Novos modelos tecnológicos para o acontecimento do contrato eletrônico: assinatura e certificação digitais

New technological models for the electronic contract: signature and digital certification

Roberto H. Pôrto Nogueira
Advogado. Professor da Faculdade Pitágoras e da PUC Minas. Mestre em Direito Privado pela PUC Minas. Especialista em Direito Tributário pela Faculdade de Direito Milton Campos.
e-mail: portonogueira@gmail.com

Rodrigo Almeida Magalhães
Advogado. Professor da PUC Minas. Doutor e Mestre em Direito pela PUC Minas. Coordenador do curso de Direito da PUC Minas em São Gabriel.

Resumo: Este trabalho visa a apresentar o modo como a certificação e assinatura digitais no Brasil influenciam os contratos e, especialmente, o contrato eletrônico, de modo a buscar soluções no Direito dos Contratos na atualidade. Desse modo, o trabalho propõe a identificação de novos modelos tecnológicos, postos ao Direito dos Contratos, bem como sua compreensão, para promover um ambiente favorável e uma estrutura jurídica direcionada ao acontecimento do contrato eletrônico.
Palavras-chave: 1. certificação digital. 2. assinatura digital. 3. contrato eletrônico. 4. princípios e interpretação. 5. novos requisitos de validade. 6. Direito dos Contratos.

Abstract: This work aims at presenting the way digital certificate services and digital signature in Brazil influenced the contracts and specially the electronic contract, in order to search for solutions in the Law Contract Subject at this present time. This way, this paper considers the identification of new technology tools available to Law Contract Subject, as well as their comprehension, to provide a favorable environment and appropriated legal structure target to electronic contract.
Keywords: 1. digital certificate services. 2. digital signature. 3. electronic contract. 4. principles and interpretation. 5. new requirements of enforceability. 6. law contract subject.

1. Considerações iniciais

O avanço tecnológico não mais admite as tradicionais definições que entendem que o contrato, enquanto produto final, "exterioriza-se por intermédio de uma ou mais folhas de papel, impressas ou escritas, assinadas pelas partes, que descrevem regras que irão disciplinar os interesses patrimoniais das partes a respeito de um determinado bem." (ROCHA, 2002, p. 49).

Atualmente, a socialização do meio eletrônico de contratação e das ferramentas disponibilizadas à garantia da conclusão eficiente do contrato eletrônico é discutida pela comunidade jurídica, e até mesmo implementada, sem que os atores desse novo cenário compreendam os novos modelos.

Ademais, tais novos modelos impõem, ao profissional do Direito, a tarefa de enfrentar os desafios evolutivos do Direito dos Contratos, em especial do contrato eletrônico[1]. Adota-se a definição de Ricardo L. Lorenzetti (2004, p. 285), para quem o contrato eletrônico "caracteriza-se pelo meio empregado para a sua celebração, para seu cumprimento ou para sua execução, seja em uma ou nas três etapas, de forma total ou parcial". Carlos Alberto Rohrmann (2005, p. 58) afirma que o contrato eletrônico é "o negócio jurídico bilateral que tem no meio virtual o suporte básico para sua celebração".

A abordagem, pelo Direito, desses novos paradoxos evolutivos da tecnologia informática é de grande relevância, para a compreensão do cenário da contratualidade e de sua documentação, nos dias atuais.

2. Novos modelos: criptografia, assinatura e certificação digitais

2.1. Criptografia

A criptografia possibilita que uma mensagem seja transmitida de forma codificada entre emissor e receptor, de modo ininteligível a estranhos ou interceptores. Para tanto, a chave para decodificação deve ser convencionada entre as partes e, usualmente, demanda a mantença de determinado segredo. A chave pode ser criada pelas partes ou elaborada por um programa de computador, sendo uma espécie de código.

É comum a identificação da utilização da criptografia com propósitos militares, para envio de mensagens secretas. Há indícios de que era conhecida no Egito, na Mesopotâmia (MENKE, 2005, p. 43), na Índia e na China. De acordo com a doutrina que se dedica ao resgate histórico da utilização da técnica, Júlio César utilizava um método para cifrar suas correspondências na Roma antiga, sendo que cada letra do texto era substituída pela terceira letra subsequente no alfabeto. Registre-se que o primeiro livro

[1] Parte da doutrina procede à diferenciação entre contrato informático e contrato eletrônico. Para Mariliana Rico Carrillo (2003, p. 101-104), os contratos informáticos têm como objeto um bem ou serviço informático, ao passo que os contratos eletrônicos são os que se realizam por meio de um sistema eletrônico de transmissão de dados, podendo, contudo, seu objeto, versar sobre qualquer prestação. Assim, para definição do contrato eletrônico, importa que algum elemento eletrônico tenha sido utilizado no processo de manifestação e processamento da vontade. O contrato eletrônico assim se identifica em razão do meio de contratação.

publicado sobre a habilidade de escrever mensagens secretas foi desenvolvido no início da Idade Moderna *Poligrafia*, publicado em 1510, pelo alemão Johannes Trithemius. Até a Primeira Guerra Mundial, as mensagens eram criptografadas de modo manual. Na Segunda Guerra Mundial, os alemães produziram a primeira máquina (eletromecânica) capaz de criptografar, conhecida como *ENIGMA* (MARCACINI, 2002, p. 10-13). Desse modo, por meio da tecnologia da criptografia, é possível codificar uma mensagem e, em momento posterior, decodificar.

Hoje, duas são as principais técnicas empregadas para criptografar: a criptografia simétrica ou convencional (de chave privada) e a criptografia assimétrica (de chave pública), sendo que a segurança da criptografia, em qualquer de suas modalidades, relaciona-se diretamente com a consistência do algoritmo utilizado no processo e do tamanho da chave (MARCACINI, 2002, p. 40).

2.2. Criptografia simétrica

Como qualquer criptografia, a chave representa um código que, em conjunto com um algoritmo, permite revelar o conteúdo da mensagem. O algoritmo é espécie de fórmula utilizada para cifrar. À mensagem aplica-se a fórmula, e somente o conhecimento de uma das incógnitas da fórmula (algoritmo) possibilita o alcance do resultado válido.

A criptografia simétrica baseia-se na simetria das chaves, ou seja, a chave utilizada para criptografar é a mesma utilizada para decriptar. Daí o porquê de ser chamada de criptografia de chave privada: a chave jamais poderá ser pública, sob pena de qualquer um poder decriptar a mensagem, ter acesso a seu conteúdo e, eventualmente, comprometer sua integridade e autenticidade. Significa que os interlocutores compartilham as chaves para cifrar e decifrar a mensagem (MENKE, 2005, p. 46).

O problema da criptografia simétrica é, portanto, que a chave privada deve ser compartilhada, de modo que se coloca em xeque a confiabilidade dos demais portadores e a transferência do algoritmo de segurança, que pode, eventualmente, ser interceptado. A técnica da criptografia simétrica é mais sujeita à quebra de sigilo.

2.3. Criptografia assimétrica

Foi proposta em 1976, por Whitfield Diffie, Martin Hellman e Ralph Merkle, em artigo intitulado "New directions of cryptografy" (MARCACINI, 2002, p. 24; MENKE, 2005, p. 46).

A criptografia assimétrica tem esse nome em razão da assimetria entre seu par de chaves. Esse par de chaves é gerado por um programa de computador, a partir do emprego de complexos cálculos matemáticos, de modo que "possam ser encontrados dois números que sejam de tal forma relacionados entre si, que sirvam um como chave pública e o outro como chave privada." (MARCACINI, 2002, p. 27).

As chaves são criadas em forma de uma combinação de letras e números bastante extensa. As chaves serão tão mais seguras quanto maiores forem. Ademais, elas complementam-se e atuam em conjunto (MENKE, 2005, p. 46-47).

Logo, as chaves são diferentes, mas necessariamente correspondentes entre si. Uma delas é publicada (a chave pública), enquanto a outra é mantida sob guarda e exclusivo controle do signatário. Ambas as chaves podem ser utilizadas para criptografar ou decriptar. Porém, a mesma chave não decripta o arquivo criptografado por ela mesma.

Não há necessidade de envio de chave privada, o que reduz sobremaneira o risco de interceptação e posse por terceiros. Quer dizer que o portador do par de chaves assimétricas deve manter uma delas sob o mais absoluto sigilo e publicar a outra, sendo que uma determinada pessoa interessada em enviar mensagem criptografada pode buscar a chave pública em um banco de dados disponibilizado por determinada instituição ou até mesmo pode recebê-la de seu proprietário, por correio eletrônico ou envio automático, quando do acesso de seu sítio[2] pessoal na internet.

Utilizada a chave pública para criptografar, a mensagem pode ser enviada com segurança. A mesma chave, a que é pública, não é capaz de decriptar a mensagem cifrada por ela mesma. Somente o proprietário, com a sua chave privada, aquela mantida sob sua custódia exclusiva, será capaz de proceder à decodificação. Assim, é importante salientar que a chave privada é de único e exclusivo domínio do titular da assinatura.

A criptografia assimétrica é desenvolvida a partir de funções matemáticas irreversíveis, ou seja, embora teoricamente reversíveis, na prática são irreversíveis em consideração ao tempo necessário para tanto (a reversão, por meio da técnica do erro e acerto, demoraria mais de dez anos para fatorar o número gerado pela utilização de uma chave).

[2] Sítio, também comumente chamado de *site* ou *home page*, significa, literalmente, lugar. "Na internet, a palavra *site* é utilizada para designar um lugar virtual, situado em algum endereço eletrônico da *World Wide Web.*" (MARCACINI, 2002, p. 192).

Desse modo, quando ocorre a criptografia do arquivo, é utilizada tal função irreversível, denominada *hash.* O resultado da aplicação da função *hash* (digestora) à mensagem é o resumo da mensagem, ou seja, a transformação do arquivo em uma sequência de dígitos ininteligíveis e de tamanho fixo. Qualquer mensagem, independentemente do tamanho, é condensada em tamanho fixo (MENKE, 2005, p. 47). O resumo da mensagem é utilizado no algoritmo[3], juntamente com a chave pública ou privada, gerando a assinatura digital.

É exatamente em razão de a função matemática ser irreversível, que a mesma chave não consegue reverter a operação, de maneira a decriptar a mensagem. Por outro lado, conhecendo o segredo para reverter a função (a outra chave do par), a decodificação da mensagem faz-se possível. A confidencialidade pode, assim, ser obtida.

Augusto Tavares Rosa Marcacini (2002, p. 35) observa, acerca da função digestora: "Como a *hash function* é uma função matemática sem retorno (*one-way function*), não é possível realizar uma operação inversa para, a partir do 'resumo da mensagem', chegar-se à mensagem que o produziu".

O professor Carlos Alberto Rohrmann, sobre a função *hash,* explica:

> Retornando à assinatura digital, pode-se dizer que ela é um identificador acrescido a determinado pacote de dados digitais que é gerado por um programa de computador que se vale de uma função *hash,* cujas entradas são uma chave privada de assinatura do assinante mais o próprio arquivo eletrônico a ser digitalmente assinado, e que só será decodificado por uma chave pública associada àquele assinante e garantida por uma autoridade certificadora (AC), que faz a identificação das partes e a posterior certificação, emitindo certificados de autenticidade do par de chaves utilizado. (ROHRMANN, 2005, p. 77).

O par de chaves é gerado pelo próprio usuário, mediante a utilização de um software apropriado, preparado para realizar as operações matemáticas necessárias à geração das chaves e aplicação das fórmulas ou funções matemáticas. Augusto Tavares Rosa Marcacini esclarece:

> [...] Tanto as operações matemáticas da *fórmula* como a escolha do par de chaves são feitos a partir de complexos cálculos. [...] É sempre oportuno destacar que o fato de a crip-

[3] "Sequência finita de regras, raciocínios ou operações que, aplicada a um número finito de dados, permite solucionar classes semelhantes de problemas (p.ex.: algoritmo para a extração de uma raiz cúbica); processo de cálculo; encadeamento das ações necessárias ao cumprimento de uma tarefa; processo efetivo, que produz uma solução para um problema num número finito de etapas; mecanismo que utiliza representações análogas para resolver problemas ou atingir um fim, noutros campos do raciocínio e da lógica; conjunto das regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas" ("Algoritmo", *Dicionário Houaiss*, 2001).

> tografia moderna exigir o emprego de fórmulas matemáticas complexas não é, contudo, um óbice ao seu uso pela população em geral. Há diversos programas de computador que realizam automaticamente todas estas operações mirabolantes e de forma transparente para o usuário. Não lhe é necessário, portanto, fazer qualquer operação, sequer de aritmética elementar... O par de chaves, por sua vez, é também gerado pelo programa a partir de sofisticados cálculos, para que possam ser encontrados dois números que sejam de tal forma relacionados entre si, que sirvam um como chave pública e outro como chave privada. (MARCACINI, 2002, p. 27).

Esse par de chaves assimétricas é o empregado para assinar digitalmente um documento eletrônico, conforme sistemática explicada a seguir.

2.4. Assinatura eletrônica

A assinatura é tradicionalmente compreendida e explicada como sendo um nome ou marca firmada na parte inferior de um escrito, designando autoria ou aprovação de seu conteúdo. A etimologia remete à ideia de deixar sinal, chancelar, ratificar ou reconhecer ("Assinatura", *Dicionário Houaiss*, 2001).

Antes da explosão e da desenvolvimento massivo da tecnologia informática, assinatura era tida quase que somente em sua acepção de forma gráfica aposta manualmente em documento físico.

O problema da assinatura aparece quando o escrito não mais se disponibiliza materializado para a aposição do nome ou marca em sua parte inferior. Na verdade, a assinatura presta-se a proceder à identificação da autoria, procedência ou autenticidade de determinado conteúdo declarativo. Logo, a assinatura é qualquer marca que possa identificar o autor ou, ainda, representar a ratificação do conteúdo de um documento específico.

Uma definição mais ampla e em consonância com o paradigma tecnológico é a de Ricardo L. Lorenzetti (2004, p. 101), para quem a assinatura é tão somente "um meio de vincular um documento ao seu autor". Esse conceito incorpora não somente a assinatura manuscrita, mas também, a assinatura eletrônica e a sua espécie assinatura digital. Estas duas últimas demandam maior atenção.

É comum a indistinção entre assinatura eletrônica e assinatura digital. A diferença é importante para a compreensão e possibilita o alcance de alguma precisão conceitual.

A assinatura eletrônica é gênero. Pertencem a este grupo: as senhas, os códigos de acesso em geral, as técnicas biométricas, as assinaturas escritas digitalizadas ou fotografadas para reprodução em larga escala, as pranchetas eletrônicas de sensibilidade

e reconhecimento da assinatura manuscrita, os meios fonográficos de reconhecimento de voz, a assinatura digital, dentre outros.

2.5. Assinatura digital

Talvez em razão do desenvolvimento tecnológico desordenado, a sociedade passou a considerar como assinatura digital toda aquela que não ocorresse em documento havido em suporte tangível. E por esse motivo, grande parte dos estudos teve que dessecar as definições de documento e documentação, para reconstruir seus contornos, ascendendo a aspecto nuclear o conteúdo documental, eventualmente havido em suporte tangível ou não. Ricardo L. Lorenzetti (2004, p. 129) conclui que o documento digital comporta-se no gênero documento, por se constituir de declaração de vontade e suporte, ainda que digital (*bits*).

Os sinais contidos em documento eletrônico ou digital podem representar assinaturas eletrônicas, sem, contudo, integrarem a espécie da assinatura digital.

A assinatura digital, como espécie do gênero da assinatura eletrônica, surge como resposta do próprio sistema da Tecnologia à sociedade, em decorrência de novos paradoxos inseridos por seu próprio desenvolvimento. Isso levou ao resgate e preenchimento do conteúdo semântico de assinatura, supra.

Ao presente trabalho compete a análise especial da assinatura digital, que abrange a assinatura que transcende a simples codificação de acesso ou identificação, mas que também emprega alguma tecnologia avançada para atingir, em seus mais diversos aspectos, a equivalência funcional com a assinatura tal qual tradicionalmente concebida. Normalmente, assim como ocorre no Brasil, a assinatura digital é relacionada à utilização da tecnologia da criptografia assimétrica, já explanada. Fabiano Menke bem explica a distinção em exame. Afirma que:

> [...] sob a denominação de assinatura eletrônica inclui-se um sem-número de métodos de comprovação de autoria empregados no meio virtual. A assinatura digital, desta feita, consiste em espécie do gênero assinatura eletrônica, e representa um dos meios de associação de um indivíduo a uma declaração de vontade veiculada eletronicamente dentre outros diversos existentes. [...] Enquanto o termo assinatura eletrônica abrange o leque de métodos de comprovação de autoria mencionados, e até mesmo outros que possam vir a ser criados, a palavra "assinatura digital" refere-se, exclusivamente, ao procedimento de autenticação baseado na criptografia assimétrica. (MENKE, 2005, p. 42).

Algumas distinções são, portanto, essenciais à compreensão da assinatura digital em sentido estrito, tal qual importa à problemática de enfrentamento proposto no presente trabalho.

Primus, não há de se confundir assinatura digital com o sinal gráfico manualmente produzido, copiado eletronicamente e aposto ou impresso em novo documento (assinatura digitalizada); tampouco, com a senha de acesso, hoje amplamente utilizada em transações eletrônicas. Tais senhas, a despeito de possibilitar algum controle, não podem ser, sequer minimamente, consideradas seguras em comparação à utilização da técnica da criptografia assimétrica. Essa última técnica é da essência da assinatura digital (ROHRMANN, 2005, p. 68).

A assinatura digital é, pois, o resultado de uma operação matemática, que, necessariamente, empregue a técnica da criptografia assimétrica (MARCACINI, 2002, p. 32). É nessa direção o entendimento de Augusto Tavares Rosa Marcacini:

> A assinatura digital, enfim, é o resultado de uma complexa operação matemática, que utiliza uma função digestora e um algoritmo de criptografia assimétrica, e em, como variáveis, a mensagem a ser assinada e a chave privada do usuário (ambas vistas pelo computador como números) (MARCACINI, 2002, p. 37).

Cumpre dizer que a assinatura digital não se confunde com a chave privada ou pública pertinentes à criptografia assimétrica.

Vale esclarecer: a mensagem, por meio do emprego de uma função irreversível, é transformada em sequência de dígitos de tamanho invariável. A essa sequência de dígitos é dado o nome de resumo da mensagem. Esta série digital é novamente submetida a uma fórmula, da qual tomará parte uma das chaves. O arquivo resultante desse processo é que constitui a assinatura digital. O documento digital constituído pelo resumo da mensagem somente será obtido após a operação inversa de decodificação, quando algum conteúdo inteligível puder ser abstraído.

2.6. Certificação digital

É exatamente na seara da autenticidade, ou seja, da garantia de procedência subjetiva, que se insere o papel das autoridades certificadoras[4] e dos certificados digi-

[4] Quando empregadas letras iniciais maiúsculas para 'autoridades certificadoras' e 'autoridades de registro', refere-se a autoridades credenciadas à infra-estrutura nacional oficial de chaves públicas.

tais. As autoridades certificadoras, por meio de certificados digitais, pretendem possibilitar a atribuição de ato jurídico específico a pessoa determinada.

A autoridade certificadora é responsável pela divulgação da chave pública, pela certificação da titularidade da referida chave por meio de um certificado, que tem um prazo de validade, podendo certificar outras informações que o signatário julgar necessárias. Ana Carolina Horta Barreto (2002, p. 39) pontua: "De modo a assegurar o seu uso confiável e a sua validade legal, bem como combater a fraude, a assinatura eletrônica depende de técnicas confiáveis de geração, armazenamento e certificação, que garantam sua autenticidade".

Desse modo, a certificação digital relaciona-se com o certificado digital que, precipuamente, registra a chave pública em nome de um titular e atesta que tal chave pública é, efetivamente, de quem a exibe. Assim, a autoridade certificadora garante a relação entre a identidade da pessoa e a chave pública por ela exibida ou ostentada em seu nome (BARRETO, 2002, p. 39).

O certificado é uma espécie de confirmação, lançada por uma terceira parte, em relação à chave pública de uma outra pessoa que assinou digitalmente um documento eletrônico (ROHRMANN, 2005, p. 76). O certificado é explícito quanto a seu objeto e validade.

Fabiano Menke (2005) salienta que os certificados digitais são emitidos com base em padrões estabelecidos em normas internacionais, sendo quem destaca os padrões ITUX.509 ou ISO 9594-8[5]. O objetivo desses padrões é garantir a interoperabilidade, que será explanada adiante. Vale trazer a definição de Fabiano Menke, acerca de certificado digital:

> O certificado digital é uma estrutura de dados sob a forma eletrônica, assinada 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, só que um certificado é emitido com prazo de validade determinado (MENKE, 2005, p. 49).

Ricardo L. Lorenzetti (2004, p. 139) destaca a função primordial do certificado digital, como sendo a de possibilitar a identificação do signatário de um documento eletrônico. Por outro lado, salienta que o certificado digital deve permitir a constatação

[5] Em nota de rodapé, Fabiano Menke (2005, p. 49) aponta que a sigla ITU diz respeito ao *Institute of Telecommunication Union,* organização internacional que possui como um de seus objetivos centrais a padronização no campo das telecomunicações, assim como a ISO, *International Organization for Standardization.*

de seu período de vigência, além de eventual revogação, nome do emitente, dentre outras informações.

De fato, há prazo de validade para os certificados digitais. Trata-se de uma medida de segurança, de modo que, quanto melhor e mais seguro o meio de armazenamento da chave privada do usuário, maior será o prazo de validade de seu certificado digital.

A autoridade certificadora (AC), por sua vez, é um terceiro garantidor de determinados dados ou identidade. A autoridade de registro (AR), ligada à autoridade certificadora, é encarregada das atividades de cadastro das titularidades e chaves públicas correspondentes.

A autoridade certificadora, que mantém atualizada e disponível uma "Lista de Revogação de Certificados" ou LRC, deve se abster de ter acesso à chave privada (BRASIL, MPV n. 2.200-2, 2001).

A assinatura digital comporta não somente o processo de aplicação da tecnologia criptográfica assimétrica no resumo do documento, como também o emprego de um certificado digital de autenticidade da chave pública, devidamente gerado, emitido e submetido aos regramentos normativos contidos na medida provisória em referência.

A chave privada pode ser armazenada no disco rígido do computador, em *smart cards*, *tokens* ou qualquer outro dispositivo apropriado. A manutenção da chave em dispositivo exclusivo para esta finalidade, certamente, afasta muitas das possibilidades de fraudes e manuseio indesejado por terceiros não autorizados. Assim, os *smart cards* e *tokens* são mais seguros que o armazenamento no disco rígido do computador.

Atualmente, há softwares que aplicam técnicas mais complexas para acesso à chave privada, qualquer que seja o dispositivo usado para seu armazenamento.

Uma das técnicas mais promissoras é a biometria, que é a ciência que se encarrega do estudo das características individuais do ser humano. Os sistemas de segurança baseados na biometria supõem a identificação de uma pessoa, através de suas características biológicas ou físicas, tais como impressões digitais, reconhecimento de face, mão e dedos, verificação de características oculares, da grafia e da voz (CARRILLO, 2003, p. 187-189). Assim, por empregar medidas e estruturas individuais, que são ímpares, prometem evitar o acesso indesejado a uma determinada chave privada.

Cabe listar algumas das Autoridades Certificadoras credenciadas junto à Infra-Estrutura de Chaves Públicas Brasileira, que será tratada adiante. O Serpro, primeira Autoridade Certificadora credenciada pela ICP-Brasil, é responsável pela criação de

seu Centro de Certificação Digital – CCD, desde 1999, além de divulgar o uso dessa tecnologia para os vários segmentos com que trabalha. A Caixa Econômica Federal emprega a tecnologia de certificação digital para realizar a comunicação segura na transferência de dados pertinentes ao FGTS e à Previdência Social, dentro do projeto Conectividade Social. A Serasa possui um contato mais direto com o usuário final, podendo emitir certificados para a comunidade em geral, o que contribui para a integração digital da sociedade. A Secretaria da Receita Federal (SRF) emprega seus certificados e a tecnologia em comento para identificar os contribuintes nas operações de comunicação, prestação de informações, recebimento de declarações e recolhimentos tributários. A Certsign, pessoa jurídica de direito privado, foi fundada em 1996. Seu objetivo social é o desenvolvimento de soluções de certificação digital para o mercado brasileiro. A Autoridade Certificadora da Presidência da República (ACPR) foi criada em abril de 2002, com o objetivo emitir e gerir certificados digitais das autoridades da Presidência da República, ministros de estado, secretários-executivos e assessores jurídicos que se relacionem com a Presidência. A Autoridade Certificadora da Justiça (AC-JUS) comporta o Conselho da Justiça Federal (CJF), o Superior Tribunal de Justiça (STJ) e os cinco Tribunais Regionais Federais. Por fim, a Imprensa Oficial, que é a Autoridade Certificadora Oficial do Estado de São Paulo, realiza oferecimento de produtos e serviços de certificação digital para os poderes executivo, legislativo e judiciário, do estado[6].

Conforme dados do Instituto Nacional de Tecnologia da Informação, até abril do ano de 2007, foram registradas mais de cinquenta mil emissões de certificados digitais pela Infra-Estrutura de Chaves Públicas Brasileira, o que representa, ainda, um número bastante irrisório para um país populoso, como o Brasil. Eram, nessa mesma data, oito Autoridades Certificadoras de primeiro nível, vinte e duas de segundo nível, além de setenta e nove Autoridades de Registro, estas detentoras de seiscentos e setenta e nove instalações técnicas para verificação e registros de chaves públicas de usuários, possibilitando, assim, a emissão de certificados digitais[7].

3. Considerações finais

O artigo partiu de alguns problemas, quais sejam, o do emprego e da compreensão dos novos modelos tecnológicos para a realização de contratos, especialmente,

[6] Disponível em: <http://www.iti.br/twiki/bin/view/Main/AutCerti>. Acesso em: 30 out. 2006 e em 05 jan. 2008.

[7] Disponível em: <http://www.iti.br/twiki/bin/view/Certificacao/Indicadores>. Acesso em: 05 jan. 2008.

em meio eletrônico. Assim, propôs-se a tratar esses novos mecanismos ou modelos que viabilizam o contrato eletrônico, especialmente, a assinatura e certificação digitais no Brasil.

A assinatura e certificação digitais, que se baseiam, no Brasil, na técnica da criptografia assimétrica, conjugadas a um modelo hierárquico, oferece soluções aos problemas da determinabilidade do sujeito, da integridade da declaração de vontade e da garantia do não-repúdio das próprias declarações.

A guisa de conclusão, insta ressaltar que, ainda no que respeita à assinatura e certificação digitais, firmou-se o modelo hierárquico de certificação digital no Brasil, buscando-se o mínimo de interoperabilidade entre sistemas e equipamentos, tudo no sentido de propiciar um meio seguro à satisfação das legítimas expectativas dos contratantes e, sobretudo, a própria conclusão eficiente do contrato eletrônico.

Não houve, tampouco foi pretendido, o esgotamento da temática. Mesmo porque, ao final do trabalho, muitas outras questões, alheias ao intuito inicial, surgiram e permanecem sem resposta. A exemplo, chama a atenção a dificuldade de, no meio eletrônico de contratação, assegurar a idoneidade do consentimento, ou melhor, que se consiga evitar a fabricação do consentimento. Contudo, o final do estudo alcança-se com muita satisfação, em razão da sistematização das polêmicas centrais do contrato eletrônico (identificáveis, a partir da assinatura e certificação digitais no Brasil), que conduziu à constatação da existência de base principiológica suficiente para a procedência do regime jurídico do contrato eletrônico, bem como ao estabelecimento de novas perguntas.

Referências

BARRETO, Ana Carolina Horta. Assinaturas eletrônicas e certificação, in: ROCHA FILHO, Valdir de Oliveira; BARRETO, Ana Carolina Horta *et al*. *O Direito e a internet.* Rio de Janeiro: Forense Universitária, 2002, p. 1-65.

BRASIL. Instituto Nacional de Tecnologia da Informação. Disponível em: <http://www.iti.br/twiki/bin/view/Main/WebHome>. Acesso em: 20 jan. 2008.

BRASIL. MPV n.º 2.200-2/2001 (MEDIDA PROVISÓRIA), de 24 ago. 2001. Diário Oficial da União. Brasília, 27 ago. 2001, p. 65. Disponível em: <www.planalto.gov.br>. Acesso em: 18 jan. de 2007.

CARRILLO, Mariliana Rico. *Comercio eletrónico, internet y derecho*. Caracas: Legis, 2003.

HOUAISS, Antônio. *Dicionário eletrônico Houaiss da língua portuguesa*. Rio de Janeiro: Objetiva, 2001, CD-rom versão 1.0, para Windows.

LORENZETTI, Ricardo L. *Comércio eletrônico.* Trad. Fabiano Menke. Anot. Claudia Lima Marques. São Paulo: Revista dos Tribunais, 2004.

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

MENKE, Fabiano. *Assinatura eletrônica***:** aspectos jurídicos no direito brasileiro. São Paulo: Revista dos Tribunais, 2005.

ROCHA, Silvio Luiz Ferreira da. *Curso avançado de direito civil:* contratos. São Paulo: Revista dos Tribunais, 2002, v.3.

ROHRMANN, Carlos Alberto. *Curso de direito virtual.* Belo Horizonte: Del Rey, 2005.