



Receita não poderia impor compra de certificado eletrônico

O conceito de criptografia por chaves públicas foi uma descoberta essencial para o desenvolvimento do mundo digital, por duas diferentes funções que exerce nas comunicações eletrônicas. De um lado, permite dispensar o uso do papel na elaboração de documentos, inclusive contratos, ao substituir a assinatura manuscrita. As vantagens quanto à rapidez na circulação, guarda e recuperação de informações, especialmente no aspecto da redução de custos financeiros, são imensuráveis.

De outro lado, e simultaneamente, é potente instrumento contra violação do sigilo das comunicações, permitindo que as informações estejam protegidas contra tentativas de acesso por terceiros, sejam eles indivíduos, empresas, ou mesmo órgãos governamentais. Assegura, portanto, a privacidade das pessoas contra incursões indevidas. Assim sumariamente pode ser exposta a importância do uso dessa tecnologia.

O Congresso Norte-Americano havia pretendido aprovar uma nova lei, definindo um padrão nacional único de encriptação por chaves públicas, de forma a resolver os problemas que as corporações empresariais vinham enfrentando, de pouca interoperabilidade de aplicativos baseados nesse conceito tecnológico.

Para desenvolvimento desse superalgoritmo criptográfico, convocaram os melhores matemáticos do país.

Era tudo o que a NSA – National Security Agency, principal agência governamental de espionagem nas comunicações eletrônicas, poderia querer para alcançar seu maior objetivo: controlar toda a informação que trafega por meio eletrônico, mesmo aquelas blindadas por criptografia.

Ora, todos os principais matemáticos e criptógrafos norte-americanos eram funcionários da NSA. E pedir a eles o desenvolvimento de um padrão criptográfico realmente seguro seria como pedir ao condenado que produzisse sua própria força.

Mas a aprovação pelo Poder Legislativo faria supor que o novo código criptográfico seria realmente forte. Isso traria a vantagem de fazer com que toda a população acreditasse que o ambiente digital, protegido por tal sistema, tornar-se-ia efetivamente seguro; daí, todos passariam a expor informações privadas, que não seriam normalmente transmitidas em redes abertas pelo receio de violação.

A EFF – Electronic Frontier Foundation, organização sem fins lucrativos que luta para assegurar a privacidade dos cidadãos norte-americanos, percebendo o conflito de interesses dos desenvolvedores do novo padrão criptográfico, denunciou a possibilidade de os funcionários da NSA acabarem produzindo um código criptográfico de baixa qualidade, de forma a permitir que futuramente a Agência pudesse quebrá-lo com facilidade e obter acesso a todas as comunicações privadas.

Em resposta, o Congresso tornou público o novo algoritmo, para que todo o mundo pudesse testá-lo e comprovar sua qualidade. Matemáticos de diferentes países examinaram o código, ficando impressionados com sua potência, declarando-o como inviolável. Um jovem programador, entretanto, chocou a sociedade ao denunciar que havia descoberto uma back door (porta traseira) escondida no algoritmo. Back door, na linguagem de segurança da informação, significa alguma fragilidade oculta,



propositalmente inserida em um sistema, para permitir sua violação por quem o fez.

A comunidade de informática ficou furiosa com a descoberta. A EFF criticou severamente a ingenuidade dos membros do Congresso Nacional e a esperteza da NSA, proclamando-a como a maior ameaça ao mundo livre desde Hitler. O padrão criptográfico estava morto e enterrado. E o jovem programador que descobrira a fraude acabou contratado pela Agência: melhor mantê-lo trabalhando para ela, do que contra ela.

Os acontecimentos acima narrados fazem parte de um dos múltiplos elementos que compõem a trama do livro **Fortaleza Digital**, ficção recém publicada no Brasil pela Editora Sextante, outro sucesso editorial de Dan Brown, conhecido autor de Código Da Vinci. Embora faça referência a entidades reais e a uma disputa que ocorreu e ocorre nos EUA, esta narrativa é fictícia. Mas sua verossimilhança é o que deixa o enredo ainda mais instigante.

Paremos um pouco para pensar e imaginemos como seria essa estória, acaso se passasse no Brasil. Num dia em que o Congresso entraria em recesso, em 2002, o Governo Brasileiro publicou uma Medida Provisória, instituindo a Infra-Estrutura de Chaves Públicas do Brasil – ICP-Br, a pretexto de estabelecer a interoperabilidade entre aplicativos com uso dessa tecnologia e, assim, fomentar o comércio eletrônico no país.

Essa Medida Provisória estabeleceu que o suporte tecnológico da infra-estrutura seria desenvolvido pelo CEPESC, braço tecnológico da Abin – Agência Brasileira de Informações, sucessora do SNI – Serviço Nacional de Informações.

Para supostamente dar mais segurança ao modelo, competiria à própria ICP-Brasil fornecer, a cada brasileiro, o seu par de chaves criptográficas. Ou seja, as chaves que geram a assinatura digital, em substituição da assinatura manuscrita, e asseguram o sigilo das informações transmitidas por meio eletrônico seriam geradas em computadores oficiais, tornando-se muito fácil aos agentes do Governo iludir o requerente e guardar um cópia delas para si.

Poucos dias após editada a Medida Provisória, ainda com o Legislativo em recesso, divulgou-se longa minuta de regulamento da ICP-Brasil, estabelecendo que o padrão criptográfico haveria de ser nacional. Mas o único organismo que tinha desenvolvido um produto do gênero era o próprio CEPESC.

A OAB – Ordem dos Advogados do Brasil, entidade de passado de lutas pela democracia brasileira, imediatamente denunciou os riscos à segurança e à privacidade dos cidadãos gerados por aquela Medida Provisória. Era um absurdo estabelecer um padrão criptográfico como pressuposto para facilitar a interoperabilidade dos aplicativos. Era um disparate que o Governo gerasse as chaves criptográficas dos cidadãos – chaves que permitiriam assinar documentos contendo manifestações de vontade com efeitos jurídicos, e que assegurariam o sigilo das comunicações eletrônicas, inclusive contra bisbilhotagem de órgãos públicos. Era inadmissível que cidadãos fossem obrigados a usar meios eletrônicos, ainda mais nesse ambiente contaminado, para desenvolver suas atividades privadas ou profissionais. E não era crível que fosse delegado a um órgão da segurança nacional atividades para favorecer o comércio eletrônico.



O Governo Federal imediatamente convoca uma coletiva de imprensa, onde se limita a dizer que advogados não deveriam falar de tecnologia, já que não dominavam o assunto. Mas, com a pressão exercida pela Ordem, por outras entidades civis e pela imprensa, já na primeira reedição da MP, a Presidência se vê obrigada a modificá-la, suprimindo tanto a emissão do par de chaves pelo Governo, quanto a expressa presença do CEPESC no desenvolvimento da infra-estrutura criptográfica. Na versão divulgada extra-oficialmente, a MP trazia ainda um artigo 13, dispondo que “ninguém será obrigado a utilizar documento ou meio eletrônico nas suas relações jurídicas privadas ou com entidades e órgãos públicos”. Embora as outras modificações fossem mantidas, aquele artigo 13 simplesmente desapareceu na versão que acabou publicada no Diário Oficial.

A OAB, embora reconhecendo os avanços na nova edição da MP, continuou a denunciar a ICP-Brasil, pelos riscos jurídicos, sociais e políticos que representava, por ferir a independência e autonomia entre Poderes e entre federativos do Brasil, por constituir uma infra-estrutura sob o domínio do Executivo Federal, a que todos os documentos, públicos e privados, de cidadãos e de empresas, do Poder Legislativo e do Poder Judiciário, dos Estados e dos Municípios, haveriam de ser subordinados. Denunciou-se os riscos para a segurança e privacidade dos usuários, diante da adoção de um certificado único. E também pelo monopólio que criava, não apenas econômico, mas o odioso monopólio da verdade, já que apenas os documentos sujeitos a esse regime teriam “validade jurídica”, como o texto da MP tentou fazer entender.

Com as modificações constitucionais no regime das Medidas Provisórias, a norma foi colocada no vácuo legislativo, e acabou tornando-se definitiva, ainda que sem aprovação do Congresso Nacional.

Saiu Governo, entrou Governo. Esperava-se que a situação sofresse mudança. Primeiro, porque a assessoria parlamentar do partido político que agora assumia o poder havia, quando na oposição, se manifestado contrariamente à MP. Segundo, porque passados alguns anos, a ICP-Brasil não decolou. No mínimo, iria caducar pelo desuso.

Surpreendentemente, no final de 2004, uma mera Instrução Normativa da Secretaria da Receita Federal, portanto, um órgão da burocracia estatal do novo Governo, sem que houvesse qualquer participação do Congresso Nacional, estabelece a obrigatoriedade de todas as pessoas jurídicas brasileiras adquirirem certificados eletrônicos, emitidos pela ICP-Brasil, a pretexto de dar maior segurança às suas declarações tributárias. E a Secretaria ainda deixa clara sua intenção de, em seguida, obrigar todos os cidadãos a fazer uso daqueles certificados.

Não havia lei que autorizasse a Secretaria da Receita Federal a impor a aquisição de certificados eletrônicos. Não poderia o contribuinte ser obrigado a comprar, junto às poucas empresas credenciadas, certificados para dar segurança à Receita Federal. Se o Fisco não estivesse satisfeito com seus atuais sistemas, que os alterasse, ou que fornecesse aos contribuintes os certificados, para uso restrito às comunicações fiscais. Não poderia ser aceito um monopólio público não previsto na Constituição Federal, com pouquíssimas empresas credenciadas a vender certificados.

Mas chamou especial atenção o fato de que o sistema que utilizará o par de chaves criptográficas será fornecido pelo próprio Governo Federal, via Secretaria da Receita Federal, sem que a população conheça



suas reais funções, e sem que se saiba se, eventualmente, contem uma back door.

O problema é que no Brasil esses fatos aconteceram ou estão acontecendo; não compõem um quadro romanceado de ficção científica.

A obra de Dan Brown, originalmente escrita em 1998, embora só agora lançada no país, está sendo plagiada ao vivo e a cores pelos nossos dois últimos Governos. Melhor fariam se tivessem escrito um best-seller, ao invés de promover tal intrusão na vida digital dos cidadãos e demonstrar tamanho descaso com a ordem jurídica.

Date Created

11/04/2005