ASSINATURAS DIGITAIS, CERTIFICADOS DIGITAIS, INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA e a ICP ALEMÃ

FABIANO MENKE

SUMÁRIO: 1. Considerações iniciais – 2. Assinaturas e certificados digitais – 3. Infra-Estrutura de Chaves Públicas e ICP-Brasil – 4. O modelo alemão de Infra-Estrutura de Chaves Públicas – 5. Considerações finais.

1. CONSIDERAÇÕES INICIAIS

No prefácio de sua Introdução à Ciência do Direito[1], escrita em 1929, o filósofo do direito alemão *Gustav Radbruch* exalta as qualidades de seu colega e compatriota, o penalista *Franz v. Liszt*. Consoante *Radbruch*: "Em Franz v. Liszt o espírito do século XVIII, o espírito do iluminismo, assumiria mais uma vez vívida figura – e seu exemplo basta para condenar ao silêncio os caluniadores da época mais frutífera da história da civilização, os agoureiros da vida apática, os encomiastas do inconsciente, todos aqueles que, em busca de esclarecimentos, queriam, na verdade, pescar em águas turvas." Seguindo a apologia, o autor diz que Liszt tinha um espírito ordeiro, assim como a língua alemã, "que expressa em duplo sentido, um espírito 'alegre e arrumado'." Adiante*, Radbruch* refere que, como nenhum homem, a caligrafia de *Liszt*, de fluidez viva e bela, decidida e clara, mostrava com exatidão o seu jeito de ser.

Esta última passagem da obra leva-nos inevitavelmente à reflexão. Interessante observar como ainda no começo do século XX os homens conheciam as caligrafias uns dos outros. Mas o fato é que hoje raramente escrevemos à mão. As cartas manuscritas foram praticamente abolidas. Em seu lugar veio o correio eletrônico, que é um meio de transmitir mensagem muito mais célere e menos custoso. A máquina de escrever e posteriormente os computadores (com o auxílio das impressoras) e a *internet* acabaram por tirar a necessidade de as pessoas escreverem com o próprio punho sobre o tradicional suporte de papel. Hoje, são raras as vezes em que temos a oportunidade de conhecer a caligrafia de nossos interlocutores e admirá-las, tal qual na relação *Radbruch-Franz v. Liszt*.

Mas parece que a ciência e o progresso, e portanto, o próprio homem, não querem parar de lançar no esquecimento práticas e hábitos tradicionais. Eis que agora estamos, senão por deixar de utilizar totalmente, pelo menos por ter de diminuir bastante a necessidade de utilização das assinaturas manuscritas. E isto se deve justamente ao desenvolvimento de conceitos matemáticos que possibilitaram o desenvolvimento da criptografia[2] assimétrica, e, com ela, a criação das assinaturas digitais, uma forma bastante segura de associar inequivocamente uma pessoa natural ou jurídica a determinada declaração de vontade manifestada no mundo virtual por meio de um documento eletrônico.

As assinaturas digitais surgem justamente para sanar uma imperfeição ínsita das comunicações veiculadas no meio digital, qual seja a de não se ter certeza da identidade da pessoa com a qual se está falando. Enquanto que no mundo físico, no mais das vezes, travamos contato presencial com a pessoa com quem contrataremos ou entabularemos algum tipo de comunicação, no mundo virtual essa já não é a regra. Conforme salienta *Cláudia Lima Marques*, nos contratos concluídos no novo meio "o fornecedor não teria mais rosto".[3]

Tal característica do meio eletrônico foi bem diagnosticada por *Lawrence Lessig*, professor de direito constitucional da Escola de Direito de Harvard, que, com um exemplo bastante ilustrativo salientou: "In the words of the famous *New Yorker* cartoon of two dogs sitting in front of a PC, 'on the internet, nobody knows you're a dog'. You can use the Net anonymously. You could build a (ro)bot to use the Net. No one need know your name, and there is no easy way to verify your age, your sex, or where you live. The Net knows only as much as you choose to tell, and it cannot even verify that information."[4]

E essa característica - que *Lessig* chama de imperfeição - faz com que o comércio eletrônico não tenha se desenvolvido ainda mais do que se desejaria, tanto nas relações entre fornecedores, quanto entre fornecedores e consumidores; porque ainda não temos total confiança na comunicação virtual que encetamos no dia-a-dia. Todos nós enviamos e recebemos e-mails diariamente. Da mesma forma, acessamos *sites* para a leitura de jornais, de revistas e de notícias sem maiores preocupações. Número um pouco menor de pessoas tem coragem de comprar um livro ou um *compact disc* pela *internet*. Quase ninguém, todavia, se arriscaria a adquirir um automóvel pela rede mundial de computadores. E por quê? Justamente pelo motivo de que até o presente momento – mas essa realidade está mudando, como será demonstrado - não nos sentimos seguros o suficiente quanto à aludida garantia da autoria da mensagem ou da declaração de vontade, da segurança da integridade dessa mensagem (ou seja, se ela foi ou não alterada em seu percurso virtual), e por último, se o documento eletrônico que tenha viabilizado a transação será aceito como meio de prova.
O objetivo do presente artigo é o de explicitar o funcionamento das assinaturas e dos certificados digitais bem como o de descrever a Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), instituída pela Medida Provisória nº 2.200, de 28 de junho de 2001 e consolidada na Medida Provisória nº 2.200-2, de 24 de agosto de 2001.[5] Na parte final far-se-á sucinta análise do modelo alemão de ICP. As questões de direito material civil não serão tratadas com maior profundidade, o que será feito em trabalho posterior.

2. ASSINATURAS E CERTIFICADOS DIGITAIS

As assinaturas e os certificados digitais servem para agregar os valores confiança e segurança às comunicações e negócios veiculados em ambiente virtual, especialmente na *internet*. Primeiramente, é preciso esclarecer – em singela conceituação - o que é assinatura digital e o que é certificação digital.

A assinatura digital é viabilizada pelo emprego da criptografia assimétrica ou criptografia de chaves públicas. Para uma melhor compreensão da criptografia

assimétrica, é preciso fazer uma rápida passagem sobre as características da criptografia simétrica. A criptografia simétrica é bastante antiga, havendo registros de que já era conhecida na época das guerras helênicas, na Mesopotâmia e no Egito. Sua utilização original esteve relacionada a finalidades militares, para a codificação das comunicações encetadas entre os chefes de Estado e os comandantes dos exércitos. *Simon Singh* relata que "o primeiro documento que usou uma cifra de substituição para propósitos militares aparece nas *Guerras da Gália* de Júlio César."[6] O método empregado por Júlio César era o do *alfabeto cifrado*, de acordo com o qual cada letra da mensagem era substituída pela terceira letra subseqüente do alfabeto. Assim, o texto original "veni, vidi, vici", cifrado, ficava assim: "YHQL, YLGL, YLFL".

O destinatário da mensagem deveria ter prévio conhecimento dessa substituição, ou seja, do número exato de letras que foi avançado (a denominada chave ou código, como se chama na linguagem técnica da criptografia), a fim de que pudesse compreender o conteúdo.

Veja-se que na criptografia simétrica, os interlocutores compartilham o código (ou chave) de cifração e de decifração da mensagem. E mais, utilizam o mesmo código para esses dois processos de ocultar e tornar claro o texto. Ocorre que a criptografia simétrica apresenta algumas limitações ou dificuldades facilmente verificáveis. A primeira delas é que previamente à comunicação entre duas pessoas que a utilizarão será necessário um contato para que elas convencionem o código a ser utilizado.

A segunda dificuldade é a de escala, ou seja, a chave que Carlos utilizar para se comunicar com Maria deverá necessariamente ser diferente daquela que utilizará na interlocução com Pedro, caso contrário, não terá a garantia da confidencialidade e da autoria da mensagem. Numa comunidade de 1.000 usuários, Carlos precisaria de 999 chaves diferentes para que a confidencialidade das mensagens não fosse comprometida. Daí pode-se imaginar os complicadores de sua aplicação para um universo maior de pessoas, como aquele verificado numa sociedade de massas.

A criptografia assimétrica ou de chave pública, por seu turno, foi desenvolvida recentemente, a partir de estudos feitos nos anos 70 pelos pesquisadores norte-americanos Whitfield Diffie, Martin Hellman e Ralph Merkle, considerados os inventores dos conceitos de criptografia de chave pública.[7] Ela consiste num método que utiliza duas chaves, uma a ser aplicada pelo remetente e outra pelo receptor da mensagem, e é sobre essa tecnologia que se funda a criação da chamada assinatura digital. As chaves são denominadas chave pública e chave privada, ou privativa. A chave privada é de único e exclusivo domínio do titular da chave de assinatura, enquanto que a chave pública poderá ser amplamente divulgada. Elas constituem combinação de letras e números bastante extensa, que não são criadas pelo usuário, mas sim por programas de computador. O que interessa saber é que as chaves se complementam e atuam em conjunto. O remetente "assina" a sua mensagem aplicando a ela a sua chave privada (que fica armazenada, usualmente, em dispositivo similar a um cartão de crédito, os chamados cartões inteligentes), enquanto que o receptor, ao receber a mensagem, aplicará a chave pública do remetente para verificar se ela efetivamente dele se originou.

Os programas de computador do receptor fazem uma checagem, e se houver correspondência entre as chaves, a mensagem abrirá com uma confirmação positiva, o que garantirá a presunção da origem bem como da integridade do conteúdo, ou seja, de sua não alteração no caminho percorrido na rede.

Diferentemente da criptografia simétrica, que utiliza a mesma chave tanto para a cifração quanto para a decifração da mensagem, a diversidade das chaves permite que possamos nos comunicar com um universo ilimitado, e, fundamentalmente, que não tenhamos que conhecer previamente o interlocutor e com ele ter contato prévio, algo bastante necessário numa sociedade como a da atualidade, que tem por característica marcante a impessoalidade.

Para agregar mais segurança às comunicações virtuais, é necessário outro elemento que dê certeza àquela pessoa que recebeu uma mensagem eletrônica assinada digitalmente de que a pessoa que a assinou é realmente quem diz ser. É aí que entram os certificados digitais. É preciso que um terceiro de confiança de ambas as partes ateste que a chave pública daquela pessoa que assinou digitalmente realmente lhe pertence.
O certificado digital é um documento eletrônico assinado digitalmente por uma terceira parte confiável que associa o nome e atributos de uma pessoa a uma chave pública. O fornecimento de um certificado digital é um serviço semelhante ao de identificação para a expedição de carteiras de identidade. O interessado é identificado mediante a sua presença física pelo terceiro de confiança – com a apresentação dos documentos necessários - e este lhe emite o certificado digital.

Na prática, quando se recebe uma mensagem assinada digitalmente, ela estará acompanhada do certificado digital do remetente, onde constará, entre outros dados, a sua chave pública. Um programa de computador do destinatário aplicará a chave pública do emissor na mensagem e confirmará a autoria e a integridade do documento eletrônico, a partir de uma rápida consulta ao repositório de chaves públicas do terceiro de confiança – Autoridade Certificadora – onde será verificado: **1)** se a chave pública realmente existe e se está associada àquela pessoa; **2)** se o respectivo certificado digital é válido, ou seja, se não foi por algum motivo (perda, comprometimento ou roubo de chave privada) revogado.

Com a confirmação positiva, tem-se a presunção de que o documento eletrônico provém da pessoa que o assinou (autoria), e que ele não foi alterado no seu percurso virtual (integridade). À presunção de autoria - e como decorrência dessa propriedade - agrega-se ainda um outro elemento constantemente enfatizado no jargão técnico das assinaturas digitais: é o denominado não-repúdio[8], que, a princípio, impedirá ao autor da declaração de vontade assinada digitalmente obter sucesso em eventual tentativa de negar a sua vinculação com o conteúdo do documento. A presunção aqui tratada não é absoluta, mas sim *juris tantum*, admitindo prova em contrário, caso em que o titular da chave de assinatura, para negar a autoria de determinada manifestação de vontade, terá o ônus de comprovar a utilização indevida de sua chave privada por outra pessoa mal-intencionada, como por exemplo, nos casos de coação ou de furto.

Vale referir que nos casos de perda, roubo ou furto da chave privada, o usuário tem o dever de comunicar imediatamente o fato ao terceiro de confiança que emitiu o seu certificado digital. Quanto a este aspecto, há exata similaridade com o que ocorre com o extravio de cartões de crédito ou talões de cheque. O usuário efetua a comunicação ao terceiro de confiança e o seu certificado digital passará a constar de uma lista de certificados revogados, as chamadas (LCR), que estão disponíveis na *internet* para o acesso de qualquer interessado.

Assim é, em apertada síntese, como funcionam as assinaturas digitais e os certificados digitais. No próximo ponto abordaremos as características, o funcionamento e o modelo da infra-estrutura implantada no Brasil para que as assinaturas digitais e os certificados digitais cheguem aos usuários finais.

3. INFRA-ESTRUTURA DE CHAVES PÚBLICAS E ICP-BRASIL

Como se referiu, os certificados digitais contém, entre outras informações, a chave pública do seu titular, ou seja, um dado fundamental para agregar segurança na tarefa de confirmação da identidade do usuário das assinaturas digitais, pois é por meio dela que o destinatário da mensagem verificará se esta foi realmente assinada com a chave privada do emissor, e, portanto, terá considerável garantia da autoria da declaração de vontade.

Uma infra-estrutura de chaves públicas (ICP) poderia ser conceituada como um sistema que tem por finalidade precípua, mas não exclusiva, atribuir certificados digitais (e conseqüentemente assinaturas digitais) a um universo de usuários. Em realidade, além de fornecerem estes documentos eletrônicos às pessoas naturais, aos órgãos e às entidades públicas e privadas, os entes que compõem uma ICP - os terceiros de confiança – desempenham a tarefa de gerenciar o ciclo de vida dos certificados, uma vez que a qualquer momento pode haver necessidade de revogar e emitir novos certificados, como no caso de comprometimento da chave privada de determinado titular de um certificado digital.

Portanto, uma infra-estrutura de chaves públicas tem o mesmo princípio de qualquer outra instalação estrutural posta à disposição da sociedade, qual seja o de prover um serviço que pode ser obtido por qualquer interessado.[9] O termo infra-estrutura de chaves públicas é tradução da expressão do inglês, *public-key infrastructure (PKI)*. Os norte-americanos bem souberam conceituar a expressão, partindo, primeiramente, da própria definição da palavra infra-estrutura. *Carlisle Adams* e *Steve Lloyd*, na obra *Understanding Public- Key Infrastructure*[10] enfatizaram que uma infra-estrutura se caracteriza por ser uma *pervasive substrate*, ou seja, uma fundação que dissemine algo para um amplo ambiente ou para um grande universo de interessados. Salientam que duas infra-estruturas comuns são a de comunicações eletrônicas (uma rede) e a de energia elétrica. Asseveram que o princípio de ambas é idêntico: a infra-estrutura existe para que qualquer usuário possa simplesmente acoplar-se a ela e dela fazer uso quando necessário.

As razões para que haja uma infra-estrutura que congregue número maior possível de pessoas e entidades é simples e facilmente perceptível. É justamente para que haja possibilidade de comunicação entre os entes envolvidos, ou, meramente, a possibilidade de pronto acoplamento. A infra-estrutura uniforme evita que sejam aplicadas soluções díspares por cada indivíduo.

Quanto a este ponto é elucidativa a explicação de *Adams* e *Lloyd*: "The pervasive security infrastructure is fundamentally the sensible architecture for many environments. This architecture avoids piecemeal, point-to-point, ad hoc, non-interoperable solutions, thereby introducing the possibility of manageable, consistent security across multiple applications and computing platforms. It is not difficult to imagine the chaos that would result from every pair of communicants running their own communications lines, or from every person running his/her own power generator at his/her own arbitrarily chosen voltage and current. Many facets of both ancient and modern society demonstrate that the uniformity and convenience offered by a well-designed, well-defined, pervasive infrastructure is worth the effort involved in the design and definition stages."[11]

Neste aspecto é que, em nível nacional, surge a importância da Infra-Estrutura de Chaves Públicas Brasileira, a ICP-Brasil, que foi instituída pela Medida Provisória nº 2.200, de 28 de junho de 2001, sendo que no momento vigora a Medida Provisória nº 2.200-2, de 24 de agosto de 2001[12]. A ICP-Brasil consiste numa estrutura composta por uma autoridade gestora de políticas, denominada de Comitê Gestor[13], pela AC-Raiz da ICP-Brasil, pelas Autoridades Certificadoras e pelas Autoridades de Registro.
O Comitê Gestor é uma espécie de conselho deliberativo que tem por atribuição principal coordenar a implantação e o funcionamento da ICP-Brasil, bem assim definir as normas técnicas a serem observadas neste âmbito. Essas diretrizes são editadas mediante resoluções[14], e, previamente, todas as matérias a serem apreciadas são analisadas pela Comissão Técnica Executiva (a COTEC) que assiste e dá suporte técnico ao órgão deliberativo.

As resoluções são aplicadas e cumpridas pela Autoridade Certificadora Raiz[15], que é o Instituto Nacional de Tecnologia da Informação, o ITI, autarquia federal vinculada à Casa Civil da Presidência da República.[16] As principais atribuições do ITI são as de auditar, credenciar e fiscalizar as Autoridades Certificadoras que postularem o seu credenciamento na ICP-Brasil para fornecer certificados digitais para os usuários finais. Cabe ressaltar, que por determinação da medida provisória, o ITI não fornece certificados digitais para os consumidores.[17] Suas funções são as de auditar, credenciar, certificar e fiscalizar as entidades, públicas e privadas, que quiserem fornecer ou comercializar os certificados digitais.[18]

O processo de credenciamento perante o ITI consiste num procedimento complexo que prevê pormenorizada auditoria das instalações, rotinas, documentos e práticas das entidades candidatas. Em suma, se o interessado provar ter capacidade técnica e organizacional para emitir certificados e para gerenciar listas de certificados revogados, se garantir a segurança da integridade e segurança de suas instalações, e outros tantos requisitos previstos nas normas, ele será credenciado pelo ITI e

passará a ter autorização para emitir certificados digitais – verdadeiras carteiras de identidade utilizadas no âmbito da internet - com o atributo da presunção de que trata o parágrafo primeiro do artigo 10 da MP 2.200-2: "As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiras em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 – Código Civil".

Vale observar que o credenciamento perante o Instituto Nacional de Tecnologia da Informação não é obrigatório para que as Autoridades Certificadoras possam emitir certificados digitais. A teor do disposto no parágrafo segundo do art. 10 da Medida Provisória: "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".
Portanto, as partes de um contrato, por exemplo, podem escolher a utilização de certificados digitais emitidos por entidades não credenciadas na ICP-Brasil. Essa diretriz adotada pela Medida Provisória, qual seja, a de não condicionar o início do funcionamento das Autoridades Certificadoras à prévia autorização do poder público, é a mesma prevista na Diretiva Européia 1999/93, que dispõe sobre o quadro legal comunitário para as assinaturas eletrônicas.

Com efeito, o artigo 3º da aludida diretiva diz que "1.Os Estados-Membros não devem sujeitar a prestação de serviços de certificação a autorização prévia." Todavia, o item 2 do mesmo artigo dispõe: "Sem prejuízo do disposto no nº1, os Estados-Membros podem introduzir ou manter regimes de acreditação facultativos que se destinem a obter níveis mais elevados na oferta dos serviços de certificação."
E é justamente esta lógica que foi seguida pela Medida Provisória, qual seja, a de estabelecer um processo de credenciamento voluntário perante o poder público, no caso perante a autarquia federal Instituto Nacional de Tecnologia da Informação, para aqueles que quiserem atingir os níveis mais elevados na oferta dos serviços de certificação.

Outra entidade que também faz parte da Infra-Estrutura de Chaves Públicas Brasileira é a Autoridade de Registro (AR). A Autoridade de Registro é a ponta inferior da cadeia, aquela que atinge o usuário final, recebendo as solicitações de emissão de certificados digitais. Uma das tarefas de grande relevância dentro de uma ICP, que é desempenhada pelas ARs, é a de identificar, mediante a presença física do indivíduo[19], os interessados em adquirir certificados digitais. Com efeito, caso não sejam tomadas todas as diligências cabíveis (exigência da presença física, atenta conferência da documentação apresentada no ato da identificação) corre-se o risco de atribuir um certificado digital a indivíduo criminoso que queira se passar por outra pessoa ou que simplesmente utilize falsa identidade para praticar atos ilícitos no meio virtual. Os prejuízos poderão ser enormes.

4. O MODELO ALEMÃO DE INFRA-ESTRUTURA DE CHAVES PÚBLICAS

O modelo de ICP adotado no Brasil não é uma invenção. Por ser uma infra-estrutura de chaves públicas, subentende-se de pronto que houve a adoção da criptografia assimétrica conjugada com a utilização da certificação digital, como soluções para os procedimentos de identificação e atribuição de autoria de mensagens e documentos nas comunicações virtuais.

Isso quanto à tecnologia adotada[20] [21]. Quanto à estruturação, o que caracteriza a ICP-Brasil é a presença de uma entidade de direito público, a autarquia federal Instituto Nacional de Tecnologia da Informação, no ápice da cadeia de certificação.

Mas também essa configuração não foi implantada somente no Brasil.

Na Europa, a Alemanha foi o primeiro país a editar uma lei específica sobre o tema. A *Signaturgesetz*[22], de 1º de agosto de 1997 introduziu as condições estruturais para a adoção das assinaturas eletrônicas (*Rahmenbedingungen für elektronische Signaturen*) naquele país. Já sob a égide desta lei, no seu parágrafo quarto, alínea 1, o legislador alemão previa a obrigatoriedade de os prestadores de serviços de certificação digital obterem uma licença perante o órgão público competente para que pudessem iniciar as suas atividades.[23]

Tendo em vista a superveniência da Diretiva Européia 1999/93 - que, conforme mencionado, estipulou que a atividade de certificação digital independeria da concessão de autorização prévia pelo poder público,[24] excepcionados os casos dos procedimentos de credenciamento voluntário, a serem implantados pelos Estados Membros para a obtenção de níveis de segurança mais avançados – o legislador alemão aboliu a exigência de autorização prévia estatal para todo e qualquer prestador de serviços de certificação.[25]

Isso foi levado a cabo com a edição da segunda *Signaturgesetz*, de 16.05.2001, que, todavia, manteve e conferiu ainda maior importância aos procedimentos de certificação credenciados (*akkreditierte Signaturverfahren*), ou seja, àqueles em que os interessados em atingir níveis mais altos de segurança na prestação de seus serviços, se submetem ao processo de credenciamento (*Akkreditierung*) perante o órgão regulador alemão, a Regulierungsbehörde für Telekommunikation und Post (RegTP), que desempenha papel idêntico ao do Instituto Nacional de Tecnologia da Informação no Brasil.
Estruturalmente, a RegTP difere um pouco do ITI, porquanto como o seu próprio nome sugere, é uma entidade reguladora das telecomunicações e do correio, e a operação da Autoridade Certificadora Raiz fica sob a responsabilidade de uma divisão deste órgão, denominada de divisão de assinaturas eletrônicas.

De 1998 até o presente[26], já foram credenciadas 23 Autoridades Certificadoras alemãs pela RegTP.[27] Entre os credenciados, encontram-se os correios alemão (Deutsche Post), diversas empresas, as entidades de classe dos advogados, as representações de consultores fiscais e etc. Na Europa, o modelo alemão é o mais

desenvolvido e o que, até o momento, mais longe andou na implementação da Diretiva 1999/93.[28]

As vantagens de uma ICP nacional com a presença de uma entidade pública na posição de supervisão do sistema são inúmeras. A primeira é que proporciona uma uniformidade de padrões técnicos e políticas implementadas[29], restando mais facilitada a interoperabilidade entre os usuários finais de titulares de certificados. Isso significa que os usuários, em regra, poderão acessar as aplicações que demandem a utilização de certificados digitais para a sua identificação com o emprego de certificado emitido por qualquer uma das Autoridades Certificadoras que fazem parte da infra-estrutura.[30] Tal característica certamente vem em benefício do consumidor, uma vez que, a princípio, não necessitará adquirir diversos certificados digitais para comprovar a sua identidade no meio virtual e assinar digitalmente.
Curiosamente, há que se ressaltar que nos Estados Unidos da América o desenvolvimento e a expansão das infra-estruturas de chaves públicas se deu de forma bastante desorganizada de sorte que hoje em dia são diversas as ICPs em funcionamento naquele país, com base tanto em iniciativas governamentais quanto em iniciativas privadas.

As razões desse fenômeno são diversas, sendo que um dos motivos principais é o fato de que a autonomia dos estados federados fez com que cada unidade da federação editasse a sua própria lei sobre assinaturas digitais e matérias afins, sem que houvesse uma harmonia principiológica permeando esses diplomas.

Todavia, cientes de que "PKI is no good if you are only talking to yourself"[31], os norte-americanos há alguns anos promoveram a iniciativa do projeto *Federal Bridge Certification Authority*, que tem por escopo fundamental viabilizar a intercomunicação entre os titulares de certificados digitais que adquiriram as suas chaves de Autoridades Certificadoras diversas. Em que pese os esforços, os próprios envolvidos no projeto têm reconhecido que a iniciativa se transformou numa "empreitada que tem sido marcada pelo lento progresso". [32]

Daí a razão de ser mais racional e de resultados certamente melhores a implementação, desde o princípio, de uma ICP nacional. Outro aspecto é que, havendo uma ICP mais abrangente, como são a brasileira e a alemã, torna-se bem mais viável e atraente a celebração de acordos internacionais de reconhecimento recíproco de certificados digitais, o que possibilitará transações eletrônicas internacionais mais seguras, entre empresas, e entre consumidores e empresas.[33]

Por outro lado, o processo de credenciamento prévio das entidades que tencionam fornecer assinaturas digitais imprime maior confiança e credibilidade ao sistema, pois tem-se uma garantia maior quanto aos procedimentos técnico-administrativos que serão empregados na atividade, restando, após o credenciamento e o início das operações, a possibilidade de fiscalização dos entes autorizados.

A doutrina alemã tem sido enfática ao caracterizar as vantagens dos procedimentos de criação de assinatura digital credenciados, quando comparados

com aqueles totalmente desregulados (*sonstige Signaturverfahren*) e que são oferecidos livremente no mercado. *Alexander Roßnagel*, professor de direito público da Universidade de Kassel, salienta, quanto ao sistema alemão: "Os prestadores de serviços de certificação credenciados são auditados antes de iniciarem seus serviços por órgãos de validação e de testes bem como pela autoridade de regulação (RegTP). A auditoria verifica se as exigências da lei de assinatura são integralmente cumpridas. Em condições normais, e de acordo com parágrafo décimo-primeiro, item 2, alínea 2, do decreto referente às assinaturas eletrônicas, os prestadores de serviços de certificação credenciados se submetem a uma nova auditoria, no mais tardar, a cada três anos. Como conseqüência, e conforme o parágrafo décimo quinto, item 1, alínea 4 da lei de assinatura, eles têm a faculdade de apresentar a qualquer momento 'a prova testada e aprovada da segurança' e podem utilizar o selo de qualidade referido no parágrafo décimo quinto, item 1, alínea 3 da lei, a fim de deixar claro no âmbito comercial o nível superior de segurança de suas assinaturas eletrônicas qualificadas."[34]

Christianne Rapp, em dissertação defendida sobre a matéria[35] perante a Ludwig-Maximilians-Universität München, ao comentar especificamente sobre o processo de credenciamento previsto no ordenamento jurídico alemão, assevera[36]: "O credenciamento (*Akkreditierung*) - assim como a licença prevista no parágrafo quarto, inciso 1, alínea 1 da lei de assinatura de 1997 - deve ser deferido quando o prestador de serviços de certificação provar que atende às exigências previstas na lei de assinatura e no decreto sobre assinaturas eletrônicas. Ao obter o credenciamento, é atribuído ao prestador de serviços de certificação um selo de qualidade (*Gütezeichen*) que é utilizado para informar a comprovação da verificação ampla da segurança técnica e administrativa dos certificados nos quais são baseadas as assinaturas eletrônicas. (...) O dispositivo previsto no parágrafo décimo quinto, alínea 1, da lei de assinatura se adequa à determinação do artigo 3º, alínea 2 da diretiva européia, referente aos sistemas de credenciamento voluntário. A auditoria prévia acerca das exigências legais serve para o incremento do nível dos serviços de certificação. É vedada uma lacuna de segurança entre o início das atividades do prestador de serviços de certificação e a primeira auditoria. Esse aspecto é de tamanha significação, tendo em vista que a *Signaturgesetz* não prevê a fiscalização sistemática dos prestadores de serviços de certificação não credenciados. Além disso, os credenciados são novamente auditados em determinados intervalos de tempo e nos casos de mudanças consideráveis em suas políticas de segurança, conforme determina o parágrafo décimo-quinto, inciso 1, alínea 3 da *Signaturgesetz*. De outra banda, com relação aos não credenciados, não foram previstas em lei quaisquer auditorias. (...) A identidade e a qualificação dos prestadores de serviços de certificação são então confirmadas por um órgão de alta competência (a RegTP), ficando assim mais robusta a confiança da parte que realiza um negócio jurídico eletrônico mediante o emprego de um certificado eletrônico qualificado, se esse certificado for expedido por um prestador de serviços de certificação credenciado."

A versão brasileira trilhou caminho plenamente justificável, e, além disso, bastante recomendável.

5. CONSIDERAÇÕES FINAIS

O desenvolvimento dos estudos da criptografia assimétrica possibilitou o seu emprego nas assinaturas digitais, que constituem, em conjugação com os certificados digitais, meio seguro e eficaz de identificação em ambientes virtuais bem assim de atribuição de autoria de documentos eletrônicos.

Uma infra-estrutura de chaves públicas (ICP) é um sistema que tem por finalidade principal atribuir certificados digitais aos indivíduos de determinado universo. A Infra-Estrutura de Chaves Públicas Brasileira, ICP-Brasil, instituída pela Medida Provisória nº 2.200-2 de 24 de agosto de 2001, implantou em nosso país um sistema que visa a disseminar os serviços de certificação digital para viabilizar comunicações e transações eletrônicas mais seguras.

O modelo dessa infra-estrutura, que tem abrangência nacional e funciona com base em padrões, normas, práticas e *standards* internacionais, inspira-se naquele adotado pela Alemanha, onde uma entidade pública, a Regulierungsbehörde für Telekommunikation und Post (RegTP), funciona como Autoridade Certificadora Raiz, e tem por funções precípuas credenciar e fiscalizar as Autoridades Certificadoras, bem como emitir os certificados digitais que essas necessitarão para desenvolver suas atividades. Pelo exame dos resultados obtidos nos diversos países europeus, conclui-se que o Brasil seguiu o caminho correto, ao optar por um sistema de Infra-Estrutura de Chaves públicas que tenha no ápice da cadeia de certificação uma entidade de direito público com a finalidade de credenciar e fiscalizar as operações das Autoridades Certificadoras que tencionem obter os níveis mais altos de segurança em suas operações.

ANEXO[37]

PAÍS	DIPLOMA LEGAL	POSSUI SISTEMA DE CREDENCIAMENTO VOLUNTÁRIO	AUTORIDADE DE SUPERVISÃO	AUTORIDADE RESPONSÁVEL PELO CREDENCIAMENTO
Alemanha	Signaturgesetz, de 23.05.2001	Sim, contando com 23 entidades credenciadas.	Reguliergunsbehörde für Telekommunikation und Post (RegTP)	Reguliergunsbehörde für Telekommunikation und Post (RegTP)
Áustria	Signaturgesetz, de 19.08.1999	Sim, contando com 2 entidades credenciadas.	Telekom-Control-Komission (RTR)	Telekom-Control-Komission (RTR)
Bélgica	Lei acerca das condições estruturais para as assinaturas eletrônicas, de 09.07.2001.	Ainda não, será implementado por decreto.	Ministério da Economia	Ainda não possui
Dinamarca	Lei nº 417, de 31.05.2000.	Sim, mas até o presente momento não foi credenciada nenhuma entidade.	Danish Tele Authority (DTA)	Ainda não possui
Espanha	Real Decreto-Ley 14, de	Sim, mas até o presente momento não foi	Secretaria General de Comunicaciones	Secretaria General de Comunicaciones do

	17.09.1999.	credenciada nenhuma entidade.	do Ministério da Ciência e Tecnologia.	Ministério do Fomento.
Finlândia	Ainda não implementou as determinações da Diretiva 1999/93.	Não	Ainda não possui	Ainda não possui
França	Lei nº 230, de 20.03.2001.	Sim	Direction Centrale de la Sécurite des Systèmes d'Information (DCSSI)	Comité Français d'Accréditation
Grécia	Decreto Presidencial nº 150/2001.	Ainda não possui.	National Telecommunications and Post Comission (EETT)	Ainda não possui.
Holanda	Electronic Signatures Act, contendo adaptação dos capítulos 3 e 6 do Código Civil à Diretiva 1999/93	Ainda não possui, o governo holandês criou uma PKI Task Force que deveria concluir os seus trabalhos até o final de 2002 para implantar a certificação digital no país.	Ainda não possui.	Ainda não possui.
Irlanda	Lei de Comércio Eletrônico de 2000.	Ainda não possui.	Será determinada pelo Ministério das Comunicações, Marinha e Recursos Naturais	Ainda não possui.
Itália	Decretos Presidenciais nº 445 de 28.12.2000 e nº 10, de 23.01.2002.	O processo de credenciamento deverá ser regulado por meio de regulamento.	AIPA (Autorità per l'informatica nella Pubblica Amministrazione)	Ainda não possui.
Luxemburgo	Lei de 22.03.2000, que criou Registro Nacional de Credenciamento e "Grand-Ducal Regulations de 01.06.2001 e de 28.12.2001.	Sim, até o presente momento foi credenciada uma entidade.	Office Luxembourgeois d'Accréditation et de Surveillance (OLAS), subordinado ao Ministério da Economia	Office Luxembourgeois d'Accréditation et de Surveillance (OLAS), subordinado ao Ministério da Economia
Portugal	Decreto nº 290, de 02.08.1999.	Está sendo implementado, mas até o presente momento não existem entidades credenciadas.	Instituto das Tecnologias da Informação na Justiça	Instituto das Tecnologias da Informação na Justiça
Reino Unido	Electronic Communications Act de 2000 e Electronic Signatures Regulations 2002	Ainda não foi implementado sistema de credenciamento pelo governo. A organização tScheme, formada por representantes da indústria, atua na	Secretary of State for Trade and Industry	Organização tScheme, formada por representantes da indústria.

		aprovação de prestadores de serviços de certificação.		
Suécia	Lei sobre Assinaturas Qualificadas de 01.01.2001.	Ainda não foi credenciada nenhuma entidade.	Agência Nacional Sueca de Correios e Telecomuniações (PTS)	Swedish Board for Accreditation (Swedac)

[1] *Introdução à Ciência do Direito*. Tradução Vera Barkow; revisão técnica Sérgio Sérvulo da Cunha. – São Paulo: Martins Fontes, 1999. p. XV.

[2] A palavra criptografia vem do grego e significa escrita oculta. O Dicionário Aurélio a conceitua como "a arte de escrever em cifra ou em código".

[3] *Contratos no Código de Defesa do Consumidor*. 3.ed. São Paulo: Editora Revista dos Tribunais, 2002. p.99

[4] *Code and other Laws of Cyberspace*. Basic Books, New York, 1999. p.28.

[5] A MP 2.200-2, em virtude do art. 2º da Emenda Constitucional nº 32, de 11.09.2001, pemanece em vigor até que medida provisória ulterior a revogue explicitamente ou até que seja deliberada definitivamente pelo Congresso Nacional.

[6] *O livro dos códigos*; tradução de Jorge Calife. 2ª ed. Rio de Janeiro: Record, 2002, p. 26. Vale referir trecho da obra: "César descreve como enviou uma mensagem para Cícero, que estava cercado e prestes a se render. Ele substituiu as letras do alfabeto romano por letras gregas, tornando a mensagem incompreensível para o inimigo. César descreve a dramática entrega da mensagem: o mensageiro recebeu instruções para que, se não pudesse se aproximar, jogasse uma lança com a mensagem amarrada por uma tira de couro, dentro das fortificações do campo...Com medo, o gaulês arremessou a lança como fora instruído. Por acaso a arma encravou-se em uma torre e passou dois dias sem ser vistas pelos nossos soldados, até que, no terceiro dia, um soldado a viu, retirando-a e entregando a mensagem para Cícero. Ele a leu e depois recitou em voz alta para a tropa em formação, trazendo grande alegria para todos."

[7] Conforme *Simon Singh* em *O livro dos códigos*, p. 305.

[8] Os termos não-repúdio e repúdio, a princípio, são estranhos ao direito contratual dos países de tradição romano-germânica. *José Carlos Moreira Alves*, na obra *Direito Romano*, localiza a existência do instituto do *repúdio* na época dos imperadores cristãos, quando a expressão designava, no direito de família, a ruptura unilateral do casamento. Salienta o autor: "Assim, Constantino – C. Th. 3, 16, 1 – admitiu, em 331 d. C., que o marido ou a mulher pudessem repudiar o outro cônjuge quando ocorressem certas causas (por exemplo, se a mulher fosse declarada culpada por adultério ou por envenenamento: ou, com relação ao marido, se réu de homicídio, envenenamento ou violação de sepulcro." *Direito Romano*, vol. II, 6ª ed., Rio de Janeiro: Forense, 1999, p. 316. *Warwick Ford* e *Michael S. Baum*, na obra *Secure Electronic Commerce – Building the Infrastructure for Digital Signatures and Encryption* observam que nos países da *common law* o termo *repudiation* está associado ao direito contratual. Num contexto, refere-se ao direito de uma parte negar "validity" ou "enforceability" de um contrato em virtude de uma multiplicidade de causas, como fraude, coação e incapacidade de uma das partes. Noutro contexto pode significar a negativa indevida de uma parte em cumprir com as suas obrigações estipuladas em contrato válido e eficaz. Por outro lado, o termo *non-repudiation* já faz parte de decisões judiciais nas cortes norte-americanas há mais de quinze anos, apenas com o significado de que uma parte não negou ou não tem a intenção de negar os termos de um contrato ou de uma declaração de vontade. Até hoje, segundo afirmam, o termo *non-repudiation* jamais foi empregado pela jurisprudência norte-americana no sentido que lhe empresta a área da segurança da informação, qual seja o de atributo de um meio de comunicação específico ou de um mecanismo de segurança da informação, que serve para impedir que a parte negue que uma mensagem específica foi recebida ou enviada. Os autores dividem as espécies de não-repúdio em não-repúdio de origem (que protege o receptor da mensagem, indicando que a mensagem efetivamente originou-se do declarante), não-repúdio de envio (que protege o declarante, comprovando que a mensagem foi efetivamente transmitida, e não-repúdio de recebimento (que também protege o declarante, comprovando que a mensagem foi efetivamente recebida pelo destinatário). Vide obra citada, p. 333-343.

[9] A definição do vocábulo "infra-estrutura" do Dicionário Aurélio, no que toca à área de urbanismo, é a mais adequada à acepção ora enfocada, *in verbis*: "Numa cidade, o conjunto das instalações necessárias às

atividades humanas, como rede de esgotos e de abastecimento de água, energia elétrica, coleta de águas pluviais, rede telefônica e gás canalizado."

[10] Obra cujo subtítulo é *Concepts, Standards, and Deployment Considerations*. Indianapolis: New Riders, 1999. p. 27.

[11] Ob.cit. p.27-28.

[12] Vide nota de rodapé nº 5, *supra*.

[13] O detalhamento da estrutura e das competências do Comitê Gestor estão nos arts. 3º e 4º da Medida Provisória nº 2.200-2. Outras disposições sobre o Comitê Gestor e sobre a Comissão Técnica Executiva encontram-se no Decreto nº 3.872, de 18 de julho de 2001.

[14] Todas as resoluções do Comitê Gestor estão disponíveis no sítio do Instituto Nacional de Tecnologia da Informação, em http://www.iti.gov.br.

[15] Vide arts. 5º, 13 e 14 da Medida Provisória nº 2.200-2.

[16] O art. 2º do Decreto nº 4.036, de 28.11.2001, alterou o art. 12 da Medida Provisória nº 2.200-2 e transferiu a vinculação do Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e Tecnologia para a Casa Civil da Presidência da República. Esta vinculação foi mantida pelo Decreto nº 4.566, 01.01.2003, vide inciso XXIV do anexo.

[17] É o que estabelece o parágrafo único do art. 5º da Medida Provisória nº 2.200-2.

[18] O Instituto Nacional de Tecnologia da Informação já credenciou seis entidades como Autoridades Certificadoras. São elas: Autoridade Certificadora Presidência da República, Autoridade Certificadora Serpro, Autoridade Certificadora Serasa, Autoridade Certificadora Certisign, Autoridade Certificadora Secretaria da Receita Federal e Autoridade Certificadora Caixa Econômica Federal. Vide essas informações em www. iti.gov.Br.

[19] O art. 7º da Medida Provisória nº 2.200-2 assim dispõe sobre as Autoridades de Registro (AR): "Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações."

[20] Bruce Schneier assim fala sobre a criptografia: "A criptografia é fantástica. Em certo nível, ela é um punhado de matemática complicada. São criptógrafos projetando transformações matemáticas ainda mais complicadas e criptoanalistas respondendo com maneiras ainda mais criativas de desmanchar a matemática. (...) Em outro nível, a criptografia é uma tecnologia básica do ciberespaço. (...) É a tecnologia que nos permite montar a segurança no ciberespaço". *Segurança.com: segredos e mentiras sobre a proteção na vida digital; p. 93*. Tradução de Daniel Vieira. Rio de Janeiro: Campus, 2001.

[21] Acerca da relativização do mito do princípio da neutralidade tecnológica, vide o artigo de Jürgen Schwemmer: *Lösungen und Probleme – Ein langer Weg zur Interoperabilität (mögliche Erklärungen)* disponível em, em alemão, no sítio www.regtp.de, clicar em Elektronische Signatur, e, após, em Veröffentlichungen. Neste texto o autor salienta que a predominância da vontade política da diretiva européia 1999/93 (que instituiu o quadro legal para as assinaturas eletrônicas) de ser neutra tecnologicamente, restou por estabelecer especificações técnicas fracas e insuficientes. Salienta ainda que interoperabilidade e neutralidade tecnológica são antagônicas. O posicionamento deste respeitável autor é francamente contrário à neutralidade tecnológica.

[22] Texto da lei disponível em www.regtp.de.

[23] Diz o dispositivo: "Der Betrieb einer Zertifizierungsstelle bedarf einer Genehmigung der zuständigen Behörde. Diese ist auf Antrag zu erteilen."

[24] Conforme o artigo 3º, item 1.

[25] É o que dispõe o item 1 do parágrafo quarto da nova *Signaturgesetz*: "Der Betrieb eines Zertifizierungsdienstes ist im Rahmen der Gesetze genehmigungsfrei."

[26] Até fevereiro de 2003, quando foi concluído este artigo.

[27] Dados obtidos em www.regtp.de

[28] Em anexo a este trabalho mostramos um quadro com o estado de implementação atual em cada país da União Européia.

[29] Dois documentos básicos da maioria das ICPs são a declaração de práticas de certificação (DPC) e a política de certificado (PC). Trata-se de documentos bastante extensos. A DPC expõe as regras operacionais das atividades de determinada Autoridade Certificadora. Ela descreve o "como" funciona a entidade. Entre tantas outras informações, nela estão contidos os procedimentos gerais para identificação dos usuários dos certificados digitais, obrigações das partes envolvidas, padrões técnicos referentes às versões das listas de certificados revogados, etc. As descrições do documento PC respondem a pergunta "o que" e contêm detalhes mais específicos sobre o certificado digital emitido (informações contidas no

certificado, formato padrão, tamanho das chaves criptográficas associadas ao certificado, etc.) já que uma Autoridade Certificadora poderá emitir diversos tipos de certificados.

[30] Um exemplo prático dessa realidade é o aplicativo da Secretaria da Receita Federal, o Receita 222, de que trata a Instrução Normativa 222, de 11 de outubro de 2002 (vide em www.receita.fazenda.gov.br), que, em sua fase inicial, já permite ao contribuinte consultar os seus dados pessoais que constam da base de dados da Receita Federal e emitir certidões negativas de débitos mediante a identificação do interessado com o emprego de certificado digital emitido por qualquer entidade credenciada na ICP-Brasil. No futuro bem próximo, as declarações de renda serão entregues com a aposição de assinatura digital, o que incrementará a segurança na prática deste ato. Outros tantos serviços como o acompanhamento da tramitação de processos fiscais, parcelamento de débitos, compensação de créditos e cadastramento eletrônico de procurações serão disponibilizados pelo sistema.

[31] São as exatas palavras proferidas por Peter Alterman, Diretor de operações do Escritório de pesquisa extra-mural do Instituto Nacional de Saúde dos Estados Unidos da América. Declaração contida no artigo PKI at the crossroads, de autoria de Jennifer Jones, capturado, em http://www.fcw.com/fcw/articles/2002/0624/tec-pki-06-24-02.asp, no dia 04.07.2002.

[32] Idem anterior. O texto original diz o seguinte: "Years in the works, a federal effort to link the public-key infrastructures (PKIs) of agencies has proved quite an undertaking and has been marked by that appears to be rather slow progress".

[33] O art. 4º, inciso VII, da MP 2.200-2, determina que compete ao Comitê Gestor da ICP-Brasil "identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP -Brasil, observado o disposto em tratados, acordos ou atos internacionais;".

[34] No artigo *Rechtliche Unterschiede von Signaturverfahren*, publicado na Revista Multimedia und Recht, vol. IV, 2002, p. 215-222. Trecho traduzido livremente pelo autor deste artigo.

[35] *Rechtliche Rahmenbedingungen und Formqualität elektronischer Signaturen*, München: Beck, 2002.

[36] Op. cit. p. 61-62. Tradução livre do autor deste artigo.

[37] Fonte: estudo denominado *The implementation of the european directive on electronic signatures, status report*, de novembro de 2002, distribuído no evento Putting e-signatures into practice – (the legal issues), realizado pelo European Forum for Electronic Business (EEMA), em Bruxelas, Bélgica, nos dias 25 e 26 de novembro de 2002.