Artigos Selecionados REDE 2017

I Encontro da Rede de Pesquisa em Governança da Internet

Rio de Janeiro, 14 de Novembro de 2017

RELAÇÕES CONTRATUAIS NA INTERNET: Segurança jurídica e segurança da informação da certificação digital em contratos eletrônicos

Mariana Palma Vidotti
Bacharel em Direito; Advogada inscrita na OAB/PR n° 63.353; Pós-graduanda em Direito Tributário pelo Instituto Brasileiro de Estudos tributários – IBET; Membro efetivo do Instituto de Direito Tributário de Londrina-PR – IDTL
marianavidottiadv@gmail.com

RESUMO

O presente estudo tem por temática a análise acerca da segurança jurídica na utilização de assinatura digital em contratos eletrônicos firmados na Internet, primando pela privacidade e segurança da informação, averiguação da existência de validade jurídica de assinatura por Certificado Digital e sua consequente produção de efeitos no mundo fático. Far-se-á análise do texto da norma trazida pela Medida Provisória nº 2.200-2/2001 que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e do artigo 411, inciso II, do Novo Código de Processo Civil – CPC/2015, no sentido de levantar entendimento favorável no Direito Brasileiro Positivado. Ainda, traçar-se-á considerações sobre o uso de criptografia assimétrica na assinatura digital por certificação digital, a fim de se comprovar a segurança jurídica do mecanismo, garantindo autenticidade, privacidade e não repúdio das relações contratuais eletrônicas assinadas digitalmente. Bem como, apresentar-se-á contexto doutrinário brasileiro e cenário global na adoção e validade de assinatura por certificado digital em contratos firmados na internet.

PALAVRAS-CHAVE: Internet. Contratos Eletrônicos. Certificado Digital. Assinatura Digital. Segurança da Informação.

Sugestão de citação (ABNT): SOBRENOME, Nome. **Título do artigo**. I ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, NOVEMBRO DE 2017. Disponível em: <endereço na web>. Acesso em: mês. ano.

1 INTRODUÇÃO

Com o advento da internet como principal meio de comunicação mundial, é indiscutível que a ferramenta ultrapassa o limite do entretenimento e alcança a esfera das relações jurídicas.

É irrefutável que o Direito, enquanto ciência que se ocupa de estudar a fenomenologia dessas relações, não pode ser entendido como ciência exata e imutável, ao passo que a interação entre indivíduos e seus consequentes direitos-deveres sofrem constantes mutações enquanto a sociedade evolui.

Diante da globalização e o estreitamento das interações interpessoais, também consequências do uso da internet, essa ferramenta passa a ser cenário de diversas transações e relações negociais, que dificilmente podem ser concretizadas por meio de contrato físico, haja vista a inviabilidade que o meio físico acarreta, seja com relação ao custo para serem colhidas as assinaturas das partes, que muitas vezes não se encontram no mesmo espaço, seja no que diz respeito ao tempo, de sorte que a própria velocidade da informação trazida pela sociedade digital não mais comporta uma delonga nas tratativas em negócios que devem ser predominantemente imediatistas.

Dessa maneira, o direito positivado tratou de normatizar o uso de Certificado Digital como assinatura, cabendo a Ciência do Direito identificar se há validade jurídica nas assinaturas digitais e a respectiva produção de efeitos no mundo fático.

Assim sendo, tem-se por objetivo geral deste estudo constatar a viabilidade e validade jurídica de assinatura digital por meio de certificação digital em contratos eletrônicos, de modo a concluir pela autenticidade, integridade e não repúdio da relação negocial eletrônica que se utiliza de certificado digital, de forma a se averiguar a segurança jurídica do instrumento.

2 BREVE HISTÓRICO DA EVOLUÇÃO DA INTERNET E A SOCIEDADE DIGITAL

A origem da Internet remota ao auge da Guerra Fria, em meados da década de 60, sendo inicialmente pensada para fins exclusivamente militares. Foi nos Estados Unidos, quando o governo criou a *Advanced Research Projects Agency* (ARPANET), que consistia em uma ligação entre computadores militares e industriais, por meio de rede telefônica, com finalidade de prevenir possíveis ataques nucleares, que se viu nascer a ideia do que se entende por Internet. Esse método, então revolucionário, foi

arquitetado em volta da preocupação de se manter dados relevantes em uma central que poderia sofrer ataques e consequente perda permanente de dados essenciais, assim sendo, a engenharia descentralizada por meio de pacotes permitiu que, em caso de ataque por forças inimigas, as informações lá existentes não se perdessem (MARTINS, 2016, p. 25).

Posteriormente, já na década de 80, a Internet passou a ser utilizada para fins acadêmicos, de forma a estabelecer a comunicação de computadores entre universidades, acadêmicos e laboratórios de pesquisa norte-americanos, permitindo a troca de informações mediante sistema de protocolos (TEIXEIRA, 2013, p. 21-22).

A saída da Internet do ambiente acadêmico teve como ponto de partida o final da década de 80, no *European Particle Physics Laboratory* (CERN), quando do desenvolvimento por Tim Berners-Lee e um grupo de pesquisadores, de um protótipo da *World Wide Web*, resultando no padrão *HyperText Markup Language* (HTML), consistente em um banco de dados de armazenamento de informações, possibilitando que dados em diversas formas fossem visualizados em único arquivo conjuntamente (MARTINS, 2016, p. 26).

Já na década de 90, a Internet passou por um processo de transformação e expansão. Foi em 1994 que surgiu a segunda geração da Internet, chamada de "*Information Superhighway*", sendo comparada a uma super-rodovia da informação, posto que conseguia conjugar dados, voz e vídeo por um único canal (MARTINS, 2016, p. 27).

Do ponto de vista técnico, a Internet pode ser entendida como a interligação de dispositivos espalhados pelo mundo inteiro, mediante a utilização de um mesmo padrão de transmissão de dados, qual seja os protocolos *Internet Protocol* (IP).

> Tecnicamente, a Internet consiste na interligação de milhares de dispositivos do mundo inteiro, interconectados mediante protocolos (IP, abreviação de Internet Protocol). Ou seja, essa interconexão é possível porque utiliza um mesmo padrão de transmissão de dados. A ligação é feita por meio de linhas telefônicas, fibra óptica, satélite, ondas de rádio ou infravermelho. A conexão do computador com a rede pode ser direta ou através de outro computador, conhecido como servidor. Este servidor pode ser próprio ou, no caso de provedores de acesso, de terceiros. O usuário navega na Internet por meio de um brower, programa usado para visualizar páginas disponíveis na rede, que interpreta as informações do website indicado, exibindo na tela do usuários textos, sons e imagens.(PINHEIRO, 2016)

Assim sendo, esta tecnologia conhecida por Internet, possibilita ao usuário, por meio de um navegador ("*browser*"), seja ele o Microsoft Internet Explorer, Opera, Google Chrome, ou outros, a abertura de uma página hospedada em um servidor, permitindo seu acesso a dados, voz, vídeos e imagens.

Juntamente com a evolução da Internet, acompanhou-se a evolução da sociedade, visto que essa tecnologia propiciou um estreitamento das relações, permitindo maior interatividade e possibilitando a multimedialidade (combinação de texto, imagem e som) e a hipermedialidade (interconexão de diversos textos entre si), o que acabou por mudar a forma do ser humano se comunicar, bem como sua percepção de mundo, tempo e espaço.

A sociedade atual prima pela a interatividade em tempo real, pelo acesso a informação de forma instantânea e pela praticidade e agilidade que o meio eletrônico proporciona.

A complexidade de tal sistema para a Ciência do Direito está nas relações jurídicas estabelecidas dessa interação, à medida que cominam em direitos e deveres. A Internet trata-se de meio estranho ao Direito enquanto ciência, dada à impessoalidade e efemeridade daquilo que transita pela web, o que resulta em uma insegurança jurídica para os atores.

À medida que a tecnologia evolui, passa-se a necessitar de novas regras para a interação dos indivíduos enquanto sujeitos de direitos e deveres, ao passo que o Direito é resultado do conjunto de comportamento e linguagem e deve acompanhar a evolução social, o que se pretende abordar em tópicos posteriores.

3 DOCUMENTO ELETRÔNICO

Primeiramente, necessário se faz pontuar que a documentação eletrônica pode ser entendida como (i) documento transmitido eletronicamente que possui suporte físico e material[1], como seria o caso de um documento digitalizado por meio de scanner e transmitido eletronicamente em momento posterior; ou (ii) poder-se-ia considerar, também, aquele documento totalmente editado em campo eletrônico.

É intrínseco à Sociedade Digital a tendência de diminuição do uso do papel – documentos físicos – e o crescente uso de documentos eletrônicos, o que acarreta na insegurança quanto à veracidade e autenticidade desses documentos, principalmente quando estes são suportes de declarações de vontade entre partes detentoras de direitos e deveres, consubstanciando relações jurídicas.

Nesse sentido, cabe esclarecer que o papel nada mais é do que a então tecnologia adotada para documentar algo, sendo um tipo de suporte físico no qual uma manifestação de vontade pode estar claramente evidenciada (PINHEIRO, 2016, p. 258).

1 TEIXEIRA, op. cit., p.7

O apego ao papel é facilmente esclarecido quando se compreende o aspecto cultural da utilização do mesmo, em via de regra, para os indivíduos o papel traz segurança de que aquilo que está escrito constitui uma verdade e será cumprido, dada a sua materialidade. Todavia, ao contrário deste crença enraizada, o Código Civil Brasileiro dispõe em seu artigo 107 que “A validade da declaração de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir.”[2]

Ocorre que, para haver o desapego do papel, é necessário que se crie nova metodologia positivada pelo Direito Positivo que traga certificação do documento eletrônico, no sentido de lhe confiar autenticidade e executabilidade, o que se abordará nos tópicos a seguir.

4 ASSINATURA DIGITAL E O CONTEXTO GLOBAL

O uso maciço da Internet pelos indivíduos torna a tecnologia um meio no qual se estabelecem diversas transações, tais como, transações bancárias, contratação de serviços, compra e venda de mercadorias (*e-commerce*), troca de documentos e informações sigilosas, entre outros.

Ocorre que a vulnerabilidade dessas relações reside em uma série de quesitos que podem afetar a função representativa da documentação eletrônica, tais como a) suplantação do autor e fonte da mensagem; b) alteração da mensagem, sem conhecimento da outra parte; c) a circunstância de o emissor negar ter enviado determinada mensagem, ou o destinatário negar ter recebido tal mensagem; e d) o acesso do conteúdo por indivíduo não autorizado (MARTINS, 2016, p. 69).

Principalmente no que se refere à identificação das partes, a assinatura digital vem para preencher esta lacuna, no sentido de constituir prova da expressão de vontade, a fim de possibilitar não só a identificação, mas a verificação de capacidade jurídica das partes, bem como, garantir a executabilidade do pacto.

> A assinatura ou firma eletrônica atende à necessidade de identificação das partes, como marca ou signo que assume o papel outrora reservado ao escrito. A própria noção de assinatura passa por uma redefinição, a partir da sua função, e não a partir da forma, de modo não só a verificação da capacidade jurídica dos contratantes, como também a melhor assegurar o cumprimento das obrigações relativas a cada uma das partes. (MARTINS, 2016, p. 70)

Nessa linha, a assinatura digital deve ser equiparada à forma escrita a próprio punho, no sentido de produzir os mesmos efeitos jurídicos, de sorte a conferir

2 BRASIL. **Código Civil**. Lei nº 10.406, de 10 de Janeiro de 2002. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm> Acesso em: 21 de Jan 2018.

reconhecimento da origem da mensagem e identificação de um usuário aceito e permitido em uma transação.

Dessa maneira, visto sua funcionalidade de contribuir para o estabelecimento de segurança jurídica na Internet, a assinatura digital é amplamente utilizada em contratos eletrônicos e comércio eletrônico.

Todavia, há que se pontuar que os governos estão criando um cenário regulatório cujas abordagens nem sempre coincidem. Pelo que se pode afirmar que, atualmente, existem ao menos três abordagens vigentes da regulamentação do tema:

i. Abordagem minimalista: trata-se de abordagem adotada por países com sistema *common law*: Estados Unidos, Canadá, Nova Zelândia e Austrália. Especifica que as assinaturas eletrônicas não podem ser negadas pois estão em formato eletrônico (KURBALIJA, 2016, p. 162).

ii. Abordagem maximalista: a qual especifica o quadro e os procedimentos das assinaturas digitais. Geralmente esta abordagem adota criptografia e autoridades certificadoras que certificarão os usuários. É o caso de países europeus como Alemanha e Itália (KURBALIJA, 2016, p. 163).

iii. Abordagem da Diretiva de Assinaturas Eletrônicas da UE: trata-se de abordagem mista que considera aspectos da abordagem minimalista e maximalista. Sendo que, adota entendimento minimalista em relação ao reconhecimento de assinaturas digitais em meio eletrônico, bem como reconhece o posicionamento maximalista, ao definir maior segurança jurídica atrelada à concessão de “assinaturas eletrônicas avançadas”, com efeitos jurídicos mais sólidos. Trata-se de posicionamento adotado por estados-membros da União Europeia (KURBALIJA, 2016, p. 162).

No Brasil, através da Medida Provisória nº 2.200-2/2001[3] foi instituída a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), positivando em nosso ordenamento jurídico a adoção de autoridades certificadoras que têm por uma de suas atribuições certificar a assinatura digital de usuários, tema que será aprofundado em tópico posterior.

Nesse sentido, no território brasileiro, a autenticidade de uma assinatura eletrônica depende da certificação de autoridade certificadora. Inclusive, cabe pontuar que o Brasil é um dos únicos países a exigir reconhecimento de firma em documentos oficiais (PINHEIRO, 2016, p. 272).

Em um cenário global, no ano de 1996, a *United Nations Commission on Internet Trade Law* (UNCITRAL), Comissão das Nações Unidas para Leis de Comércio

3 BRASIL. Medida Provisória n° 2.200-2/2001 de 24 de Ago. de 2001. **Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm> Acesso em: 24 de Jan. 2018

Internacional, elaborou a Lei Modelo sobre Comércio Eletrônico[4] que, embora não adentrar especificamente ao tema, dispõe que os registros eletrônicos, para receberem o mesmo nível de reconhecimento legal, devem satisfazer, no mínimo, o exato grau de segurança que os documentos em papel oferecem, de modo a se interpretar que por meio de requisitos técnicos específicos o documento eletrônico poderia alcançar a mesma validade jurídica que um documento em papel assinado a próprio punho.

Posteriormente, no ano de 2001, a UNCITRAL adotou a Lei Modelo sobre Assinaturas Eletrônicas (MLES) que visa habilitar e facilitar o uso de assinaturas eletrônicas, estabelecendo critérios de confiabilidade técnica para a equivalência entre assinaturas eletrônicas e escritas à mão (UNCITRAL, s.d.).

> O MLES baseia-se nos princípios fundamentais comuns a todos os textos da UNCITRAL relativos ao comércio eletrônico, nomeadamente a não discriminação, a neutralidade tecnológica e a equivalência funcional. O MLES estabelece critérios de confiabilidade técnica para a equivalência entre assinaturas eletrônicas e manuscritas, bem como regras básicas de conduta que podem servir de diretrizes para avaliar os deveres e responsabilidades para o signatário, a parte confiante e terceiros confiáveis que intervêm no processo de assinatura. Finalmente, o MLES contém disposições que favorecem o reconhecimento de certificados estrangeiros e assinaturas eletrônicas com base em um princípio de equivalência substancial que ignora o local de origem da assinatura estrangeira. (UNCITRAL, 2001)

Destarte, em um nível global resta clara a viabilidade e a confiabilidade da utilização de assinaturas eletrônicas, haja vista sua equivalência em termos de efeitos jurídicos com a assinatura manuscrita. Sendo necessário, agora, entender de que modo o legislador brasileiro tratou tal matéria e como se dá a segurança jurídica da assinatura digital em contratos eletrônicos.

5 DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

A Medida Provisória 2.200-1/2001[5] instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) no ordenamento jurídico brasileiro, sendo posteriormente reeditada pela Medida Provisória 2.200-2/2001 que transformou o Instituto Nacional de Tecnologia da Informação (ITI) em autarquia.

---

4 UNCITRAL. Resolução 51/162 de 16 de Dez. de 1996. **Lei Modelo sobre Comércio Eletrônico.** Disponível em: < http://www.lawinter.com/1uncitrallawinter.htm> Acesso em: 22 de Jan. 2018

5 BRASIL. Medida Provisória n° 2.200-1 de 27 de Julho de 2001. **Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências**. Disponível em: < http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-1.htm> Acesso em: 24 de Jan. 2018.

Nos termos do artigo 1° da Medida Provisória n° 2.200-2/2001 determina-se que:

> Fica instituída a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. (BRASIL, 2001e)

Assim sendo, a ICP-Brasil consiste em uma estrutura hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão, composta pelos entes a seguir:

5.1 COMITÊ GESTOR DA ICP-BRASIL

A função de autoridade gestora de políticas da ICP-Brasil é de competência do Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República. Nos termos do artigo 3° da Medida Provisória supracitada, o Comitê é composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares: Ministério da Justiça; Ministério da Fazenda; Ministério do Desenvolvimento, Indústria e Comércio Exterior; Ministério do Planejamento, Orçamento e Gestão; Ministério da Ciência, Tecnologia, Inovações e Comunicações; Casa Civil da Presidência da República; e Gabinete de Segurança Institucional da Presidência da República.

Desta maneira, dentre algumas competências do Comitê Gestor da ICP-Brasil estão: (i) adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil; (ii) estabelecer a política e as normas técnicas para o credenciamento das Autoridades Certificadoras (AC), das Autoridades de Registro (AR) e dos demais prestadores de serviço de suporte à ICP-Brasil; (iii) estabelecer a política de certificação e as regras operacionais da Autoridade Certificadora Raiz (AC Raiz), das AC e das AR, bem como definir níveis da cadeia de certificação; (iv) homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço; (v) aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR; entre outras.[6]

---

6 BRASIL. Medida Provisória n° 2.200-2/2001 de 24 de Ago. de 2001. **Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm> Acesso em: 24 de Jan. 2018

5.2 ENTES DA ICP-BRASIL

Ainda, são Entes da ICP-Brasil a Autoridade Certificadora Raiz (AC-Raiz), Autoridades Certificadoras (AC) e Autoridades de Registro (AR). Bem como, também compõem a cadeia a Autoridade Certificadora do Tempo (ACT), Prestador de Serviço de Suporte (PSS), Prestador de Serviço Biométrico (PSBio).[7]

5.2.1 AUTORIDADE CERTIFICADORA RAIZ

A Autoridade Certificadora Raiz da ICP-Brasil é a primeira autoridade da cadeia de certificação. Dente as competências da AC-Raiz está emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu, bem como, executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil.[8]

Cabe esclarecer que A AC-Raiz no Brasil é o Instituto Nacional de Tecnologia da Informação, uma autarquia federal, ligada a Casa Civil da Presidência da República, que tem por missão manter e executar as políticas da Infraestrutura de Chaves Públicas Brasileira.

5.2.2 AUTORIDADES CERTIFICADORAS

As Autoridades Certificadoras são entidades credenciadas a emitir certificados digitais. Dessa forma, competem a elas 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. Além de estabelecer e fazer cumprir, pelas Autoridades de Registro a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação realizada.[9]

Podem ser Autoridade Certificadora entidades públicas e privadas. Atualmente, são 17 (dezessete) Autoridades Certificadoras de 1º Nível credenciadas na ICP-Brasil, entre elas se pode citar: Caixa Econômica Federal, SERASA Experian, Certisign,

7 ITI. **Entes da ICP-Brasil**. Disponível em: < http://www.iti.gov.br/icp-brasil/57-icp-brasil/76-como-funciona> Acesso em: 24 de Jan 2018.
8 ITI. **Entes da ICP-Brasil.** Disponível em: < http://www.iti.gov.br/icp-brasil/57-icp-brasil/76-como-funciona> Acesso em: 24 de Jan 2018.
9 Ibidem

Receita Federal do Brasil, Valid Certificadora Digital, Casa da Moeda do Brasil, Soluti Certificadora Digital, Ministério das Relações Exteriores (AC-MRE), AC Boa Vista, entre outras.[10]

5.2.3 AUTORIDADES DE REGISTRO

Cabe a Autoridades de Registro identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações, sendo a interface Autoridade Certificadora e usuários. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.[11]

5.2.4 AUTORIDADE CERTIFICADORA DO TEMPO

Uma Autoridade Certificadora do Tempo é responsável pelo Carimbo do Tempo, documento eletrônico emitido por uma parte confiável, com finalidade de comprovar que uma informação digital existia numa determinada data e hora no passado, cujo o uso é regulamentado pela ICP-Brasil.[12] Ou seja, trata-se de selo que atesta a data e a hora exatas em que um documento foi criado e/ou recebeu a assinatura digital, servindo assim para comprovar sua autenticidade.

5.2.5 PRESTADOR DE SERVIÇO DE SUPORTE

O Prestador de Serviço de Suporte (PSS) se divide em três categorias, sendo elas: disponibilização de infraestrutura física e lógica; disponibilização de recursos humanos especializados; ou disponibilização de infraestrutura física e lógica e de recursos humanos especializados. Cabe ao PSS desempenhar atividades constantes nas Políticas de Certificado (PC) e na Declaração de Práticas de Certificação (DPC) da AC a que estiver vinculado, diretamente ou por intermédio da AR, ou nas Políticas de Carimbo do Tempo (PCT) e na Declaração de Práticas de Carimbo do Tempo (DPCT) da ACT a que estiver vinculado, bem como nas atividades de Prestador de

10 ITI. **Estrutura da ICP-Brasil.** Disponível em: < http://www.iti.gov.br/images/repositorio/autoridades-certificadoras/estrutura_detalhada.pdf> Acesso em: 24 de Jan 2018.

11 ITI. **Entes da ICP-Brasil.** Disponível em: < http://www.iti.gov.br/icp-brasil/57-icp-brasil/76-como-funciona> Acesso em: 24 de Jan 2018.

12 ITI. **Carimbo do Tempo.** Disponível em: < http://www.iti.gov.br/conteudo-do-menu-superior/28-perguntas-frequentes/131-carimbo-do-tempo> Acesso em: 24 de Jan 2018.

Serviço Biométrico.[13] Assim como outros entes da cadeia hierárquica de certificação o PSS deverá atender rigorosamente aos requisitos estipulados pela ICP-Brasil para que possa atuar.

5.2.6 PRESTADOR DE SERVIÇO BIOMÉTRICO

Para a emissão de um certificado digital é necessária a coleta da biometria do requerente, cabendo ao Prestador de Serviço Biométrico a identificação biométrica, verificação e comparação e biometria através de um ou mais bancos/sistemas de dados biométricos para toda ICP-Brasil, de acordo com os padrões internacionais de uso.[14]

Assim sendo, todos os entes da cadeia hierárquica ICP-Brasil estão envolvidos em seu fim maior, qual seja garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

6 DA SEGURANÇA JURÍDICA E SEGURANÇA DA INFORMAÇÃO EM DOCUMENTOS ELETRÔNICOS ASSINADOS COM CERTIFICAÇÃO DIGITAL

Primeiramente, necessário se faz conceituar o termo certificado digital, que consiste em um arquivo eletrônico gerado por uma Autoridade Certificadora, armazenado em um *hardware* ou *software* a depender do caso, com fim de personificar o indivíduo na rede mundial de computadores, ou seja, identificar com segurança pessoas, físicas ou jurídicas, do autor de uma mensagem ou transação feita em meios eletrônicos como na web, por meio de um par de chaves criptográficas (TEIXEIRA, 2013, p. 111-112).

Nesse sentido, o certificado digital consiste em ferramenta que possibilita que aplicações como comércio eletrônico, assinatura de contratos digitais, operações bancárias virtuais, iniciativas de governo eletrônico, entre outras, sejam realizadas em meio virtual, onde não é necessária a presença do interessado, porém é indispensável a identificação das partes envolvidas.

---

13 ITI. **Entes da ICP-Brasil**. Disponível em: < http://www.iti.gov.br/icp-brasil/57-icp-brasil/76-como-funciona> Acesso em: 24 de Jan 2018.

14 ITI. **Entes da ICP-Brasil**. Disponível em: < http://www.iti.gov.br/icp-brasil/57-icp-brasil/76-como-funciona> Acesso em: 24 de Jan 2018.

6.1 CRIPTOGRAFIA

6.1.1 CONCEITO E BREVE HISTÓRICO

A palavra criptografia tem origem grega, com significado de “escrita secreta”, consiste em estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de maneira que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por agentes não autorizados, ou seja, criptografia é a arte de escrever em códigos de maneira a esconder a informação na forma de um texto incompreensível (MORENO ET AL, 2005, p. 11).

O primeiro relato da história da criptografia aconteceu por volta de 1900 a.C. quando o escriba de Khnumhotep II, então arquiteto do faraó Amenemhet II, teve a ideia de substituir algumas palavras ou trechos de texto, em relação a monumentos construídos para o faraó que deveriam ser documentados e mantidos em sigilo.[15]

Contemporaneamente, a criptografia alcançou grande relevância histórica quando a Enigma, máquina para codificar mensagens desenvolvida por Arthur Scherbius em 1918, inicialmente utilizada para fins comerciais, levantou interesse por parte da marinha de guerra alemã em 1926. Em 1927/28, o exército elaborou sua própria versão, a Enigma G, sendo adotada por todo o exército alemão.[16]

Atualmente, a criptografia moderna é conhecida como criptografia de rede e sua ascensão é diretamente relacionada com o uso em massa da Internet. Na criptografia de rede, a mensagem é criptografada usando-se algoritmos, gerando diversos códigos que executam a criptografia.[17]

6.1.2 CRIPTOGRAFIA SIMÉTRICA E ASSIMÉTRICA

Atualmente, existem dois tipos de criptografia, sendo elas, a simétrica e a assimétrica.

O tipo de criptografia simétrica é o mais comum e pressupõe que uma mesma chave usada para ocultar informação precisa ser aplicada para revela-la na outra ponta[18], ou seja, a mesma chave é usada tanto na codificação (cifragem) quanto na

15 FRANÇA, Waldizar Borges de Araújo. **Criptografia**. Disponível em: < http://www.ucb.br/sites/100/103/TCC/22005/WaldizarBorgesdeAraujoFranco.pdf > Acesso em: 26 de Jan 2018.

16 KRISCHER, Thais Cristine. **Um Estudo da Máquina Enigma**. Disponível em: < https://www.lume.ufrgs.br/bitstream/handle/10183/66106/000870987.pdf> Acesso em 26 Jan. 2018.

17 FRANÇA, Waldizar Borges de Araújo, op. cit.

18 MORENO, Edward David; PEREIRA, Fábio Dacênio; CHIARAMONTE, Rodolfo Barros, op. cit., p. 28.

decodificação (decifragem). Os dois protocolos mais usados para proteção de dados na Internet, o *Secure Sockets Layer* (SSL) e o *Transport Layer Security* (TLS) utilizam a criptografia simétrica para proteger os dados transmitidos e armazenados.[19]

Já a criptografia assimétrica, utiliza-se de duas chaves, uma pública e outra privada. A chave privada deve ser mantida em sigilo e protegida por quem gerou as chaves, enquanto a chave pública é disponibilizada e tornada acessível a qualquer indivíduo que deseje se comunicar com o proprietário da chave privada. Assim, o transmissor cifra a mensagem usando a chave pública do destinatário pretendido, que deverá usar a sua respectiva chave privada para conseguir recuperar a mensagem original (MORENO ET AL, 2005, p. 28).

Cabe ressaltar que a criptografia utilizada em certificação e assinaturas digitais é a assimétrica, na qual utilizando-se da chave privada para criptografar o *hash* da mensagem a chave pública irá conferir a autencidade do documento, ou seja a assinatura digital é formada pegando *hash* da mensagem e criptografando-a com a chave privada do criador.

Para verificar a autenticidade da assinatura é necessário recorrer ao banco de chaves públicas da entidade certificadora, comparando-a com a chave pública de quem enviou a mensagem e com a chave privada do autor da assinatura. Desse modo, a assinatura digital é mecanismo de autentificação que possibilita ao autor da mensagem anexar a esta um código que atue como assinatura. (STALLINGS, 2008).

6.1.3 IMPORTÂNCIA DA CRIPTOGRAFIA

Primeiramente, cabe ressaltar que o advento da rede mundial de computadores no final do século XX abriu a possibilidade de velocidade, comunicação e interatividade em tempo real, tendo por consequência a aceleração dos processos globais, causando a sensação de redução de tempo-espaço, o que por si só justifica a popularização da Internet, que deixou de ter utilidade exclusivamente em meio acadêmico e por órgãos governamentais no início dos anos 90 e passou a fazer parte da rotina da maioria da sociedade, inclusive passando a compor o rol de direitos da população a ser garantido pelo Estado, positivado pelo artigo 2º, inciso I, da Lei Geral de Telecomunicações, Lei nº 9.472/97.[20]

---

19 NOBRE, Erick Pedretti. **Criptografia, você deveria conhecer**. Disponível em: < https://canaltech.com.br/seguranca/Criptografia-voce-deveria-conhecer/> Acesso em 26 de Jan. 2018.

20 BRASIL. Lei nº 9.472, de 16 de Julho de 1997. **Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995.** Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L9472.htm > Acesso em: 22 de ago 2017.

Nesse sentido, diante da rápida ascensão do meio, ainda é tema nebuloso para a ciência, até mesmo para Ciência do Direito, tendo em vista que essa em específico não apenas se ocupa de estudar os aspectos técnicos e históricos da rede mundial de computadores, mas também, tem como principal objeto aquilo que transita pelo meio.

Os símbolos, caracteres, sinais, escritos, imagens, sons e informações de qualquer natureza que trafegam via Internet ganham significado para Ciência do Direito quando observados como relação entre indivíduos que são detentores de direitos e deveres, não pode a Internet ser meio estranho, tendo em vista que é realidade alheia ao mundo físico, e negligenciada pelo Direito em sentido amplo.

Nesse sentido, a nebulosidade do meio gera insegurança quanto à garantia de cumprimento de direitos e deveres em atendimento ao direito positivado, tendo em vista que a Internet, cada vez mais indispensável para a sociedade, deixou de se limitar ao entretenimento e alcançou as relações jurídicas, que passam a ser estabelecidas em campo frágil, efêmero e, muitas vezes, impessoal.

Um dos mecanismos utilizados para assegurar uma experiência segura ao usuário, é a criptografia, que tem por finalidade garantir a confidencialidade (garante acesso a informação apenas aqueles devidamente autorizados), autenticidade (garante a identidade do usuário), não repúdio (garante que a pessoa realizou a transação) e integridade (garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação) daquilo que trafega pelo meio, de um usuário para outro.

Dessa forma, pode-se citar que, entre outras utilidades, a criptografia é a base para o funcionamento de: certificados e assinaturas digitais; mecanismos de autenticação; conexão segura na Web (HTTPS); conexão segura para outras aplicações na Internet (SSL/TLS, IPSec); proteção de dados armazenados em disco, em mídias removíveis e dispositivos móveis; e integridade de consultas DNS (DNSSEC).

6.2 PROCEDIMENTOS PARA EMISSÃO DE CERTIFICADO DIGITAL E REQUISITOS OPERACIONAIS DO PRESTADOR DE SERVIÇOS DE CONFIANÇA DA ICP-BRASIL

Conforme já mencionado no presente artigo, o certificado digital constitui arquivo digital armazenado em um *hardware* ou *software*, a depender do modelo, que contém dados do requerente e serve como uma identidade em meio eletrônico, sendo que, uma de suas utilidades é a assinatura digital.

Ainda, apresentou-se neste artigo a tecnologia envolta na certificação digital, que é a criptografia assimétrica, que tem por escopo garantir à segurança da informação, autenticidade e identificação dos sujeitos envoltos na relação digital.

Contudo, vale, também, ressaltar que, além da criptografia assimétrica, é de grande relevância para a segurança jurídica e segurança da informação do certificado o processo burocrático da sua emissão.

6.2.1 PROCEDIMENTOS PARA EMISSÃO DE CERTIFICADO DIGITAL

O processo de emissão do certificado digital inicia-se com a pessoa (física ou jurídica) solicitando o mesmo perante uma Autoridade Certificadora de sua escolha.

Posteriormente, para a emissão do certificado digital é necessário que o solicitante vá pessoalmente a uma Autoridade de Registro da Autoridade Certificadora escolhida para validar os dados preenchidos na solicitação. Além de levar os documentos obrigatórios, o solicitante passará pelo processo de cadastramento biométrico, com a coleta da biografia facial (foto) e das digitais. Esse processo é chamado de validação presencial.[21]

Vencidas estas etapas, o certificado estará pronto para ser armazenado em *software* ou *hardware* homologados pelo ICP-Brasil.

6.2.2 REQUISITOS OPERACIONAIS DO PRESTADOR DE SERVIÇOS DE CONFIANÇA DA ICP-BRASIL

Ainda, a ICP-Brasil estabelece diversos requisitos indispensáveis para o desenvolvimento de procedimentos na emissão da certificação digital pelos Prestadores de Serviços de Confiança (PSC)[22] - entidade da ICP-Brasil regulamentada pelos DOC-ICP-17 e DOC-ICP-17.01 – tais como[23]:

i. Segurança Pessoal: que estabelece a política de gestão de pessoas que deve ser obrigatoriamente adotada pelo prestadores de serviços de confiança da ICP-Brasil, entre elas:

---

21 ITI. **Como Obter**. Disponível em: < http://www.iti.gov.br/certificado-digital/58-certificado-digital/87-como-obter> Acesso em 26 de Jan, 2018.

22 O PSC tem por tarefa armazenar de chaves privadas dos usuários finais de certificados digitais ICP-Brasil em hardwares criptográficos com acesso remoto, além de facilitar o uso e padronizar as assinaturas digitais e as respectivas verificações.

23 ICP-Brasil. **DOC-ICP-17.01**. Procedimentos Operacionais Mínimos para os Prestadores de Serviço de Confiança da ICP-Brasil. Versão 1.0. Disponível em: < http://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/DOC-ICP-17.01-vero_1.0_PROCEDIMENTOS_OPERACIONAIS_MNIMOS_PARA_OS_PRESTADORES_DE_SERVIO_DE_CONFIANA_DA_ICP-BRASIL.pdf> Acesso em 26 de Jan , 2018.

a) Todo pessoal envolvido nas atividades realizadas pelo PSC, do próprio quadro ou contratado, deverá assinar um termo, com garantias jurídicas, que garanta o sigilo das informações internas e de terceiros, mesmo após a demissão ou o término do contrato;

b) O quadro de pessoal do PSC e contratados deverão possuir um dossiê contendo os seguintes documentos: Contrato de trabalho; Comprovante da verificação de antecedentes criminais; Comprovante da verificação de situação de crédito; Comprovante da verificação de histórico de empregos anteriores; Comprovação de residência; Comprovação de capacidade técnica, entre outros;

ii. Segurança Física: apresenta requisitos mínimos do estabelecimento do prestados de serviços de confiança da ICP-Brasil, entre eles:

a) São definidos pelo menos 4 (quatro) níveis de acesso físico aos diversos ambientes do PSC, sendo que no quarto nível, é especificamente para os PSC de armazenamento de chaves, devendo obrigatoriamente estar no interior ao terceiro nível, é onde deverão ocorrer atividades especialmente sensíveis da operação PSC de armazenamento de chaves privadas.

No quarto nível, todas as paredes, piso e teto deverão ser revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto deverão ser inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não deverão permitir a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem as chamadas salas-cofre - deverão possuir proteção contra interferência eletromagnética externa.

b) O ambiente físico do PSC deverá conter dispositivos que autentiquem e registrem o acesso de pessoas informando data e hora desses acessos, entre outros;

iii. Segurança Lógica: trata de requisitos de proteção de máquinas e arquivos eletrônicos, tais como:

a) O acesso lógico ao ambiente computacional do PSC se dará no mínimo mediante usuário individual e senha, que deverá ser trocada periodicamente;

b) Todos os equipamentos do parque computacional deverão ter controle de forma a permitir somente o acesso lógico a pessoas autorizadas;

c) Os equipamentos deverão ter mecanismos de bloqueio de sessão inativa;

d) As informações como log, trilhas de auditoria (do armazenamento de chaves privadas e serviço de assinatura), registros de acesso (físico e lógico) e

imagens deverão ter cópia de segurança cujo armazenamento será de 6 anos; entre outros.

Assim sendo, a segurança da informação e segurança jurídica da certificação digital é cuidadosamente pensada pela ICP-Brasil, englobando desde a tecnologia criptográfica adotada, até todos os procedimentos a serem adotados pelo entes envolvidos na cadeia de certificação.

7 DO POSICIONAMENTO FAVORÁVEL POSITIVADO NO CÓDIGO CIVIL BRASILEIRO

Conforme supramencionado, o artigo 1° da Medida Provisória n° 2.200-2/2001 determina expressamente sobre a autenticidade, integridade e validade jurídica de documentos em forma eletrônica, que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Coaduna com este posicionamento, o disposto no artigo o artigo 411, inciso II, do Novo Código de Processo Civil – CPC/2015 que considera-se autêntico o documento quando "a autoria estiver identificada por qualquer outro meio legal de certificação, inclusive eletrônico, nos termos da lei".[24]

Na mesma linha, dispõe o artigo 3° da Lei 12.682/2012[25], que no armazenamento de arquivos eletromagnéticos, o processo de digitalização deverá ser realizado de forma a manter a integridade, a autenticidade e, se necessário, a confidencialidade do documento digital, com o emprego de certificado digital emitido no âmbito da ICP-Brasil.

8 CONCLUSÃO

A assinatura de contratos eletrônicos por meio de certificado digital é uma realidade mundial. Entende-se pela validade jurídica das assinaturas por meio da certificação, diante da legislação brasileira citada no presente estudo, assim como acredita-se na segurança jurídica do instituto, haja vista a adoção de criptografia assimétrica, que tem por escopo assegurar a integridade, a privacidade, a autenticidade e não repúdio dos documentos eletrônicos assinados digitalmente. Por

24 BRASIL. **Código de Processo Civil**. Lei 13.105 de 16 de Março de 2015. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm > Acesso em: 19 de set 2017.

25 BRASIL. Lei 12.682 de 9 de Julho de 2012. **Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12682.htm> Acesso em: 26 de Jan. 2018.

conseguinte, defende-se a produção de efeitos no mundo fático de contratos firmados via Internet e assinados por certificado digital, vinculando as partes em seus direitos e deveres.

REFERÊNCIAS

BRASIL. **Código Civil**. Lei nº 10.406, de 10 de Janeiro de 2002. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm> Acesso em: 21 de Jan 2018.

BRASIL. Lei 12.682 de 9 de Julho de 2012. **Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12682.htm> Acesso em: 26 de Jan. 2018.

BRASIL. Lei nº 9.472, de 16 de Julho de 1997. **Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995**. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L9472.htm > Acesso em: 22 de ago 2017.

BRASIL. Medida Provisória n° 2.200-1 de 27 de Julho de 2001. **Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências**. Disponível em: < http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-1.htm> Acesso em: 24 de Jan. 2018.

BRASIL. Medida Provisória n° 2.200-2/2001 de 24 de Ago. de 2001. **Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências**. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm> Acesso em: 24 de Jan. 2018

FAULKNER, William. **Sartoris**. San Diego, California: Harcourt Brace, 1929.

FRANÇA, Waldizar Borges de Araújo. **Criptografia**. Disponível em: < http://www.ucb.br/sites/100/103/TCC/22005/WaldizarBorgesdeAraujoFranco.pdf > Acesso em: 26 de Jan 2018.

ICP-Brasil. **DOC-ICP-17.01**. Procedimentos Operacionais Mínimos para os Prestadores de Serviço de Confiança da ICP-Brasil. Versão 1.0. Disponível em: < http://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/DOC-ICP-17.01-vero_1.0_PROCEDIMENTOS_OPERACIONAIS_MNIMOS_PARA_OS_PRESTADORES_DE_SERVIO_DE_CONFIANA_DA_ICP-BRASIL.pdf> Acesso em 26 de Jan 2018.

ITI. **Carimbo do Tempo**. Disponível em: < http://www.iti.gov.br/conteudo-do-menu-superior/28-perguntas-frequentes/131-carimbo-do-tempo> Acesso em: 24 de Jan 2018.

ITI. **Como Obter**. Disponível em: < http://www.iti.gov.br/certificado-digital/58-certificado-digital/87-como-obter> Acesso em 26 de Jan. 2018.

ITI. **Entes da ICP-Brasil**. Disponível em: < http://www.iti.gov.br/icp-brasil/57-icp-brasil/76-como-funciona> Acesso em: 24 de Jan 2018

ITI. **Estrutura da ICP-Brasil**. Disponível em: < http://www.iti.gov.br/images/repositorio/autoridades-certificadoras/estrutura_detalhada.pdf> Acesso em: 24 de Jan 2018.

KRISCHER, Thais Cristine. **Um Estudo da Máquina Enigma**. Disponível em: < https://www.lume.ufrgs.br/bitstream/handle/10183/66106/000870987.pdf> Acesso em 26 Jan. 2018.

KURBALIJA, Jovan. **Uma Introdução à Governança da Internet**. São Paulo: Comitê Gestor da Internet no Brasil, 2016

MARTINS, Guilherme Magalhães. **Contratos Eletrônicos de Consumo**. 3 ed., rev., atual., e ampl. São Paulo: Atlas, 2016

MORENO, Edward David; PEREIRA, Fábio Dacênio; CHIARAMONTE, Rodolfo Barros. **Criptografia em Software e Hardware**. São Paulo: Novatec, 2005

NOBRE, Erick Pedretti. **Criptografia, você deveria conhecer**. Disponível em: < https://canaltech.com.br/seguranca/Criptografia-voce-deveria-conhecer/> Acesso em 26 de Jan. 2018

PINHEIRO, Patricia Peck. **Direito Digital**. 6 ed. rev. atual. ampl. São Paulo: Saraiva, 2016

STALLINGS, Willian. **Criptografia e Segurança de Redes**. São Paulo: Pearson Prentice Hall, 2008

TEIXEIRA, Tarcisio. **Curso de Direito e Processo Eletrônico:** doutrina, jurisprudência e prática. São Paulo: Saraiva, 2013

UNCITRAL. **Lei Modelo da UNCITRAL sobre Assinaturas Eletrônicas (2001)**. Disponível em: < http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html> Acesso em: 22 de Jan. 2018

UNCITRAL. **Model Law on Electronic Signatures**. Disponível em: <http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf> Acesso em: 22 de Jan. 2018

UNCITRAL. Resolução 51/162 de 16 de Dez. de 1996. **Lei Modelo sobre Comércio Eletrônico**. Disponível em: < http://www.lawinter.com/1uncitrallawinter.htm> Acesso em: 22 de Jan. 2018