

**PARTIDO DOS TRABALHADORES
ASSESSORIA TÉCNICA**

PARECER TÉCNICO

MEDIDA PROVISÓRIA Nº 2200-1, DE 27 DE JULHO DE 2001.

MEDIDA PROVISÓRIA Nº 2.200, DE 28 DE JUNHO DE 2001.

Institui a Infra-Estrutura de Chaves Públicas
Brasileira-ICP-Brasil, e dá outras providências.

Editada pelo Presidente da República, a Medida Provisória nº 2.200, de 28 de junho de 2001, institui a Infra-estrutura de Chaves Públicas Brasileira – **ICP-Brasil**.

A MP trata da validade jurídica de todos os documentos emitidos de forma eletrônica, com o objetivo de lhes dar autenticidade e integridade. Assim, dispõe seu artigo 1º: “*Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira-ICP, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.*” Já o seu artigo 12, assim dispõe: “*Consideram-se documentos públicos ou particulares para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.*”

A MP também define que a ICP-Brasil terá sua organização definida em regulamento. A sua estrutura contará com uma Autoridade Certificadora Raiz – **AC Raiz**, que será o Instituto Nacional de Tecnologia da Informação, do MCT; com as Autoridades Certificadoras – **AC**; e com as Autoridades de Registro – **AR**.

Ao mesmo tempo, cria um Comitê Gestor para regular e dispor sobre os métodos digitais de representação da vontade humana, em nosso país. Esse Comitê, formado por onze membros, sendo quatro representantes da sociedade civil e sete representantes do Governo, todos designados pelo Presidente da República, terá a função de autoridade gestora de políticas. Para isso, será assessorado pelo Centro de Pesquisa e Desenvolvimento para a Segurança das

Comunicações, o CEPESC, órgão de segurança das comunicações do Poder Executivo, vinculado à ABIN.

O Comitê Gestor terá como competência a coordenação da implantação e funcionamento da ICP-Brasil, a formulação de políticas de licenciamento das AC, das AR e dos demais prestadores de serviços da cadeia de certificação. Além disso, terá a competência de formular políticas de certificação, homologação, auditoragem e fiscalização da AC Raiz e seus prestadores de serviços.

Ao mesmo tempo, o Comitê Gestor deverá aprovar políticas de certificação, licenciamento e autorização do funcionamento das AC e das AR. Caberá, também, ao Comitê, negociar e aprovar acordos de certificação bilateral e outras formas de cooperação internacional. Ou seja, subtrai poderes do Legislativo brasileiro.

A AC Raiz é a autoridade maior da cadeia de certificação, cabendo-lhe executar as políticas de certificação aprovadas pelo Comitê Gestor. É a entidade responsável pela concessão, fiscalização, controle e auditoria das atividades de certificação das AC, de nível imediatamente subsequente ao seu, das AR e dos demais prestadores de serviço habilitados na ICP-Brasil.

Mantendo a lógica neoliberal do Governo FHC, o parágrafo único do art. 7º, da MP, autoriza a AC Raiz, que é o INTI, do MCT, a funcionar através da contratação de serviços de terceiros.

Em seu art. 8º, a MP trata das Autoridades Certificadoras que estão autorizadas a emitir certificados digitais vinculando determinado código criptográfico ao respectivo titular, competindo-lhe emitir, expedir, distribuir, revogar e gerenciar os certificados e as correspondentes chaves criptográficas". A atribuição dada neste artigo de "expedir, distribuir, revogar e gerenciar os certificados e as correspondentes chaves criptográficas" não define essas chaves que correspondem ao certificado. Aqui, há um problema de conceito do termo certificado digital. Segundo Resende¹, *o conceito de assinatura digital originou-se de forma dedutiva. Os arquitetos pioneiros do ciberespaço chegaram a ela pela interpretação semiótica de teoremas matemáticos na teoria da informação, desenvolvida por Claude Shannon a partir de 1949.* Para

¹ RESENDE, Pedro D. de. *Totalitarismo Digital*. <http://www.cic.unb.br/docentes/pedro/segdadtop.htm>. 29/06/01. Brasília.

ele, o problema central da teoria é o seguinte: dada uma seqüência de zeros e uns, constituindo a representação digital de um documento, de que meios digitais poderá dispor seu autor para credibilizar a declaração de sua vontade ou autoria, ali nomeada? Este termo surgiu com o uso da criptografia assimétrica. A criptografia assimétrica é um conceito que recorta o universo das tecnologias digitais, separando aquelas que, na sua capacidade autenticatória, ofereçam ao identificado a possibilidade de controlar a dificuldade de forja desta identificação. Funcionam por meio do uso de pares de chaves tituladas, que, nesta capacidade, ganharam o nome de mecanismos de assinatura digital. Neles, uma das chaves do par é **privada**, usada para lavrar marcas pessoais únicas em documentos eletrônicos - as assinaturas digitais. E a outra é **pública**, usada para verificar a autenticidade dessas marcas. A chave pública, ao verificar uma tal lavra, identifica o assinante como titular deste par de chaves e autor do documento, além da integridade do documento desde sua assinatura. Este par funciona, portanto, como senha e contra-senha, para que a senha não precise ser compartilhada com quem poderia dela abusar, e para quem a contra senha poderá comprovar a ação da senha. São longas e aleatórias seqüências de zeros (0) e uns (1), impossíveis de serem memorizadas como as senhas comuns, e que por isso precisam ser armazenadas em meio eletrônico, conclui Resende..

Segundo especialistas, os mecanismos que a ciência classifica como de assinatura digital, recebem esta classificação por oferecerem ao assinante a possibilidade de controlar a dificuldade da forja indetectável das assinaturas que propicia. Através do custo computacional para se obter uma chave do par a partir da ação da outra. Esta dificuldade é que permite vincular a identificação do assinante à representação de sua vontade. Mas esta lógica vinculante só se sustenta sob a hipótese de que o titular seja o único a conhecer a chave usada para lavrar suas assinaturas.

Para os juristas que analisaram a MP², a questão não se trata se documento não está em sua “*validade jurídica*”, ou seja, se uma contratação eletrônica terá ou não valor jurídico. O ato jurídico, salvo exceções previstas em lei, como a compra e venda de um imóvel, que requer escritura pública, independe de maiores formalidades. Uma contratação pode ser inclusive verbal (artigos 82 e 129 do Código Civil).

² COSTA, M., MARCACINI, A. T. R. *O apagão do comércio eletrônico*. OAB-SP. 2001.

Segundo documento divulgado pela Ordem dos Advogados do Brasil, OAB, *a questão jurídica controvertida que o documento eletrônico tem nos apresentado está no seu valor probante, ou seja, se será ou não admitido como prova do ato praticado, quando apresentado em juízo. Qualquer documento, para servir como prova, deve permitir o conhecimento de sua autoria, bem como a apuração de eventual fraude. Um impresso apócrifo, por exemplo, dificilmente bastará como prova judicial, exatamente pela dificuldade em se conhecer seu autor. Da mesma maneira, o documento eletrônico precisa ter sua autoria demonstrada. Além disso, o documento eletrônico, uma seqüência de bits facilmente alterável, deve ser assinado por sistema que permita apurar se sofreu modificação após a assinatura ter sido emitida.*

O seu art. 8º destrói as garantias oferecidas pelos mecanismos de assinatura digital, ao forçar a violação da premissa vinculante de posse única para a certificação credenciada. Assim, a MP busca asfixiar as certificações em protocolos abertos e livres.

Embora muitos governos ocidentais tenham aversão à criptografia e a sistemas de criptografia, segundo nos relatou Werner Koch, em sua visita à Câmara dos Deputados, a convite da Liderança do PT para participar do Fórum Internacional de Software Livre de Brasília, em março deste ano, o Governo Americano tem pressionado outros países para impor restrições ao seu uso. A respeito disso, os EUA solicitaram que a Alemanha controlasse a exportação de criptografia de seqüência. A resposta do governo alemão foi a de não impor nenhuma restrição a produto de criptografia, passando a desenvolver o GnuPG, *software* livre e estimular o desenvolvimento de outros produtos livres.

Embora os métodos de assinatura digital tenham caído todos em domínio público, com a expiração da patente do algoritmo RSA em 20 de setembro do ano passado, implementações em software livre desses métodos podem agora ampliar seus benefícios de auditabilidade e gratuidade, minando o controle de indústrias monopolistas sobre necessidades artificialmente criadas para seus produtos, as pressões de grupos empresariais têm continuado. Talvez, isso justifique o Governo FHC ter editado uma MP para um assunto que não requer qualquer premência.

Por fim, o art. 9º da MP nº 2200 estabelece que as AR identificarão e cadastrarão os usuários sem, contudo, dispor em seu texto quais métodos os cidadãos e pessoas jurídicas deverão usar, para representar suas vontades.

Ao disparate de expedir MP para tratar de um assunto que está sendo discutido, não só no legislativo, mas em todo mundo, com a participação de técnicos, especialistas, juristas e entidades da sociedade civil organizada, o Executivo atropela o legislativo brasileiro e desconsidera que acaba de ser aprovado no Senado Federal o Projeto de Lei SF 672/99, que já chegou na Câmara, regulamentando, dentre outras coisas, o uso de mecanismos de identificação digital em contratos eletrônicos.

Esse PL do Senado é baseado no modelo da UNCITRAL, e é fruto de intenso lobby global de grandes corporações da indústria da informática. Seu artigo 7º prevê, por exemplo, que deve valer, como substituto da assinatura de punho, o método de identificação que as partes concordarem que vale. Outrossim, não identifica quem são as partes. A parte que propuser um método, certamente estará interessada em dividendos ou vantagens que lhe ofereçam a tecnologia escolhida. E que métodos serão esses?

Por outro lado, tramita na Câmara dos Deputados o PL nº 1.483, de 1999, do Deputado Dr. Hélio, que pretende instituir a fatura eletrônica e a assinatura digital nas transações de comércio eletrônico. Justifica sua iniciativa pela necessidade de normatizar as relações comerciais entre empresas e entre cidadãos e empresas, dentro do novo paradigma que vem sendo introduzido nas transações comerciais com o rápido avanço da Internet em nosso País.

À proposição foi apensado o Projeto de Lei nº 1.589, de 1999, de autoria do Deputado Luciano Pizzato e outros, que também dispõe sobre o comércio eletrônico, tratando em especial da validade jurídica do documento eletrônico e da assinatura digital. Referido projeto pretende tratar desde já as novas relações sociais que surgiram com o advento do comércio eletrônico, seguindo tendência observada em diversos países.

Para discutir esses projetos foi instituída Comissão Especial que colheu subsídios de Michael Nelson, Diretor de Tecnologia e Estratégia de Internet da IBM Corporation, Marcos da Costa, Presidente da Comissão Especial de Informática Jurídica da Ordem dos Advogados de São Paulo, Ivan Moura Campos, Coordenador do Comitê Gestor da Internet, Henrique César Conti, Diretor de Serviços aos Associados da BRISA – Sociedade para o Desenvolvimento da Tecnologia da Informação, Fernando Nery, Diretor da ASSESPRO, Rogério Vianna, Coordenador Geral de Comércio Eletrônico do Ministério do Desenvolvimento, Indústria e Comércio Exterior, Pedro Luiz César Bezerra, Coordenador de Tecnologia da Receita Federal,

Odécio Grégio, Diretor de Comércio Eletrônico do BRADESPAR, Caio Túlio Costa, Diretor-Geral do Universo Online, Murilo Tavares, Presidente da Submarino do Brasil, Juliana Behring, Diretora de Parceria do Amelia.com.br, do Grupo Pão de Açúcar, Ruy Rosado de Aguiar Júnior, Ministro do Superior Tribunal de Justiça e Marcos Diegues, Coordenador do Departamento de Atendimento do IDEC – Instituto Brasileiro de Defesa do Consumidor.

O relator, deputado Julio Semeghini (PSDB-SP), apresentou seu Substitutivo em 20 de junho de 2001, ao qual esta Assessoria propôs que se apresentassem emendas, visando melhorá-lo, garantido-se o respeito à privacidade dos cidadãos e o uso e protocolos abertos.

As emendas foram as seguintes:

1. Estabelecer que se evite conflito com a jurisprudência atual do direito comercial, garantindo-se que a assinatura digital *seja passível de verificação pública*. (inciso II, do art. 4º)
2. Estabelecer que a assinatura eletrônica reproduza, da melhor forma possível, a função da assinatura de punho existente na jurisprudência do direito comercial, o que já está disponível nas tecnologias atuais de assinatura digital, portanto, é fundamental que a lei estabeleça que a assinatura digital *esteja sob controle exclusivo do signatário, inclusive, quanto à dificuldade da forja de sua assinatura, a partir do mecanismo de verificação de sua validade*. (inciso III, do art. 4º)
1. Não ferir direitos constitucionais, portanto, o *subscritor de assinatura digital estará isento das obrigações dispostas no inciso III, nos casos em que o uso da assinatura eletrônica for obrigatório e os meios a ele disponíveis, para lavra de sua assinatura, não ofereçam garantias de auditabilidade e controle de risco*. (inciso II do art. 7º)
2. Suspender e revogar certificados digitais através de *sistema de suspensão e revogação de certificados, procedendo à imediata publicação nas hipóteses previstas nesta lei*. (inciso IV do art. 9º)
3. Estabelecer que não é viável à certificadora responder pela validação cronológica de documentos assinados pelas chaves que certifica, pois esta responsabilidade é dos contratantes. Como contratante, a certificadora responde pela validação

cronológica apenas dos certificados que assina. Assim, deve-se *proceder à validação cronológica de certificados*.(inciso IX do art. 9).

4. Assegurar a eficácia dos requisitos de confiabilidade já alcançados pelas tecnologias atuais na disseminação de novas tecnologias autenticatórias, garantindo que se possa *aferir a capacidade de outros meios de autenticação e identificação, a que se referem o art. 6º, para atender aos requisitos de confiabilidade especificados nos incisos II, III e IV, do artigo 4º, respeitados os princípios de transparência do processo, auditabilidade do método em exame, e rigor científico em todos os procedimentos de aferição a ele submetíveis*. (art. 17)
5. Assegurar que são duas as tecnologias a que se reportam os certificados: a da assinatura no certificado, lavrada pela certificadora; e a das assinaturas do titular do certificado, cuja chave pública ali transportada irá verificar. Para isso, a lei deve dispor sobre *o nome da entidade certificadora e indicação da tecnologia utilizada na certificação e da tecnologia a ser utilizada na verificação de assinatura, com a chave que transporta*. (inciso II, do art.11)

Assim, esta Assessoria considera que a MP constitui-se em uma intervenção antidemocrática do Estado brasileiro, na esfera pública e privada do conjunto da sociedade. Dessa intervenção, podem advir todos os riscos à privacidade e às liberdades democráticas do povo brasileiro.

A MP 2000, portanto, apresenta dispositivos que ferem a privacidade do cidadão e intervêm nos seus direitos mais fundamentais.

A reedição da MP introduziu alterações na redação anterior do artigo 12, acrescentando dois parágrafos, assim dispostos:

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.

§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

A nova redação, dada pela MP 2200-1, retirou o dispositivo que obrigava que todas as autoridades certificadoras estivessem vinculadas à AC Raiz. Assim, também, a alteração proposta passou a dispor que poderão ser usados outros meios de prova de autoria e integridade de documentos, inclusive emitidos fora da ICP-Brasil.

Também alterou o artigo 8º dispondo que o par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Ampliou o número de representantes da sociedade civil no Comitê Gestor da ICP-Brasil, de quatro para cinco, o que não representa muita coisa haja vista que todos são indicados pelo Presidente da República.

Enfim, as alterações não foram tão profundas assim.

Portanto, urge que se denuncie que existe uma manifestação expressa, de setores distintos das classes dominantes, em se posicionarem contra a MP, não só para lutar contra a presença do Estado nas relações de comércio no ambiente virtual - os neoliberais -, propondo um ambiente sem qualquer tipo de regulação, mas para criar mecanismos que penetrem na privacidade dos cidadãos brasileiros para que passem a ser vistos, exclusivamente, como consumidores no *cyberspace*. Aqui está o grande risco de prevalecer uma legislação que reproduza no ambiente virtual a mesma lógica mercantilista do ambiente real.

Neste aspecto, proponho que a Bancada do PT, à luz dos debates que tem realizado sobre políticas públicas para uso das Tecnologias da Informação e Comunicação (TIC), com base no uso do software livre, atente para as questões que apresentamos nesta Nota. E, portanto, recomendamos um posicionamento firme contra essa MP, questionando os seus aspectos de uso de tecnologias e protocolos proprietários que visam, unicamente, submeter o país a interesses de uma única nação.

Israel Fernando de Carvalho Bayma

Criado em 02/08/01 17:38