extravio.

O segundo problema também é derivado da necessidade de compartilhamento de chaves. É muito difícil manter relações sigilosas dentro de uma empresa. Se existirem tantas chaves quantos funcionários, a

[9] Com as devidas ressalvas e distinções, seria o equivalente ao INMETRO (Instituto Nacional de Metrologia, Normalização e Qualidade Industrial).

gestão será um sistema demasiadamente complexo. Este possuirá tantas possibilidades de vazamento quantas chaves compartilhadas existirem. Se estas tiverem que ser trocadas sempre, a possibilidade de perda dos dados aumenta, pois, sem uma chave, não se abre a mensagem. Se a chave for única para a empresa toda, sua perda ou cópia significará exposição total. Imagine um caso mais complicado, em que as comunicações ocorrem pela *Internet*. Em algum momento da conversa, haverá troca de chave entre emissor e receptor. Assim, se ela for interceptada por um terceiro não-autorizado, toda a comunicação ficará comprometida. Mais grave ainda, este terceiro poderá intervir como se fosse tanto o emissor quanto o receptor.

A criptografia assimétrica resolve esse dilema porque nela não há troca de chaves. Há chaves públicas e privadas. As chaves públicas podem ser acessadas por qualquer um a partir de um repositório público. Dessa forma, apesar de sua publicidade, há uma chave correspondente, privada, que lhe faz par e deve ser mantida em segredo por seu portador.

2.2.2 Criptografia assimétrica

Consiste na utilização de duas chaves, uma para cifrar e a outra para decifrar. O algoritmo é público, como em toda criptografia de uso civil. Entretanto, a força e a segurança da criptografia pública não estão no segredo de seu algoritmo, mas na chave criptográfica gerada com ele. No caso da criptografia assimétrica, o segredo estará na chave privada e no seu

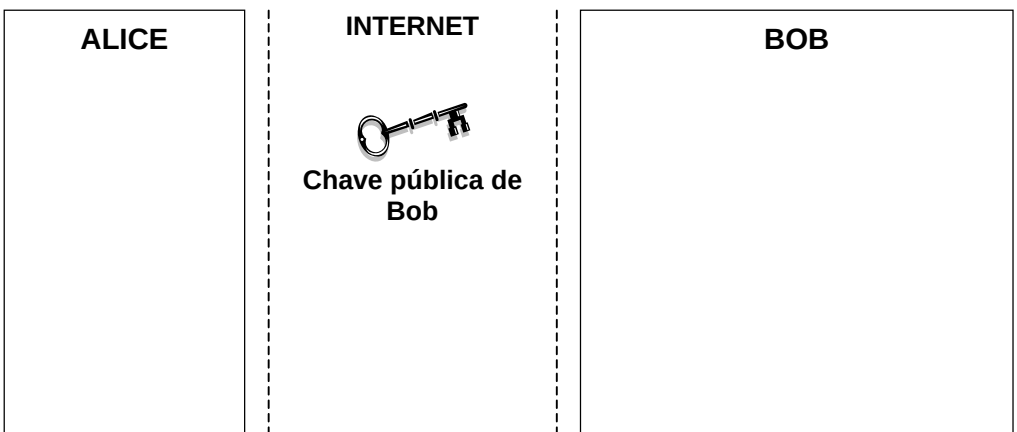
gerenciamento. É interessante notar que a técnica permite o aparecimento de um meio mais seguro para a cifração de informações e, principalmente, para a montagem de sistemas de certificação digital (infra-estruturas de chaves públicas). Apresenta-se, assim, como um meio técnico e social central para o funcionamento da *Internet*.

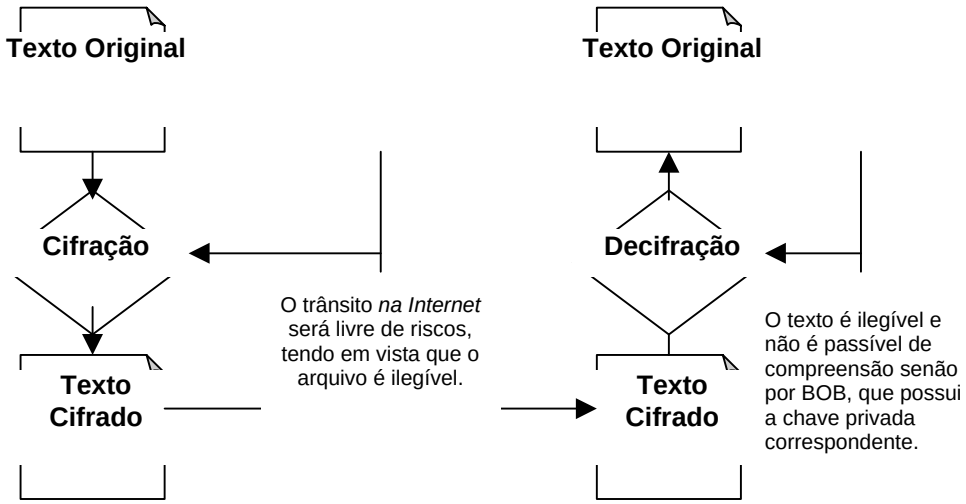
Existem duas aplicações técnicas importantes em relação à criptografia assimétrica: a cifração de mensagens e a assinatura digital, aplicações correntes em sistemas de certificação digital.

2.3. Aplicações: cifração de mensagens e assinatura digital

A cifração por meio de chaves públicas decorre do uso técnico da criptografia assimétrica. A figura 2 ilustra o processo. 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 geradas pelo mesmo algoritmo assimétrico. Essa operação pode ser compreendida a partir da figura a seguir.

Fig. 2. Simplificação da operação de cifração com criptografia assimétrica (chaves públicas)



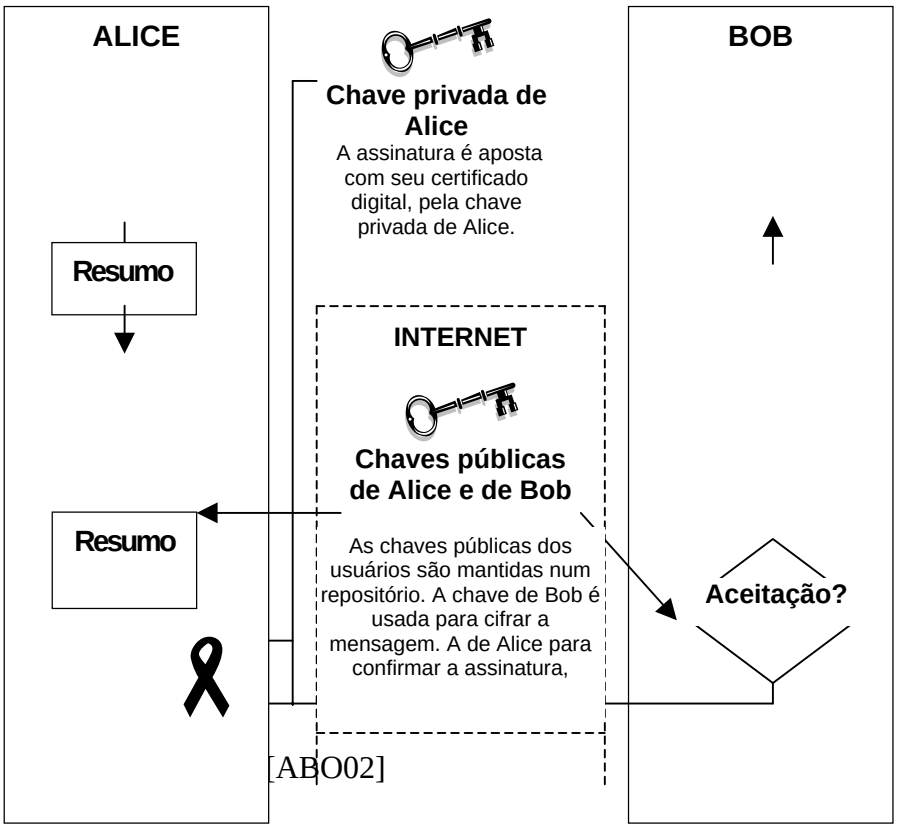


Fonte: Adaptado de [ABO02]

Compreendido o esquema simplificado da figura acima, cabe entender o que é uma assinatura digital. É realizada com a utilização do par de chaves das duas partes, sendo que 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 (função “hash”): um valor único criado a partir de uma operação matemática que permite comparação posterior para checar a inalterabilidade. 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). O sistema pode ser visualizado na figura a seguir.

Fig. 3. Simplificação da operação de assinatura digital certificada.



[ABO02]

Ao invés de cifrar a mensagem, pode-se cifrar apenas o resumo. Isso decorre de uma solução técnica razoável para o problema de decifrar mensagens muito grandes, quando são utilizados sistemas de criptografia assimétrica. Outra solução seria remeter, junto com o pacote, uma chave simétrica cifrada por meio de criptografia assimétrica. Nesse caso, usar-se-ia

a chave pública de Bob para cifrá-la, tendo em vista que o texto só poderia ser acessado por ele, já que possui a chave privada para decifrar a chave simétrica e, então, decifrar o texto.

O desenvolvimento principal que a criptografia assimétrica possibilita é a emissão de certificados digitais para serem apostos às mensagens e, dessa forma, por meio de uma entidade de certificação chamada de “terceiro de confiança”, garantirem que aquela assinatura digital seja realmente do remetente. A forma lógica de um certificado digital é a “virtualização” de um documento oficial (como uma carteira de identidade) que atesta, para quem recebe a mensagem, que ela foi, de fato, remetida por aquele que a assinou. Para a realizar essa operação, há que existir uma entidade cuja tarefa seja emitir os certificados digitais padronizados, em relação às assinaturas digitais feitas por meio das chaves privadas.

Em síntese, a figura reproduz uma operação cujo objetivo é ter certeza de que a mensagem tenha sido expedida de Alice para Bob com segurança. Com esse modelo, duas características importantes são garantidas. A primeira é a confiança de que quem assinou o pacote é o remetente. A segunda é a sua integridade e a impossibilidade de repúdio, tendo em vista o fato de que não é possível a revogação do envio da mensagem.

Apesar de a operação parecer complexa, os programas de e-mails disponíveis (“Windows Outlook” ou “Mozilla Thunderbird”, por exemplo) realizam essas operações com grande simplicidade para o usuário.

Um elemento importante, ausente na figura 3, é a descrição do funcionamento do terceiro de confiança: uma entidade de certificação digital que é uma infra-estrutura de chaves públicas (ICP). Essa entidade fornece os certificados, as assinaturas, as chaves privadas e mantém os repositórios das correspondentes chaves públicas, acessadas pela *Internet* para conferência. Nesse sentido, tal infra-estrutura de chaves públicas funciona sob a forma de uma pirâmide, cujo vértice é uma instituição que a gerencia do ponto de vista técnico. No Brasil, a opção do governo foi estabelecer uma única infra-estrutura (ICP-Brasil), qualificada legalmente, tendo como vértice o Instituto Nacional de Tecnologia da Informação (ITI). Entender os dois períodos dessa institucionalização permite compreender como o Instituto, no primeiro período de sua história, norteou-se por um foco significativamente restrito, relacionado com o desempenho de uma tarefa identificada com o interesse estatal. Já no segundo período, o Instituto é reorganizado para a difusão de outras tecnologias, em programas que se apóiam mutuamente, como o de *software* livre, em uma agenda que exibe possibilidades de conciliação prática entre segredo e democracia.

3. O Instituto Nacional de Tecnologia da Informação e a construção da Infra-Estrutura de Chaves Públicas (ICP-Brasil)

Durante o ano de 2000, foi expedido um decreto presidencial fixando as bases do que deveria ser a política de segurança da informação do governo federal brasileiro: o Decreto n. 3.505 (de 13 de junho de 2000)[10]. Este ainda vige e tem como objetivo definir uma grande política de segurança da informação em relação aos meios eletrônicos nas diversas atividades empreendidas pelo governo federal. Posteriormente, o Decreto n. 3.396 regulamentou os serviços de certificação digital prestados no âmbito da ICP-Brasil[11]. Com isso, formou-se o arcabouço normativo e institucional sob o qual se assenta a ICP-Brasil e o Instituto Nacional de Tecnologia da Informação.

Assim, a origem da construção do sistema brasileiro de certificação digital foi a formação de um ponto central de uma rede que ainda hoje serve ao poder executivo federal. Posteriormente, esse ponto foi ampliado, atingindo todo o Estado (incluindo os estados e municípios) e as demais esferas da sociedade.

---

10 Esse decreto foi acrescido, em 21 de junho de 2004, pelo Decreto n. 5.110.

11 Tal decreto ainda vige, tendo sido parcialmente modificado por decreto posterior, em 2002 (Decreto n. 4.414, de 07 de outubro).

A Medida Provisória n. 2.200, de 2001, organizou a infra-estrutura de chaves públicas (ICP-Brasil), localizada no Instituto Nacional de Tecnologia da Informação, como a única ICP a ser reconhecida no país do ponto de vista jurídico estatutário, ou seja, por força de lei, não de acordo entre as partes. De uma forma geral, houve certa polêmica com essa opção, tendo em vista as dúvidas sobre a possibilidade de o governo fixar restritivamente o que valeria como assinatura e certificado digital em termos legais. A questão seria se essa iniciativa não iria fragilizar a possibilidade de que os indivíduos contratantes pudessem eleger uma outra ICP e seus certificados digitais como válidos para relação social e econômica pela *Internet*. As críticas mais fortes vieram do Conselho Federal da Ordem dos Advogados do Brasil (OAB) e referiam-se não só aos negócios privados, mas aos atos processuais realizados pela *Internet* (protocolo de petições eletrônicas, por exemplo). Estes, por serem estatais em essência, teriam sido obrigatoriamente inseridos no escopo da ICP-Brasil. Tal polêmica, atualmente, não está mais tão intensa[12] [Maca02] e [KaVo04]. Entretanto, o problema persiste, tendo em vista o fato de os atores sociais ainda não terem alcançado o consenso. A externalidade negativa é o empecilho imposto à

[12] A paulatina pacificação decorre da entrada em vigor da Autoridade Certificadora do Poder Judiciário Federal (AC-Jus). Se os tribunais exigirem certificados da ICP-Brasil, os advogados serão obrigados a usá-los. Mas a questão ainda se encontra em aberto, tendo sido inclusive tomadas medidas judiciais para coibir o uso de certificação digital em desconformidade com o ponto de vista do Conselho Federal da OAB.

informatização dos processos judiciais, pois os advogados são parte indissociável dos processos.

O sistema criado pela referida medida provisória desemboca na formação de uma pirâmide, ou cadeia de certificação digital, que tem como vértice o Instituto Nacional de Tecnologia da Informação. Esse vértice não significa controle direto, mas resulta em fiscalização de padrões (auditoria, credenciamento, etc.) e determinação na observância de procedimentos fixados por normas técnicas internacionais e pelas entidades que efetivamente certificam digitalmente os cidadãos. Também significa a geração das chaves criptográficas para outras entidades, subordinadas tecnicamente ao vértice. Assim, no Brasil, optou-se por um modelo que centrou toda uma infra-estrutura, legalmente qualificada, sob a fiscalização técnica do Poder Executivo Federal no âmbito do Instituto Nacional de Tecnologia da Informação.

O Instituto de Tecnologia da Informação foi criado em 2000, por meio de um desdobramento do Centro de Pesquisas Renato Archer (CenPRA), sediado em Campinas. O novo Instituto, bem como o CenPRA, eram vinculados ao Ministério da Ciência e Tecnologia (MCT), que havia concentrado, em 1999, todas as suas unidades de pesquisa, dispersas entre o Ministério e o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). Todas foram agregadas em uma única secretaria, na

administração federal direta. A medida provisória que criou o Instituto teve duas reedições, com algumas alterações. A mais importante dizia respeito à transferência do novo Instituto do Ministério da Ciência e Tecnologia para a Casa Civil da Presidência da República, onde está até hoje localizado.

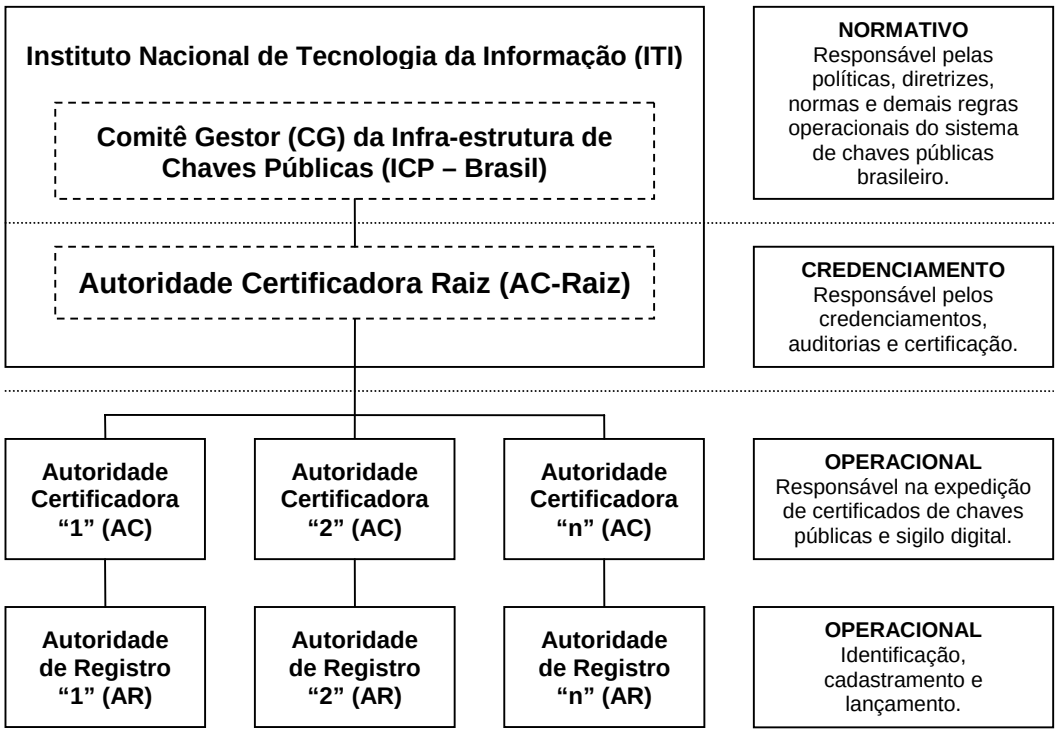
O contexto político de criação do Instituto Nacional de Tecnologia da Informação foi bastante polêmico. Em primeiro lugar, foi criado a partir de medida provisória, uma ação política entendida como pouco democrática por ser um processo legislativo unilateral da Presidência da República[13]. De um lado, havia atores sociais contrários à decisão. Eram grupos que já empreendiam ações sobre o mesmo tema ou tinham interesses em relação às questões de certificação digital. Alguns esperavam gerir Autoridades Certificadoras - Raiz (AC-Raiz), como era o caso do Conselho Federal da Ordem dos Advogados do Brasil (OAB). Este postulava que a iniciativa do poder executivo cassava sua competência de emitir livremente certificados digitais aos advogados, o que seria competência legal sua.

Outro grupo de críticos, oriundo da comunidade acadêmica, desenvolveu todo o projeto desde seu início e foi deixado de lado. A principal crítica a esse fato centra-se na explicação de exclusão desse grupo

[13] Quando da criação do ITI, ou seja, antes da Emenda Constitucional n. 32, de 2001, eram possíveis reedições sistemáticas da mesma medida provisória. Na prática, esta peculiaridade conferia poder de legislar, sem o Congresso Nacional, ao Presidente da República.

visando ao benefício da área financeira. O atual modelo pode ser compreendido a partir da figura a seguir.

Fig. 4. Simplificação do sistema de certificação digital brasileiro.



O Instituto possui competência para desenvolvimento de funções normativas (deliberadas pelo Comitê Gestor, que inclui representantes externos, inclusive da sociedade civil e da comunidade acadêmica) e de credenciamento, ou seja, de garantia técnica e confiabilidade do sistema. Suas partes operacionais estão localizadas nas Autoridades de Certificação (AC) e nas Autoridades de Registro (AR). É importante frisar que a

terminologia deve ser alterada – em futura lei específica de consolidação do sistema – para “Prestador de Serviços de Certificação”. A designação de autoridade (decorrente do jargão técnico) induz ambigüidade na interpretação jurídica. As Autoridades de Certificação garantem os certificados emitidos. Já as Autoridades de Registro, funcionam como cadastradoras. Um exemplo pode ser dado com a emissão do Cadastro Eletrônico de Pessoas Físicas (e-CPF), que pode ser emitido por várias entidades, como o Serviço de Processamento de Dados (SERPRO) e a empresa CertiSign S/A. Todas funcionam como Autoridades Certificadoras derivadas da Autoridade Certificadora da Secretaria da Receita Federal que, por sua vez, é credenciada e auditada pelo Instituto. Todas possuem suas Autoridades de Registro (AR) subordinadas para essa função específica de cadastro.

O tempo da tecnologia não é o tempo da política, ou seja, a implementação de uma solução técnica tem muitos empecilhos que não são de natureza tecnológica. Os artefatos tecnológicos, além de socialmente construídos, são aplicados mediante a execução de políticas específicas visando à sua utilização pela sociedade civil. Uma vez pronta, a tecnologia conhece, além do espaço técnico de sua produção, o espaço jurídico-institucional da implementação. Será visto, adiante, o processo de incorporação do espaço técnico da criptografia ao cenário político nacional.

Esse processo abrange mudanças, alterações e estratégias do espaço jurídico-institucional, sem o qual o artefato não integra o domínio público e nem adquire, conseqüentemente, visibilidade pública.

Tal problema decorre do fato de a certificação digital ter sido criada em ambiente muito restrito. Assim, o Instituto de Tecnologia da Informação tinha como sua única missão fomentá-la, tornando-se um espaço técnico excessivamente especializado. A mudança ocorre em tempos recentes com a percepção de que a fixação dos programas centrados nessa agenda restrita não colaboraria para a popularização da tecnologia da certificação digital. Apenas a ampliação de agendas serviria para produzir tal efeito, uma vez que a tecnologia existente precisa de aplicações. Ou seja, ela requer usos sociais que só podem ser construídos com a ampliação da agenda de políticas públicas voltadas para as tecnologias da informação. Este tema é tratado no próximo tópico.

4. Políticas públicas para tecnologias da informação e o Instituto de Tecnologia da Informação

O desenvolvimento das várias experiências internacionais das infra-estruturas de chaves públicas está ligado indissociavelmente ao fenômeno da popularização do uso da *Internet* e, principalmente, ao crescimento de seu uso comercial. Os vários modelos de certificação digital que utilizam sistemas de chaves públicas possuem algumas convergências decorrentes do

fato de várias de suas características serem normatizadas (IEEE, ISO, etc[14]). Entretanto, possuem também grandes diferenças, oriundas de opções políticas e gerenciais feitas em cada país.

A favor da medida provisória que estabelecia a ICP única no Brasil estavam os grupos interessados no desenvolvimento da tecnologia para o sistema financeiro. Segundo o Pedro Dourado de Rezende, que acompanhou atentamente a história de criação da Infra-Estrutura de Chaves Públicas brasileira (ICP-Brasil), a medida provisória foi publicada com o intuito de atender ao sistema financeiro mediante a oferta de soluções para os problemas de uso intensivo da *Internet* em serviços de varejo bancário:

> O diretor-geral da Federação Brasileira dos Bancos - Febraban, Sr. Hugo Dantas Pereira, antigo diretor executivo de varejo, serviços bancários, tecnologia e infra-estrutura do Banco do Brasil, e que em julho foi nomeado um dos representantes da sociedade civil no Comitê Gestor da ICP-Brasil, teria defendido, em evento patrocinado pela OAB em 26 de julho para debater a MP 2200, a adoção de uma certificadora raiz única e a dependência da assessoria técnica do CEPESC, alegando serem o CEPESC e as agências militares os únicos centros de expertise em criptografia no país. Esta ilação, vindo de uma figura pública tão importante, conspurca a estatura profissional de brasileiros ilustres que centralizam ampla bagagem de conhecimento criptográfico, como o Dr. Paulo Barreto, e de outros não tão ilustres. O Dr. Barreto, que trabalha na empresa brasileira Scopus, é o criptoanalista da equipe belga vencedora do concurso promovido pelo NIST para escolha do próximo padrão

[14] IEEE significa “Institute of Electrical and Electronics Engineers”, que gerou e mantém padrões técnicos para uso na *Internet*. ISO é a sigla de “International Organization for Standardization”, que gere padrões técnicos internacionais.

> americano aberto de cifra simétrica, o AES, num concurso onde participaram mais de duzentas empresas de todo o mundo e que durou mais de dois anos.[15]

A medida provisória permitiu a agilização e otimização de todos os negócios realizados entre bancos no país, que passaram a ser feitos mediante autenticação, ou assinatura digital, da ICP-Brasil, no sistema de pagamentos brasileiros (DOC e TED, por exemplo). Essa autenticação, por sua vez, é realizada com o certificado digital da ICP-Brasil. Afirmar que a ICP-Brasil foi criada com relativa rapidez para atender ao sistema financeiro significa dizer que o interesse central da iniciativa foi promover uma relação mais eficiente entre os bancos e entre estes e seus clientes. Com a existência da Infra-Estrutura de Chaves Públicas, várias transações no mercado financeiro foram facilitadas, como a assinatura de contratos de câmbio e as demais operações realizadas entre pessoas jurídicas.

Os dois grupos mencionados até aqui (acadêmicos e pessoal do sistema financeiro) participavam ativamente das discussões a respeito da questão, apresentando posições antagônicas que refletiam, na verdade, objetivos distintos. Interessa mencionar que, na prática, com a mudança para a Presidência da República, a comunidade científica perdeu parte do espaço para outro grupo de servidores públicos que iria corporificar a nova instituição. Esse grupo, constituído de assessores técnicos ligados à Agência

---

15 Cf. http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=243

Brasileira de Inteligência (ABIN), também integrou o cenário e passou a ter, juntamente com egressos do sistema financeiro, atuação e peso com a transferência do Instituto para a Casa Civil. Novamente, críticas foram dirigidas ao processo:

> Por mais iluminados que sejam, não conseguirão abarcar todas as possibilidades do debate aberto com a sociedade. Caberá ao Cepesc (Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações), controlado pela Agência Brasileira de Inteligência, herdeira do SNI, propiciar assessoria, inclusive tecnológica, ao órgão central da ICP-Brasil. A fiscalização, para ser eficiente, implica autonomia de atuação. Pode-se esperar tal postura do Cepesc ou abriremos mais um flanco para incontáveis transgressões à cidadania, perpetradas pelos novos arapongas?[16]

Os técnicos mencionados assumiram a responsabilidade pelo desenvolvimento do sistema criptográfico nacional naquele período. Dando continuidade ao processo, foi nomeado um servidor da ABIN para atuar como Diretor-Presidente do Instituto. As duas diretorias foram assumidas pelos dois grupos centrais de atores. A Diretoria de Infra-Estrutura e Chaves Públicas, que opera o ambiente seguro do sistema (conhecido como a “sala cofre”), foi entregue à área de inteligência. A Diretoria de Auditoria foi gerida por técnicos oriundos das instituições do setor financeiro. Dessa forma, o Instituto Nacional de Tecnologia da Informação passou a desenvolver uma política específica de segurança da informação no governo

federal com um foco significativamente restrito: resolver a necessidade de transações bancárias e de segurança de comunicação eletrônica no núcleo central do governo (ou seja, entre a presidência e os primeiros escalões dos ministérios).

A criptografia nasceu, assim, como um "segredo de estado", um instrumento destinado a preservar interesses estatais e a salvaguardar informações, com um escopo muito próximo aos interesses de um segmento da vida social: as instituições financeiras. Vale ressaltar que não está sendo negada a necessidade da existência ou manutenção de uma dimensão da criptografia que será sempre de responsabilidade militar em cada país. Observa-se, contudo, especialmente com base na origem técnica dos dirigentes, que houve uma estratégia central na origem do modelo.

De acordo com essa estratégia, mantinha-se o quadro existente de prestação de um serviço de interesse do Estado sem a necessidade de ampliá-lo para o uso geral. Essa tendência restritiva funcionava como um empecilho à difusão da certificação digital em outros setores sociais e econômicos. Progressivamente, esse cenário foi sendo modificado. Assim podem ser entendidas as alterações recentes na agenda desse Instituto com o intuito de aliar ou conjugar a certificação digital a outros programas de democratização do acesso à informação, como a difusão do *software* livre no Brasil.

---

[16] Cf. http://observatorio.ultimosegundo.ig.com.br/cadernos/cid250720011.htm

A possível aliança ou coordenação entre tais programas pode ser questionada, já que a certificação digital sempre esteve relacionada à manutenção da confidencialidade e, por isso, à noção de segredo. O *software* livre, por sua vez, associa-se à liberdade de acesso à informação, à noção de informação sem segredos, distribuída de forma democrática.

A partir da análise das agendas voltadas para a implementação de políticas públicas na área de tecnologias de informação, especialmente a do Instituto Nacional de Tecnologia da Informação, observa-se que uma suposta contradição entre segredo e democracia não existe, uma vez que se percebe, cada vez mais, a necessidade de popularizar a certificação digital, podendo esta associar-se aos objetivos de implementação do *software* livre.

5. O que é s*oftware* livre

Um pressuposto para entender a questão associada ao *software* livre ("open source") é visualizar os problemas das aplicações de *software* proprietário ("closed source"). Ambas estão relacionadas com questões de propriedade intelectual[17]. Os *softwares* em regime proprietário possuem um esquema similiar às outras formas de propriedade intelectual, ou seja, só podem sofrer alteração ou utilização com o consentimento do seu titular por

[17] A maior parte dos países considera os programas de computador como parte do ramo jurídico da propriedade intelectual como direito autoral (ou seja, equivalente a um livro ou música). O Brasil, inclusive. Uma minoria, onde se incluem os Estados Unidos da América, consideram o *software* como patente. A diferença se refere ao sistema de registro

meio de licenças. Assim, o código fonte, que é central no *software*, só pode ser acessado com a devida permissão.

O código fonte do s*oftware* livre é diferente do tipo citado anteriormente, pois está disponível aos usuários e pode ser usado, copiado, modificado e distribuído, seja ele alterado ou sob sua forma original. Vale ressaltar que *software* livre não significa grátis, pois a liberdade associada a ele não depende de gratuidade.

O *software* livre apresenta algumas vantagens. Segundo Sérgio Amadeu da Silveira, haveria quatro básicas [Amad03, p. 40-43]. A primeira seria a adoção do *software* livre em projetos de telecentros e escolas para inclusão digital. Isso faria com que houvesse maior aproveitamento didático-pedagógico do *software*. Os alunos poderiam, com seu uso, ultrapassar a condição de usuários passivos para a de usuários criativos.

A segunda vantagem relaciona-se ao "custo para o Estado", que seria reduzido. Nesse caso, a análise do autor menciona, equivocadamente, o fato de o *software* livre ser "mais barato" que os demais. Essa pretensa segunda vantagem é contraditada pelo terceiro benefício relacionado pelo autor, que seria a necessidade de manutenção e suporte, podendo acarretar altos custos. A implantação generalizada de plataformas em *software* livre pode, assim, ser mais cara do que o licenciamento de um proprietário. Além disso, o

---

e força de proteção. As patentes possuem uma sistemática mais complexa e rígida). Cf. [Wipo02]

software livre exige a contratação e formação de técnicos para se dedicarem ao desenvolvimento da plataforma. O regime proprietário, por outro lado, terceiriza esses investimentos para empresas.

A quarta vantagem, na opinião de Amadeu da Silveira, diz respeito à questão de alfabetizar os cidadãos para o uso de um *software* que pode ser realmente conhecido. Esta talvez seja a maior vantagem oferecida pelo *software* livre ao usuário: conhecer o que está sendo executado pelo seu sistema. Tal vantagem permite maior controle e estabilidade (passível de tradução em segurança), bem como maior democracia do conhecimento sobre o *software* em termos gerais. A opção por uma política de *software* livre centra-se no debate sobre o conhecimento e sua difusão, e não nos custos e benefícios financeiros. Isso ocorre porque as vantagens não são necessariamente financeiras, mas técnicas e, principalmente, humanas, como a formação de novas gerações e maior publicidade para conhecimento para todos. Esse é o diagnóstico de Lawrence Lessig:

> "uma parte dessa questão da propriedade está no núcleo do atual debate entre *software* aberto e fechado. No sentido do que os 'pais fundadores' americanos [participantes da Assembléia Constituinte] teriam instintivamente entendido, o 'software livre' ou 'software de fonte aberta' é, em si, uma posição contra a arbitrariedade". [Less99, p. 7-8].

O foco do debate, portanto, relaciona-se à democratização do conhecimento. O objetivo central é definir um espaço para o *software* livre

de modo a que todos possam ter acesso ao que é basilar no desenvolvimento humano relativo à ciência e tecnologia.

6. Integração da certificação digital e do *software* livre

6.1. Programas governamentais de *software* livre e o Projeto João de Barro

A adesão ao *software* livre está relacionada à difusão do conhecimento e à garantia de espaços de liberdade para criação. Não é uma questão econômica, em princípio, mas possui um componente econômico relacionado à liberdade. Tendo as pessoas mais liberdade para criar – o que equivale, em termos práticos, a menos constrangimentos legais – haverá maior desenvolvimento tecnológico e científico.

Essa pressuposição está na base de uma ruptura na política para as tecnologias da informação e comunicação, presente na história do Instituto Nacional de Tecnologia da Informação (ITI). De um espaço precário, até do ponto de vista jurídico, passa-se à possibilidade de um espaço para a atuação política.

A agenda de difusão do *software* livre foi absorvida em ampla gama de projetos de desenvolvimento tecnológico e científico para o país. Esse *software* apresenta-se como alternativa para formação de especialistas em uma linguagem que não é propriedade de determinada empresa. Além disso,

é possível construir produtos que possam ser modificados sem necessidade de contratação de apenas um grupo. Cria-se, por exemplo, a possibilidade de licitação para manutenção e suporte, o que sempre diminui custos. Aumenta-se, ainda, a possibilidade de segurança e controle dos sistemas computacionais. Assim, situações constrangedoras são evitadas, como o fato de bases de dados públicas serem monopolizadas, na prática, por um contrato com uma única empresa. Tal contrato acaba não tendo horizonte de término, obrigando o Estado a construir um monopólio.

Um exemplo da necessidade de desvinculação entre propriedade e conhecimento está na formação de uma plataforma criptográfica em *software* livre. No caso dos algoritmos criptográficos assimétricos, é importante que sejam bastante difundidos e testados. Tal difusão não compromete a segurança do sistema. O que a comprometeria seria a divulgação da chave criptográfica privada da raiz, gerada pelo algoritmo assimétrico. Assim, a segurança está no produto do mecanismo, não no mecanismo em si. Mas se o mecanismo for um *software* proprietário (com código fechado), todo o sistema de certificação digital dependerá da "caixa preta" fornecida por uma única empresa. Assim, parece razoável que uma ICP pública tenha por base um *software* livre.

O projeto João de Barro demonstra a convergência de uma política de certificação digital com a política de *software* livre. O problema central não

é econômico, mas de domínio de uma tecnologia para todos e não por uma empresa apenas. Como a tecnologia terá um uso público, parece interessante que seja financiada com recursos públicos. O programa é desenvolvido como uma ação conjunta do Instituto Nacional de Tecnologia da Informação (ITI) e diversas entidades para construção de uma plataforma criptográfica em *software* livre visando à substituição do sistema atual[18].

6.2. Complementaridade normativa e política.

A complementaridade normativa pode ser depreendida do Projeto de Lei n. 7.316, de 2002, em fase final de tramitação na Câmara dos Deputados. Ele visa a substituir a Medida Provisória n. 2.200, de 2001. Nesse projeto, há a perspectiva de agregar às competências do Instituto de Tecnologia da Informação a difusão do *software* livre. No inciso XII, do art. 17, afirma-se que ao Instituto Nacional de Tecnologia da Informação compete desenvolver e disseminar soluções em *software* aberto e livre na Administração Pública Federal. Pode-se afirmar que existe uma complementaridade política nesse assunto pelo fato de o órgão deixar de ter a função restrita de centro de auditoria e fiscalização de prestação de serviços de certificação digital para tornar-se um ponto de passagem para a difusão do conhecimento.

---

[18] Mais dados podem ser visualizados no sítio do Projeto. Cf. http://www.labsec.ufsc.br [link João de Barro].

O Instituto Nacional de Tecnologia da Informação foi, em curto período de tempo, retirado da estrutura do Ministério da Ciência e Tecnologia e alocado na Casa Civil da Presidência da República. Isso aconteceu porque o Instituto foi entendido apenas como órgão de prestação de serviços associados ao interesse do Estado. Com as transformações até então observadas, o Instituto contém, hoje, potencial para tornar-se um espaço de formulação de políticas públicas voltadas para essa área. Ampliando sua agenda, poderá dedicar-se também ao desenvolvimento científico e tecnológico de forma abrangente, contribuindo para a difusão democrática do conhecimento.

7. Da contradição à complementaridade

A história da formação e consolidação do Instituto Nacional de Tecnologia da Informação traz consigo a história da certificação digital no Brasil. A princípio, controlado por uma agenda bastante limitada, o Instituto, atualmente, coordena programas voltados para democratizar a informação e o conhecimento, com propostas de políticas públicas que visam a expandir o uso social da tecnologia da informação. Os princípios que vigoram no Instituto indicam que a política de implementação da Infra-Estrutura de Chaves Públicas (ICP) – garantindo a privacidade, autenticidade e segurança das informações enviadas pelo ciberespaço – é tão importante quanto a política voltada para a quebra de monopólios no setor

de *software*. Para tanto, o Instituto vem estimulando o debate e ações voltadas para o uso, por parte do governo federal e de toda a sociedade civil, de *software* livre.

O Instituto procura ampliar sua agenda, o que se revela positivo, já que o governo federal não possui outro órgão exclusivamente dedicado à construção de políticas para a sociedade da informação. O que existem são experiências dispersas em diversos órgãos públicos e em organizações da sociedade civil.

As políticas públicas referentes às tecnologias da informação encontram um grave problema na sua dispersão ao longo da complexa administração federal brasileira. A tendência a operar com comitês não resolve o dilema. Os servidores que deles participam costumam ficar sobrecarregados com as tarefas de seus órgãos e aquelas determinadas pelos comitês. A solução seria juntar grupos operacionais, retirados de variados órgãos, em espaços novos, sem pôr fim às equipes dedicadas às tarefas em curso. Não é fácil resolver essa equação dada a restrição de recursos. Entretanto, o Instituto Nacional de Tecnologia da Informação possui todas as condições para tornar-se um centro que coordene essas equipes e auxilie na elaboração de políticas públicas para o setor, tanto pelo fato de ser uma instituição nova e dedicada exclusivamente à tarefa quanto pela posição

estratégica – normativa e política – que advém de sua ligação direta com o órgão central do Executivo brasileiro: a Presidência da República.

8. Conclusão

A política de implementação de *software* livre tem, como um de seus princípios, o acesso democrático ao conhecimento. O Instituto Nacional de Tecnologia da Informação pretende, com a associação da plataforma criptográfica ao s*oftware* livre, indicar direções de convergência entre tecnologias que, apesar de aparentemente díspares, podem contribuir, de forma coordenada, para a afirmação da democracia no Brasil. O Instituto, espelhando as diretrizes da atual gestão governamental, visa a influir decisivamente na formação de uma agenda mais estruturada e ampla, voltada para as políticas públicas em tecnologias da informação e comunicação. Pretende-se, com isso, promover a democratização do conhecimento em todas as instâncias e esferas governamentais, conjugando tecnologias e políticas que possam promover a inclusão social. A intenção é aproximar a política de certificação digital do cidadão brasileiro, incluindo-o nos benefícios gerados por seu uso. Para tanto, a proposta é substituir os cartões usados com banda magnética por “smart cards” com certificado digital. Seria atender, além do sistema financeiro nacional, toda a população

brasileira que também se beneficiaria com as vantagens do uso de cartões eletrônicos (como aquele utilizado pelo Bolsa Família).

A política nacional de certificação digital, no momento, encontra-se extremamente associada aos princípios democráticos de inclusão social, ilustrados pela política de implementação do *software* livre. De um lado, há a criptografia, uma tecnologia que sempre esteve atrelada à noção de segredo; de outro, o *software* livre, tecnologia que tem como objetivo não guardar segredos e promover a possibilidade de conhecimento aberto e acessível a todos. Apesar de as aplicações dessas duas tecnologias terem sido sensivelmente distintas ao longo de suas histórias, percebe-se hoje que as políticas que as integram não se apresentam como incompatíveis. A história do Instituto revela a conexão possível. O sistema criptográfico nacional existe como um recurso para garantir a segurança do cidadão contra uma eventual violação de sua privacidade. O segredo, necessário em alguns aspectos e dimensões da vida humana, não é incompatível com a democratização do conhecimento que o *software* livre proporciona.

A criptografia protege a informação que não pertence à esfera pública e que, portanto, deve permanecer sob o controle dos indivíduos. O sistema criptográfico surge como uma forma de salvaguardar as informações individuais, evitando o risco de crimes e a invasão de privacidade,

fenômeno cada vez mais ameaçador e presente nas sociedades contemporâneas.

Tanto a criptografia quanto o *software* livre representam necessidades atuais, associadas à expansão e consolidação da democracia, respeitando as garantias individuais por meio da promoção das liberdades individuais. A expansão das duas agendas, mutuamente sinérgicas, implica robustecimento de estruturas sociais e políticas que possam dar suporte à implementação de políticas complementares.

As políticas de certificação digital e de difusão do software livre são convergentes. Democratizar o conhecimento inserido em tais sistemas técnicos é interesse de todos. Ter a privacidade garantida por meio de sistemas criptográficos também é importante para todos. Ambos são almejados pela sociedade e podem apresentar-se como elementos complementares na elaboração de políticas públicas para o desenvolvimento das tecnologias da informação voltadas para maior inclusão social e digital.

Agradecimentos

O presente artigo utilizou-se de dados coletados com recursos do Departamento de Pesquisa e Documentação da Ordem dos Advogados do Brasil (Seção do Rio de Janeiro). A CertiSign - Certificadora Digital S/A - também colaborou com a empreitada na forma de uma bolsa para a realização de curso técnico sobre o assunto em 2003. Uma versão

preliminar deste trabalho foi apresentada ao Grupo de Trabalho Sobre Sociedade de Informação no XII Congresso Brasileiro de Sociologia (01 jun. 2005; Belo Horizonte, MG).

Keywords

Public Policies – Digital Certification – Open Source Software – Digital Inclusion

Abstract

The National Institute of Information Technology (ITI) was created in 2000 focused at developing the digital certification system in Brazil by building the country's public key infrastructure. Since then, the Institute has become responsible for other governmental programs, such as the Open Source Software, Digital Inclusion and Software Quality. In this article, we suggest that it would be reasonable to suppose that the notion of *secret* – frequently associated to cryptography and therefore to Digital Certification – and the expansion of democracy (exemplified by the Institute's attempt to implement Open Source software in government agencies) do not represent antagonism but are complementary elements in the context of public policies' implementation. The central question guiding the article refers to a possible convergence among the programs previously highlighted. Are they part of a same group of coherent strategies directed to the elaboration and implementation of public policies? The central hypothesis discussed is that there is a persistent tension between public policy programs developed by Brazilian democratic scenario – such as the Open Source Software program – and others that are not favored in this political scene such as the Digital Certification program. The tension exists, but that does not eliminate the complementarities between them. First, we present cryptography in the international panorama: from the State secret to the guarantee of free Internet communication. Furthermore, we discuss the process of the Institute's creation and the Digital Certification policy agenda. We conclude the article discussing the role and the importance of the institute at the

center of political dilemmas concerning digital inclusion public policies in Brazil.

Referências bibliográficas

[Amad03] AMADEU DA SILVEIRA, Sérgio. Inclusão digital, software livre e globalização contra-hegemônica. In: AMADEU DA SILVEIRA, Sérgio (Org.); CASSINO, João (Org.). **Software livre e inclusão digital**. São Paulo: Conrad Livros, 2003.

[ABO02] AUTRET, Thierry; BELLEFIN, Laurent; OBLE-LAFFAIRE, Marie-Laure. **Sécuriser ses échanges életroniques avec une PKI: solutions techniques et aspects juridiques**. Paris: Eyrolles, 2002.

[BeLe99] BENSOUSSAN, Alain; LE ROUX, Yves. **Cryptologie et signature életronique: aspects juridiques**. Paris: Hermes, 1999.

[GiCa00] GILLIES, James; CAILLIAU, Robert. **How the web was born: the story of world wide web**. Oxford: Oxford University Press, 2000.

[Grab03] GRABOSKY, Peter. Cibercrime. Cadernos Adenuer, v. 6. Rio de Janeiro. Fundação Konrad-Adenuer, 2003. Trad. Alexandre Veronese.

[Faus01] FAUSSE, Arnaud-F. **La signature életronique: transactions et confiance sur Internet**. Paris: Dunod, 2001.

[KaVo04] KAMINSKI, Omar; VOLPI, Marlon Marcelo. A evolução da certificação digital no Brasil. In: ROVER, Aires José. (Org.). **Direito e informática**. Barueri: Manole, 2004.

[KaRi02] KATZ, James E.; RICE, Ronald E. **Social consequences of internet use**. Cambridge, MA; Massachussets Institute of Technology Press, 2002.

[Koop99] KOOPS, Bert-Jaaps. **The crypto controversy: a key conflict in the information society**. The Hague: Kluwer Law International, 1999.

[Lemo05] LEMOS, Ronaldo. **Direito, tecnologia e sociedade**. Rio de Janeiro: Editora FGV, 2005.

[Less99] LESSIG, Lawrence. **Code and other laws of cyberspace**. New York: Basic Books, 1999.

[Levy00] LEVY, Steve. **Crypto: secrecy and privacy in the new code war**. London: Allen Lane, The Penguin Press, 2000.

[Maca02] MACARCINI, Augusto Tavares Rosa. **Direito e informática: uma abordagem jurídica sobre criptografia**. Rio de Janeiro: Forense, 2002.

[Sche04] SCHELLEKENS, M. **Eletrocnic signatures: authentication technology from a legal perspective**. The Hague: TMC Asser Press, 2004.

[Schn00] SCHNEIER, Bruce. **Secrets & lies: digital security in a networked world**. Indianapolis, IN: Wiley, 2000.

[Schn03] SCHENEIER, Bruce. **Beyond fear: thinking sensibly about security in a uncertain world**. New York: Copernicus, 2003.

[Sing02] SINGH, Simon. **O livro dos códigos: a ciência do sigilo – do antigo Egito à criptografia quântica**. Rio de Janeiro: Record, 2002.

[Sorj03] SORJ, Bernardo. **Brasil@povo.com: a luta contra a desigualdade na sociedade da informação**. Rio de Janeiro: Jorge Zahar Editor, 2003.

[Ster98] STERN, Jacques. **La science du secret**. Paris: Odile Jacob, 1998.

[Wipo02] World Intellectual Property Organization. **Intellectual property on the Internet: a survey of issues**. Geneva: WIPO, dez. 2002.

Sobre os autores

CHRISTIANA SOARES DE FREITAS

Pesquisadora associada do Núcleo de Estudos sobre Educação Superior (NESUB) da Universidade de Brasília (UnB).

Doutora em Sociologia (UnB).

Áreas de interesse: sociologia da ciência e tecnologia; políticas públicas de ciência e tecnologia.

ALEXANDRE VERONESE

Professor do Departamento de Direito Público da Universidade Federal Fluminense (UFF), pesquisador do Núcleo de Práticas e Instituições Jurídicas (Área de Direito, Tecnologia e Sociedade) do Programa de Pós-Graduação em Sociologia e Direito (PPGSD).

Mestre em Sociologia e Direito (UFF) e Doutorando em Sociologia (Iuperj).

Áreas de interesse: direito, *internet* e sociedade; sociologia jurídica.