REVISTA DOS TRIBUNAIS

CADERNO ESPECIAL

A REGULAÇÃO DA CRIPTOGRAFIA NO DIREITO BRASILEIRO

A criptografia, concebida originalmente como a técnica de codificar uma mensagem de forma que ela não possa ser compreendida por outros que não o seu destinatário, proporcionou o desenvolvimento de novas utilidades, que vão desde projeções exponenciais de suas utilizações originais (como a possibilidade de massificação das comunicações interpessoais criptografadas) até mesmo desdobramentos dificilmente previsíveis e devidos à disponibilidade de recursos computacionais (em tecnologias como o *Blockchain*).

Esse crescimento de seu potencial e o mencionado desdobramento das possibilidades de sua utilização proporcionaram à criptografia estar no coração de uma série de inovações tecnológicas que vêm causando concretos efeitos em diversas searas. Nesse sentido, justamente por ter sido a criptografia a indutora e elemento indispensável a essas mudanças, ela passou igualmente a fomentar a discussão sobre a oportunidade de que sua própria utilização fosse eventualmente passível de ser objeto em si de regulação – isso em diversas esferas e sentidos, desde a previsão de sua utilização compulsória para proporcionar maior segurança em comunicações, até limitações introduzidas justamente para evitar que a extrema segurança que possa proporcionar seja de livre utilização.

Assim, a partir de uma seleção criteriosa de temas e autores que vêm se destacando por proporcionar abordagens sobre a questão da criptografia que levam em conta a sua importância fundamental como tecnologia particularmente capaz de, pelas suas características, funcionar como indutor e garantidor de direitos e garantias em plataformas tecnológicas, procuramos oferecer neste volume uma seleção de textos que possam contribuir para os debates que vêm se engendrando, no Brasil e no mundo, sobre os seus efeitos jurídicos.

Da Apresentação

ISBN 978-85-203-6888-6

42173865

THOMSON REUTERS

REVISTA DOS TRIBUNAIS

CADERNO ESPECIAL

A REGULAÇÃO DA CRIPTOGRAFIA NO DIREITO BRASILEIRO

ORGANIZADOR:
DANILO DONEDA

COAUTORES:
GABRIEL ALEIXO
FABIANO MENKE
DIEGO C. MACHADO
DANILO DONEDA

THOMSON REUTERS

REVISTA DOS TRIBUNAIS™

Revista dos
TRIBUNAIS

CADERNO ESPECIAL
A REGULAÇÃO DA CRIPTOGRAFIA NO DIREITO BRASILEIRO

Diretora de Conteúdo e Operações Editoriais
JULIANA MAYUMI ONO

Gerente de Conteúdo
MILISA CRISTINE ROMERA

Editorial: Andréia Regina Schneider Nunes, Diego Garcia Mendonça, Karolina de Albuquerque Araújo, Marcella Pâmela da Costa Silva e Thiago César Gonçalves de Souza

Direitos Autorais: Viviane M. C. Carmezim

Assistente Editorial: Francisca Lucélia Carvalho de Sena

Produção Editorial
Coordenação
IVIÊ A. M. LOUREIRO GOMES

Especialistas Editoriais: Gabriele Lais Sant'Anna dos Santos e Maria Angélica Leite

Analista de Projetos: Larissa Gonçalves de Moura

Analistas de Operações Editoriais: Bruno Capassi, Damares Regina Felício, Danielle Castro de Morais, Felipe Augusto da Costa Souza, Maria Eduarda Silva Rocha, Marília Gabriela Gradin, Mayara Macioni Pinto, Patrícia Melhado Navarra e Rafaella Araujo Akiyama

Analistas de Qualidade Editorial: Carina Xavier e Daniela Medeiros Gonçalves Melo

Estagiários: Miriam da Costa Leite, Nicolas Eugênio Almeida Bueno e Sthefany Moreira Barros

Capa: Andréa Cristina Pinto Zanardi

Adaptação capa: Carla Lemos

Equipe de Conteúdo Digital
Coordenação
MARCELLO ANTONIO MASTROROSA PEDRO

Analistas: Ana Paula Cavalcanti, Jonatan Souza, Luciano Guimarães e Rafael Ribeiro

Administrativo e Produção Gráfica
Coordenação
MAURICIO ALVES MONTE

Analista de Produção Gráfica: Aline Ferrarezi Regis

Revista dos
TRIBUNAIS
CADERNO ESPECIAL
A REGULAÇÃO DA CRIPTOGRAFIA NO DIREITO BRASILEIRO

THOMSON REUTERS
REVISTA DOS TRIBUNAIS™

Sumário

A criptografia e a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)

Fabiano Menke

Professor da Faculdade de Direito e do Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul. Advogado em Porto Alegre.
fabiano.menke@ufrgs.br

1. Introdução

Entre as diversas utilizações possíveis para a criptografia, encontra-se aquela atinente à Infraestrutura de Chaves Públicas, aos certificados digitais e às denominadas assinaturas digitais. Uma breve conceituação desses três elementos é o objeto do presente trabalho, com o escopo de preparar o caminho para a abordagem de como é utilizada a criptografia no contexto específico da ICP-Brasil.

2. A Infraestrutura de Chaves Públicas Brasileira e os certificados digitais

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), regida pela Medida Provisória 2.200-2, de 24 de agosto de 2001[1],é formada por um conjunto

1. Apesar da nomenclatura "medida provisória", a Medida Provisória 2.200-2 vigora no Brasil indefinidamente, em virtude do previsto no art. 2º da EC 32/2001: "Art. 2º As medidas provisórias editadas em data anterior à da publicação desta emenda continuam em vigor até que medida provisória ulterior as revogue explicitamente ou até deliberação definitiva do Congresso Nacional".

de pessoas jurídicas de direito público e de direito privado[2] que, no âmbito de suas atribuições, tem por escopo comum permitir que pessoas jurídicas e pessoas físicas se identifiquem virtualmente e assinem digitalmente documentos eletrônicos, tudo isso, com um incremento de segurança em comparação com uma comunicação sem maiores cuidados do usuário e com a agregação de um *status* jurídico-probatório diferenciado[3].

Uma Infraestrutura de Chaves Públicas, como a ICP-Brasil, 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.[4] O termo Infraestrutura 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 infraestrutura. Carlisle Adams e Steve Lloyd, na obra *Understanding Public-Key Infrastructure*[5] enfatizaram que uma infraestrutura se caracteriza por ser uma *pervasivesubstrate*, ou seja, uma fundação que dissemine algo para um amplo ambiente ou para um grande universo de interessados. Salientam que duas infraestruturas comuns são a de comunicações eletrônicas (uma rede) e a de energia elétrica. Asseveram que o princípio de ambas é idêntico: a infraestrutura existe para que qualquer usuário possa simplesmente acoplar-se a ela e dela fazer uso quando necessário.

As razões para que haja uma infraestrutura que congregue número maior possível de pessoas e entidades são simples e facilmente perceptíveis. É justamente para que haja possibilidade de comunicação entre os envolvidos, ou, meramente, a possibilidade de pronto acoplamento. A infraestrutura uniforme evita que sejam aplicadas soluções díspares por cada indivíduo[6].

Atente-se bem a esse ponto: uma infraestrutura de segurança disseminada, uniforme, evita soluções díspares, isoladas, não interoperáveis. Pode-se tomar o exemplo fornecido por Adams e Lloyd acerca do caos que resultaria do fato de cada indivíduo operar as suas próprias linhas de comunicação ou de geração de energia é emblemático.

Uma Infraestrutura de Chaves Públicas pode ser configurada basicamente em dois modelos: o hierárquico e o de confiança distribuída.[7] O primeiro é configurado numa hierarquia, na forma de uma árvore invertida, situando-se no topo uma entidade na qual todos os que vêm abaixo, inclusive os usuários, devem confiar.[8] A confiança se dissemina de cima para baixo: a entidade localizada no ápice da hierarquia, a denominada Autoridade Certificadora Raiz, emite um certificado para uma autoridade certificadora de segundo nível, e esta emite um certificado para o usuário final.[9]

2. Lembre-se de que há autorização, no âmbito das normas da ICP-Brasil, para que os serviços notariais e de registro atuem como instalação técnica de Autoridades de Registro. Como se sabe, esses serviços são exercidos pela pessoa natural responsável e não apresentam a natureza de pessoa jurídica. Confira-se o teor da regra do DOC-ICP-03: "3.2.1.3 Os serviços notariais e de registro, nos termos do art. 236 da Constituição Federal, desde que formalmente vinculados a uma AR já credenciada, poderão ser autorizados a funcionar como instalação técnica e seus delegados, prepostos e funcionários a atuar como agentes de registro". Para acesso às regras da ICP-Brasil, ver [www.iti.gov.br/legislação].
3. Quanto à questão dos efeitos jurídicos probatórios do emprego da assinatura digital ICP-Brasil, atentar ao seguinte aspecto: *"Em decorrência, no direito brasileiro, via de regra, só terá os mesmos efeitos da assinatura manuscrita aquela assinatura digital aposta com base em certificado digital emitido por uma das autoridades certificadoras credenciadas pelo Instituto Nacional de Tecnologia da Informação, entidades que têm a obrigação de cumprir com todos os requisitos técnicos, administrativos, operacionais e jurídicos elencados nas normas da ICP-Brasil"* (MENKE, Fabiano. *Assinatura eletrônica no direito brasileiro*. São Paulo: Ed. RT, 2005. p. 140-141. Os grifos apostos no destaque não estão no original da publicação). Para uma abordagem mais detalhada acerca dos efeitos jurídicos da assinatura digital, verificar o seguinte texto: MENKE, Fabiano. Apontamentos sobre o comércio eletrônico no direito brasileiro. In: COELHO, Fábio Ulhoa; RIBEIRO, Maria de Fátima. *Questões de direito comercial no Brasil e em Portugal*. São Paulo: Saraiva, 2014. p. 347-375.
4. A definição do vocábulo "infraestrutura" 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".
5. ADAMS; LLOYD. *Understanding public-key infrastructure:* concepts, standards, and deployment considerations. Indianapolis: New Riders, 1999. p. 27.
6. ADAMS; LLOYD. *Understanding public-key infrastructure:* concepts, standards, and deployment considerations. Indianapolis: New Riders, 1999. p. 27-28.
7. Também denominado no inglês de *shallow model*.
8. Sobre os modelos e a designação árvore invertida, ADAMS, LLOYD. Op. cit., p. 133-141. Na obra, Adams apresenta ainda outros modelos, como o modelo de rede (*web-model*) e o modelo de confianças no usuário central (*user centrictrust*).
9. É bastante comum e possível um número maior de níveis intermediários de autoridades certificadoras, com autoridades certificadoras emitindo certificados digitais para outras autoridades certificadoras, até chegarem ao usuário final.

MENKE, Fabiano. A criptografia e a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). *Revista dos Tribunais*. vol. 998. Caderno Especial. p. 83-97. São Paulo: Ed. RT, dezembro 2018.

As pessoas jurídicas que integram a ICP-Brasil são, basicamente, a Autoridade Certificadora Raiz[10], as Autoridades Certificadoras[11], e as Autoridades de Registro[12]. Sua atuação tem por finalidade, de maneira sucintamente explicada, a identificação presencial dos usuários e a posterior emissão do certificado digital, que é um elemento fundamental para que se possa utilizar uma assinatura digital.

O certificado digital é uma estrutura de dados sob a forma eletrônica, em que constam dados relacionados ao seu titular, como nome, endereço de e-mail, número de CPF, e a denominada chave pública, que, como se verá adiante, é a informação mais importante para que se utilize a assinatura digital, que, por sua vez, é baseada na criptografia assimétrica.

O titular do certificado digital poderá ser, de acordo com a legislação brasileira, uma pessoa física ou uma pessoa jurídica[13]. Adquire um certificado digital aquele que tema intenção ou a necessidade de se identificar (função de

10. A função de Autoridade Certificadora Raiz, no âmbito da Infraestrutura de Chaves Públicas Brasileira, é desempenhada pelo Instituto Nacional de Tecnologia da Informação, autarquia federal vinculada à Casa Civil da Presidência da República. Destaque-se, assim, que no ápice do que se pode denominar de cadeia de certificação, encontra-se o poder público. Esse modelo de Infraestrutura de Chaves Públicas adotado pelo Brasil foi inspirado na legislação alemã que vigorava à época da edição da MP 2.200-2. Especialmente na *Signaturgesetz* de 1997, bem como na *Signaturgesetz* de 2001. Acerca da influência alemã na criação da legislação brasileira sobre o assunto, ver o artigo de MENKE, Fabiano, Assinaturas digitais, certificados digitais, infra-estrutura de chaves públicas brasileira e a ICP alemã. *Revista de Direito do Consumidor*, n. 48. p. 132.

11. Art. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

12. Art. 7º 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.

13. É o que determina o item 1.1.5. do DOC-ICP-04 da ICP-Brasil: "Certificados dos tipos de A1 a A4 e de S1 a S4, de assinatura ou de sigilo, podem, conforme a necessidade, ser emitidos pelas ACs para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações". No que diz respeito a equipamentos ou aplicações, a emissão ocorre ou para pessoas jurídicas ou para pessoas físicas.

autenticação[14]) ou assinar documentos (função de comprovação de autoria) no meio eletrônico de uma forma que agregue mais segurança técnica e jurídica. Exemplo de utilização do certificado digital na função de autenticação, entre outros tantos, é o da identificação perante as aplicações de *homebanking* de instituições financeiras, em que a pessoa comprova que é a titular da conta bancária que pretende acessar. Exemplo de utilização do certificado digital na função de assinatura é o das partes que se valem dessa ferramenta para assinar contratos eletrônicos.

A necessidade de incrementar a segurança técnica e jurídica advém da realidade de que existem vulnerabilidades[15] que são intensificadas no meio eletrônico, especialmente no que diz respeito: à identificação[16], em sentido amplo; à autoria de declarações de vontade, bem como à integridade dos documentos eletrônicos, ou seja, quanto ao fato de que não foram alterados em seu percurso virtual.

Veja-se que o *Guia para a incorporação ao direito interno da lei modelo de assinaturas eletrônicas da Uncitral* alerta que no ambiente eletrônico o original de uma mensagem é indistinguível da cópia, não comporta uma assinatura manuscrita e não é veiculado em papel. Além disso, o potencial para a ocorrência de fraudes é considerável, devido às facilidades de interceptação e de alteração, sem detecção, da informação sob a forma eletrônica e à velocidade de processamento de múltiplas transações.[17]

14. Função de autenticação, no contexto que ora se cuida, nada tem a ver com a autenticação que é levada a cabo por notários e tabeliães de notas no âmbito da Lei 8.935/1994, quando se alude a autenticação de fatos ou de documentos. Neste trabalho, o termo "autenticação" é empregado no sentido da tecnologia da informação, ou seja, de identificação de usuário.

15. Ver sobre o tema, com excelente descrição dos aspectos de vulnerabilidade, ROSSNAGEL, Alexander. Einleitung Signaturgesetz. *Beck'scher Kommentarzum Recht der Telemediendienste*. Munique: CH Beck, 2013. p. 427.

16. No sentido de que qualquer relação pelo meio eletrônico pode ser estabelecida sem qualquer elemento de segurança que ateste a identidade de quem a integra, e, portanto, pode-se, por exemplo, concluir um contrato com pessoa que não é a pessoa quem diz ser.

17. UNCITRAL *Model Law on Electronic Signatures with Guide to Enactment*. Nova York, 2002. p. 20.

Para que se compreenda de onde vem o incremento da segurança, é preciso abordar, primeiramente, o conceito de assinatura eletrônica, e, posteriormente, o conceito de assinatura digital.

3. O CONCEITO DE ASSINATURA ELETRÔNICA

Um dos conceitos técnicos para resolver o problema das vulnerabilidades no meio virtual é a denominada assinatura eletrônica. Tendo em vista a precisão da definição apresentada no Guia para a incorporação ao direito interno da Lei Modelo da Uncitral, calha a sua citação:

> o escopo de várias técnicas atualmente disponíveis no mercado, ou ainda em desenvolvimento, é o de oferecer os meios técnicos pelos quais algumas ou todas as funções identificadas como características das assinaturas manuscritas podem ser desempenhadas em um ambiente eletrônico. Tais técnicas podem ser, em sentido largo, denominadas de 'assinaturas eletrônicas' [...] por exemplo, certas técnicas seriam respaldadas na autenticação por meio de dispositivos biométricos baseados em assinaturas manuscritas. Em tais dispositivos, o signatário assinaria manualmente, utilizando uma caneta especial, ou em uma tela de computador ou em uma planilha digital. A assinatura manuscrita seria então analisada pelo computador e armazenada como um conjunto de valores numéricos, que poderia ser anexado a uma mensagem de dados e recuperada pelo relyingparty[18] para fins de conferência da autoria. Um tal sistema de comprovação de autoria seria baseado no pressuposto de que amostras da assinatura manuscrita tenham sido previamente analisadas e armazenadas utilizando o dispositivo biométrico. Outras técnicas compreenderiam a utilização de números de identificação pessoal (os PINs), versões digitalizadas de assinaturas manuscritas, e outros métodos, como o clicar numa opção de uma janela de diálogo.[19]

18. Nesse ponto, cabe um esclarecimento que não consta na publicação transcrita. *Relyingparty* é a denominação da parte que recebe uma mensagem assinada digitalmente, e, portanto, poderá ou não confiar no certificado digital. Uma das cautelas que devem ser tomadas pelo *relyingparty* é a de acessar a LCR (lista de certificados revogados) da Autoridade Certificadora que emitiu o respectivo certificado digital, a fim de verificar a sua validade, ou seja, se o certificado que embasa a assinatura digital aposta estava válido no momento em se assinou. O certificado pode ter sido revogado, entre outras razões, por perda ou furto.

19. UNCITRAL *Model Law on Electronic Signatures with Guide to Enactment*. Nova York, 2002. p. 20-21, tradução livre.

Portanto, sob a denominação de assinatura eletrônica inclui-se uma gama de métodos de comprovação de autoria empregados no meio virtual. Exemplo de consagração legal desse conceito de assinatura eletrônica como gênero de mecanismos de comprovar a autoria se encontra na Lei 11.419/2006 (Lei do Processo Eletrônico), que assim dispôs sobre a questão:

> Art. 1º O uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais será admitido nos termos desta Lei.
>
> [...]
>
> § 2º Para o disposto nesta Lei, considera-se:
>
> [...]
>
> III – assinatura eletrônica as seguintes formas de identificação inequívoca do signatário:
>
> *a)* assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica;
>
> *b)* mediante cadastro de usuário no Poder Judiciário, conforme disciplinado pelos órgãos respectivos.
>
> Art. 2º O envio de petições, de recursos e a prática de atos processuais em geral por meio eletrônico serão admitidos mediante uso de assinatura eletrônica, na forma do art. 1º desta Lei, sendo obrigatório o credenciamento prévio no Poder Judiciário, conforme disciplinado pelos órgãos respectivos.

Consoante se verifica da leitura desses dispositivos, a utilização do meio eletrônico para a transmissão de peças processuais é permitida (art. 1º, *caput*), desde que seja utilizada assinatura de protocolo criptográfico, anotam Hans Delfs e Helmut Knebl 1º, § 2º, III, assinatura eletrônica é a assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada (alínea *a*) ou o cadastro do usuário no Poder Judiciário (alínea *b*), que é implementado, na prática, pela atribuição de senhas ao advogado mediante o seu comparecimento presencial.

A assinatura digital, dessa 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 os diversos existentes.

MENKE, Fabiano. A criptografia e a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). *Revista dos Tribunais*. vol. 998. Caderno Especial. p. 83-97. São Paulo: Ed. RT, dezembro 2018.

Há, pois, uma diferença entre as nomenclaturas "assinatura eletrônica" e "assinatura digital", que não poderão ser utilizadas como sinônimas.[20]

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[21] baseado na criptografia assimétrica. Essa modalidade de assinatura eletrônica, qual seja a assinatura digital baseada em criptografia assimétrica, foi a opção adotada pela Medida Provisória 2.200-2 de 2001.

4. A ASSINATURA DIGITAL E A CRIPTOGRAFIA ASSIMÉTRICA

A assinatura digital é viabilizada pelo emprego da criptografia assimétrica ou criptografia de chaves públicas. Para melhor compreensão da criptografia assimétrica, é preciso fazer uma rápida passagem pelas 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*

20. Sobre as diferenças, ver ADAMS, Carlisle; LLOYD, Steve. *Understandig Public-Key Infrastructure:* concepts, standards, and deployment considerations. Indianapolis: New Riders, 1999. p. 189. Os autores norte-americanos observam que não há acordo universal acerca do significado desses termos, todavia, dizem que seria mais correta a definição de assinatura eletrônica como qualquer assinatura que possa ser representada eletronicamente. Isso poderia ser desde uma assinatura manuscrita digitalizada (com a utilização do aparelho *scanner*) até uma assinatura digital de criptografia de chave pública. Assim, a assinatura digital seria espécie da classe de assinaturas referidas como assinaturas eletrônicas. Ver também BURNETT, Steve; PAINE, Stephen. *Criptografia e segurança:* o guia oficial RSA. Trad. Edson Fumankiewicz. Rio de Janeiro: Campos, 2002. p. 261. Esses autores assim se pronunciam sobre o tema: "Em termos simples, uma assinatura eletrônica é um símbolo ou método qualquer, realizado por um meio eletrônico, que é executado ou adotado por uma parte com uma intenção presente de ser associado e autenticado por um registro. Uma assinatura eletrônica pode ser criada por qualquer meio eletrônico. [...] Ao contrário, uma assinatura digital refere-se a uma implementação de criptografia de chave pública em particular".

21. Relembre-se que no contexto deste escrito "autenticação" não será utilizada no sentido relacionado à sua tradicional acepção da função notarial, mas sim à ideia de identificação do autor de determinada declaração de vontade.

da Gália de Júlio César".[22] 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 subsequente 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. É fácil de perceber que essas características da criptografia simétrica implicam limitações ou dificuldades para que seja adotada como mecanismo de maior segurança no âmbito da contemporânea sociedade da informação.

O fato de haver um compartilhamento do código ou chave de cifração entre as pessoas que realizarão a comunicação ou o negócio tem um desdobramento no aspecto jurídico que não poderá ser desprezado. É que, no caso de haver fraude, ou suspeita de comprometimento do código ou chave, ambos os polos da relação serão, pelo menos de início, considerados como pontos em que a vulnerabilidade pode ter sido causada. Como adiante se verá, a criptografia assimétrica afasta este potencial de imputação a ambas as partes do vazamento da chave.

Por outro lado, outra dificuldade da criptografia simétrica localiza-se na necessidade de que previamente à comunicação entre duas pessoas que a uti-

22. SINGH, Simon. *O livro dos códigos*. Trad. Jorge Calife. 2. 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 vista 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".

lizarão será necessário um contato para que elas convencionem o código a ser utilizado.

E, por fim, há o problema 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 1970 pelos pesquisadores norte-americanos Whitfield Diffie, Martin Hellman e Ralph Merkle, considerados os inventores dos conceitos de criptografia de chave pública.[23] Ela consiste num método que utiliza duas chaves, uma a ser aplicada pelo remetente e outra pelo receptor da mensagem, e é sobre esse conceito 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. Fundamental nesse contexto 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 cartões inteligentes,[24] dispositivos similares a um

23. SINGH, Simon. *O livro dos códigos*. Trad. Jorge Calife. 2. ed. Rio de Janeiro: Record, 2002. p. 305.

24. BURNETT, Steve; PAINE, Stephen. *Criptografia e segurança:* o guia oficial RSA. Trad. Edson Fumankiewicz. Rio de Janeiro: Campos, 2002. p. 60: "Um cartão inteligente é simplesmente um cartão plástico, semelhante a um cartão de crédito, que contém um microprocessador. Um dos objetivos dos fornecedores de cartões inteligentes é substituir a versão atual dos cartões de crédito. Assim como cartões de crédito com faixas magnéticas substituíram os cartões mais simples impressos em relevo, a esperança é que os cartões inteligentes substituirão os cartões de crédito. Mas pelo fato de os cartões inteligentes conterem pequenos computadores, eles serão capazes de fazer outras coisas além de servir como cartões de crédito". Outro equipamento importante para o funcionamento dos cartões inteligentes é a leitora, que consiste em dispositivo

cartão de crédito), enquanto que o receptor, ao receber a mensagem, aplicará a chave pública do remetente, que consta no certificado digital, para verificar se ela efetivamente dele se originou.

A princípio não é possível derivar uma chave privada a partir da respectiva chave pública, a menos que seja empregado um esforço computacional considerável. As chaves criptográficas assimétricas podem possuir tamanho variável – de acordo com o grau de segurança desejado – e serão tanto mais seguras quanto maiores forem. Na ICP-Brasil, por exemplo, as chaves criptográficas da denominada Autoridade Certificadora Raiz chegam a 4096 bits, valor este que pode ser revisto conforme o desenvolvimento da técnica.[25]

Os programas de computador do receptor fazem uma conferência, 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.

Cabe, nesse momento, a comparação com a criptografia simétrica, que, como visto, utiliza a mesma chave tanto para a cifração quanto para a decifração da mensagem. É justamente a diversidade das chaves presente na criptografia assimétrica que permite a comunicação com um universo ilimitado, e, fundamentalmente, que não se tenha 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.

Repise-se essa fundamental característica da criptografia assimétrica: não ocorre, como na criptografia simétrica, a necessidade operacional de compartilhamento da chave secreta entre as partes. Há, aqui, um desdobramento de índole jurídica que vai no sentido oposto ao anteriormente descrito, pois, na criptografia assimétrica, apenas a parte que tem a posse ou o controle sobre a chave privada é que será imputável pelas vicissitudes que com ela ocorram.

Dito de outro modo, há um ônus de guarda e cuidado alocados ao único titular da chave privada, não havendo como, pela natureza do procedimento como ocorre a distribuição das chaves, imputar o comprometimento da chave ou a autoria de determinada declaração àquele que não titulariza a chave pri-

no qual o cartão inteligente é inserido para o processamento das informações nele constantes. Existem leitoras inseridas até mesmo em teclados.

25. Ver, quanto à questão, o interessante artigo de BERTOL, Viviane Regina Lemos: *O que esperar da cadeia V5 da ICP-Brasil*. Disponível em: [https://cryptoid.com.br/banco-de-noticias/o-que-esperar-da-cadeia-v5-da-icp-brasil/]. Acesso em 30.05.2018.

vada, a menos que se considere a prática de ato ilícito, o que geraria um novo desdobramento na seara da responsabilidade civil.

Acerca do ponto, cabe a lição de Augusto Marcacini[26]:

> A desvantagem é que não teremos a quem culpar, pela eventual negligência em manter a chave privada segura, já que a apropriação indevida dessa chave pode ser considerada o maior risco que afeta a segurança do sistema. Portando, toda a cautela possível deve ser tomada na proteção da chave privada pelo seu titular.

Essa característica é confirmada pelo disposto no parágrafo único do art. 6º da Medida Provisória 2.200-2[27]: "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."

Importante salientar que no processo de aposição de uma assinatura digital em documento eletrônico, o texto em si que é assinado não é criptografado, mas apenas o seu resumo. O texto da mensagem, portanto, trafega pelo seu percurso virtual de modo que pode ser lido por qualquer pessoa que o interceptar. Isso se deve ao fato de que a criptografia assimétrica tem a desvantagem de ser lenta.[28] Na prática, qualquer mensagem – não importando o tamanho, se de 10 bytes ou de 10.000 bytes – é condensada em 20 bytes.[29] O resumo da mensagem ou função *hash* é um algoritmo[30] que recebe uma informação de

26. MARCACINI, Augusto Tavares Rosa. *Direito e informática*: uma abordagem jurídica sobre a criptografia. Rio de Janeiro: Forense, 2002. p. 115.
27. É o seguinte o teor do *caput* do art. 6º da MP 2.200-2: "Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações".
28. BURNETT, Steve; PAINE, Stephen. *Criptografia e segurança:* o guia oficial RSA. Trad. Edson Fumankiewicz. Rio de Janeiro: Campos, 2002. p. 120.
29. BURNETT, Steve; PAINE, Stephen. *Criptografia e segurança:* o guia oficial RSA. Trad. Edson Fumankiewicz. Rio de Janeiro: Campos, 2002. p. 120.
30. Consoante BURNETT, Steve; PAINE, Stephen. *Criptografia e segurança:* o guia oficial RSA. Trad. Edson Fumankiewicz. Rio de Janeiro: Campos, 2002. p. 14, "a palavra 'algoritmo' é um termo científico para uma receita ou procedimento passo a passo. Ela é uma lista de instruções ou coisas a serem feitas em uma determinada ordem. Um algoritmo talvez tenha uma lista rígida de comandos a ser seguida ou talvez contenha uma série de perguntas e, dependendo das respostas, descreve os passos apropriados a serem seguidos. Um algoritmo matemático talvez liste as operações a serem realizadas em uma ordem em particular para 'encontrar x'. Por exemplo, um algoritmo de diagnóstico de automóvel pode fazer perguntas sobre a pressão do óleo, torque,

qualquer tamanho e a transforma em dado de largura fixa. Portanto, para se ganhar em velocidade, cifra-se o resumo da mensagem ou do arquivo, e não o conteúdo da mensagem em si.

No âmbito da ICP-Brasil, há a possibilidade de utilizar um segundo certificado digital, oferecido ao lado do certificado de assinatura, chamado de certificado digital de sigilo, que provê a funcionalidade de ocultação do conteúdo[31].

5. Conclusão

Diante do abordado neste trabalho, podemos apresentar as seguintes conclusões sintéticas:

a) A Infraestrutura de Chaves Públicas tem os traços característicos de outras infraestruturas postas à disposição da coletividade, como a de saneamento e de telecomunicações, quais sejam os de viabilizar ao maior número de usuários possível o acesso a um serviço; no caso da ICP, o que se põe à disposição dos usuários são os certificados digitais e as assinaturas digitais.

b) O Brasil criou uma Infraestrutura de Chaves Públicas no ano de 2001, a denominada ICP-Brasil, por meio da Medida Provisória 2.200-2, organizada na forma de hierarquia, e que conta, no ápice da cadeia de certificação, com a denominada Autoridade Certificadora Raiz, papel desempenhado pela Autarquia Federal Instituto Nacional de Tecnologia da Informação.

níveis de fluido, temperatura e outros itens para determinar o que há de errado. Um programa de computador também pode implementar um algoritmo, o que significa que o programa converte a lista de comandos, perguntas e operações do algoritmo em uma linguagem de computador, permitindo que ele realize os passos em uma ordem apropriada. Na criptografia computadorizada, os algoritmos são às vezes operações matemáticas complexas ou apenas manipulações de bits. Existem vários algoritmos de criptografia e cada um tem sua própria lista particular de comandos ou passos. Assim como você pode ter um programa que jogue paciência ou um que compute a trajetória de satélites, você pode ter um programa que implemente um algoritmo de criptografia que receba seus dados e os converta em algo sem sentido".

31. A previsão das espécies de certificado digital no âmbito da ICP-Brasil está disposta nos seguintes itens do DOC-ICP-04: "1.3.5.4. Certificados de tipos A1, A2, A3 e A4 serão utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações. 1.3.5.5. Certificados de tipos S1, S2, S3 e S4 serão utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo".

c) Os certificados digitais são documentos eletrônicos que contêm dados de identificação do usuário, como, entre outros, o nome e uma chave pública, e são emitidos pelas Autoridades Certificadoras, após a identificação presencial dos usuários perante as Autoridades de Registro.

d) A chave pública é obtida e inserida no certificado digital após a emissão do par de chaves criptográficas (chave pública e chave privada) pelo próprio usuário.

e) A partir da emissão do certificado digital, o usuário poderá utilizar essa ferramenta como mecanismo de simples identificação no ambiente virtual, onde provará sua identidade, ou utilizará o certificado digital na função de assinatura digital, de modo a associar a sua assinatura a uma declaração de vontade.

f) A assinatura digital é uma espécie de assinatura eletrônica, baseada em criptografia assimétrica. A criptografia assimétrica é o conceito técnico-matemático que embasa uma Infraestrutura de Chaves Públicas e, diferentemente da criptografia simétrica, não ocorre o compartilhamento da chave secreta ou privada entre as partes, o que tem fundamental relevância jurídica nas questões de disputa sobre a identificação de atos praticados e negócios firmados eletronicamente.

g) Com o emprego da assinatura digital baseada em criptografia assimétrica, o titular do par de chaves deve ter a posse e o controle exclusivo da chave privada, armazenada em mecanismos seguros, como cartões inteligentes e *tokens*, e assinará os seus documentos com o seu emprego, enquanto que o destinatário do documento fará a conferência da assinatura, atestando a sua autoria, a partir do elemento chave pública, contido no certificado digital.

Referências

ADAMS, Carlisle; LLOYD, Steve. *Understandig Public-Key Infrastructure:* concepts, standards, and deployment considerations. Indianapolis: New Riders, 1999.

BERTOL, Viviane Regina Lemos. *O que esperar da cadeia V5 da ICP-Brasil*. Disponível em: [https://cryptoid.com.br/banco-de-noticias/o-que-esperar-da-cadeia-v5-da-icp-brasil/]. Acesso em: 30.05.2018.

BURNETT, Steve; PAINE, Stephen. *Criptografia e segurança:* o guia oficial RSA. Trad. Edson Fumankiewicz. Rio de Janeiro: Campos, 2002.

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

MENKE, Fabiano. *Assinatura eletrônica no direito brasileiro*. São Paulo: Ed. RT, 2005.

MENKE, Fabiano. Assinaturas digitais, certificados digitais, infra-estrutura de chaves públicas brasileira e a ICP alemã. *Revista de Direito do Consumidor*, n. 48.

MENKE, Fabiano. Apontamentos sobre o comércio eletrônico no direito brasileiro. In: COELHO, Fábio Ulhoa; RIBEIRO, Maria de Fátima. *Questões de direito comercial no Brasil e em Portugal*. São Paulo: Saraiva, 2014.

ROSSNAGEL, Alexander. Einleitung Signaturgesetz. *Beck'scher Kommentar zum Recht der Telemediendienste*. Munique: CH Beck, 2013.

SINGH, Simon. *O livro dos códigos*. Trad. Jorge Calife. 2. ed. Rio de Janeiro: Record, 2002.

UNCITRAL *Model Law on Electronic Signatures with Guide to Enactment*. Nova York, 2002.