

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
CORDENADORIA GERAL DE ESPECIALIZAÇÃO, APEFEIÇOAMENTO E
EXTENSÃO – COGEAE

SORAYA NOLASCO NOUSIAINEN

VALIDADE DA ASSINATURA DIGITAL

São Paulo

2013

**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
CORDENADORIA GERAL DE ESPECIALIZAÇÃO, APEFEIÇOAMENTO E
EXTENSÃO – COGEAE**

VALIDADE DA ASSINATURA DIGITAL

por

Soraya Nolasco Nousiainen

Monografia de final de curso

Professora Mestre Dra. Me. Karla Cristina F. Castro.

São Paulo

2013

SORAYA NOLASCO NOUSIAINEN

VALIDADE DA ASSINATURA DIGITAL

Monografia apresentada à banca examinadora da Coordenadoria Geral de Especialização, Aperfeiçoamento e Extensão – COGEAE / PUC-SP, como exigência parcial para obtenção do certificado de especialização em Direito Contratual, sob a orientação da Professora Dra. Me. Karla Cristina F. Castro.

São Paulo

2013

Dedico este trabalho ao meu filho Lucas Nolasco Nousiainen Farias que apesar de tão novo é o meu “sopro de vida” diário, que me faz quebrar muros e derrubar barreiras para vencer o que parece impossível.

Agradeço à Deus pela concretização de um sonho que eu tenho deste o primeiro ano de faculdade de Direito, que é de ser especialista em contratos. Não a nós, Senhor, nenhuma glória para nós, mas sim ao teu nome, por teu amor e por tua fidelidade! Salmos 115:1

“O pessimista vê dificuldade em cada oportunidade; o otimista vê oportunidade em cada dificuldade.”

(Winston Churchill)

RESUMO

O principal objetivo do presente trabalho é descrever o histórico e a evolução da internet e do comércio eletrônico, conceituar, classificar e descrever a formação do contrato eletrônico para adentrar na questão da validade jurídica da assinatura digital. A assinatura digital é composta por chaves que decodificam mensagens criptografadas e dão segurança, autenticidade e identidade ao signatário do documento eletrônico. Neste trabalho, apresentamos o conceito de criptografia, chaves públicas e privadas, certificação digital e autoridade certificadora. Ao final do trabalho, é apresentado um estudo para identificar a validade jurídica da assinatura digital.

Palavra chave: Assinatura digital

ABSTRACT

The main objective of this work is to describe the history and evolution of the internet and electronic commerce, conceptualize, classify and describe the formation of the electronic contract to enter on the question of legal validity of digital signature. The digital signature consists of keys that decode encrypted messages and provide security, authenticity and identity of the signatory of the electronic document. In this paper, the concept of cryptography, public and private keys, digital certificates and certificate authority. At the end of the paper, we present a study to identify the legal validity of the digital signature.

Keyword: Digital Signature

SUMÁRIO

SUMÁRIO.....	9
INTRODUÇÃO	10
1. COMÉRCIO ELETRÔNICO	12
1.1 Histórico e Conceito de comércio eletrônico.....	12
1.2 Conceito do Contrato Eletrônico	17
1.3 Classificação dos Contratos eletrônicos	19
1.4 Formação e validade do Contrato Eletrônico	22
1.5 Conceito e finalidade da assinatura formal.....	26
2 ASSINATURA DIGITAL	29
2.1 Questão da privacidade, do sigilo e da segurança.	29
2.2 Criptografia, Chaves, Certificação Digital e Autoridade Certificadora.....	31
2.3 Conceito de Assinatura Digital	38
2.4 Validade e eficácia probante.....	41
2.5 Legislações	47
CONCLUSÃO.....	50
BIBLIOGRAFIA	51

INTRODUÇÃO

Com a evolução de novas tecnologias, também se modificam os modos de contratar e conseqüentemente foi necessário criar métodos para permitir atestar a validade do contrato.

A internet foi criada para fins militares, mas atualmente é amplamente usada para o comércio, surgindo assim o contrato eletrônico, mudando a forma de contratar e trazendo diversos questionamentos quanto a segurança e validade destes novos contratos.

Um relatório “Economia Digital Emergente” do governo norte-americano demonstrou que a internet esta crescendo que forma assustadora, segundo este documento, o numero de pessoas que utilizam a rede mundial de computadores tem dobrado a cada cem dias.

Em 2002, foi estimado que o comércio eletrônico ultrapassaria trezentos bilhões de dólares. Mudam as formas de contratar, mudam os meios para proteger os interesses e dar segurança a esses negócios jurídicos.

Os contratos eletrônicos têm como principais características a rapidez e a economia que proporciona aos contratantes. Além disso, caracteriza-se pela desmaterialização, complexidade, simultaneidade devido a sua virtual realização e sua autonomia.

Várias técnicas de contratação eletrônica foram se aperfeiçoando conforme o tempo para assegurar a autenticidade do contrato eletrônico, surgindo assim a Assinatura digital, uma espécie do gênero assinatura eletrônica.

Diante do exposto, o presente trabalho objetiva estudar a validade da assinatura digital nos contratos eletrônicos, ou seja, demonstrar que assinatura digital pode sim assegurar a validade jurídica, eficácia e autenticidade aos contratos eletrônicos.

É importante ressaltar que esta pesquisa não visa aprofundar o estudo que digam respeito às noções elementares dos contratos em geral, tema que entendemos ser de conhecimentos dos especialistas em contratos.

A assinatura digital foi criada a partir da criptografia assimétrica, que visa garantir autenticidade ao contrato eletrônico.

Visando maior compreensão da finalidade do estudo com intuito esclarecer a validade da assinatura digital, o presente trabalho encontra-se dividido em duas partes. A primeira parte denominada Comércio Eletrônico introduz o histórico da Internet e do comércio eletrônico; conceito do contrato eletrônico; classificação dos contratos eletrônicos, formação e validade do contrato eletrônico; e, conceito e finalidade da assinatura formal e a criação de novas formas de assinaturas.

A segunda parte, trata o tema central deste trabalho, a Assinatura Digital, a questão da privacidade e do sigilo nas contratações eletrônicas e a necessidade de uma forma de validar os contratos eletrônicos; conceito e características da criptografia, chaves, certificado digital e autoridade certificadora; e, por fim, a busca da validade jurídica e eficácia da assinatura digital.

Finalizando este trabalho estão a conclusão se há validade na assinatura digital, e por fim, as referências bibliográficas utilizadas neste trabalho.

1. COMÉRCIO ELETRÔNICO

1.1 Histórico e Conceito de comércio eletrônico

A descoberta do telégrafo, como um dos meios de comunicação de massa, em 1838, marca o surgimento de uma era denominada universo da informação, que buscava a necessidade de difundir as informações por meio de aparelhos que unissem a comunicação.

O primeiro computador foi denominado de ENIAC (*Electronic Numeral Integrator Analyzer and Computer*)¹.

Em 1951 foi lançado na Inglaterra o LEO – *Lyons Electronic Office*², o primeiro computador para uso comercial.

Neste contexto, a internet surgiu na Guerra Fria, na década de 1960, quando os norte-americanos criaram uma rede para se comunicar com as bases militares.

Naquela época os Estados Unidos temia um ataque russo às bases militares que poderia trazer a público, informações sigilosas. A rede seria construída para que computadores em diferentes pontos do país fossem ligados entre si, sem depender de uma central. Assim, se Nova Iorque fosse destruída, os outros pontos poderiam continuar comunicando-se sem problemas.

Em 1969 foi criada a *Advanced Research Projects Agency* - ARPA-net³, da Agência de Projetos Avançados do Departamento de Defesa norte-americano, e foi elaborado pela Rand Corporation e foi financiada pelo Ministério da Defesa dos Estados Unidos.

¹ Disponível em: http://www.museudocomputador.com.br/historia_eniac.html

² Disponível em: http://pt.wikipedia.org/wiki/LEO_computer

³ “A ARPA net Consistia na criação de pequenas redes locais (LAN) e coligadas por meio de redes de telecomunicação geográfica (WAN)” - PAESANI, Lilliana Minardi. *Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil*.³ ed. São Paulo: Atlas, 2006- Coleção Temas Jurídicos, p.25

Em 1973 é que iniciou o grande desenvolvimento quando Vinton Cerf, do Departamento de Pesquisa avançada da Universidade da Califórnia registrou o protocolo TCP/IP⁴, que permitiu que diversos computadores, em locais diferentes, a partir de uma linha telefônica comum, se comunicassem, passando assim a ter um custo acessível ao uso particular e individual.

O mais importante elemento, detonador dessa verdadeira explosão, criado em 1989, que permitiu à Internet se transformar num instrumento de comunicação de “massa”, foi o Word Wide Web ⁵(ou WWW, ou ainda W3, ou simplesmente Web), a rede mundial.

Nesses termos, bastava ter um computador, com modem, uma linha telefônica, um provedor e um programa próprio para poder “viajar” pela Internet.

No fim da década de 1980, após ter deixado de ser de interesse militar, essa rede foi expandida pela Nacional Science Foundation (NSF), dos Estados Unidos, e possibilitou a interligação entre Universidades, Agências governamentais e institutos de pesquisas até que, em 1993, o desenvolvimento da tecnologia de informática passou a permitir a comunicação entre um dos objetivos da Internet era permitir que as informações não ficassem limitadas a transmissão de um computador para outro, mas que fosse possível enviar uma informação para uma cadeia de computadores, assim se um computador falhasse a informação estaria disseminada e segura.

A internet é um conjugado de computadores interligados em várias redes, que se comunicam em protocolos unificados, tais como o *transmission Control Protocol* (TCP ou Protocolo de controle de transmissão) e o *Internet Protocol* (IP ou Protocolo da Internet), de

⁴ “ TCP/IP, Protocolo de Controle da Transmissão/Protocolo Internet, que se trata de um código que consente aos diversos networks incompatíveis devido a diferenças de programas e sistemas, comunicarem-se entre si diversos computadores, em locais diferentes - PAESANI, Liliana Minardi-*Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil*.3. ed. São Paulo: Atlas,2006- Coleção Temas Jurídicos, p.25

⁵ A World Wide Web - termo da língua inglesa que, em português, se traduz literalmente por "teia mundial".- disponível em: http://pt.wikipedia.org/wiki/World_Wide_Web

forma que as pessoas que estão conectadas usufruam de serviços de informação e comunicação de alcance mundial.

O IP permite que cada pessoa que acessa a rede, tem uma identidade distinta da outra e, a cada conexão o IP é alterado.

Sendo assim, é possível identificar qualquer internauta (usuário da internet) por meio dos dados armazenados por seu provedor e, correspondentes a aquele IP específico em determinado dia e hora.

Gustavo Testa Correa define internet como:

[...] um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina à outra máquina conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento.⁶

Em 29 de Outubro de 1969 foi enviado o primeiro e-mail da história, o texto que se pretendia enviar era a palavra "LOGIN", mas o computador no *Stanford Research Institute*, que recebia a mensagem, parou de funcionar após receber a letra "O".

A Internet no Brasil teve início em 1991, com o advento da RNP (Rede Nacional de Pesquisa), que era um sistema acadêmico ligado ao MCT (Ministério de Ciência e Tecnologia). Ainda hoje, a RNP é o "backbone"⁷ principal, e abrange instituições e centros de pesquisa, universidades e laboratórios. Com isso, a RNP se responsabiliza pela infra-estrutura de interconexão e informação, controlando o "backbone"⁸.

Apenas oito anos depois do seu lançamento, a internet foi disponibilizada para uso comercial, atingiu a marca de 148 milhões de usuários no mundo inteiro, surgindo assim, o comércio eletrônico através da utilização de contratos eletrônicos.

⁶ CORRÊA, Gustavo Testa. *Aspectos Jurídicos da internet*. São Paulo: Saraiva, 2000. P. 8

⁷ "Backbone traduzindo para português, espinha dorsal, significa rede de transporte, designa o esquema de ligações centrais de um sistema mais amplo." - Disponível em: <http://pt.wikipedia.org/wiki/Backbone>

⁸ "Backbone traduzindo para português, espinha dorsal, significa rede de transporte, designa o esquema de ligações centrais de um sistema mais amplo." - Disponível em: <http://pt.wikipedia.org/wiki/Backbone>

Nos últimos trinta anos o comércio eletrônico foi se moldando, no começo o comércio eletrônico significava a facilitação de transações comerciais, introduzidas no final dos anos 70, permitindo que empresas mandassem documentos comerciais como ordem de compras e contas eletronicamente.

No Brasil, o comércio eletrônico surgiu em 1995, após a internet comercial. As empresas pioneiras em internet comercial nesta época foram: Livraria Cultura, Grupo Pão de Açúcar, Lojas Americanas, Magazine Luiza e Booknet, esta última foi comprada por um grupo de investidores e mudou o nome para Submarino.

A Internet revolucionou as relações de consumo. Desde a sua criação nas universidades americanas⁹ no final da década de sessenta até a sua difusão para o mundo.

Antigamente, os contratos eram realizados pessoalmente, com a criação da internet surgem os contratos eletrônicos, onde a impessoalidade parece ser a nova característica de um mercado cada vez mais globalizado e sem fronteiras.¹⁰

Comércio eletrônico ou e-commerce, ou venda não presencial ou ainda comércio virtual, é um tipo de transação comercial feita por meio eletrônico.

No comércio eletrônico as transações são celebradas à distância desde um telefone celular até o computador, ferramenta mais utilizada nas contratações à distância.

Para Ricardo Lorenzetti¹¹, “o comércio eletrônico seria o conjunto de atividades que tenham por escopo a circulação de bens físicos e/ou digitais no meio eletrônico.”

Para o Ilustre Roberto Senise Lisboa, “Comércio Eletrônico é aquele que se desenvolve pelos meios de comunicação admitidos pelo Direito.”¹²

⁹ FINKELSTEIN, Maria Eugênia Reis. *Aspectos jurídicos do comércio eletrônico*. Porto Alegre. Síntese, 2004, p. 54.

¹⁰ OIKAWA, Allyson Hautsch, *Considerações acerca da possibilidade de concorrência desleal nos links patrocinados em serviço de busca na Internet*. <http://jus2.uol.com.br/doutrina/texto.asp?id=6412>, 04-09-2008, p. 2.

¹¹ LORENZETTI, Ricardo Luis. *Comércio eletrônico*. Buenos Aires: Abeledo Perrot, 2001, p. 53.

Atualmente há dois tipos de contratação básica na internet:

business-to-business (B2B) é a transação entre empresas, envolvendo a comercialização de produtos e prestação de serviços entre produtores, fabricantes, fornecedores e importadores, sem a participação direta do consumidor final.

business-to-consumer (B2C) trata-se dos negócios efetuados através da Internet entre empresas, na qualidade de produtoras, fabricantes, fornecedoras, etc., tendo o consumidor final como último destinatário dos respectivos produtos e serviços. Podemos incluir nesta categoria de transações os populares Internet Banking Systems, que são oferecidos pela quase totalidade dos bancos de varejo à seus clientes e que permitem todo tipo de movimentação financeira.

Contudo, estas relações não se restringem à esfera privada, podendo ocorrer o denominado *Business to Government* - B2G onde o Estado negocia com o empresário, bem como o *Consumers to Government* – C2G onde o Estado trata com os consumidores, porém este tema será abordado nas seções posteriores quando se discorrer sobre a caracterização da relação de consumo via Internet.

O surgimento da internet é um marco para a sociedade, sua utilização tem sido cada vez maior pelas pessoas, em seu dia-a-dia, principalmente para o comércio eletrônico, o que promoveu o surgimento de um fenômeno de ordem global: os contratos eletrônicos.

¹² LISBOA, Roberto Senise. *Manual de Direito Civil*. São Paulo: Ed. Revista dos Tribunais, 2005. p.79

1.2 Conceito do Contrato Eletrônico

O mundo digital, ou internet, trouxe a possibilidade de realização de diversos negócios por meio do computador, os contratos eletrônicos representam a principal característica da inovação trazida pela *internet*.

Tentaremos entender melhor neste capítulo o conceito deste fenômeno global trazido pela *internet*, denominado Comércio eletrônico.

Não é unânime pela doutrina o conceito de contrato eletrônico, variando desde sua nomenclatura até os elementos característicos.

Temos duas posições diferentes na doutrina, sendo que a primeira que defende como contrato eletrônico é o contrato realizado por meio de computador e, a segunda, afirma ser o contrato realizado “*de modo audiovisual através de uma rede internacional de telecomunicações e de uma aceitação suscetível de manifestar-se por meio de interatividade*”.¹³

A segunda posição entende o contrato eletrônico como aquele contrato realizado por qualquer meio de telecomunicação, tais como telefone, fax, incluindo o computador.

Deve-se entender que, “eletrônico” é o meio pelo qual as partes escolheram para efetivar o contrato, uma vez que, em regra, a lei não exige uma forma específica, o contrato pode ser realizado sob qualquer forma, desde que não contrária à lei¹⁴.

Segundo Manoel J. Pereira dos Santos, contratos eletrônicos são “*os negócios jurídicos que utilizam o computador como mecanismo responsável pela formação e instrumentalização do vínculo contratual...*”¹⁵

13 ITEANU, Oliver. Internet et lê droit: aspects juridiques du commerce électronique. Paris: Eyrolles, 1996, apud, LEAL, Sheila do Rocio Cercal Santos. *Contratos Eletrônicos: validade jurídica dos contratos via internet*. São Paulo: Editora Atlas, 2007, p. 78

14 Art. 104. A validade do negócio jurídico requer (...)III - forma prescrita ou não defesa em lei. LEI No 10.406, DE 10 DE JANEIRO DE 2002.

Corretamente, o Projeto de Lei 1.589/99 (posteriormente apensado ao Projeto de Lei 4.906/01), que trata sobre a regulamentação jurídica do comércio eletrônico, não definiu os contratos eletrônicos, limitando-se a indicar os requisitos necessários à validade desses instrumentos, deixando a cargo da doutrina conceituá-la.¹⁶

Não faremos aqui uma análise das nomenclaturas de contratos informáticos, contratos virtuais e contratos artificiais-cibernéticos, pois cada uma delas, com base no vernáculo, levar-nos-ia a outros entendimentos, afastando-se assim do tema deste estudo.

Tendo em vista muitos entendimentos sobre o conceito dos contratos eletrônicos, lançamos mão à definição acertada de Eurípedes Brito Cunha Junior¹⁷:

Contrato eletrônico é o acordo de vontades, celebrado ou executado por via eletrônica, que visa constituir, modificar, conservar ou extinguir direitos, obrigando os respectivos acordantes.

Acrescentamos não menos brilhante definição da Maria Helena Diniz: *“o contrato eletrônico é modalidade de negócio à distância ou entre ausentes, efetivando-se via internet por meio de instrumento eletrônico, no qual está consignado o consenso das partes contratantes.”*¹⁸

Importante, ainda, ressaltar que o contrato deve ser eletrônico na sua formação, pois o objeto contratual pode ou não ser eletrônico.

Nesse sentido, antes de entender o momento da formação do contrato eletrônico é necessário classificá-lo, pois cada classificação de contrato eletrônico possui uma peculiaridade no momento de sua formação.

¹⁵ SANTOS, Manoel J. Pereira dos. *Contratos Eletrônicos*. In: ROVER, Aires José (Org.) *Direito, sociedade e informática: limites e perspectivas da vida digital*. Florianópolis: Boiteux, 2000. P.197

¹⁶ SILVA JUNIOR, Ronaldo Lemos Da e Ivo Waisberg (organizadores). *Comércio eletrônico*. São Paulo: Editora Revista dos Tribunais, 2001, p. 198.

¹⁷ CUNHA JUNIOR, Eurípedes Brito, *Contratos Eletrônicos e o Novo Código Civil*. Artigo da Revista CEJ, nº 19, out./dez.2002. p. 68.

¹⁸ DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro: Teoria das obrigações contratuais e extracontratuais*. São Paulo: Editora Atual, 2009, 3 v. apud TUCCI, José Rogério Cruz e. *Eficácia Probatória dos Contratos Celebrados pela Internet*, in *Direito e Internet*, p. 751.

1.3 Classificação dos Contratos eletrônicos

Mariza Delapieve Rossi e Pereira dos Santos, mencionada na obra de Sheila Leal¹⁹, classificam os contratos eletrônicos em Contratos intersistêmicos, interpessoais e interativos.

Os contratos eletrônicos intersistêmicos são aqueles realizados automaticamente, entre máquinas, previamente programadas, sem que haja nenhuma intervenção humana no momento da contratação.

Sobre os contratos intersistêmicos, Sheila do Rocio²⁰:

Usualmente, as empresas envolvidas na contratação, via EDI, precedentemente ao início das operações comerciais eletrônicas, já disciplinaram e detalharam os direitos e obrigações e as atribuições de cada parte. Contudo, após a programação dos programas aplicativos, não há mais manifestação de vontade humana. As máquinas operam, automaticamente, sem qualquer intervenção do homem.

EDI (Electronic Data Interchange) é a forma de comunicação em que diversos aparelhos eletrônicos trocam informações por meio de protocolos. A tradução literal do tema seria “Troca Eletrônica de Dados”.

Um exemplo que operação comercial através de EDI²¹ se estabelece quando um sistema de comoras de uma empresa comunica-se com o sistema de vendas da empresa fornecedora.

Como há a intervenção de uma pessoa para a programação das máquinas, podemos entender que há manifestação da vontade humana, que participa em linhas gerais do processo de contratação. Sendo assim, há participação da certa intervenção humana nos contratos intersistêmicos.

19 LEAL, Sheila do Rocio Cercal Santos. *Contratos eletrônicos: Validade jurídica dos contratos via internet*. São Paulo: Atlas, 2007, p.225.

²⁰ LEAL, Sheila do Rocio. *Contratos Eletrônicos: Validade Jurídica dos Contratos via Internet*, Ed. Atlas, 2007, p. 83

²¹ O EDI é um método de efetivar comunicação por meio de computador, tendo por base o intercâmbio de transmissão e recepção de dados [...] – BOIAGO JUNIOR, José Wilson p. 88-89. *Contratação Eletrônica: Aspectos Jurídicos*. Curitiba-Juruá, 2005.

A segunda classificação dos contratos eletrônicos, refere-se aos contratos eletrônicos interpessoais, que se realiza através da comunicação entre pessoas por meio de um computador em todas as fases do contrato, por exemplo, em salas de bate papo ou correio eletrônico (*e-mail*).

A principal característica desta forma contratual é a necessidade de uma manifestação ativa das partes, ou seja, é necessária a ação humana tanto para enviar uma proposta através de mensagem, quanto para emitir mensagem de resposta de aceitação.

Assim, segundo os autores Manoel Santos e Mariza Rossi, “as duas manifestações volitivas essenciais ao preenchimento dos requisitos de existência da relação jurídica ocorrem, cada uma ao seu turno, no momento em que seus autores transmitem a mensagem eletrônica”.

Os contratos interpessoais podem ser simultâneos quando comunicação entre o contratante e o contratado se faz em tempo real, como nos contratos realizados pelo telefone, videoconferência ou chats, consideram-se realizados entre presentes.

De acordo com Sheila Leal, no tocante à classificação feita por Erica Brandini Barbagalo²²:

Os contratos eletrônicos interpessoais podem ser simultâneos, quando “celebrados em tempo real, *on line*”, propiciando interação imediata das vontades das partes, a exemplo dos contratos em salas de conversação ou videoconferência, e, como tal, considerados entre presentes; não simultâneos, quando entre a manifestação de vontade de uma das partes e a aceitação pela outra decorrer espaço mais ou menos longo de tempo. A esta última categoria pertencem os contratos por correio eletrônico, equiparados aos contratos entre ausentes, já que mesmo estando as partes se utilizando de seus computadores, concomitantemente, faz-se necessária nova operação para se ter acesso à mensagem recebida.

Quando a manifestação de vontade de uma das partes e a aceitação pela outra decorrer espaço mais ou menos longo de tempo, consideram-se contratos não simultâneos esta

²² ABUD LEAL, Sheila do Rocio. *Contratos Eletrônicos: Validade Jurídica dos Contratos via Internet*, Ed. Atlas, 2007, p. 86.

categoria pertence aos contratos por correio eletrônico, equiparados aos contratos entre ausentes.

Podem-se confundir os contratos eletrônicos interpessoais via e-mail com os efetuados por correio convencional. No entanto, os contratos eletrônicos via e-mail, percorre todo um caminho virtual, através de servidores, até atingir o seu destinatário, sendo assim, tais contratos não se equiparam aos contratos via correio, que denominamos de contratos à distância.

A distinção apresentada é importante, pois dependendo da classificação dos contratos (entre presentes ou entre ausentes), os efeitos jurídicos serão diversos.

Os contratos eletrônicos interativos se caracterizam pela comunicação entre uma pessoa e uma máquina, como por exemplo, a compra em uma loja virtual.

Os contratos eletrônicos interativos são também chamados de “contratos por clique”, pois através do clique do mouse o indivíduo realiza a confirmação dos seus dados e, efetiva o contrato.

É importante ressaltar que estes contratos interativos são considerados de adesão, em razão da impossibilidade de discussão das cláusulas previstas.

Assim como nos contratos interpessoais, os interativos são contratos à distância, tendo em vista que são feitos por meio do computador e não na presença de ambas as partes contratantes, sendo aplicáveis aos contratos de consumo efetivados por esta modalidade, as normas relativas à contratação à distância previstas no Código de Defesa do Consumidor.

Após entender a classificação dos contratos eletrônicos: interpessoais, interativos e intersistêmicos, podemos então passar para o estudo do momento de sua formação, uma vez que como já mencionado cada contrato terá um momento de formação.

1.4 Formação e validade do Contrato Eletrônico

Primeiramente, antes de adentrar a questão da formação do contrato eletrônico, é necessário reforçar que o contrato eletrônico, assim como qualquer outro contrato só será válido juridicamente caso preencha os requisitos legais do artigo 104 do Código Civil: agente capaz, objeto lícito possível, determinado ou determinável, e forma prescrita ou não defesa em lei.

Conforme os ensinamentos de Maria Helena Diniz²³, *"alguns requisitos legais deverão ser preenchidos para que o contrato eletrônico tenha validade e eficácia no mundo jurídico."*

Portanto, para avaliar a validade de um contrato eletrônico, é necessário observar seus elementos de validade, os quais podem ser subjetivos, objetivos ou formais.

Requisitos objetivos: dizem respeito ao objeto do contrato; a validade e eficácia do contrato, como um direito creditório, dependem da: a) licitude de seu objeto; b) possibilidade física ou jurídica do objeto; c) determinação de seu objeto, pois este deve ser certo ou, pelo menos, determinável; d) economicidade de seu objeto, que deverá versar sobre interesse economicamente apreciável, capaz de se converter, direta ou indiretamente, em dinheiro.

Requisitos formais: são atinentes à forma do contrato; a regra é a liberdade de forma, celebrando-se o contrato pelo livre consentimento das partes contratantes.

Requisitos subjetivos: existência de duas ou mais pessoas; capacidade genérica das partes contratantes para praticar atos da vida civil; aptidão específica para contratar; consentimento das partes contratantes.

²³ DINIZ, Maria Helena. Curso de Direito Civil Brasileiro: Teoria das obrigações contratuais e extracontratuais. São Paulo: Editora Atual, 2009, 3 v. apud TUCCI, José Rogério Cruz e. *Eficácia Probatória dos Contratos Celebrados pela Internet*, in *Direito e Internet*. P. 756.

Quanto à formação no negócio jurídico, as ofertas realizadas por intermédio da internet obedecem à regra do art. 427 do CC que determina:

Art. 427: A proposta de contrato obriga o proponente, se o contrário não resultar dos termos dela, da natureza do negócio, ou das circunstâncias do caso.

Neste sentido, o contrato precisa de proposta e aceitação válidas para tornar o negócio virtual existente, válido e eficaz.

O artigo I do artigo 428 do Código Civil trata da proposta “por telefone ou outro meio de comunicação semelhante”, assim concluímos que temos a presença da proposta nos contratos pela internet.

O enunciado 173 do CEJ, com base no artigo 434 do código Civil , preconiza “A formação dos contratos realizados entre pessoas ausentes, por meio eletrônico, completa-se com a recepção da aceitação pelo proponente.”, o que nos remete a presença da aceitação.

Neste sentido, a formação do consentimento nos contratos eletrônicos ocorre, da seguinte forma:

- a) Nos contratos intersistêmicos: no momento da celebração do acordo entre ambas as partes operadoras dos sistemas que, posteriormente irão efetuar a troca de mensagens eletrônicas automaticamente;
- b) Nos contratos interpessoais: o consentimento se dá com o envio do e-mail de confirmação para a outra parte;
- c) Nos contratos interativos: geralmente se concretiza com um clique no botão “confirma” ou qualquer outro correspondente.

A emissão de declaração de vontade efetivada através da Internet, esta se dá através da troca de mensagens eletrônicas entre os contratantes, que, pela definição contida no art. 2º. da Lei Uncitral Sobre Comércio Eletrônico Organização Das Nações Unidas - Nova

York, 1997, é a “*informação gerada, enviada, recebida ou arquivada eletronicamente, por meio óptico ou similares*”.

Cabe ressaltar que a Lei do Comércio Internacional, *United Nations Commission on International Trade Law* – Uncitral foi criada em 1996 pela Organização das Nações Unidas (ONU) por intermédio da Comissão das Nações Unidas .

Por fim, sobre a formação é indispensável agregar a posição da Uncitral em sua Model Law que ensina no seu art. 11²⁴ que menciona que a aceitação de uma oferta pode ser expressa por meio de mensagens de dados, quando uma mensagem de dados é usada na formação de um contrato, o contrato não pode ser negada validade ou exequibilidade com o único fundamento de que a mensagem de dados foi usada para essa finalidade.

Nesse sentido, o Brasil deu um passo à frente no estabelecimento da segurança das contratações virtuais ao estabelecer no Projeto de lei nº 4.906/2001, requisitos para atribuir validade às mensagens enviadas eletronicamente, como se vê:

Título V – Do Comércio Eletrônico

Capítulo I – Da contratação no âmbito do comércio eletrônico

[...]

Art. 26. Sem prejuízo das disposições do Código Civil, a manifestação de vontade das partes contratantes, nos contratos celebrados em meio eletrônico, dar-se-á no momento em que o destinatário da oferta enviar documento eletrônico manifestando, de forma inequívoca, a sua aceitação das condições ofertadas.

§1º A proposta de contrato por meio eletrônico obriga o proponente quando enviada por ele próprio ou por sistema de informação por ele programado para operar automaticamente.

§2º A manifestação de vontade a que se refere o caput deste artigo será processada mediante troca de documentos eletrônicos, observado o disposto nos artigos 27 a 29 desta lei.

Art. 17. O documento eletrônico considera-se enviado pelo remetente e recebido pelo destinatário se for transmitido para o endereço eletrônico definido por acordo das partes e neste for recebido.

Art. 28. A expedição do documento eletrônico equivale:

I – à remessa por via posta registrada, se assinado de acordo com os requisitos desta lei, por meio que assegure sua efetiva recepção; e

II – à remessa por via postal registrada com aviso de recebimento, se a recepção for comprovada por mensagem de confirmação dirigida ao remetente e por este recebida.

²⁴ Article 11. Formation and validity of contracts

In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose. Consulte: http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf -

Assim, considerar-se-ão válidos os atos concluídos eletronicamente, desde que preenchidos os devidos requisitos, pois os contratos são regidos pelo princípio da liberdade das formas, desde que não prescrita ou defesa em lei.

Além disso, deve-se observar se o consentimento manifestado pelas partes está livre de vícios, considerando como tais, todos aqueles aplicáveis aos contratos em geral.

Os contratos eletrônicos têm como principais características a rapidez e a economia que proporciona aos contratantes, caracterizam-se pela desmaterialização, complexidade, simultaneidade devido a sua virtual realização e sua autonomia.

Aquele que utilizar-se do meio eletrônico para divulgar seus produtos ou serviços deve acatar a legislação do Código de Defesa do consumidor, prestar as informações corretas, claras e objetivas, fazer referencia aos riscos à saúde ou segurança dos produtos, indicar os preços, qualidade, quantidade etc.

Quando as informações são disponibilizadas na internet considera-se feita a oferta ao público. A manifestação de vontade do consumidor fica manifestada no momento em que ele acessa o *site*, preenchendo os campos eletrônicos para a contratação e conclui a aceitação.

Importante ressaltar que as regras de contratação pelo comércio eletrônico estão no Decreto nº 7.962, de 15 de março de 2013, que basicamente estabelece que o fornecedor deve disponibilizar ao consumidor informações claras dos produtos ou serviços e do contrato.

Sheila Leal²⁵, no tocante à divulgação dos produtos no ciberespaço, assevera:

No momento em que tais informações são disponibilizadas na Internet considera-se feita a oferta ao público e, conseqüentemente, manifestada a vontade do fornecedor. Já a vontade do consumidor é manifestada no momento em que ele acessa o sistema aplicativo e com ele interage, preenchendo os campos eletrônicos à sua disposição. Ao confirmar os dados, o consumidor conclui a aceitação.

²⁵ LEAL, Sheila do Rocio. *Contratos Eletrônicos: Validade Jurídica dos Contratos via Internet*, Ed. Atlas, 2007, p. 87.

O estabelecimento virtual tem as mesmas obrigações do fornecedor comum perante o consumidor.

O que preocupa a doutrina e a jurisprudência atualmente quanto a validade jurídica do contrato eletrônico é a autenticidade da emissão de declaração de vontade, requisitos presentes na assinatura formal.

1.5 Conceito e finalidade da assinatura formal

A forma mais comum de conferir a autenticidade da emissão de declaração de vontade e identificar os contratantes é assinatura formal.

Segundo a definição do O Dicionário Aurélio , a “assinatura” é o “conjunto de indicações gravadas em talho-doce, xilogravura ou litografia, esclarecedoras dos nomes dos respectivos artistas e artesãos (...)”.²⁶

Dessa forma, assinatura ou firma é um símbolo ou uma marca escrita inserida em algum documento com a finalidade de identificar a sua autoria.

Para Ângela Bittencourt Brasil, membro do Ministério Público do Estado do Rio de Janeiro, a assinatura forma é:

“uma marca personalíssima e tem eficácia e validade jurídica, podendo ser levada ao tabelião para que este faça o seu reconhecimento por semelhança, já que pode ser conservada em arquivos e periciada por meios grafológicos”.²⁷
"A assinatura tal qual hoje se reconhece pode ser conceituada como sendo o ato físico por meio do qual alguém coloca em um suporte físico a sua marca ou sinal, sendo personalíssima"

26 FERREIRA, Aurélio Buarque de Holanda. *Novo dicionário da língua portuguesa*. 1 ed., Rio de Janeiro : Nova Fronteira, 1975, p. 149.

27 BRASIL, Angela Bittencourt. *Assinatura digital não é assinatura formal*. Jus Navigandi, Teresina, Ano 5, N. 48, dez. 2000. Disponível em: <<http://jus2.uol.com.br/doutrina/texto.asp?id=1783>>. Acesso em: 31 mai. 2007.

Francesco Carnelutti,²⁸ menciona três funções da assinatura: a função de autoria (identificar o autor), a função declaratória (atestar a declaração do autor) e a função probatória (possibilitar a averiguação de autenticidade do documento).

As funções mencionadas acima está de acordo com a exegese do nosso Código de Processo Civil:

“Art. 368. As declarações constantes do documento particular, escrito e assinado, ou somente assinado, presumem-se verdadeiras em relação ao signatário. (...)Parágrafo único. Quando, todavia, contiver declaração de ciência, relativa a determinado fato, o documento particular prova a declaração, mas não o fato declarado, competindo ao interessado em sua veracidade o ônus de provar o fato.

" Art. 369. Reputa-se autêntico o documento, quando o tabelião reconhecer a firma do signatário, declarando que foi aposta em sua presença. (...)

Art. 371. Reputa-se autor do documento particular:

I – aquele que o fez e o assinou;

II – aquele, por conta de quem foi feito, estando assinado;

III – aquele que, mandando compô-lo, não o firmou, porque, conforme a experiência comum, não se costuma assinar, como livros comerciais e assentos domésticos”.

O Artigo 368, caput, menciona às funções de *autenticidade* e *declaração* do autor; o Artigo 369 autoriza que a autenticidade possa ser *comprovada por um terceiro legalmente autorizado* (o tabelião); e o Artigo 371 e seus incisos mencionam a questão da *autoria*, bem como seu Inciso III dá *legitimidade para documentos que não tenham sido assinados por força de práticas comerciais*. pois à época ainda não havia sido padronizada a autenticação eletrônica.

Visando a celeridade das relações contratuais atuais, outra forma de assinatura passou a ser aplicada, a assinatura digital, o que abriu margens para diversos questionamentos com a segurança e validade jurídica.

A problemática que se instala refere-se à insegurança quanto à identidade dos contratantes. Em razão da ausência da presença física dos contratantes surge a questão da segurança desta forma de contratação.

28 CARNELUTTI, Francesco. *A prova civil. Título original: La prova civile*. Traduzido por Lisa Pary Scarpa. 2 ed., Campinas : Bookseller, 2002. *Apud* JAEGER, Estêvão Ervino. O valor probante dos documentos eletrônicos e as assinaturas digitais., p. 24

Tentaremos adiante entender o que é uma assinatura digital e, assim buscar nela a mesma segurança que a assinatura formal nos disponibiliza, buscando assim a mesma validade.

2 ASSINATURA DIGITAL

2.1 Questão da privacidade, do sigilo e da segurança.

Antes de adentrar ao conceito da Assinatura Digital, precisamos entender por qual motivo ela foi criada, que foi para garantir privacidade, sigilo e segurança nas contratações pela internet, que cresceu de forma assustadora nos últimos anos.

O total de pessoas com acesso à internet no Brasil no primeiro trimestre de 2013 chegou a 102,3 milhões, segundo o IBOPE Media²⁹.

Esses números nos mostram claramente que com o desenvolvimento da internet cada vez mais as pessoas preferem contratar eletronicamente em virtude da comodidade oferecida.

Em linha gerais, Lorenzetti³⁰ afirma que a internet debilita os limites do lar como espaço privado, é considerada um estágio superior ao rádio, correio, televisão em que indivíduo ou a família pode trabalhar, comprar e até mesmo votar, sem sair de casa.

O que preocupa os juristas com a evolução da internet é desmaterialização do negócio jurídico e com isso a falta de privacidade, sigilo e segurança destes contratos.

Segundo o Professor Newton De Lucca³¹ “estamos progressivamente suprimindo a presença física das partes na celebração do negócio e também a formalidade a eles inerente?

Quanto a evolução da internet, destacamos a doutrina italiana³².

²⁹ Disponível em: <http://www.ibope.com.br/pt-br/noticias/Paginas/Numero-de-pessoas-com-acesso-a-internet-passa-de-100-milhoes.aspx>

³⁰ LORENZETTI, Ricardo L. Comércio eletrônico. São Paulo: Revista dos Tribunais, 2004.

³¹ LUCCA, Newton De. Contratos pela Internet e via Computador. Requisitos de Celebração, validade e eficácia: legislação aplicável. Contratos e Operações bancárias, Revista do TRF da 3ª Região n.º33 jan/mar de 1998. Lejus. São Paulo. P.23

³² “Cio que distingue L'EDI e l'e-mail [...] dalle altre modalità di comunicazioni a distanza è il fatto che i documenti trasferiti attraverso questi media possono essere ulteriormente elaborati elettronicamente e che soprattutto, i messaggi trasmessi non traggono necessariamente origine da un atto stilato su carta né devono subire la conversione su supporto cartaceo per poter essere compresi dagli operatori è invero insito nella loro

Os usuários estão conectados desde sua intimidade, o que abre espaço aos fornecedores para chegarem com suas ofertas diretamente à casa do consumidor.

Preciosa é a contribuição de Diniz, segundo a qual, entende que o dano moral ou patrimonial causado ao usuário do serviço disponível pelo servidor deverá ser reparado por todos os que interferiram na cadeia de consumo, como site, bancos, provedores, que deverão responder solidariamente, podendo o consumidor exigir de qualquer um deles a indenização.

É de verificar que a privacidade é a principal preocupação com a segurança de quem tem relações jurídicas contratuais por meio da internet, sobretudo, a respeito dos dados pessoais que são fornecidos durante o momento da transação comercial, que pode ser captados por terceiros em benefício próprio e ilícito. Portanto, a atenção deve ser o foco principal nas empresas que fornecem os produtos e serviços pela rede. É necessário se ter em mente que comprar pela internet é tão comum quanto se comprar em qualquer estabelecimento

Com efeito, é importante dizer que, havendo violação dos direitos daquele que celebra o contrato eletrônico, há a total responsabilidade do fornecedor por quaisquer danos materiais e morais causados. Ademais, deve-se salientar que tal responsabilidade é solidária entre todos aqueles que interferem na cadeia de consumo, e pode atingir outros direitos da vítima, como, por exemplo, direitos autorais, direitos sobre marcas e patentes etc:

No contrato eletrônico qualquer dano moral ou patrimonial acarretado ao usuário do serviço disponível pelo servidor deverá ser reparado, inclusive por todos os que interfiram na cadeia de consumo, como site, bancos, provedores, spammers etc., que responderão solidariamente, de sorte que o consumidor poderá exigir de qualquer deles a indenização

Conforme disciplina Paulo Sá Elias³³, há preocupação da doutrina com relação aos contratos eletrônicos e sua regulamentação, uma vez que estes contratos já representam parcela considerável das transações comerciais realizadas nos dias de hoje.

Existem técnicas para solucionar a questão, tais como: código secreto, senha ou número de identificação pessoal; leitura por caixa eletrônica da impressão digital da pessoa; reconhecimento de caracteres físicos a longa distância; transmissão de fotografia e criptografia assimétrica, pela qual o contratante se identifica por duas senhas, códigos ou chaves, uma de acesso geral, por ser de conhecimento público e outra particular, mantida em sigilo pelo usuário.

Por fim, creio que o Ilustre Regis Magalhães Soares de Queiroz³⁴ explica exatamente a questão da segurança que buscamos nos contratos eletrônicos e sua possível solução:

Historicamente, segurança eletrônica significa confinamento de dados. Entretanto, confinamento é a antítese da internet. Por isso, hoje a ênfase é dirigida para buscar a tecnologia capaz de garantir a integridade, a autenticidade e a disponibilidade da informação quando necessária. E isso é possível graças ao desenvolvimento da criptografia.

Como vimos, com o crescente número de contratos eletrônicos realizados pela internet, foi necessário que criássemos meios de garantir a privacidade e segurança dos contratantes, uma dessas técnicas, a que mais importa para o presente estudo, foi a assinatura digital, que entenderemos a seguir sua funcionalidade para concluir se essa validade.

2.2 Criptografia, Chaves, Certificação Digital e Autoridade Certificadora.

33 ELIAS, Paulo Sá. *Contratos Eletrônicos e a formação do vínculo*. São Paulo: Lex Editora S.A. 2008, p. 13.

34 QUEIRÓZ, Regis Magalhães Soares de. *Assinatura Digital E O Tabela Virtual. Direito & Internet – aspectos jurídicos relevantes*- Editora Edipro. Bauru, São Paulo, 2000. P 369

Para entendermos o que é a assinatura digital e aprofundar na questão de sua validade é necessário esclarecer os elementos que compõe a assinatura digital: criptografia, chaves, certificado digital e autoridade certificadora.

A palavra criptografia vem do grego *kryptós*, "escondido", e *gráphein*, "escrita", é a ciência ou técnica que transforma um texto de uma mensagem legível em códigos ou cifras ilegíveis, assim só a o destinatário desejável (detentor da chave secreta) da mensagem poderá decodificar e ler a mensagem, tornando a mensagem difícil de ser lida por alguém não autorizado, ou seja, a criptografia transforma textos legíveis, ou texto claro em um texto cifrado ou codificado, que usualmente tem a aparência de um texto randômico ilegível.

A criptografia é tão antiga quanto a própria escrita, os egípcios utilizavam a criptografia no sistema de escrita hieroglífica.

Conta na história que a criptografia era utilizada por Júlio César, os romanos utilizavam códigos secretos para comunicar planos de batalha.

A técnica da criptografia não mudou com o passar do tempo, só após a Segunda Guerra Mundial, com a invenção do computador, que a criptografia foi se aprimorando, incorporando complexos algoritmos matemáticos que hoje são usados em aplicações comerciais.

A criptografia, conforme os ensinamentos de Monteiro Diniz³⁵:

Consiste em uma escrita que se baseia em um conjunto de símbolos cujo significado é conhecido por poucos, permitindo com isso que se criem textos que serão incompreensíveis aos que não saibam o padrão de conversão para sua leitura.

A tecnologia da criptografia foi patenteada em 1983 por professores do Instituto de Tecnologia de Massachusetts (MIT), nos Estados Unidos.³⁶

³⁵ DINIZ, Maria Helena. *Tratado teórico e prático dos contratos*, 5ª. ed., São Paulo, Saraiva, 2003, v. 1.

³⁶ PINHEIRO, Patricia Peck. *Direito Digital*. 5º ed. Editora Saraiva.2013,p 222

Em informática, a criptografia possibilita a alteração do arquivo digital estabelecendo uma posição arbitrária entre seu conteúdo e um novo arquivo criado a partir deste, de modo que, somente através de um procedimento específico de decodificação pode-se reverter a operação, e alcançar novamente compreensão direta das informações que contiver.

Cabe ressaltar o entendimento do Ilustre Roberto Senise Lisboa³⁷:

Na contratação via internet, adota-se a forma virtual para o negócio jurídico, mediante documento eletrônico, que pode ou não se submeter à chamada assinatura criptografada, o que confere maior garantia da conclusão da avença.

As chaves são fundamentais que interagem com um conjunto de algoritmos para a cifragem/decifragem de informações.

As chaves de criptografia são similares às senhas de acesso. Usando a senha correta, o usuário tem acesso ao conteúdo da informação, caso contrário, o acesso é negado. No caso da criptografia, as chaves estão relacionadas com o acesso ou não à informação cifrada. Assim como as senhas, as chaves na criptografia também possuem diferentes tamanhos, sendo seu grau de segurança relacionado ao tamanho da chave.

Há dois tipos de chaves criptográficas: chaves simétricas e chaves assimétricas.

A criptografia simétrica ou chave secreta usa a mesma chave tanto para criptografar como para descriptografar dados.

A criptografia assimétrica usa duas chaves diferentes, porém matematicamente relacionadas, para criptografar e descriptografar dados. Essas chaves são conhecidas como chaves privadas e chaves públicas. Em conjunto, essas chaves são conhecidas como par de chaves. A criptografia assimétrica é considerada mais segura do que a criptografia simétrica, porque a chave usada para criptografar os dados é diferente da que é usada para

37 LISBOA, Roberto Senise. *Manual de Direito Civil*. São Paulo: Ed. Revista dos Tribunais, 2005. p.79

descriptografá-los. Uma chave, chamada pública, é usada para cifrar, enquanto a outra, chamada chave privada ou secreta, é usada para decifrar.

A chave privada é necessariamente sigilosa, permanecendo com seu criador, e a outra (chave pública) é de livre conhecimento por terceiros, devendo ser alvo de ampla divulgação.

Para Patrícia Peck Pinheiro³⁸, no Brasil, o sistema já utiliza duas chaves, publica e privada.

Seguindo ainda a linha de pensamento de Marques³⁹ é importante destacar que:

O padrão criptográfico utilizado para cifrar ou decifrar mensagens é conhecido como chave, quando esta mesma chave é utilizada para cifrar e para decifrar a mensagem, temos a denominada criptografia simétrica, ou chave privada, normalmente utilizada em redes fechadas ou computadores isolados. Esta modalidade de criptografia exige que o destinatário da mensagem conheça o algoritmo utilizado para criptografar a mensagem, pois caso contrário não poderá decifrar o conteúdo dela.

Para garantir que mensagem não foi alterada no percurso do receptor até o destinatário aplica-se sobre o documento editado um algoritmo de autenticação, conhecido como sistema hash⁴⁰, que nada mais é do que um resumo da mensagem, a partir do qual, não é possível recuperar a mensagem original.

Desta forma, sendo aplicada, novamente essa função à mesma mensagem, se obterá a mesma síntese ou mesmo resumo, sendo impossível que duas mensagens distintas dêem lugar a uma síntese idêntica, pelo que se permite verificar que a mensagem coincida com a original.

³⁸ PINHEIRO, Patricia Peck. *Direito Digital*. 5º ed. Editora Saraiva. 2013. p 223

³⁹ SANTOS, Manoel J. Pereira dos. *Contratos Eletrônicos*. In: ROVER, Aires José (Org.) *Direito, sociedade e informática: limites e perspectivas da vida digital*. Florianópolis: Boiteux, 2000

⁴⁰ “Hash é uma complexa equação matemática que utiliza o texto para criar um código chamado “mensagem digest”” - SAMPAIO, Andre Luís Sampaio e MORALES, Guilherme Bacellar Moralez. *Protegendo sua aplicação de ataques Spoofing*. Disponível em: <http://webcache.googleusercontent.com/search?q=cache:ITUsEcbDrToJ:www.microsoft.com/brasil/msdn/Tecnologias/aspnet/Spoofing.msp+&cd=4&hl=pt-BR&ct=clnk&gl=br;>

É perfeitamente possível que uma pessoa intercepte uma mensagem, gerando uma chave pública e retransmitir a mensagem a um destinatário, sem que esse desconfie das alterações do conteúdo do documento, no momento em que decifrar a mensagem.

Dessa forma, para garantir a segurança e evitar fraudes, foi necessário criar um sistema de certificação, a certificação digital, onde a identidade do proprietário das chaves é previamente verificada por uma terceira entidade de confiança dos interlocutores, a Autoridade Certificadora, que terá a incumbência de certificar a ligação entre chave pública e a pessoa que a emitiu, bem como a sua validade.

Além disso, a própria entidade certificadora tem a responsabilidade de disponibilizar os pares de chaves, certificados em diretórios seguros, os quais poderão ser consultados e verificados por qualquer interessado, possibilitando a obtenção de cópias autenticadas dessas chaves.

Pode-se entender que a autoridade certificadora surge como sendo determinada empresa ou organização que emite a certificação digital, ou seja, "é uma entidade independente e legalmente habilitada para exercer as funções de distribuir as chaves," pode ser consultada a qualquer tempo certificando que determinada pessoa é a titular da assinatura digital, da chave pública e da respectiva chave privada.

Esse sistema garante que ninguém receberá uma chave pública, a não ser de uma autoridade certificadora confiável, que a certificou, permitindo na hipótese de ocorrer interceptação da mensagem por um terceiro, saber qual o conteúdo inserto no documento se efetivamente é verdadeiro ou não.

Sendo assim, através do processo de certificação digital a chance se ter fraudada uma chave pública é pequena, uma vez que baste ao destinatário ter o conhecimento da chave pública, única autoridade certificadora, para que possam ser verificados os fatos⁴¹

O certificado digital contém informações como chave pública do autor, nome e endereço do e-mail do autor, data de validade da chave pública, nome da autoridade certificadora, reconhecida. Identifica-se o software e quem o desenvolveu para outras pessoas, além de identificar servidores, usuários e autoridades certificadoras.

No entanto, podemos concluir que as funções das autoridades certificadoras se consubstanciam na geração e registro de chaves, identificação de peticionários, emissão de certificado, armazenamento na autoridade certificadora da chave privada, manutenção das chaves vigentes e revogadas, e serviços de diretórios.

Portanto, as Autoridades Certificadoras são empresas que se encarregam de averiguar a identidade de pessoas e, em função desta averiguação, emitem uma identidade eletrônica. No Brasil, tanto a OAB quanto a SERASA foram alçadas à categoria de Autoridades Certificadoras. Em 2002 a CertSign obteve também a autorização para operar como Autoridade Certificadora Digital dentro da ICP-Brasil. Com isso, poderá emitir certificados de acordo com as normas da entidade governamental, responsável por regulamentar a emissão de Certificados Digitais que darão garantia de integridade e validade jurídica aos documentos eletrônicos

Quando as chaves, tanto públicas quanto privadas, e o certificado perdem sua validade, poderá ocorrer à substituição das mesmas. As autoridades certificadoras certificam a si próprias, simplesmente assinando a sua própria chave pública e postando os certificados em

⁴¹ MARQUES, Antônio Terêncio G. L. *A prova documental na internet: validade e eficácia do documento eletrônico*. Curitiba: Juruá. 2005.

seus sites. Isto é possível, porque contam com o prestígio e a confiança de outras atividades desenvolvidas, tais como os serviços postais ou atividades bancárias.

Conforme o Projeto Lei nº 1.589/99, capítulo II afirma que compete ao tabelião a tarefa de Certificação Eletrônica, impondo regulamentação no tocante à maneira como esses serviços devem ser prestados. A Medida Provisória nº 2.200-2/01 definiu o Comitê Gestor da ICP-Brasil como autoridade gestora de políticas, vinculado à Casa Civil da Presidência da República, com 5 representantes da sociedade civil designados pelo Presidente da República e por representantes de 7 órgãos.

A Autoridade Certificadora Raiz é a primeira autoridade da cadeia de certificação executora das políticas aprovadas pelo Comitê Gestor, competindo-lhe emitir, expedir, distribuir, revogar e gerenciar os certificados das Autoridades Certificadoras de nível imediatamente subsequente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das autoridades Certificadoras e das autoridades de Registro e de seus respectivos prestadores de serviço.

O Projeto de Lei nº 1.589/99 tratou da questão da Autoridade Certificadora também. Dividiu a atividade da certificação em dois grupos distintos:

- 1- as certidões eletrônicas por entidades privadas, de caráter comercial;
- 2 – as certidões eletrônicas por tabeliães, de caráter público;

A Autoridade Certificadora será credenciada a emitir certificados digitais, vinculando pares de chaves criptográficas ao respectivo titular, competindo-lhe emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes, além de manter registro de suas operações.

Após transcorrer sobre cada um dos elementos da assinatura digital podemos então conceituar a assinatura digital com mais clareza.

2.3 Conceito de Assinatura Digital

A assinatura digital é um processo tecnológico que utiliza pares de chaves, publica e privada para decodificar documentos, como principal propósito garantir o sigilo, integridade, autenticidade dos documentos envolvidos em transações eletrônicas e identidade dos contratantes.

Segundo Ribeiro⁴², a assinatura digital é constituída por:

Um conjunto de caracteres alfanuméricos, resultantes de complexas operações matemáticas de criptografia, efetuadas por um computador sobre um documento eletrônico, chamado de "sistema assimétrico de encriptação de dados", este sistema requer a utilização de um par de chaves, uma denominada privada e outra denominada chave pública, uma deverá ser usada para encriptar a mensagem e outra para desencriptá-la. Lembrando que apenas a chave de um dado par é capaz de desencriptar uma mensagem encriptada pela outra do mesmo par, e vice versa.

Para Patricia Peck Pinheiro⁴³, a assinatura eletrônica é, portanto, uma chave privada, ou seja, um código pessoal e irreproduzível que evita riscos de fraude e falsificação.

Primeiramente é importante deixar claro que a assinatura digital é espécie do gênero assinatura eletrônica, que compreende diversas espécies de processos eletrônicos de identificação, tais como: senhas, assinaturas digitalizadas, biometria etc.

Cabe aqui ressaltar a diferença entre a assinatura eletrônica da assinatura digitalizada. A assinatura digital é um tipo de assinatura eletrônica e a assinatura digitalizada trabalha basicamente com captura e análise de dados biométricos como: impressão digital, íris

⁴² SILVA, Rosana Ribeiro. Coordenadores: JUNIOR. Nelson Nery; NERY, Rosa Maria de Andrade: Revista de direito privado. Revista dos Tribunais: São Paulo, 2001, v. 8.

⁴³ PINHEIRO, Patricia Peck. *Direito Digital*. 5ª ed. Editora Saraiva. 2013. p 223

e assinatura manuscrita. Assim, um documento do tipo fax, assinado, ao ser recebido, possuirá uma assinatura digitalizada.

A assinatura digital tem como objetivo garantir principalmente o reconhecimento da autoria e da integridade do conteúdo das declarações de vontades, inseridas no documento eletrônico, essa essência da aplicação da assinatura digital, proporciona aos interlocutores, através das decifrações, chaves, a tradução da mensagem ou até mesmo a verificação da assinatura do remetente com a certeza de que não foi subscrita.

Na contratação eletrônica é muito difícil saber se as partes que estão contratando são as mesmas pessoas que pensamos, sendo grande a dificuldade e a garantia dessas identidades sem o uso da assinatura eletrônica ou digital e as certificações digitais, pois todas as identificações podem ser alteradas e utilizadas por outra pessoa, que não a mesma que estamos pensando realizar o contrato⁴⁴.

A assinatura digital de um documento informático possui três etapas: geração do resumo da mensagem pelo logaritmo *hash*⁴⁵; aplicação da chave privada ao resumo da mensagem, obtendo-se um resumo da mensagem criptografada; e a anexação do certificado digital do autor, contendo, obviamente, a chave pública. Através desse mecanismo, possibilita-se que a assinatura digital ou as assinaturas digitais de um mesmo usuário, utilizando à mesma chave privada, sejam diferentes de documento para documento, pois o sistema *hash* gerado varia em função do conteúdo de cada documento.

A assinatura se divide em duas modalidades:

⁴⁴ PANICHI, Raphael Antonio Garrigoz. Meios de prova nos contratos eletrônicos realizados por meio da internet. (Coordenadores) NERY JÚNIOR, Nelson; NERY, Rosa Maria de Andrade. Revista de direito privado. São Paulo. Revista dos Tribunais. dez 2003, v. 16.

⁴⁵ SAMPAIO, Andre Luís Sampaio e MORALES, Guilherme Bacellar Moralez. Protegendo sua aplicação de ataques Spoofing. Disponível em: <http://webcache.googleusercontent.com/search?q=cache:ITUsEcbDrToJ:www.microsoft.com/brasil/msdn/Tecnologias/aspnet/Spoofing.msp+&cd=4&hl=pt-BR&ct=clnk&gl=br;>

1- A Assinatura Autógrafo: É a inscrição manual comum escrito do próprio nome, pseudônimo ou sinal identificativo da pessoa.

2- A Assinatura Eletrônica: são os vários tipos diferentes de processos técnicos através de meios informáticos para serem aplicados dentre os mais comuns destacamos:

Código Secreto: É uma combinação de algarismos ou letras que condiciona o acesso a sistemas informatizados (password).

Assinatura Digitalizada: é a reprodução da assinatura autógrafa como imagem por um equipamento tipo “scanner” para posterior ou imediata inserção como cópia da original no documento que se objetiva assinar.⁴⁶

Assinatura Digital: Modalidade de assinatura eletrônica criptográfica que consiste, basicamente, em:

Criptografia com Chave Privada (simétrica): Funciona a partir de uma mesma chave possuída pelo emitente e pelo receptor da mensagem e que serve, simultaneamente, para codificá-la e decodificá-la.

Criptografia com Chave Pública (assimétrica): É a utilização de uma chave privada para codificar um resumo (chamado hash) da forma original de um documento e de uma senha distinta (Chave Pública) para decodificar o resumo (hash), que é comparado (após decifrado) ao documento enviado, permitindo, assim, auferir com segurança a origem e a integridade do documento.⁴⁷

Apenas o conceito da assinatura digital não é o bastante para avaliar se está possui a validade necessária para auferir ao contrato eletrônico a validade jurídica que buscamos incessantemente neste estudo. Dessa forma, elaboraremos agora a conclusão de todos os

⁴⁶ SILVA JUNIOR, Ronaldo Lemos Da e Ivo Waisberg (organizadores) . *Comércio eletrônico* . São Paulo: Editora Revista dos Tribunais, 2001 , p. 300.

⁴⁷ BLUM, Renato M. S. Opice (coordenador) e outros . *Direito Eletrônico : a Internet e os Tribunais* . Bauru, SP: EDIPRO,2001, p. 48.

conceitos apresentados até aqui para responder a seguinte questão: A assinatura digital auferir aos contratos eletrônicos autenticidade da emissão de declaração de vontade para sua validade jurídica?

2.4 Validade e eficácia probante

É importante ressaltar que quem pode ter validade jurídica é o contrato e, para que o contrato tenha validade jurídica requer os requisitos do artigo 104 do Código Civil, portanto, o contrato terá validade jurídica se cumprir os requisitos objetivos, subjetivos e formais, já estudados anteriormente.

Para responder se o contrato eletrônico tem validade jurídica, o presente estudo buscou demonstrar a presença dos mencionados requisitos de validade nas contratações eletrônicas e, chegou a presente conclusão: de todos os requisitos destrinchados, o que não houve um entendimento unânime pela doutrina e a jurisprudência sobre sua validade foi a autenticidade da emissão de declaração de vontade produzida pela assinatura eletrônica, mas especificamente, sua espécie, a assinatura digital.

Dessa forma, voltaremos o objeto desta pesquisa para o tema central do presente trabalho: se a assinatura digital é válida para o cumprimento do requisito de validade jurídica do contrato eletrônico, ou seja, a validade da assinatura digital.

Entenda-se que se a assinatura digital for considerada válida, ela não só dará a validade jurídica ao contrato eletrônico, mas terá eficácia probante.

Nesse sentido, Andrea Graziosi ensina que, para que a declaração de vontade seja considerada válida é necessário identificar o emissor, se não podemos identificar o autor não

podemos dizer que estamos diante de uma verdadeira declaração de vontade, e, portanto seu conteúdo não tem força vinculatória ao Direito.⁴⁸

Para o Ilustre Mauricio de Souza Matte⁴⁹:

Para que a assinatura eletrônica tenha a mesma força que a assinatura autografa, é necessário que, de igual forma, sejam garantidos três requisitos:

- 1) identidade: que é a possibilidade de se identificar naquela representação volitiva a autoria, ligando-a a alguém (ou computador), com garantias de certeza;
- 2) integridade: é quando temos certeza que o documento, durante o percurso entre o remetente ou destinatário, não foi adulterado, danificado, etc., ou que, acontecendo, seja possível identificar (assim como nos de papel-vestígios); e
- 3) perenidade: que se refere à durabilidade da validade ao longo do tempo.

Esses fundamentos estão sedimentados nos artigos 332, 368, 369, 371 e seguintes do Código de Processo Civil, como já visto anteriormente.

Para Vinicius Roberto Prioli de Souza⁵⁰

Não exige um exercício reflexivo muito árduo compreender que a assinatura é um dos requisitos que comprovam a autenticidade e integridade de um documento elaborado no mundo real; do mesmo modo ocorre no mundo virtual.

Com a finalidade de legitimar o documento eletrônico como espécie de prova, isto é, meio probatório, segundo Lima Neto, do disposto no art. 332 do Digesto Processual Civil: *“Todos os meios legais, bem como moralmente legítimos, ainda que não especificados neste código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou defesa.”*.

Dessa forma, concluímos que para que a assinatura digital, assim como a assinatura formal, seja considerada válida, devem estar presentes dois requisitos básicos, são eles: autenticidade e integridade.

⁴⁸ GRAZIOSI, Andrea. “*Premesse ad una Teoria Probatoria del Documento Informatico*” n.º 5 pgs 503 e ss. In Revista Trimestrale di Diritto e Procedura Civile, 1998, ano lii, n.º 2 giuffrè, milao

⁴⁹ MATTE, Mauricio de Souza. *Internet*. São Paulo: LTr, 2001.p. 71

⁵⁰ SOUZA, Vinicius Roberto Prioli de. *Contratos Eletrônicos & Validade da Assinatura Digital*. Curitiba: Ed. Juruá. 2012. p. 134

Autenticidade é o registro que permite associar de maneira inequívoca o documento ao seu autor, afastando dúvidas quanto à autoria da manifestação de vontade consubstanciada nos termos do documento eletrônico. Nos documentos físicos a autenticidade é evidenciada pela firma, ou assinatura, que poderá ainda ser reconhecida por tabelião que passa a afirmar sua legitimidade.

Integridade é a certeza da inteireza do conteúdo do documento eletrônico, ou seja, a garantia de que o documento tem seu conteúdo preservado, íntegro durante sua transmissão. Além disso, o processo eletrônico que atribuir integridade a um determinado conteúdo, deve ser de tal forma estabelecido que permita identificar a ocorrência de violação do conteúdo original.

Segundo Antônio Terêncio Marques⁵¹ o ponto nodal que desponta preocupações relacionadas ao documento eletrônico, diz respeito à segurança eletrônica, ao confinamento de dados, entretanto, tal significado é a antítese da internet, devido a isto, a busca de uma tecnologia capaz de garantir a autenticidade, integralidade e a disponibilidade da informação incerta no documento digital.

No Brasil, para garantir a autenticidade, a integridade e a validade dos documentos em forma eletrônica, foi a criação de certificados digitais e autoridades certificadoras pelo Poder Executivo em 24 de Agosto de 2001, que editou a Medida Provisória nº 2.200-2, instituindo a infra-estrutura de Chaves Públicas Brasileiras – ICP Brasil:

A Medida Provisória nº 2.200-2, de 24 de agosto de 2.001, “Art. 1º, Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade e a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações que utilizem certificados digitais, bem como a realização transações eletrônicas seguras” (grifo nosso).

⁵¹ MARQUES, Antônio Terêncio G. L. *A prova documental na internet: validade e eficácia do documento eletrônico*. Curitiba: Juruá. 2005

A Infraestrutura de Chaves Públicas é um conjunto de normas e padrões tecnológicos para garantir a integridade e segurança das comunicações por meio de documentos eletrônicos.

Essa infraestrutura é formada pelas seguintes entidades:

1) *Presidência da República – Casa Civil*: Escolhe os integrantes do Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira e os coordena (Artigo 3º da MP Nº 2.200-2/2001);

2) *Comitê Gestor da ICP-Brasil*: Entidade responsável pela política e normas de certificação, bem como por fiscalizar a atuação da Autoridade Certificadora Raiz (Artigo 4º da MP Nº 2.200-2/2001);

3) *Autoridade Certificadora Raiz*: É responsável por gerar e manter o primeiro certificado digital na estrutura hierárquica da infraestrutura de chaves públicas, sua atividade é exercida pelo Instituto Nacional de Tecnologia da Informação (Artigo 5º da MP Nº 2.200-2/2001);

4) *Autoridades Certificadoras de Nível 1*: Submetidas a requisitos de segurança, integridade, disponibilidade e confiabilidade maiores que as Autoridades Certificadoras de Nível 2, são responsáveis por emitir, gerenciar, revogar e assinar digitalmente os certificados destas (Artigos 6º, 8º e 9º da MP Nº 2.200-2/2001);

5) *Autoridade Certificadora de Nível 2*: É a entidade responsável por emitir, gerenciar, renovar, revogar e assinar digitalmente os certificados digitais das pessoas solicitantes (Artigos 6º, 8º e 9º da MP Nº 2.200-2/2001);

6) *Autoridades Registradoras*: fazem a verificação presencial dos usuários de certificados digitais e podem ou não estar fisicamente ligadas à Autoridade Certificadora à qual se subordinam (Artigos 7º e 8º da MP Nº 2.200-2/2001).

Com relação a autenticação, essa é necessária para identificar com segurança as partes contratantes, a data da realização do contrato, dar proteção contra a adulteração do conteúdo dos documentos e proporcionar, com isso, força de prova aceitável juridicamente. Para tanto, esse método deve proporcionar segurança, por meio da combinação dos seguintes fatores:

1) *Autenticidade*: certeza jurídica sobre o criador do documento, conseguida em parte por meio da entidade certificadora, em parte pela segurança dos algoritmos de criptografia;

2) *Integridade*: impedir a adulteração da mensagem digitalmente assinada, conseguida pela proteção que a assinatura digital dá à mensagem;

3) *Não repúdio*: uma vez assinado o documento e enviado para a outra parte, não pode haver dúvidas quanto sua à criação pelo remetente, conseguida pela força do algoritmo de criptografia mais a proteção da chave privada;

4) *Tempestividade*: a entidade certificadora pode se tornar responsável por atestar a data e a hora nas quais o documento eletrônico foi assinado, de forma a possibilitar a averiguação da tempestividade da mensagem ou documento eletrônicos, ao mesmo tempo em que resolve o problema da testemunha eletrônica;

5) *Confidencialidade*: somente os destinatários da mensagem (partes e entidade certificadora) e autorizados por estes podem lê-la (para impedir que o conteúdo de um contrato seja interceptado durante o processo de certificação eletrônica, que envolve a comunicação do documento à entidade certificadora)

A certificação digital das transações eletrônicas, torna-se menos complexo para as partes poderem exigir uma das outras o cumprimento das obrigações, pois há a figura do terceiro confiável, a entidade certificadora autorizada por lei a atuar como espécie de notário

das transações eletrônicas. Porém, isso não torna absolutamente certo que com o uso das chaves digitais, dentro das normas da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, todo contrato eletronicamente assinado será sempre exigível.

A assinatura digital é apenas um meio de prova com o suporte de novos dispositivos legais e técnicos, com o qual se identificam as partes que usam meios eletrônicos para comunicação com segurança maior, mas não absoluta. Nada impede que um dos contratantes alegue que houve uma quebra na chave e consiga provar perante o juiz: não se pode esquecer que ela possui validade temporal justamente para minimizar, mas não eliminar de vez, os riscos de segurança no ambiente cibernético. Esse é um argumento facilmente utilizável pelo consumidor pessoa física, mas não pelo fornecedor ou consumidor enquanto pessoa jurídica:

A própria legislação a qual deu validade aos certificados eletrônicos permite essa interpretação:

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

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

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

Portanto, tendo em vista os argumentos apresentados neste estudo das técnicas de criptografia e assinaturas assimétrica, bem como a criação de certificados digitais e autoridades certificadoras pelo Poder Executivo em 24 de Agosto de 2001, que editou a Medida Provisória nº 2.200-2, instituindo a infra-estrutura de Chaves Públicas Brasileiras – ICP Brasil, a assinatura digital é válida como requisito de validade jurídica do contrato eletrônico.

Estudaremos adiante os projetos de leis e as legislações vigentes sobre o tema de contratação eletrônica.

2.5 Legislações

As primeiras legislações referentes à assinatura digital e aos contratos comerciais eletrônicos foram criadas nos Estados Unidos ("United Nations Commission on International Trade Law" - UNCITRAL) e, na Alemanha (Lei Federal que trata dos serviços de comunicação e informação, regulamentando a própria assinatura digital).

Não temos no Brasil uma legislação específica sobre contrato eletrônico. No entanto, preocupados em acompanhar o ritmo da evolução da Informática, revogaram a Lei nº. 7.646, de 18 de dezembro de 1987, que falava sobre propriedade intelectual. Ela foi substituída pela atual Lei nº 9.609, de 19 de fevereiro de 1998. Com essa nova lei, os questionamentos sobre propriedade intelectual ficaram mais específicos para o uso de programa de computadores.

Há vários projetos de Lei sobre assinatura digital em tramitação, dentre eles destacamos, o Projeto de Lei 2161/91, Projeto de Lei 5067/91, Projeto de Lei 1713/96, Projeto de Lei 1233/99, Projeto de Lei 1532/99, Projeto de Lei 1589/99, Projeto de Lei 2504/2000, Projeto de Lei 3475/2000, Projeto de Lei 6896/2002, Projeto de Lei 6965/2002, Projeto de Lei 7316/02 e o Projeto de Lei 1237/2003.

De todos os projetos mencionados, um dos mais importantes é o Projeto de Lei 4906/01, apensados os Projetos de Lei 1483/99 e 1589/99 (OAB) , que dispõe sobre o valor probante do documento eletrônico e da assinatura digital, regula a certificação digital, institui normas para as transações de comércio eletrônico e dá outras providências.

Quanto às legislações vigentes, as mais importantes são:

1 - A Medida Provisória nº 2.200-2, de 24 de agosto de 2001 instituindo a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil e MP 22000 - Todos os contratos assinados são feitos dentro dos padrões estabelecidos pelos Órgãos Reguladores e amparados pela MP 2200-2.

2- Circular 3.234 do BACEN de 16 de abril de 2004 – Câmbio: desde 10/05/2004 todas as Instituições que operam em câmbio estão autorizadas a realizar a assinatura digital de contratos de câmbio. O normativo alterou a regulamentação cambial para prever a assinatura digital por meio da utilização de certificados digitais no âmbito da Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil).

3 - Circular 277 - Susep - Faculta a utilização da assinatura digital nos documentos eletrônicos relativos às operações de seguros, de capitalização e de previdência complementar aberta, por meio de certificados digitais emitidos no âmbito da Infra-estrutura de Chaves Públicas (ICP-Brasil), e dá outras providências.

4 – Lei 9755 de 16 de dezembro de 1998 – criação do homepage do TCU.

5 – Lei 9800 de 26 de maio de 1999 – Sistema de transmissão de dados para prática de atos processuais.¹

6 - Lei 9983 de 14 de julho de 2000 - Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências. 2

7 - O Decreto Lei nº 3.587/00 define finalidades e os efeitos que os documentos eletrônicos poderão produzir.

8- Lei 11.419/06 - Dispõe sobre a informatização do processo judicial; altera a Lei no 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências.

Podemos dividir o processo de regulamentação especificamente para assinatura digital no Brasil, até o presente momento, em 6 (seis) fases ou etapas:

- Fase 1: Lei Modelo das Nações Unidas sobre Comércio Eletrônico em 1996 (UNCITRAL).

- Fase 2: Projeto de Lei n. 672, de 1999, do Senado Federal: Incorpora, na essência, a lei modelo da UNCITRAL.

- Fase 3: Projeto de Lei n. 1.483, de 1999, da Câmara dos Deputados. Em apenas dois artigos, pretende instituir a fatura eletrônica e a assinatura digital (certificada por órgão público).

- Fase 4: Projeto de Lei n. 1.589, de 1999, da Câmara dos Deputados. Elaborado a partir de anteprojeto da Comissão de Informática Jurídica da OAB/SP, dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital.

- Fase 5: Edição de Decreto pelo Governo Federal n. 3.587, de 5 de setembro de 2000. Institui a Infraestrutura de Chaves Públicas do Poder Executivo Federal.

Fase 6: Edição da Medida Provisória 2.200 de 2001. Esse diploma legal instituiu a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil para garantir a autenticidade e a integridade de documentos eletrônicos através da sistemática da criptografia assimétrica.

Dessa forma, a legislação mais adequada ao tema deste estudo é a Medida Provisória 2.200 de 2001.

CONCLUSÃO

Após estudar a evolução da internet, verificou-se que a assinatura digital foi criada para garantir privacidade e segurança para as transações eletrônicas.

Estudando os elementos e a funcionalidade da assinatura digital, somadas com as legislações aplicáveis, confluímos que:

A assinatura digital com chave pública, quando usada corretamente, isto é, sem o compartilhamento dos dados privados com terceiros e o uso de uma senha longa e complicada para a decodificação da própria assinatura digital, garante ao leitor do documento por ela assinado que somente poderia ter sido criado “com informações privadas do signatário”, dado que a descoberta da chave privada por meio de ataques à chave pública pode levar tempo considerável em anos, conforme o tamanho das chaves, suas renovações e a qualidade dos algoritmos criptográficos aumente para acompanhar a capacidade dos computadores os quais possam ser usados para realizar a criptoanálise.

Portanto, é possível “provar para um terceiro (juiz em um tribunal) que só o proprietário da chave privada poderia ter gerado a mensagem”, alcançando assim as finalidades da assinatura formal e auferindo aos contratos eletrônicos autenticidade da emissão de declaração de vontade para sua validade jurídica.

Para tornar possível a identificação da parte e a integridade do documento eletrônico, a assinatura digital individualiza o autor do documento, uma vez que é constituída por signos ou chaves que pertencem exclusivamente ao proprietário.

Haverá presunção *juris tantum* da validade do documento digitalmente assinado e do fato de que houve transmissão dos sinais por pessoas autorizadas.

BIBLIOGRAFIA

- BLUM, Renato M. S. Opice (coordenador) e outros . Direito Eletrônico : a Internet e os Tribunais . Bauru, SP: EDIPRO,2001
- BRASIL, Angela Bittencourt. Assinatura digital não é assinatura formal. Jus Navigandi, Teresina, Ano 5, N. 48, dez. 2000. Disponível em: <<http://jus2.uol.com.br/doutrina/texto.asp?id=1783>>. Acesso em: 31 mai. 2007.
- BOIAGO JUNIOR, José Wilson p. 88-89. *Contratação Eletrônica: Aspectos Jurídicos*. Curitiba-Juruá,2005
- CARNELUTTI, Francesco. A prova civil. Título original: La prova civile. Traduzido por Lisa Pary Scarpa. 2 ed., Campinas : Bookseller, 2002. Apud JAEGER, Estêvão Ervino. O valor probante dos documentos eletrônicos e as assinaturas digitais.
- CORRÊA, Gustavo Testa. Aspectos Jurídicos da internet. São Paulo: Saraiva, 2000. CUNHA JUNIOR, Eurípedes Brito, Contratos Eletrônicos e o Novo Código Civil. Artigo da Revista CEJ, nº 19, out./dez.2002.
- DINIZ, Maria Helena. Curso de Direito Civil Brasileiro: Teoria das obrigações contratuais e extracontratuais. São Paulo: Editora Atual, 2009, 3 v. APUD TUCCI, José Rogério Cruz e. Eficácia Probatória dos Contratos Celebrados pela Internet, in Direito e Internet.
- DINIZ, Maria Helena. Curso de Direito Civil Brasileiro: Teoria das obrigações contratuais e extracontratuais. São Paulo: Editora Atual, 2009, 3 v. , APUD BASSO, Maristela. Contratos Internacionais de Comércio, 1998.
- DINIZ, Maria Helena. Curso de Direito Civil Brasileiro: Teoria das obrigações contratuais e extracontratuais. São Paulo: Editora Atual, 2009, 3 v.
- ELIAS, Paulo Sá. Contratos Eletrônicos e a formação do vínculo. São Paulo: Lex Editora S.A.2008.
- FERREIRA, Aurélio Buarque de Holanda. Novo dicionário da língua portuguesa. 1 ed., Rio de Janeiro : Nova Fronteira, 1975, p. 149.
- FINKELSTEIN, Maria Eugênia Reis. Aspectos jurídicos do comércio eletrônico. Porto Alegre. Síntese, 2004
- GRAZIOSI, Andrea. “Premesse ad una Teoria Probatoria del Documento Informatico” n.º 5 pgs 503 e ss. In Revista Trimestrale di Diritto e Procedura Civile, 1998, ano lli, n.º 2 Giuffrè, Milão.
- ITEANU, Oliver. Internet et lê droit: aspects juridiques du commerce électronique. Paris: Eyrolles, 1996, apud, LEAL, Sheila do Rocio Cercal Santos. Contratos Eletrônicos: validade jurídica dos contratos via internet. São Paulo: Editora Atlas, 2007.
- LEAL, Sheila do Rocio Cercal Santos. Contratos eletrônicos: Validade jurídica dos contratos via internet. São Paulo: Atlas, 2007, p.225.
- LEI No 10.406, DE 10 DE JANEIRO DE 2002.
- LISBOA, Roberto Senise. Manual de Direito Civil. São Paulo: Ed. Revista dos Tribunais,2005.
- LORENZETTI, Ricardo L. Comércio eletrônico. São Paulo: Revista dos Tribunais, 2004.
- LORENZETTI, Ricardo Luis. Comércio eletrônico. Buenos Aires: Abeledo Perrot, 2001.
- LUCCA, Newton De. Contratos pela Internet e via Computador. Requisitos de Celebração, validade e eficácia: legislação aplicável. Contratos e Operações bancárias, Revista do TRF da 3º Região n.º33 jan/mar de 1998.Lejus. São Paulo.
- MARQUES, Antônio Terêncio G. L. A prova documental na internet: validade e eficácia do documento eletrônico. Curitiba: Juruá. 2005
- MATTE, Mauricio de Souza. Internet. São Paulo: LTr, 2001.

OIKAWA, Allyson Hautsch, Considerações acerca da possibilidade de concorrência desleal nos links

PANICHI, Raphael Antonio Garrigoz. Meios de prova nos contratos eletrônicos realizados por meio da internet. (Coordenadores) NERY JÚNIOR, Nelson; NERY, Rosa Maria de Andrade. Revista de direito privado. São Paulo. Revista dos Tribunais. dez 2003, v. 16.

patrocinados em serviço de busca na Internet. <http://jus2.uol.com.br/doutrina/texto.asp?id=6412>, 04-09-2008.

PAESANI, Liliana Minardi. Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil. 3. ed. São Paulo: Atlas, 2006- Coleção Temas Jurídicos

PICCOLO, Paolo e ZANOLINI. Giovanna. II documento eletrônico e la firma digitale, in I Problemi Giuridici di internet, 1999, Giuffrè, Milão.

PINHEIRO, Patricia Peck. Direito Digital. 5º ed. Editora Saraiva. 2013

QUEIRÓZ, Regis Magalhães Soares de. Assinatura Digital E O Tabela Virtual. Direito & Internet – aspectos jurídicos relevantes- Editora Edipro. Bauru, São Paulo, 2000

SANTOS, Manoel J. Pereira dos. Contratos Eletrônicos. In: ROVER, Aires José (Org.) Direito, sociedade e informática: limites e perspectivas da vida digital. Florianópolis: Boiteux, 2000.

SILVA JUNIOR, Ronaldo Lemos Da e Ivo Waisberg (organizadores). Comércio eletrônico. São Paulo: Editora Revista dos Tribunais, 2001

SILVA, Rosana Ribeiro. Coordenadores: JUNIOR. Nelson Nery; NERY, Rosa Maria de Andrade: Revista de direito privado. Revista dos Tribunais: São Paulo, 2001, v. 8

SOUZA, Vinicius Roberto Prioli de. Contratos Eletrônicos & Validade da Assinatura Digital. Curitiba: Ed. Juruá. 2012.

Consulte: http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

<http://www.ibope.com.br/pt-br/noticias/Paginas/Numero-de-pessoas-com-acesso-a-internet-passa-de-100-milhoes.aspx>

http://www.museudocomputador.com.br/historia_eniac.html

http://pt.wikipedia.org/wiki/LEO_computer

http://pt.wikipedia.org/wiki/World_Wide_Web

<http://pt.wikipedia.org/wiki/Backbone>