CURSO DE DIREITO

“Validade da Assinatura Digital no Contrato Eletrônico”

NILSON MINEO MORISAVA
RA 481.724/0
Turma 3209C1
Cel. (11) 8237-2653
E-mail : nilsonmm@hotmail.com

SÃO PAULO
2007

CURSO DE DIREITO

"Validade da Assinatura Digital no Contrato Eletrônico"

NILSON MINEO MORISAVA
RA 481.724/0
Orientadora:
Profa. Dra. Liliana Minardi Paesani

Monografia apresentada à Banca Examinadora do Centro Universitário das Faculdades Metropolitanas Unidas, como pré-requisito para obtenção do título de Bacharel em Direito, sob a orientação da Profa. Dra. Liliana Minardi Paesani.

SÃO PAULO
2007

Avaliação da Monografia:

BANCA EXAMINADORA:

Profa. Orientadora: Dra. Liliana Minardi Paesani

Prof. Argüidor: _____

Prof. Argüidor: _____

Comentários:

_____
_____
_____
_____
_____
_____
_____
_____

Resultado da Avaliação:

Nota: _____ (_____)

_____

Profa. Dra. Liliana Minardi Paesani

_____ _____

1º Prof. Argüidor: 2º Prof. Argüidor:

DEDICATÓRIA

Aos meus pais que sempre me apoiaram em tudo, desde o ginásio, posteriormente no Curso Técnico e em meu primeiro curso superior em Engenharia que me formei, porém meu pai, *in memorian* não pode ver-me formado. Minha mãe que continua comigo sempre me incentivou e principalmente nesta outra graduação que hoje falta apenas um semestre e meio, se orgulha pelo que conquistei até hoje e faço tudo isso por eles. Estas conquistas são para provar tamanha gratidão que tenho por eles, pela educação e dignidade que tenho hoje.

A todos os meus amigos que compartilharam comigo os anos de estudo e expectativas no cotidiano da vida, sabendo cultivar uma amizade que o tempo amadureceu, com os quais vivemos juntos tantas horas e carregamos as marcas das experiências comuns que tivemos. Foram vários anos de luta, dias e noites em claro para estudar, uma batalha árdua que vencemos, juntos, um ajudando o outro, que sem estes não teria tanto êxito.

Foram tantos os professores nesses anos, que de alguns me foge a lembrança neste momento, mas lembro dos grandes ensinamentos que nos passaram. Foram tantas as lições aprendidas, e uma coisa é certa: das salas de aula saímos melhores e mais fortes para enfrentar este mercado tão concorrido.

Minhas homenagens àqueles que dedicaram suas vidas ao ensino, pois deles é o mérito de moldar as vocações e incentivar o raciocínio do estudante, transformando os ideais em realizações.

Não posso deixar de destacar dentre o corpo docente minha grande orientadora Dra. Liliana Minardi Paesani que confiou em mim e ao meu amigo e orientador de 2 anos de iniciação científica Dr. Irineu Francisco Barreto Junior que me preparou para o êxito nesta monografia.

E não poderia deixar de lembrar de minha companheira, minha noiva e futura esposa Elaine Mikie Futenma que me agüentou todos estes anos e devo minha vida a ela.

SUMÁRIO

PARTE I – INTRODUÇÃO

1 - Estudos Iniciais

No Brasil não se encontrava nada muito específico na legislação sobre o Contrato Eletrônico. Todavia, os nossos legisladores, 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 n° 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.

Além disso, houve vários projetos de Lei muitos ainda em tramitação, dentre eles 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, que serão novamente tratados ao final da monografia.

Um dos mais importantes é o Projeto de Lei 4906/01 – apensados os Projetos de Lei 1483/99 e 1589/99 (OAB) - 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.

Não poderia deixar de citar também:

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 Orgãos 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.

E as Leis e Decreto Leis:

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

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

3 - 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]

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

O computador é dividido em duas partes. O hardware é a máquina em si e o software é aquilo que vai fazer essa máquina funcionar. É o conjunto de informações organizadas que diz a máquina como ela deve reagir. O contrato de licença de uso é um dos mais utilizados em todo o mundo na comercialização de software, onde as empresas detentoras dos direitos autorais dos programas de computador negociam seus produtos com os interessados.

Há vários tipos de negócios jurídicos pela internet. Além dos contratos com objeto de Internet, a vida digital possibilitou o surgimento de uma nova espécie de instrumento que serve à realização de negócios jurídicos: os contratos eletrônicos. O Projeto de Lei n.1.589, de 1999 e o Projeto de Lei n. 4906/01, 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 definição a cargo da doutrina.

---

[1] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros. Direito & Internet : aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2º. Edição, 2005, p.46.

[2] ITAU. Disponível em <www.itaubank.com.br/popups/ contratos_digitais /legislacao.asp> Acesso em: 20 ago.2007.

Os contratos eletrônicos, que posteriormente será mais bem conceituado, podem ser definidos como instrumentos obrigacionais de veiculação digital. São todas as espécies de sinais eletrônicos transmitidos pela Internet que permitem a determinação de deveres e obrigações jurídicos. Os contratos eletrônicos, que nada mais são do que uma espécie de documento eletrônico, que caracteriza um negócio jurídico, traz ainda grande discussão quanto à sua validade, vez que não podem ser efetivamente tratados como documentos jurídicos.

Dentre as questões mais polêmicas, temos a identidade das partes (falsidade ideológica, incapazes, etc.), a integridade do conteúdo do contrato (possibilidade de alterações), e a falta de assinatura de próprio punho dos contratantes, talvez um dos maiores problemas envolvendo os contratos eletrônicos. Mas é evidente que algum elemento de prova deve nos levar a identificar o seu autor, fato que não se presume. Assim, mesmo nestas circunstâncias, aquele que juntar documentos não subscritos, se contestada a autoria, terá o ônus de prová-la.

Por isso os contratos eletrônicos precisam ser assinados para conferir maior segurança às partes contraentes. A mesma regra se aplica para documentos eletrônicos em geral. A assinatura digital surgiu para suprir uma necessidade imposta pelo comércio eletrônico, em que nem sempre a presença física dos contraentes é possível, utilizando-se de sua assinatura tradicional. Ademais, sabe-se que no mundo real, várias situações são resolvidas apenas pelo fato de as partes se encontrarem. No mundo virtual, esse contato não existe e esta troca de informações visuais é inexistente. As várias impressões que nossa pessoa física provoca na parte contrária, não ocorrem no mundo virtual. Este anonimato é que torna tão diferente do mundo real.

A assinatura digital não é física como nos contratos tradicionais, uma vez que normalmente os contratos eletrônicos não são impressos. As partes não chegam a se encontrar para formalizar a contratação e os contratos eletrônicos devem ser assinados eletronicamente. Esse conceito, por ser novo para o mundo jurídico, gera efeitos diferenciados e possui forma própria. É importante destacar-se, ainda, que novas regulamentações acerca da assinatura digital vêm sendo produzidas pelos órgãos legislativos brasileiros e estrangeiros até hoje.

Hoje, a palavra de ordem é repensar e mudar o comportamento. Ninguém discute que a popularização do uso da informática trouxe vários questionamentos e conflitos jurídicos que, requerem atenção imediata e urgente dos doutrinadores e legisladores do mundo inteiro, já

que os contratos, os negócios e todos os seus derivados derrubaram fronteiras entre países através da telemática. [3]

Dentre os questionamentos feitos por todos que acessam a Internet e que por esse meio fazem negócios ou estabelecem relações de qualquer nível, a segurança é a que mais preocupa, pois como qualquer outro compromisso ele pode ser desvirtuado e comprometer as partes envolvidas. Por isso da preocupação em resguardar os meios de segurança dos documentos e a necessidade do meio técnico absolutamente pessoal para o sucesso dessas relações.

Mesmo no mundo real, assinaturas são falsificadas e documentos são forjados, porque o ser humano é falho e será sempre assim, tanto no campo real como no campo virtual. Temos sistemas de proteção para todo o tipo de fraudes nos documentos materiais e a legislação, tanto civilista quanto penalista, dispõe de normas inibidoras e repressoras para defender a sociedade, como deve ser.

Mas e no mundo virtual? Esse é o novo desafio e esta é uma pequena abordagem sobre esse assunto que será estudado e discutido para que as novas relações possam alcançar o fim esperado, ou seja, a globalização completa e segura.[4]

O conteúdo do conceito técnico será baseado na apostila da e-Sec Tecnologia em Segurança de Dados - Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > , pois o grande foco da monografia foi a parte jurídica e não técnica, porém foi imprescindível a abordagem técnica da área de informática para provar a segurança jurídica que a tecnologia nos trouxe nos dias atuais.

PARTE II – DESENVOLVIMENTO

1 – EVOLUÇÃO HISTÓRICA

[3] A telemática tem como objetivo o estudo do intercâmbio da informação contida em dados manipulados por computadores ligados através dos meios de telecomunicação (bem como a possibilitação técnica de interligação entre computadores). Em suma é a combinação dos meios de telecomunicação e de informática.

[4] BRASIL, Angela Bittencourt. Assinatura digital . Jus Navigandi, Teresina, ano 4, n. 40, mar. 2000. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1782>. Acesso em: 06 jul. 2007.

A internet nasceu durante a guerra fria, nos Estados Unidos, logo após a Segunda Guerra Mundial, como um instrumento de estratégia militar: o governo e os militares dos EUA decidiram criar um sistema de comunicações que não fosse destruído caso alguma bomba nuclear fosse detonada.

O sistema seria construído 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. Esse projeto tornou-se realidade em 1969 e foi batizado de ARPA-net (Advanced Research Projects agency) da Agência de Projetos Avançados (ARPA) do Departamento de Defesa norte-americano, e foi elaborado pela Rand Corpotation .[5]

Foi financiada pelo Ministério da Defesa dos Estados Unidos, interessado em desenvolver um instrumento de comunicação flexível e descentralizado para interligar a estrutura militar, garantindo a continuidade da comunicação de dados mesmo em caso de parcial destruição da estrutura, em virtude de conflito armado.[6]

Consistia na criação de pequenas redes locais (LAN) e coligadas por meio de redes de telecomunicação geográfica (WAN). A partir de 1973 é que iniciou o grande desenvolvimento quando Vinton Cerf, do Departamento de Pesquisa avançada da Universidade da Califórnia registrou o protocolo 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.[7]

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 possibilitaram 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

[5] PAESANI, Liliana Minardi. Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil. 3. ed. São Paulo: Atlas,2006- Coleção Temas Jurídicos, p.25.

[6] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes .São Paulo: Quartier Latin, 2º. Edição, 2005, p.421.

[7] PAESANI, Liliana Minardi-Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil.3. ed. São Paulo: Atlas,2006- Coleção Temas Jurídicos, p.25.

diversos computadores, em locais diferentes, a partir de uma linha telefônica comum, em vista de equipamentos e programas de computador muito mais desenvolvidos e rápidos, que passaram 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 (ou WWW, ou ainda W3, ou simplesmente Web), a rede mundial.[8]

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

Em 2000, segundo noticiado no Canal Web Digital, a Internet mundial tinha 300 milhões de usuários, o Brasil ocupava entre os países por número de Hosts o 12º lugar no mundo, e hoje estaremos chegando muito perto do número mágico de um bilhão de internautas no âmbito mundial. O Brasil em 2004 já contava com aproximadamente doze milhões de internautas e com previsão de movimentar 60 milhões de dólares no comércio eletrônico.[9] Ninguém mais põe em dúvida a extrema importância da internet, em geral, e do comércio eletrônico, em particular, para a sociedade contemporânea e, por via da conseqüência, para a reflexão jurídica. É incontroverso, aliás, que nosso país está em posição de liderança, em termos de crescimento da internet na América do Sul e vem melhorando a sua posição no cenário mundial[10]. Uma grande prova é a difusão brasileira no Orkut, que foi criado pela Google, empresa americana e no dado estatístico de 30 de junho de 2007 o Brasil correspondia a 55,29% dos usuários e o próprio país criador possuía 18,88%. [11]

Hoje, um dos principais motivos desse grande interesse das pessoas está no fato de que, através da internet, é possível obter informações de qualquer ordem, pelo mundo, com rapidez e facilidade, por um preço razoavelmente baixo, sem falar nesse caso, dos locais e

---

[8] PAESANI, Liliana Minardi. Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil. 3. ed. São Paulo: Atlas,2006 - Coleção Temas Jurídicos, p.26.

[9] FINKELSTEIN, Maria Eugênia. Aspectos jurídicos do comércio eletrônico. Porto Alegre: Síntese, 2004, p. 55.

[10] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros. Direito & Internet: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2º. Edição, 2005, p.71.

[11] WIKIPEDIA. Disponível em: <http://pt.wikipedia.org/wiki/Orkut>. Acesso em 24 ago. 2007

provedores que gratuitamente disponibilizam o uso da Internet, além de ter sido uma das ferramentas que foi utilizado nesse trabalho.

Portanto, esse novo meio de comunicação constitui uma nova e importante realidade deste momento histórico em que vivemos.[12]

2 – CONCEITOS INFORMÁTICOS

2.1 - COMÉRCIO ELETRÔNICO

O Comércio sempre foi uma atividade dinâmica ao longo de sua história. As inovações tecnológicas trazidas pela informática, após a segunda metade do séc. XX, foram sendo rapidamente incorporadas pela atividade comercial.

A telemática, através do uso das redes de computadores, reduziu as distâncias, aproximou clientes e chegou a unificar certos mercados. Em uma época histórica na qual se discutia a importância dos blocos comerciais e o grau de interdependência das diversas economias, o chamado "comércio eletrônico" aparece como um componente importante dessa nova ordem.

Em decorrência da estreita relação entre os computadores e o comércio, surge o Comércio Eletrônico e, paralelamente, o Direito Comercial Virtual (ou Direito Comercial Eletrônico) para regulamentar tal atividade desenvolvida com o auxílio da telemática.

É uma modalidade de compra à distância, consistente na aquisição de bens e/ou serviços, através de equipamentos eletrônicos de tratamento e armazenamento de dados, nos quais são transmitidas e recebidas informações.[13]

Alguns exemplos concretos do que como se desenvolveu a área em análise são as primeiras legislações referentes à assinatura digital e aos contratos comerciais eletrônicos nos Estados Unidos e na Alemanha (na Lei Federal que trata dos serviços de comunicação e informação, regulamentando a própria assinatura digital) e o modelo de lei uniforme da

[12] BLUM, Renato M.S. Opice (coordenador) e outros. Direito Eletrônico: A Internet e os Tribunais. Bauru , SP : EDIPRO ,2001, p.357.

[13] FINKELSTEIN, Maria Eugênia. Aspectos jurídicos do comércio eletrônico. Porto Alegre: Síntese, 2004, p. 53.

UNCITRAL para o comércio eletrônico. Trata-se de um relatório da "United Nations Commission on International Trade Law" (UNCITRAL), apresentado na 29ª Assembléia Geral realizada entre 28 de maio a 14 de junho de 1996. Muitos dos conceitos tratados pelos diplomas citados acima serão objeto desta monografia.

O governo norte-americano, através da Casa Branca, publicou, em primeiro de julho de 1997, uma diretiva assinada pelo Vice-Presidente Al Gore e pelo Presidente William Clinton acerca do posicionamento dos Estados Unidos em face do Comércio Eletrônico e sua regulamentação jurídica.

Alguns princípios foram traçados neste relatório da UNCITRAL, quais sejam: que a liderança deve ser outorgada ao setor privado; os Estados devem evitar restrições ao comércio virtual; a participação do Estado deve restringir-se à manutenção do ambiente jurídico que possibilita tal comércio; os governos devem reconhecer as características únicas da Internet, tais como a origem e a sua natureza descentralizada e, finalmente, deve reconhecer que a Internet, como um "mercado global", leva às diversas nações o dever de procurar facilitar o correio eletrônico em uma base global.

Nota-se que a rede é um meio onde os negócios são realizados e que, embora não tenha seu controle específico a um determinado Estado, já chama a atenção da maior potência econômica da atualidade. Em 2000, a doutrina já se mostrava preocupada com a crescente evolução do comércio eletrônico. Nesta época, era da ordem de bilhões de dólares as transações virtuais no mundo diariamente. Estimava-se que seria de 2.3 trilhões de dólares em 2003.[14]

A utilização dos termos em idioma inglês que é utilizado nesta monografia tem o mesmo fundamento que uma das doutrinas estudadas. Há uma grande influência norte-americana nestes estudos, pois foi onde primeiramente se desenvolveu e é onde ainda conta com o maior número de usuários e empresas dedicadas à criação de aplicativos. A linguagem jurídica é uma das finalidades do estudo do direito, pois é a linguagem que traça os reais limites do conhecimento humano. A principal característica do comércio eletrônico é a de eliminar fronteiras físicas, por isso a importância que todos os países utilizem a mesma linguagem.[15]

[14] BLUM, Renato M. S. Opice (coordenador) e outros . Direito Eletrônico. a Internet e os Tribunais. Bauru, SP: EDIPRO,2001, p. 227.

[15] FINKELSTEIN, Maria Eugênia . Aspectos jurídicos do comércio eletrônico . Porto Alegre: Síntese, 2004 , p. 23.

Tentar discorrer acerca de todos os atos de comércio que podem ser praticados através das redes de computadores seria um tanto quanto inócuo e tornaria esta monografia muito extensa. Todavia, três são os grandes grupos de categorias de comércio eletrônico:

1 - os contratos de fornecimento de produtos ou a prestação de serviços na própria rede, aí incluídas as compras de software pelo processo de "download"[16], como também o desenvolvimento de um programa ou de uma "home page";

2 - os contratos de venda de produtos (ou prestações de serviços) a serem entregues fora da rede (compra de livros, passagens aéreas, etc.); e

3 - as transferências de dinheiro (cybercash) e valores mobiliários pela rede.[17]

Inúmeras outras situações correspondentes a negócios podem surgir nas redes de computadores todos os dias. É o caso do uso de Assinatura Digital para operações de Câmbio, utilização na Justiça da Assinatura Digital para petições, o e-CPF, o e-CNPJ, etc. O objeto deste estudo é uma análise genérica e menos exemplificativa dos tipos de negócios e contratos específicos. Um ponto que retrata bem e comprova de forma sucinta a importância do meio computacional na realização de negócios é a publicidade na rede. São valores elevados associados à discussão acadêmica acerca dos direitos à publicidade na rede.

Outro ponto do Direito Comercial Virtual que pode ser considerado quase como "um mundo à parte" é o que cuida da proteção à propriedade intelectual nas redes de computador e que não será objeto específico desta análise, pois será aprofundado no estudo da Assinatura Digital e sua regulamentação.[18]

2.2 - CONTRATO ELETRÔNICO

A fixação do conceito não é tarefa simples em Direito.

---

[16] Procedimento através do qual o programa de computador é transferido de um computador para outro que estão interligados através das redes de computadores.

[17] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros. Direito & Internet: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2º. Edição, 2005, p.415.

[18] ROHRMANN, Carlos Alberto. A Assinatura Digital. Disponível em: <http://www.direitodarede.com.br/AssDg.html>. acesso em: 16 jul. 2007.

Qual seria o nome correto: contrato informático, contrato por computador, contrato eletrônico, contrato on-line, e-commerce ou contrato telemático?

Verifica-se não haver maior dificuldade no tocante à distinção entre contrato informático e telemático. Ao falar-se em contratos eletrônicos, no entanto, torna-se transparente a ambigüidade do termo. É que ora a expressão é tomada no seu sentido mais amplo como sendo todo e qualquer contrato que se utilizasse de uma via eletrônica, qualquer que fosse ela, e ora em sentido estrito, exatamente equivalente ao de telemática. Tomada a palavra eletrônico em sentido amplo, teríamos uma relação de gênero e espécie, relativamente ao contrato telemático, isto é, todo contrato telemático (espécie) é um contrato eletrônico (gênero), mas nem todo contrato eletrônico é contrato telemático. Já no sentido estrito, as expressões seriam tidas como sinônimas. [19]

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.[20]

Tecnicamente, o contrato via Internet, é um contrato entre ausentes e será válido se respeitar os requisitos básicos para a existência de qualquer contrato: duas ou mais pessoas, a livre manifestação de vontade e capacidade civil para o ato que está sendo praticado. É necessário ainda que este contrato verse sobre o objeto lícito e respeite as formalidades que a lei estipular de acordo com seu objeto, mas não há de se falar em não validade do contrato eletrônico unicamente por ele não estar impresso em uma folha de papel. Se aplicados corretamente os meios disponíveis para proteção dos documentos digitais eles podem ser mais seguros que os atuais métodos contra falsificação em papel (papel especial, selo e autenticações), que será provado através da utilização da assinatura digital.[21]

---

[19] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros. Direito & Internet: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2º. Edição, 2005, p.66.

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

[21] BLUM, Renato M. S. Opice (coordenador) e outros. Direito Eletrônico: a Internet e os Tribunais. Bauru, SP: EDIPRO,2001, p. 232.

O contrato eletrônico apresenta as seguintes particularidades:

1 – utiliza o meio eletrônico para a expressão do consentimento

2 – utiliza-o para produzir prova do contrato escrito, que é um documento eletrônico

Os contratos eletrônicos apresentam grandes problemas a serem superados. Entre estes problemas destacam-se:

1 – a presença de cláusulas abusivas nos contratos eletrônicos, em face da normal falta de negociação física;

2 – o fato da maioria dos contratos eletrônicos caracterizarem contrato de adesão;

3 – a falta de segurança acarreta riscos à privacidade do usuário; e

4 – a questão da assinatura digital e da autoridade certificadora. [22]

De qualquer forma, Contrato eletrônico é aquele celebrado por meio de programas de computador ou aparelhos com tais programas. Dispensam assinatura ou exigem assinatura codificada ou senha. A segurança de tais contratos vem sendo desenvolvida por processos de codificação secreta, chamados de criptografia.[23]

Será inevitável a necessidade de acrescentar nesta monografia conceitos específicos sobre criptografia, programa, informação digital, cifra, arquivos etc. para o melhor entendimento do mecanismo e da eficácia da assinatura digital.

2.2.1 – FORÇA PROBANTE DOS CONTRATOS ELETRÔNICOS

Os contratos eletrônicos, citados anteriormente no item 2.1, podem ser classificados portanto em três grandes grupos.No primeiro os contratos que, embora celebrados através de redes de computadores, têm a presença humana nos dois pólos. O segundo grupo refere-se aos contratos firmados por computadores, independentemente da atuação humana. Um usuário programa seu *software* de busca na Internet para procurar um determinado livro em diversas livrarias virtuais e armazenar os respectivos preços. Ao final da busca, o programa "retorna" à livraria que vende mais barato e preenche os campos necessários ao fechamento da compra e

[22] FINKELSTEIN, Maria Eugênia . Aspectos jurídicos do comércio eletrônico. Porto Alegre: Síntese, 2004 , p. 188.

[23] GLANZ, Semy . Internet e Contrato Eletrônico. Revista dos Tribunais, volume nº 757, novembro de 1998, p.72.

venda. Trata-se de algo muito interessante: computadores negociando e celebrando contratos digitais sem a interferência humana. Estabelecidos os parâmetros para o aperfeiçoamento daqueles contratos, entende-se que o computador, de posse da assinatura digital dos contratantes, seria apenas uma extensão das pessoas envolvidas, em nada impedindo o fechamento de contratos comerciais válidos e, conseqüentemente, juridicamente protegidos.

Inúmeras são as questões ligadas aos contratos comerciais virtuais. Deve-se sempre manter em mente que a Internet é uma entidade global: a partir do momento em que uma página é colocada na rede, todo o mundo tem pleno acesso a ela. Disso decorrem três problemas legais básicos e que sempre serão levantados nos conflitos decorrentes das atividades comerciais virtuais: onde o contrato foi firmado, qual a legislação aplicável e o fórum competente para solucionar os conflitos.

O primeiro problema que surge quando se pensa num contrato firmado através de redes de computadores refere-se à certeza de que, efetivamente, é a pessoa que se encontra do outro lado da rede para fechar o contrato.

Por exemplo, num contrato comercial de compra e venda de um determinado produto através da Internet, o vendedor coloca as cláusulas do contrato, por escrito, na sua página; o consumidor as lê e, concordando (com os termos do contrato de adesão[24]) clica seu mouse na opção "concordo". Daí surge a dúvida: quem efetivamente clicou no aceite do contrato? Teria sido o consumidor ou uma criança? Ou ainda, o mouse estava no chão e um cachorro o pisara?

Uma proposta de solução seria, ao invés de o usuário clicar na opção "eu concordo", ele escreveria, por extenso, tal expressão. Embora a situação do cachorro estivesse definitivamente afastada, ainda assim não haveria garantias jurídicas de que foi efetivamente o comprador quem clicou as letras em seu teclado.

Alguns dispositivos foram criados no sentido de aprimorar a segurança na Rede, dentre os quais podem ser destacados:

[24] Na verdade, aplica-se a mesma idéia dos contratos de adesão utilizados pelos fabricantes de programas e implementados através da técnica do "Shrinkwrap", recurso através do qual o disco contendo o programa é vendido dentro de um envelope de plástico que, uma vez rompido, corresponde ao aceite, pelo consumidor, com os termos do contrato de licença de uso. Daí a proposta de venda de software pela Internet usando o clique na opção "eu concordo" ser conhecida como "Clickwrap"

1 – controle de acesso, subdividido em autorização e autenticação;

2 – Firewall, um dispositivo de defesa composto por um sistema ou grupo de sistemas, que reforça o controle de acesso, permitindo somente tráfego de informação autorizada;

3 – Virtual Private Network – VPN, Rede Privada Virtual, tecnologia que permite a troca segura de informações por meio de redes públicas, utilizando criptografia, criando um túnel seguro;

4 – Monitoramento de log, caracterizado pelo monitoramento de arquivos de registros gerados pelos serviços de rede, procurando por padrões que possam indicar ataque de um intruso;

5 - Snnifers, sistemas compostos por hardware e software capazes de capturar de forma passiva, informações destinadas a um outro dispositivo de um mesmo segmento da Rede;

6 – Criptografia e Assinatura Digital, que serão melhor tratadas ao longo desta monografia.[25]

Desse conjunto de problemas surgiu a melhor das idéias, daquilo que se chama "assinatura digital", um recurso técnico que visa atribuir a cada pessoa um único código identificador e protegido. Dois aspectos se inter-relacionam: a questão eminentemente jurídica e a da técnica da informática que possibilita a operação com segurança (trata-se da criptografia).

Importante ressaltar que contratos eletrônicos que contenham reconhecimento de dívida não poderão constituir título executivo, não podendo ensejar uma ação de execução. No entanto, a ação monitória será cabível, com base na prova escrita, nos termos do artigo 1102a do Código de Processo Civil.[26]

Com o uso da criptografia assimétrica para gerar assinaturas digitais cria-se um vínculo entre a assinatura e o corpo do documento, impedindo a sua alteração posterior. Entretanto, o direcionamento da proteção é outro, o documento, em si, ainda pode ser alterado,

[25] FINKELSTEIN, Maria Eugênia. Aspectos jurídicos do comércio eletrônico. Porto Alegre: Síntese, 2004 , p. 61.

[26] FINKELSTEIN, Maria Eugênia. Aspectos jurídicos do comércio eletrônico . Porto Alegre: Síntese, 2004 ,p. 171.

sem deixar vestígios no meio físico, mas se isto for feito, perderá o vínculo que mantém com a assinatura, perdendo todo seu valor probante.[27]

Dentro desta visão, é de se dizer que o documento eletrônico assim assinado é dotado de um maior grau de confiabilidade que o próprio documento tradicional. A verdadeira assinatura digital, legitimamente gerada pelo seu titular, não tem como ser falseada. No fundo, inexiste falsidade a ser apurada no próprio documento eletrônico. O problema se resume exclusivamente na verificação da autenticidade da chave pública. Sabendo ser autêntica a chave pública, com um simples uso do programa de criptografia que utiliza tais chaves, pode-se conferir a autenticidade e veracidade do documento eletrônico.[28]

Há, na verdade, não só a necessidade da garantia jurídica do vendedor de que está negociando com a pessoa certa bem como de que eventuais exigências legais quanto à obrigatoriedade da presença da assinatura das partes. Em outras palavras, um documento digital "assinado" deve ser aceito como se fora um documento escrito que atende às formalidades legais. É exatamente o que dispõe o Modelo de Lei da UNCITRAL para o comércio eletrônico:

"Artigo 7º - Assinatura

§ 1º - Onde a lei exige a assinatura de uma pessoa, tal exigência será satisfeita em relação a uma mensagem de dados se:

a) For usado um método capaz de identificar a pessoa que aprova a informação e a confirmação de tal aprovação sobre a mensagem de dados;

b) Se esse método for confiável, como apropriado para o fim que a mensagem de dados for gerada ou comunicada, sob quaisquer circunstâncias, inclusive sob acordos, os mais relevantes;

§ 2º - O parágrafo 1º se aplica se a exigência ali contida estiver sob a forma de uma obrigação ou simplesmente sob a de previsão de conseqüências pela falta de assinatura;"[29]

---

[27] MARCACINI, Augusto Tavares Rosa. Direito e Informática: Uma abordagem jurídica sobre a criptografia. Rio de Janeiro: Forense,2002 , p. 44.

[28] MARCACINI, Augusto Tavares Rosa. Direito e Informática: Uma abordagem jurídica sobre a criptografia. Rio de Janeiro: Forense,2002 , p. 50.

[29] ROHRMANN , Carlos Alberto. A Assinatura Digital. Disponível em: <http://www.direitodarede.com.br/ AssDg. html> . acesso em: 16 jul. 2007.

Hoje as técnicas de certificação disponíveis permitem garantir razoável segurança ao comércio eletrônico, até porque as entidades financeiras e importantes empresas não teriam investido tantos recursos na comunicação via internet se porventura houvesse risco acentuado aos seus potenciais clientes. A eficácia probante dos Contratos Eletrônicos deve ser autorizada sem quaisquer óbices e subordinada à prudente análise do julgador, recorrendo aos demais meios de prova, se achar necessário.[30]

Portanto um documento eletrônico instrumentalizado por técnica cuja eficácia e segurança possam ser comprovadas, além de atestar a sua autenticidade, dentro do contexto de liberdade probatória, deve ser aceito como válido e, assim, obrigar as partes a ele relacionadas. A MP 2200-2/01 e a Assinatura Digital de Chave Pública vieram para facilitar o reconhecimento da legalidade desse tipo de documento, liberando as partes de recorrerem a meios externos e excepcionais para fazer a prova da sua validade.[31]

2.3 - DOCUMENTO ELETRÔNICO

A palavra "documento" que deriva do latim *documentum* designa qualquer base de conhecimento, fixada materialmente e disposta de maneira que se possa utilizar para consulta, estudo, prova etc, um meio real de representação gráfica do fato ou toda representação material destinada a reproduzir determinada manifestação do pensamento.[32]

Historicamente nossos doutrinadores têm definido o documento como algo material, uma representação exterior do fato que se quer provar e, sempre conhecemos a prova documental como a maior das provas, pois consistente da representação fática do acontecido. Na esteira desses pensamentos, ao ligarmos o fato jurídico à matéria como uma coisa tangível,

[30] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet: aspectos jurídicos relevantes .São Paulo: Quartier Latin, 2º. Edição, 2005, p.318.

[31] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros. Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.429.

[32] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet: aspectos jurídicos relevantes .São Paulo: Quartier Latin, 2º. Edição, 2005, p.71.

teríamos dificuldades em conceituar o documento eletrônico, pois este é intangível e muito longe se encontra do conceito de "coisa" como matéria.

Partindo-se do conceito conhecido de que o documento é uma coisa representativa de um fato, não se pode dizer que o documento eletrônico é um Documento, porque ele não é uma coisa e, portanto não pode ser representativa de um fato. Mas se olharmos pelo prisma do registro do fato, veremos que ele se adequa perfeitamente a este conceito, porque como uma seqüência de bits ele pode ser traduzido por meio de programas de informática que vai revelar o pensamento ou a vontade daquele que o formulou, exigindo do intérprete uma concepção abstrata para compreendê-lo.

Como um escrito que pode ser reproduzido, se o documento eletrônico for copiado na mesma seqüência de bits, ele será sempre o mesmo, tal qual o documento físico que se reproduz por meio de vários sistemas, tais como, cópia xérox ou fotografia. Na verdade não há cordão umbilical entre o trabalho feito eletronicamente e o meio onde foi criado.

Evidentemente que ele pode ser reproduzido por uma série de processos, sendo o mais usual o CD que armazena dados retirados dos computadores e são guardados fora do disco rígido. A única diferença existente nesse aspecto é que não podemos falar em Original e Cópia entre os dois se não houver uma identificação pessoal do seu autor, porque num programa de computador, os dados ali existentes são sempre os mesmos, não se podendo dizer nunca qual é a fonte original deles sem a necessária autenticação. Não se pode fazer, por exemplo, um exame grafo técnico para conferir à determinada pessoa a autoria de um texto eletrônico.

Por isso que se, por acaso, houver um descompasso entre o material apresentado e o que foi registrado no Computador, o documento eletrônico então terá que ser analisado e a assinatura do seu autor pode e deve ser reconhecida através de um sistema próprio.

O documento eletrônico não é caracterizado por um suporte instrumental, mas sim através de um suporte eletrônico. Conforme salienta Ricardo Lorenzetti[33] , no documento eletrônico a declaração de vontade está assentada sobre bytes e não sobre átomos e pode tanto conter assinatura como não.[34]

[33] LORENZETTI, R. L. Comercio Eletrônico. Buenos Aires: Abeledo Perrot, 2000 , p. 62.

[34] FINKELSTEIN, Maria Eugênia. Aspectos jurídicos do comércio eletrônico. Porto Alegre: Síntese, 2004 , p. 161.

Se o original é o documento eletrônico, deve ele conter requisitos que permitam conferir sua autenticidade e integridade, enquanto a sua cópia em meio físico é passível de autenticação. A conferência da cópia há de ser feita com o original eletrônico, utilizando-se de um computador e dos softwares necessários. A cópia física do documento eletrônico não conterá qualquer assinatura, mas apenas a reprodução do texto. Nenhum significado teria, para esta cópia, imprimir a assinatura digital em meio físico, já que a conferência com o original só é possível por meio eletrônico. [35]

Tivemos uma atualização a esse respeito com o advento do novo Código Civil brasileiro (Lei 10.406, de 10 de janeiro de 2002), em vigor desde o dia 11 de janeiro de 2003. Não há dúvida de que, nesse diploma legal, houve evolução no que se refere ao conceito de documento, conforme se verifica na Seção II, do Capítulo I do Título V, do Livro I, da Parte especial, acerca da formação dos contratos com o acréscimo do "por meio de comunicação semelhante", no art. 428, inciso I.[36]

Os problemas fundamentais em relação ao documento eletrônico estão ligados a três requisitos: autenticidade(certeza da autoria da manifestação), integridade(certeza de que não houve adulteração no envio) e perecimento do conteúdo(validade ao longo do tempo), além de uma evidente função probatória. [37]

Diante dessas colocações temos que o documento eletrônico é a representação de um fato concretizado por meio de um computador e armazenado em programa específico capaz de traduzir uma seqüência da unidade internacional conhecida como bits.[38]

2.4 - PROGRAMA OU SOFTWARE

[35] MARCACINI, Augusto Tavares Rosa . Direito e Informática: Uma abordagem jurídica sobre a criptografia. Rio de Janeiro: Forense ,2002 , p. 69.

[36] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet . aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.73.

[37] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet . aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.426.

[38] BRASIL, Angela Bittencourt. Assinatura digital . Jus Navigandi, Teresina, ano 4, n. 40, mar. 2000. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1782>. Acesso em: 02 jul. 2007.

Um programa de computador representa um conjunto de ações que devem ser tomadas pela máquina com o objetivo de atingir um resultado específico. O programa, em si, nada faz. Ele apenas dita quais as ações que o computador deve tomar de acordo com cada situação. Esses programas, normalmente, recebem um conjunto de dados, que serão a matéria prima do seu processamento, transforma esses dados de acordo com as regras estipuladas no programa e apresenta os resultados através de uma das interfaces de saída do computador (monitor de vídeo, impressora, disquete, rede, etc). [39]

O Programa é o conjunto de instruções que possibilitam o processamento da informação. Neste caso pode-se distinguir em: 1- programa operativo chamado de Sistema Operacional, todo programa que é executado no computador está subordinado hierarquicamente ao Sistema Operacional; 2 – programa aplicativo, que permite realizar uma determinada função.

O programa pode ser elaborado especialmente ajustando-se a necessidade do solicitante ou ser um produto padrão para adquirentes pré-definidos. Essa diferença tem relevância jurídica sempre que na primeira hipótese houver uma locação de programas, ao passo que no segundo caso geralmente se trata de uma compra e venda. Nesta última hipótese, o programa é definido, não passível de alteração, é dirigido ao mercado em geral e não a um usuário particular, sua concepção permite que seja fornecido a muitos usuários para uma mesma aplicação ou função .[40]

2.5 – REDE DE COMPUTADORES

A rede de computadores surgiu para ampliar as formas de comunicação dos computadores. A rede nada mais é que um meio eletrônico de ligação entre computadores.

Outro aspecto importante diz respeito à forma de comunicação entre os computadores. Todo tipo de comunicação precisa de um protocolo para que a informação que

[39] E-SEC: Tecnologia em Segurança de Dados . Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > . Acesso em 02 jul. 2007.

[40] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.494.

sai de uma ponta seja entendida pela outra. No caso de uma conversa entre duas pessoas, o protocolo pode ser a linguagem de comunicação. Se uma pessoa fala em inglês e a outra não entende inglês, a comunicação não se completa.

No mundo dos computadores a regra é idêntica. Para que dois computadores se comuniquem através da rede devem ser definidos protocolos de comunicação para que a informação saia de um computador e seja entendido pelo outro. No mundo das redes de computadores esses protocolos existem em várias camadas de acordo com as funcionalidades. Porém somente duas camadas são importantes de serem mencionadas nesse documento: Camada de Rede e Camada de Aplicação. O protocolo da camada de rede diz respeito a como uma informação digital sai de um computador, sua rota é definida e o pacote é entregue ao computador destino. O protocolo da camada de rede diz respeito a como o conteúdo do pacote digital deve ser interpretado. Isto é, a camada de rede se preocupa em como entregar a mensagem no outro computador e a camada de aplicação se preocupa em como deve ser interpretada a mensagem que chegou.

O protocolo de rede/transporte mais conhecido hoje é o TCP/IP. Ele é amplamente usado na internet e na maioria das redes locais conhecidas. Os protocolos de aplicação dependem de qual aplicação está usando a rede. Apenas como exemplo podemos citar: 1)HTTP – Usado pelos navegadores de internet para interpretar as páginas (home-pages) dos sites da internet; 2) SMTP – Usado pelos programas de e-mail para interpretar uma mensagem de correio eletrônico que chega pela rede.[41]

2.6 – ALGORITMO

É difícil diferenciar algoritmo de programa, pois o conceito dos dois é muito parecido. Conceitualmente algoritmo é um modelo esquemático de solução de um problema. Isto é, o conceito de algoritmo extrapola o campo da informática. Um exemplo claro de algoritmo é uma receita de bolo. Ela diz quais os ingredientes e como você deve combiná-los para que ao final você tenha um bolo pronto. Quando uma cozinheira de posse da receita

[41] E-SEC: Tecnologia em Segurança de Dados . Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > . Acesso em 02 jul. 2007.

executá-a para fazer o bolo, uma série de decisões práticas que não constam da receita devem ser tomadas, como decidir qual marca de farinha ou manteiga ela vai usar, qual assadeira deve usar para assar o bolo, a que temperatura ele será assado, etc.

Quando trazemos o conceito de algoritmo para o mundo da informática dizemos que o algoritmo é um modelo esquemático para a resolução de um problema computacional. Isto é, no caso do desenvolvimento de um programa, o algoritmo diz quais ações devem ser tomadas e em qual ordem. O programador de posse do algoritmo transforma aquele modelo em um programa verdadeiro. Ora, um programa é, então, a realização física de um algoritmo.[42]

Basicamente, a segurança da criptografia, seja simétrica ou assimétrica, que será alvo das próximas explanações, está relacionada com a consistência do algoritmo e o tamanho da chave.

O programa de criptografia que empregar algoritmos conhecidos e públicos será mais seguro. Porém é impossível, mesmo a um expert no assunto, construir um algoritmo de criptografia e ter a imediata certeza de sua segurança. Esta certeza somente advém do estudo prolongado das operações matemáticas envolvidas, na tentativa de encontrar falha de decifrar a mensagem sem conhecer a chave. Sendo pública estará sujeita ao crivo da comunidade científica que poderá testá-la por muito mais tempo. [43]

2.6.1 - ALGORITMOS CRIPTOGRÁFICOS

Chama-se de algoritmos criptográficos aos algoritmos que implementam funções que utilizem algum tipo de criptografia para garantir sigilo, integridade, autenticação ou certificação. Os algoritmos criptográficos refletem a forma como um determinado cientista, que o inventou, descreveu um mecanismo para prestar um dos quatro serviços descritos acima. Porém, os algoritmos criptográficos não implementam o serviço em si, mas são instrumentos

[42] E-SEC: Tecnologia em Segurança de Dados . Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > . Acesso em 02 jul. 2007.

[43] MARCACINI, Augusto Tavares Rosa . Direito e Informática: Uma abordagem jurídica sobre a criptografia . Rio de Janeiro: Forense,2002 , p. 40.

para que o serviço seja prestado. Assim, um mesmo algoritmo pode ser usado para implementar serviços diferentes dependendo da forma como é usado.[44]

2.7 – CRIPTOGRAFIA

A criptografia é um campo de estudo da matemática que tem suas origens na Roma antiga. Os primeiros estudos em criptografia visavam desenvolver métodos que escondessem o conteúdo de uma mensagem sendo transportada de um ponto para outro. A criptografia sempre foi uma ciência de uso militar. Desde o Império Romano a criptografia era usada para cifrar as comunicações militares. No início as mensagens em papiro eram cifradas e enviadas por mensageiros a pé ou a cavalo. Na primeira e segunda guerra mundial, as mensagens eram cifradas em máquinas mecânicas e transmitidas por rádio. Porém, somente com o surgimento das redes de computadores na década de 70 é que a criptografia atingiu o meio comercial e acadêmico. As empresas precisavam garantir sigilo nas comunicações entre as filiais e fornecedores. Até então, todos os estudos em criptografia estavam restritos aos órgãos militares e toda a teoria matemática envolvida era mantida em absoluto sigilo dentro desses órgãos. A criptografia foi levada tão a sério pelos governos que a exportação não autorizada de código criptográfico, nos Estados Unidos, estava enquadrada como crime de guerra.

Porém, desde que foi aplicada à informática a criptografia, esta sofreu grande evolução. Inclusive no que diz respeito à sua aplicação. Inicialmente, ela era usada apenas para garantir o sigilo nas comunicações.

Com o crescimento das transações comerciais no ciberespaço, tornou-se imprescindível um modo para certificar a titularidade das assinaturas nos documentos eletrônicos, seja em forma de correspondência eletrônica entre empresas, seja em forma de contratos, possibilitando a sua integridade, genuinidade e segurança.[45]

---

[44]E-SEC: Tecnologia em Segurança de Dados. Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > . Acesso em 02 jul. 2007.

[45] FINKELSTEIN, Maria Eugênia . Aspectos jurídicos do comércio eletrônico . Porto Alegre: Síntese, 2004 ,p. 179.

Atualmente, sua aplicação se expandiu para além do mero sigilo, tornando-se um elemento essencial na formação de uma infra-estrutura para o comércio eletrônico e a troca de informações. O mecanismo funciona pela aplicação de um padrão secreto de substituição dos caracteres, de maneira que a mensagem se torne indecifrável para quem não conheça o padrão criptográfico utilizado.[46]

As transações bancárias utilizam-se da criptografia. As emissoras de TV por assinatura também se utilizam desta tecnologia, para que apenas seus assinantes possam assistir a programação através de seus aparelhos decodificadores. Da mesma forma os cartões de créditos e correios eletrônicos podem manter sigilo através deste sistema.[47]

A criptografia moderna é usada para prover quatro tipos de serviços distintos. São eles:

Sigilo – Neste caso a criptografia é usada para garantir que o conteúdo de uma informação sendo trafegada ou armazenada não seja conhecido por pessoas não autorizadas;

Integridade – Neste caso a criptografia é usada para garantir que uma informação não seja adulterada durante a transmissão ou armazenamento. Veja que nesse caso qualquer pessoa pode ter acesso ao conteúdo da informação, porém ninguém poderá alterá-la. Quando fala-se em adulteração pode-se tratar tanto de adulteração acidental por problemas de má qualidade do sinal de rede ou intencional quando alguém deseja adulterar uma informação em benefício próprio;

Autenticação – Neste caso a criptografia é usada para identificar uma pessoa através de uma transação remota. Aqui se pode fazer um paralelo com o mundo real. Quando se faz uma compra em uma loja, o caixa solicita que o comprador apresente seus documentos de identificação para que ele possa ter certeza de que a pessoa é realmente quem diz ser. Ela faz isso através de uma identificação visual ou mesmo da confrontação da assinatura da pessoa. Quando se fala de transações remotas através da rede, não existe contato físico tornando qualquer tipo de identificação pelos métodos tradicionais ineficaz. Existe um pouco de

[46] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet: aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.432.

[47] MARCACINI, Augusto Tavares Rosa . Direito e Informática: uma abordagem jurídica sobre a criptogafia . Rio de Janeiro: Forense, 2002 , p. 13.

indefinição dos autores quanto ao conceito de autenticação onde alguns colocam a autenticação e a certificação como tendo o mesmo significado. Optou-se nesse texto por duas definições distintas por se entender que, apesar de se aplicarem mecanismos criptográficos idênticos, os resultados alcançados são distintos. Entende-se nesse texto como autenticação o processo puro e simples de identificar uma pessoa através da rede, porém sem gerar nenhum tipo de prova do procedimento. É como quando o caixa de posse da identidade do comprador analisa o documento, confronta a fotografia e se dá por satisfeito entendendo ter identificado a pessoa. Na rede isso se faz através de um desafio. A pessoa que deseja identificar a outra no outro lado da linha lança um desafio que ela tem certeza que somente quem poderá respondê-lo corretamente é a pessoa com quem ele acha que está falando. Quando chega a resposta do desafio é que ela verifica se a resposta está correta. Se estiver, dá-se por satisfeito e continua a transação tendo certeza de com quem ela está falando. Porém, esse processo não gera nenhuma prova da transação, é apenas um processo de identificação.

Certificação – Neste caso a criptografia é usada para gerar prova de uma transação, de um fato, de uma intenção, etc. Isto é, gerar um certificado. O conceito genérico de certificado é o documento onde alguma pessoa ratifica pessoalmente o conteúdo ali escrito. No mundo real, existem várias formas de se ratificar o conteúdo de um documento, porém a forma mais comum é através da assinatura da pessoa aposta ao documento. Assim diz-se que qualquer documento assinado é um certificado. No mundo virtual, usa-se a criptografia para ratificar o conteúdo de uma mensagem digital, sejam eles texto, imagem, som, etc. Esse processo é comumente chamado de assinatura digital e será descrita mais à frente nesse texto.[48]

A criptografia moderna utiliza conceitos matemáticos avançados e abstratos, que servem como padrão para cifragem das mensagens, com o uso dos algoritmos. Na computação, os algoritmos são utilizados não para embaralhar as palavras das frases ou as letras das palavras, mas os próprios bits do documento digital. Atualmente, para que um sistema criptográfico seja considerado seguro e completo, precisa estar capacitado para atender, basicamente, a três parâmetros:

[48]E-SEC: Tecnologia em Segurança de Dados . Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > . Acesso em 02 jul. 2007.

1- identificação/autenticação: verificação da identidade do remetente e a integridade do conteúdo da mensagem;

2- impedimento de rejeição: garante que o remetente não poderá negar o envio da mensagem; e

3- privacidade: a capacidade de ocultar o conteúdo da mensagem de todos que não sejam o destinatário dela.

É bom ressaltar que a segurança de um sistema criptográfico está ligada a uma relação tempo/custo para decifração, pois todo o algoritmo criptográfico pode ser decifrado, mas a empreitada será impraticável.[49]

2.7.1 – DIREITO À PRIVACIDADE E À CRIPTOGRAFIA

Um ponto que já foi brevemente citado neste trabalho é o que envolve a questão da privacidade do indivíduo em suas operações realizadas através das redes de computadores. No presente tópico, busca-se motivar a necessidade do estudo aprofundado do tema que se relaciona não só a aspectos éticos como também a questões que podem envolver até mesmo os direitos constitucionais à vida privada[50].

Os dados que trafegam pela Internet e pelas demais redes de computadores não estão, em absoluto, protegidos com total segurança contra interceptações indesejáveis. O problema de a Internet, ao virtualizar as relações jurídicas, ocasiona uma distorção dos aspectos "público" e "privado" e explica bem essa preocupação. Quando alguém está em sua casa, dentro de seu ambiente privado, ligado à Internet, de certa forma o lado público tem acesso a seu computador e, conseqüentemente, podem ocorrer trocas de dados.

Uma pessoa, navegando pela Internet, pode deixar rastros. Os computadores visitados também podem e deixam mensagens em seu computador pessoal, dando conta das visitas. Trata-se de arquivos pequenos inseridos em seu disco rígido e que contêm informações

[49] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.433.

[50] Art. 5º, inciso X da Constituição da República.

sobre as últimas visitas; são os "cookies"[51]. Assim, patente é o risco de alguém não autorizado estar tendo acesso aos dados de uma pessoa. Daí a importância de a criptografia prover a segurança dos dados.

Um aspecto técnico da maior relevância na estrutura da assinatura digital à base do par de chaves (pública e privada) é que a chave privada de criptografia de uma pessoa não navega, em hipótese alguma, pela rede de computador. Ao contrário da hipótese do uso de senhas, por mais complexa que seja, a senha teria que ser enviada através dos meios físicos da rede, o que acarreta em um risco grande de cópia e posterior uso indevido.

A despeito de toda essa justificativa, o Governo norte-americano vem insistindo na idéia de que o particular deve fazer um depósito da sua chave privada em um órgão estatal. Ocorre certo temor do Governo Americano em face da evidência de que o uso da criptografia forte tornará impossível a interceptação de algumas mensagens. A título exemplificativo, tome-se o seguinte caso: em 1992, o FBI conseguiu "descriptografar" uma agenda eletrônica contendo clientes da Máfia, o que seria impossível se tratasse da moderna criptografia forte. Em resumo, mais uma vez, o combate ao crime busca justificar a ofensa dos direitos particulares à privacidade.

No Brasil, um caso análogo ocorreu com a Lei nº. 9.296/96 que, ao regulamentar a quebra do sigilo telefônico nos casos de investigação ou instrução criminal[52], ampliou tal hipótese para a comunicação de dados, o que ofende o texto da Carta Magna.

Uma proposta de criptografia surgida nos Estados Unidos ficou conhecida como "Clipper Chip". Trata-se de um "chip"[53] de computador a ser inserido no telefone, por exemplo, o qual contém a chave privada de criptografia de cada pessoa. Ocorre que, para tal, o Governo norte-americano requer que ele mantenha o conhecimento da chave privada contida no "chip".

---

[51] Os "cookies" são arquivos inseridos por computadores ligados à Internet nos computadores dos usuários que os visitam. Os programas de navegação incluem a opção (desabilitada na configuração padrão) de avisar o usuário do recebimento de "cookies".

[52] Trata-se do art. 5º, inciso XII da Constituição da República de 1988.

[53] O termo inglês "chip" refere-se às pastilhas de silício usadas em computadores. A melhor tradução é "circuitos integrados". O termo "chip", a exemplo de "software" e "hardware" é amplamente utilizado na literatura técnica da Ciência de Computação. Podem existir "chips" das mais variadas aplicações: memórias, processadores, unidades assíncronas de recepção e transmissão, dentre outros.

Trata-se de uma solução absolutamente segura. Ninguém poderia ter acesso a sua chave privada, à exceção dos agentes do governo. Esse modelo seria usado para as mais variadas aplicações eletrônicas, desde os contratos virtuais, passando pelos títulos de crédito virtuais até o dinheiro eletrônico (como cartões representativos de certa quantidade de dinheiro).

A legislação brasileira não deve, caso siga o modelo americano ou alemão, adotar tal medida, de conteúdo inconstitucional, em face das garantias constitucionais[54].

Nota-se que a justificativa maior daqueles que defendem tal medida é o risco de se tornar inoperante uma medida governamental em face da impossibilidade de acesso à chave privada de, por exemplo, um criminoso que haja desviado valores que deverão ser devolvidos. É muito importante observar que, no modelo técnico de funcionamento da criptografia forte, a chave privada só interessa a seu dono.[55]

Além disso, a criptografia surge no mundo da Internet como uma necessidade para preservação de garantias individuais. Nos Estados Unidos, a comunidade tem se manifestado insistentemente contra as propostas governamentais de restrição ou enfraquecimento de sistemas criptográficos, ou contra a lei que proíbe a exportação de produtos que utilizem criptografia forte. Se os norte-americanos relutam em dar às autoridades constituídas de seu país poder bastante para decifrar o correio eletrônico, maiores razões temos nós para desconfiar de propostas que enfraqueçam o poder de sistemas criptográficos ou que permitam ao Governo manter uma chave mestra. Quem detiver tal mecanismo central, para decifrar mensagens alheias, cumulará em suas mãos um poder descomunal e por demais perigoso para a ordem democrática. Eventual restrição não impediria que organizações criminosas obtivessem o produto e dele se utilizassem. Nem seria razoável supor que o crime organizado, que pratica ilícitos muito mais graves, fosse temer a ameaça de condenação penal por uso indevido desta técnica. Uma eventual proibição, restrição ou controle da criptografia, enfim, em nada resolverá para o combate da crescente criminalidade, mas acarretará desproporcional desvantagem para a

[54] Constituição da República, art. 5º, inciso X c/c inciso XII.

[55] E-SEC: Tecnologia em Segurança de Dados . Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > . Acesso em 02 jul. 2007.

população em geral, impedindo-lhe de utilizar mecanismos para proteção de suas comunicações privadas e informações pessoais.[56]

2.8 – CIFRA

Denomina-se cifra os algoritmos criptográficos usados para garantir sigilo nas informações. As cifras têm por premissa mesclar no seu processo um método de embaralhar as informações e desembaralhar baseado em um segredo. O segredo é a chave para desfazer o processo. Dessa forma para desfazer a codificação efetuada pela cifra deve-se conhecer o método de embaralhamento e o segredo que foi utilizado para embaralhar o texto. Dessa forma, a cifra bem elaborada é aquela em que nem o seu inventor consegue decodificar o texto se não possuir o segredo usado na codificação. Ao método de embaralhamento dá-se o nome de cifra e ao segredo usado para cifrar e decifrar dá-se o nome de chave.[57]

2.8.1 – CHAVE SIMÉTRICA

Cifra simétrica ou algoritmo simétrico é aquele onde a chave de cifragem é a mesma usada para decifrar. A essa chave dá-se o nome de chave simétrica ou chave secreta. Alguns exemplos de cifras simétricas são: DES, 3DES, IDEA, RC4, RC2, Blowfish, AES.[58]

É muito utilizada a técnica da criptografia simétrica para assinatura de documentos eletrônicos. Também conhecida como “criptografia de chave privada”, esse tipo de assinatura eletrônica exige que o destinatário da mensagem conheça o algoritmo utilizado para assinar a mensagem, caso contrário, não poderá reconhecer a assinatura, invalidando o seu conteúdo. Para que a criptografia simétrica funcione, o destinatário deve possuir a chave usada pelo remetente.

---

[56] MARCACINI, Augusto Tavares Rosa . Direito e Informática: uma abordagem jurídica sobre a criptogafia . Rio de Janeiro: Forense, 2002 , p. 124.

[57] E-SEC: Tecnologia em Segurança de Dados . Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > . Acesso em 02 jul. 2007.

[58] E-SEC: Tecnologia em Segurança de Dados . Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc >. Acesso em 02 jul. 2007.

Caso contrário, este terá de preocupar-se em enviar-lhe uma cópia do algoritmo. Por isso, este tipo é mais utilizado em redes fechadas, ou apenas para garantir o sigilo de arquivos pessoais, armazenados em computadores isolados ou em conjunto com outros métodos mais modernos. [59]

A segurança de um sistema de criptografia não depende apenas do universo possível de senhas a utilizar, mas também na consistência da fórmula matemática utilizada(algoritmo).[60]

A criptografia simétrica padece de limitações, pois as partes devem ter, ao menos uma vez, um meio seguro de comunicação para combinar as chaves secretas. E isso nem sempre é possível. Com o advento da criptografia assimétrica permitiu superar essas limitações.[61]

2.8.1.1 – SEGURANÇA DA CHAVE PRIVADA

O certificado digital garante a segurança da chave pública de alguém. Porém, para proteger a chave privada utiliza-se outros métodos. Qualquer pessoa que tenha acesso à chave privada de outro, pode se passar por ela em todo tipo de transação, visto que ele passa a assinar pela pessoa. Por essa razão o proprietário da chave privada deve ter muita preocupação em manter o sigilo da sua chave privada. Existem várias formas de fazer isso. Uma é trancando num cofre um disquete com a sua chave privada. Esse processo é muito seguro, porém muito burocrático, visto que a chave não pode ser levada para outros lugares. Outra forma de fazer isso é cifrando a chave com uma senha que somente você conheça. Esse é um processo bom, pois uma vez a chave cifrada você pode guardá-la num disquete e leva-la para qualquer lugar. O inconveniente dessa solução é que se a sua senha for fraca alguém que tenha acesso a sua chave cifrada pode efetuar tentativas múltiplas de decifrar a sua chave.

O processo mais confiável, atualmente, para guardar a chave privada são os smart-cards (cartões inteligentes) que possuem um chip interno à prova de invasão e somente podem ser acessados através de uma senha ou algum tipo de biometria (impressão digital, por

[59] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.435.

[60] MARCACINI, Augusto Tavares Rosa . Direito e Informática: uma abordagem jurídica sobre a criptogafia . Rio de Janeiro: Forense, 2002 , p. 13.

[61] MARCACINI, Augusto Tavares Rosa . Direito e Informática: uma abordagem jurídica sobre a criptogafia . Rio de Janeiro: Forense, 2002 , p.23.

exemplo). Esses cartões possuem chips, isto é, podem fazer processamento interno. Assim podem ser gravados internamente a eles programas que geram o par de chaves públicas e privada e protegem a chave privada contra qualquer tipo de invasão. O usuário nunca tem acesso ao conteúdo do cartão, ele somente solicita ao cartão que faça determinado tipo de ação, por exemplo que assine um documento digital usando a chave privada do proprietário do cartão. Essas ações somente são executadas se o possuidor do cartão digitar corretamente a senha de acesso ou opuser a sua impressão digital sobre o mesmo. Ele não permite que, se o cartão for roubado ou perdido sejam feitas tentativas sucessivas de se obter a senha, pois depois de um número determinado de tentativas ele tem seu funcionamento suspenso por tempo indeterminado. Além disso, o chip contém mecanismos de autodestruição caso seja rompido. [62]

2.8.2 – CHAVE ASSIMÉTRICA

Cifra assimétrica ou algoritmo assimétrico é aquele onde a chave de cifragem é diferente da chave de decifragem. Isto é usa-se uma chave para cifrar o texto e no momento de decifrá-la usa-se outra chave que é inversa da primeira. Dessa forma não se fala mais de uma chave de cifragem e sim de um par de chaves únicos e inversos usadas no processo. Na literatura técnica costuma-se chamar as cifras assimétricas de cifras de chave pública e chave privada. Isso porque na maioria dos casos uma das chaves do par é tornada pública e a outra é mantida em segredo pelo proprietário da mesma. Isso propicia que este tipo de cifra possa ser usado para outros fins que não o sigilo dos dados. Essas cifras, como será mostrado mais à frente, poderão ser usadas para implementar os serviços de autenticação e certificação. Porém, conceitualmente existe uma diferença entre cifra assimétrica e de chave pública e privada. O primeiro conceito é mais amplo que o segundo. Isto é, toda cifra de chave pública é uma cifra assimétrica, porém a recíproca não é verdadeira. Isso porque uma cifra para ser assimétrica basta que a chave de cifragem seja distinta da chave de decifragem, porém nada é garantido que a partir de uma chave não se deriva a outra. Uma cifra para ser de chave pública/privada deve haver garantia da impossibilidade da prática de se derivar uma chave a partir da outra. Sem essa

[62] E-SEC: Tecnologia em Segurança de Dados . Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > . Acesso em 02 jul. 2007.

garantia o método não poderia ser aplicado à autenticação e à certificação, somente ao sigilo. São exemplos de cifras assimétricas: RSA, Diffie-Hellman, El Gamal.

Portanto, são geradas duas chaves diferentes, uma das chaves ficará em poder do proprietário do sistema, que terá exclusividade no seu uso e será a chave privada, e a outra poderá ser distribuída a todos aqueles com quem o proprietário precisa manter uma comunicação segura ou identificada e esta será uma chave pública. Essas chaves são inseridas em pequenos programas de computador, que integram os editores de correio eletrônico normais e são postas em funcionamento mediante um simples clique do mouse no ícone respectivo.[63]

Para entender o mecanismo, o sistema funciona desta forma:

Encriptando a mensagem com a chave pública, geramos uma mensagem cifrada que não pode ser decifrada com a própria chave pública que a gerou. Só com o uso da chave privada que poderemos decifrar a mensagem que foi codificada com a correspondente chave pública. E o contrário também é verdadeiro: o que for encriptado com o uso da chave privada, só poderá ser decriptado com a chave pública.[64]

Não se tem mais problema de combinar previamente qual será a senha, como era necessário na criptografia simétrica.

Dado que as operações feitas com a criptografia assimétrica são mais pesadas e demandam maiores recursos computacionais, há sistemas (PGP) que cifram a mensagem utilizando uma chave de sessão. Na seqüência, esta chave de sessão é cifrada com a chave pública do destinatário. Assim, a mensagem cifrada a ser enviada é composta de dois blocos: um primeiro, com a mensagem cifrada convencionalmente e outro com a chave secreta do primeiro bloco, codificada por criptografia assimétrica com a chave pública do destinatário. Apenas o destinatário, com uso de sua chave privada, poderá decifrar o segundo bloco, extraindo a chave que abrirá a mensagem cifrada no primeiro bloco.[65]

---

[63] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.435.

[64] MARCACINI, Augusto Tavares Rosa . Direito e Informática: uma abordagem jurídica sobre a criptogafia . Rio de Janeiro: Forense, 2002 , p. 24.

[65] MARCACINI, Augusto Tavares Rosa . Direito e Informática: uma abordagem jurídica sobre a criptogafia . Rio de Janeiro: Forense, 2002 , p. 28.

2.8.2.1 – SEGURANÇA DA CHAVE PÚBLICA

Somente no ano de 2001 foi promulgado o já referido marco regulatório das assinaturas eletrônicas e, conseqüentemente, dos documentos eletrônicos e assinaturas digitais.

A Medida Provisória 2.200-2, de 24 de agosto de 2001 instituiu a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil", para garantir a autenticidade , a integridade e a validade jurídica de documentos em forma eletrônica. A ICP-Brasil é composta por uma autoridade estatal, gestora da política de certificação, e por uma cadeia de autoridades certificadoras, subordinada a primeira. É composta por uma estrutura de autoridades certificadoras hierarquicamente dispostas, onde a autoridade suprema é o Comitê Gestor da ICP-Brasil, órgão deliberativo com poder para definir as políticas e normas técnicas que garantem o pleno funcionamento. Das diversas competências do Comitê Gestor destacamos a de identificar e avaliar as políticas de infra-estrutura de chaves públicas, negociar e aprovar acordos de certificação bilateral e de certificação cruzada, bem como das regras de interoperabilidade e outras formas de cooperação internacional, certificando a sua compatibilidade com a ICP-Brasil, observando o disposto em tratados, acordos ou atos internacionais.

Continuando com a descrição das entidades partícipes da cadeia de autoridades certificadoras, logo abaixo do Comitê Gestor encontra-se a denominada Autoridade Certificadora Raiz ou AC-Raiz, a quem compete fazer observar as resoluções deliberadas pelo Comitê Gestor. Seu papel é exercido pelo Instituto Nacional da Tecnologia da Informação – ITI[66] , conforme determina o art. 13, da MP nº 2.200-2/01.[67]

2.8.3 – FUNÇÕES UNIDIRECIONAIS OU HASH

[66] Depois, o art. 2º, do Decreto nº 4.036/01 transferiu o Instituto Nacional da Tecnologia da Informação – ITI, do Ministério da Ciência e Tecnologia para a Casa Civil da Presidência da República.

[67] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.440.

Uma função é dita unidirecional ou de hash quando possui a característica de transformar um texto de qualquer tamanho em um texto ininteligível de tamanho fixo. Além disso, ela também se caracteriza por ser fácil de calcular e difícil de serem invertidas. Um exemplo simples de uma função unidirecional, porém não aplicada à criptografia é o cálculo do resto da divisão de um número por outro. Se, por exemplo, cria-se uma função que calcule o resto da divisão de qualquer número por 10 o que temos é que qualquer que seja o número que será dividido por 10 o resultado é sempre um número entre 0 e 9. Isto é, o processo de cálculo é bem simples porém como saber se o resultado do resto for, por exemplo, 9 qual foi o número que divido por 10 gerou resto 9. É muito difícil afirmar com certeza visto que existem infinitos números que divididos por 10 darão resto 9. A esse fato damos o nome de colisão. Isto é, quando dois números diferentes aplicados à função de hash geram o mesmo resultado dizemos que houve uma colisão. Nesse ponto é que se faz a diferença entre uma função de hash criptográfica e uma não criptográfica. A função de hash criptográfica é aquela que foi elaborada a possuir o mínimo de colisões possível.

Este tipo de função é normalmente usado para efetuar cálculos de integridade de mensagens. Isto por uma característica muito peculiar da função de hash. O tamanho do seu resultado é sempre fixo e pequeno. Uma função de hash tem em média 20 bytes de saída independente do tamanho do texto de entrada.[68]

3 – ASSINATURA ELETRÔNICA

A primeira iniciativa em legislar sobre a assinatura eletrônica ocorreu nos Estados Unidos, mais precisamente no Estado de Utah, com o objetivo de permitir a autenticação dos documentos eletrônicos e facilitar o comércio e outras relações contratuais via Internet, seguindo o sistema de Criptografia e cuja chave ainda se encontra naquele país.

O país norte americano promulgou a "Digital signature and eletronic authentication law" de 02/02/1998 que facilitou sobremaneira o seu uso pelas Instituições financeiras, permitindo a autenticação dos documentos por meio da Criptologia.

[68] E-SEC: Tecnologia em Segurança de Dados . Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > . Acesso em 02 jul. 2007.

Na mesma esteira, a Alemanha já tem a sua "Informations Und Kommunikationsdienste Gesetz Iukdg", lei federal que estabelece condições gerais para o uso das assinaturas digitais, tanto ao seu aspecto de segurança e se baseia no mesmo sistema da Criptografia.

E assim, outros países, como a Itália e a Bélgica adotaram procedimentos semelhantes A ONU, por meio da comissão UNCITRAL (Comissão das Nações Unidas sobre o Direito do Comércio Internacional) voltaram os seus olhos para essa questão da segurança nas relações cibernéticas e reconhecem os certificados emitidos por uma entidade certificadora de outro Estado membro da União Européia, se este possuir um grau de segurança equivalente ao dos países membros da ONU.

O crescimento exponencial das redes e utilizadores da Internet constitui um fortíssimo elemento de pressão da procura no sentido do aumento dos investimentos em infra-estruturas de redes de telecomunicações, bem como a necessidade de se normatizar as suas regras, porque se isso não for feito certamente haverá uma parada econômica.

Não temos no Brasil uma definição legal do que sejam dados de computador e muito menos uma legislação que ampare as negociações cibernéticas o que faz com que a estagnação econômica virá se nada for feito à respeito. [69]

A assinatura se divide em duas modalidades:

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

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

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

15.2.2 – 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.[70]

[69] E-SEC: Tecnologia em Segurança de Dados . Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > . Acesso em 02 jul. 2007.

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

15.2.3.1 – 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.

15.2.3.2 – 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.[71]

Portanto a assinatura eletrônica não se confunde com a assinatura digital. A assinatura eletrônica seria qualquer método ou símbolo baseado em meios eletrônicos utilizado por uma parte com a intenção de autenticar um documento, cumprindo todas as funções de uma firma manuscrita. A assinatura seria uma forma específica de assinatura eletrônica, em que há um processo criptográfico que dá segurança àquele que assina o documento, através de uma chave privada de assinatura e da integridade dos dados com o uso de uma chave pública de assinatura sustentada por um certificado de chave de assinatura utilizada, fornecida por uma autoridade de certificação.[72]

3.1 – MECANISMOS DA ASSINATURA DIGITAL

Nesse ponto passa-se a analisar como os conceitos apresentados acima podem ser utilizados para implementar o que se costuma chamar de assinatura digital.

Os mecanismos de assinatura digital foram criados com o objetivo de substituir a assinatura manuscrita, por uma que levasse para o mundo digital as mesmas garantias do mundo

---

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

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

[72] FINKELSTEIN, Maria Eugênia . Aspectos jurídicos do comércio eletrônico . Porto Alegre: Síntese, 2004 , p.174.

real. A simples digitalização da imagem da assinatura manuscrita não é suficiente para alcançar esse propósito, pois a mesma pode ser copiada e anexada a qualquer documento tornando-a simples de ser forjada.

No processo convencional, um sinal gráfico (pessoal) é aposto a um papel para ratificar o seu conteúdo. O processo é válido porque a assinatura está atrelada ao papel de forma permanente. A mesma não pode ser transferida para uma outra folha. É fato que esse processo não é inforjável visto que o sinal gráfico pode ser copiado de forma idêntica por uma pessoa habilidosa.

O processo de assinatura digital se utiliza de algoritmos criptográficos para fundir um segredo (pessoal) a um conjunto de bytes (mensagem a ser assinada). A garantia é que somente quem conhece o segredo pode reproduzir o mesmo resultado. O resultado desse processo é a assinatura digital.

O processo de verificação da assinatura (reconhecimento de firma) utiliza-se de uma informação pública acrescida da mensagem original para verificar se a referida pessoa efetivamente assinou a mensagem. Note que as características descritas acima têm princípios idênticos aos da assinatura manuscrita: a) Assinatura privada; b) Verificação pública. Porém a assinatura digital é inforjável, sendo dessa forma mais segura que a assinatura convencional. Além disso, a assinatura digital pode ser remetida pela rede e verificada remotamente através de uma cópia da mesma. Essa característica não é válida para a assinatura tradicional.

As Assinaturas Digitais assim produzidas ficam de tal sorte vinculada ao documento eletrônico “subscrito” que, ante a menor alteração, a assinatura se torna inválida. A técnica não só permite demonstrar a autoria do documento, como estabelece uma “imutabilidade lógica”[73] do seu conteúdo. [74]

[73] Imutabilidade Lógica é que apesar de poder alterar o documento, a posterior alteração deste invalidará a assinatura.

[74] BLUM, Renato M. S. Opice (coordenador) e outros . Direito Eletrônico : a Internet e os Tribunais . Bauru, SP: EDIPRO,2001, p. 49.

O texto acima descreve os requisitos básicos de um mecanismo de assinatura digital. A seguir descreveremos o que é então a assinatura digital e qual o mecanismo mais utilizado atualmente que implementa os requisitos descritos acima.[75]

3.2 – ASSINATURA DIGITAL

Para que alcancemos uma total eficácia nos contratos pela Internet é preciso a presença de um fator, sem o qual essas relações estão fadadas ao fracasso, ou seja, a segurança, que hoje é a maior preocupação de todos aqueles que negociam pelos meios eletrônicos.

A credibilidade desses documentos está ligada essencialmente à sua originalidade e à certeza de que ele não foi alterado de alguma maneira pelos caminhos que percorreram até chegar ao destinatário.

Os fatores de risco podem advir por fatores internos ou externos, sendo que os internos podem acontecer por erro humano ou mesmo falha técnica. O fator externo, e aí está o maior risco, consiste na atuação fraudulenta de estranhos que pode alcançar meios para adentrar no programa enviado e desviar o objetivo do mesmo, em prejuízo das partes envolvidas no negócio.

Portanto, para a segurança desses documentos é necessário que abordemos dois aspectos que devem ser equacionados antes de se ter o documento como totalmente confiável:

Primeiramente, como todo documento e para que assim possa ser chamado, é preciso a identificação do seu autor por meio da correspondência entre a autoria aparente e a autoria real. Isso se faz por meio de um sinal pessoal que chamamos de assinatura ou firma.

Em seguida, é preciso a preservação do documento, que deve ser mantido ou na memória do computador ou transmitido para um CD, longe de possíveis alterações que deturpem o seu conteúdo. Por ser uma máquina, o computador pode sofrer uma pane, pode ser apagado, pode ser manipulado por terceiros e por isso consideramos a guarda do documento em um CD, a forma mais segura para a sua conservação intacta.

[75]E-SEC: Tecnologia em Segurança de Dados . Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > . Acesso em 02 jul. 2007.

Para que uma declaração de vontade seja considerada como tal pelo seu receptor é necessário que o emissor seja perfeitamente identificável. Se o seu conteúdo não puder ser atribuído a algum sujeito determinado, que assuma a autoria, então não estaremos diante de uma verdadeira declaração e, portanto, o seu conteúdo não terá força vinculatória para o Direito. A identificação do emitente da declaração é o elemento constitutivo da própria declaração. A assinatura autográfica utilizada nos documentos físicos não é adequada aos documentos eletrônicos. Evidente que a simples digitação de um nome ao pé da mensagem eletrônica não pode ser considerada assinatura autográfica. Atualmente o problema da identificação e da integridade dos documentos eletrônicos foi solucionado pela assinatura digital, pela tecnologia da criptografia assimétrica.[76]

Felizmente, existem hoje soluções tecnológicas que, se não podem garantir absoluta certeza quanto a identidade dos contratantes, coisa que nem no meio não digital também não o pode, são capazes de dotar a comunicação eletrônica com ferramenta seguras com a assinatura digital.[77]

A Criptologia é a ciência que estuda a maneira mais segura e secreta para a realização das comunicações virtuais. É composta de Criptografia e Criptoanálise que nada mais representam do que foi exposto acima, ou seja, a criação de uma senha e a chave para decifrá-la.

As técnicas de assinatura feitas por meio da Criptografia consistem numa mistura de dados ininteligíveis onde é necessário o uso de duas chaves, a pública e a privada, para que ele possa se tornar legível. É como se fosse um cofre forte que somente para quem tem o seu segredo é acessível.

Assim, ele em nada se assemelha à assinatura com a qual estamos acostumados, pois na verdade a assinatura eletrônica é um emaranhado de números que somente poderá ser codificado para quem possua a chave privada e sua decodificação então deverá ser feita por meio de uma chave pública. O mundo da teleinformática que se avizinha cada vez mais, antes

[76] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.440.

[77] SILVA JUNIOR, Ronaldo Lemos Da e Ivo Waisberg (organizadores) . Comércio eletrônico . São Paulo: Editora Revista dos Tribunais, 2001 , p. 201.

restrito a um grupo pequeno de internautas, converteu-se rapidamente numa fonte inesgotável de possibilidades em todos os campos das comunicações humanas.

A argumentação de alguns autores de que o documento eletrônico não pode ser considerado juridicamente por lhe faltar a firma, numa visão hoje ultrapassada, mais uma vez nos leva a crer que urge uma legislação específica tuteladora desses interesses, sob pena de uma paralisação na economia do país que não acompanhar de forma rápida a evolução tecnológica mundial e a realidade do mundo virtual.

A verificação positiva de uma assinatura digital enseja um elevado grau de certeza jurídica da autenticidade da autoria e da integridade da mensagem ou outro tipo de documento, pois se prova com certeza substancial que o documento não foi alterado. E que provém do seu emissor.[78]

Não há como por meio da chave pública, desvendar os segredos da chave privada devido às operações matemáticas que são utilizadas para a confecção da chave privada. As operações são de tal forma intrincada que a segurança delas pode ser considerada total e impedem que a chave pública possa descobrir os segredos numéricos da chave privada. Esta é como uma complicada senha.

A assinatura digital, diferentemente da assinatura real, modifica-se a cada arquivo, transformando-o em documento, sendo que o seu autor não poderá repetí-la como faz com as assinaturas apostas nos documentos reais.[79]

O autor envia o documento ao destinatário, com a assinatura digital e este, por meio da chave pública faz a descriptação para fazer a prova da autenticidade do documento. Para descriptar a mensagem o destinatário usa o mesmo algoritmo usado no software e cria um resumo da mensagem, ou função *hash,* que é comparado ao resumo enviado pelo autor. Se o resultado dos dois for igual, o documento é autêntico e confiável.

Somente deste modo, usando o processo de Encriptação dos documentos é que as partes podem ter certeza da identidade uma da outra. Essa tecnologia como dissemos é o resultado de um conjunto alfanumérico que é conhecido como "sistema assimétrico de

[78] SILVA JUNIOR, Ronaldo Lemos Da e Ivo Waisberg (organizadores) . Comércio eletrônico . São Paulo: Editora Revista dos Tribunais, 2001 , p. 305.

[79] FINKELSTEIN, Maria Eugênia . Aspectos jurídicos do comércio eletrônico . Porto Alegre: Síntese, 2004 , p.174.

encriptação de dados". Essa técnica permite que a informação se torne inteligível para todos, menos para o destinatário, pois este vai usar da Criptoanálise para recuperar a informação recebida.

A mensagem que vai para o destinatário e que passa livremente pela rede chama-se Plaintext – o texto simples- e depois de encriptada recebe o nome de Ciphtext – texto cifrado- e sua transformação é feita através do antes citado algoritmo e da chave.

Mesmo que o algoritmo possa ser de conhecimento público ele dependerá fundamentalmente das chaves para ser decifrado.

Apesar de parecer complicado, o sistema é fácil de ser usado pelos usuários da Internet. Suponhamos que eu queira mandar este arquivo confidencialmente para o leitor X. Primeiramente vou procurar a chave pública do leitor X em um diretório, e utilizo essa chave para encriptar o artigo e o envio. Recebida a mensagem, o meu leitor X usa a chave privada que tem e descodifica o texto para lê-lo.

Estes sistemas que se denominam Sistemas Cifrados são fundamentados em operações matemáticas que criam os sistemas simétricos e assimétricos de encriptação de dados que viajam na grande auto estrada das informações.

No criptosistema simétrico, usa-se apenas uma chave tanto para o emissor quanto para o receptor da mensagem, o que torna frágil a segurança do seu teor e por isso, gostamos mais do sistema assimétrico que se utiliza de duas chaves, ou seja, a pública e a privada.

Mas como ter a certeza absoluta de que a assinatura procede da pessoa que está enviando o documento? Mais um processo de segurança é usado com a presença da Autoridade Certificadora, que é a pessoa encarregada de fornecer os pares de chaves. Essa Autoridade é uma entidade independente e legalmente habilitada para exercer as funções de distribuidor das chaves e pode ser consultado a qualquer tempo, certificando que determinada pessoa é a titular da assinatura digital , da chave pública e da respectiva chave provada.

Esse documento é equiparado a um documento Notarial e por ter força de certificar a verdade, é preciso que a lei normatize o seu conteúdo.

O processo de assinatura digital descrito aqui utiliza algoritmo de chave pública e algoritmo de hash para montar a assinatura. A assinatura digital nada mais é que a mensagem cifrada através da chave privada do assinante. O algoritmo de chave pública garante que se um

determinado texto for cifrado com a chave privada somente poderá ser decifrada com a chave pública correspondente. Como a chave privada é mantida em segredo sendo somente conhecida pelo proprietário essa operação constitui uma assinatura digital, pois garante que ela fica atrelada ao texto e somente o possuidor da chave privada poderia efetuar aquela operação. Da mesma forma o processo de verificação passa por decifrar a mensagem utilizando a chave pública. Assim a pessoa que verifica pode ter certeza de que quem realmente gerou a assinatura foi a pessoa correta. O processo é muito simples e pode ser aplicado não somente a um texto, mas também a qualquer tipo de arquivo digital (imagem, som, etc).

Na prática como o resultado de uma cifragem é do tamanho da mensagem original seria inviável fazer somente a cifragem no processo de assinatura. Isso porque a assinatura ficaria do tamanho da mensagem original. Se estiver falando de 1kbyte isso não chega a ser problema. Porém, se está falando de 10Mbytes ter-se-ia uma assinatura de 10Mbytes. Por essa razão, na prática o que se faz é aplicar um cálculo de hash sobre a mensagem e cifrar o resultado do hash e não a mensagem. O hash é usado aqui porque independente do tamanho da mensagem o resultado dele é de no máximo 20 bytes[80]. E dessa forma a assinatura ficaria com tamanho pequeno independente do tamanho da mensagem a ser assinada.

Observe que o reconhecimento de firma digital é um pouco diferente do processo convencional. Neste, somente o sinal gráfico da assinatura é comparado não se dando nenhuma importância ao conteúdo do papel. Na assinatura digital o reconhecimento da firma sempre envolve o conteúdo da mensagem. Qualquer adulteração do texto original torna a verificação da assinatura incorreta.

Outra observação interessante é o fato de que na verificação da assinatura, a comparação é feita sobre o hash da mensagem e não sobre o texto original da mesma. Isso se dá, pois uma vez calculado o hash de uma mensagem o processo não pode ser revertido. Dessa forma, a única forma de se comparar as mensagens é fazendo a comparação do hash das mesmas. [81]

[80] O algoritmo SHA1 sempre retorna uma saída de 20 bytes e o MD5 sempre retorna uma saída de 16bytes independente do tamanho da entrada.

[81] E-SEC: Tecnologia em Segurança de Dados . Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > . Acesso em 02 jul. 2007.

Antes de adentrar-se no estudo do aspecto técnico e doutrinário da assinatura digital, é interessante buscar na legislação alemã (alínea 1 do § 2º do art. 3º da Lei de Assinatura Digital de 1º de agosto de 1997) um conceito de assinatura digital:

"(1) Para os propósitos desta Lei, "assinatura digital" significa um selo afixado aos dados digitais, o qual é gerado por uma chave privada de assinatura e comprovador do dono da chave de assinatura e da integridade dos dados com o uso de uma chave pública de assinatura sustentada por um certificado da chave de assinatura utilizada, fornecido por uma autoridade de certificação, de acordo com o §3º desta Lei."

Sem embargo do conceito supracitado, colhido da legislação alemã, também o Direito norte-americano contribui significativamente com a matéria. Embora o primeiro Estado a legislar a matéria tenha sido o de Utah, há uma onda de legislações tratando de assinaturas digitais e assinaturas eletrônicas varrendo os demais Estados norte-americanos. No intuito de ser coerente com o projeto da UNCITRAL, bem como na busca de uma maior segurança jurídica, a legislação brasileira deve adotar o modelo alemão e eleger a "assinatura digital", como aquela que utiliza o modelo de chaves privada e pública de criptografia.

É da maior relevância que fique claro o seguinte: a assinatura digital é um substituto eletrônico para a assinatura manual. Ela exerce o mesmo papel, e mais, serve também para proteger a mensagem digital transmitida através da rede de computadores, uma vez que o texto é codificado através dos algoritmos de criptografia.

Nota-se, ainda, que a assinatura digital não é uma imagem digitalizada da assinatura manual, e sim, um conjunto muito grande de caracteres alfanuméricos.

Nota-se a presença dos conceitos de "chave privada" e "chave pública". Para que se possa melhor entendê-los, faz-se mister uma breve referência ao estudo da criptografia, matéria relacionada à Ciência da Computação.

“Criptografar uma mensagem corresponde a codificá-la, tornando-a protegida no caso de uma interceptação não desejada. Para tal, podem-se fazer uso de recursos singelos como aqueles utilizados pelas crianças ao trocar cada letra do alfabeto por um símbolo convencionado. As principais aplicações da criptografia surgiram relacionadas às aplicações militares, devido à necessidade de se trocar mensagens secretas sem que o inimigo tivesse acesso. Foram, assim, sendo desenvolvidos programas de computador contendo algoritmos

cada vez mais sofisticados de criptografia. O nível de segurança do programa está associado à possibilidade matemática cada vez menor de se conseguir descobrir, a partir de uma mensagem criptografada, qual o conjunto numérico capaz de "descriptografá-la". Os atuais programas de criptografia trabalham com probabilidades de falha de proporções exageradamente remotas a ponto de se dizer matematicamente impossível (ou improvável, em face do tempo de processamento que seria necessário)".

Uma vez que o objetivo deste trabalho está associado ao estudo jurídico da assinatura digital, não há como aprofundar-se tecnicamente no tema da criptografia e seus algoritmos. A RSA Laboratories disponibiliza, através da Internet, maiores informações técnicas acerca do tema, bem como inúmeras publicações científicas. Para os propósitos desta monografia, faz-se necessário admitir a segurança matemática do uso da moderna criptografia, o que pode ser chancelado pelas inúmeras legislações estrangeiras supracitadas que já a aceitam.

Um ponto interessante que, embora escape um pouco do objetivo central deste texto, é o relacionado à proibição do governo americano de exportar programas de criptografia moderna. Cuida-se de uma posição do governo americano sob a alegação de que se trata de ferramenta estratégica para a segurança nacional. Todavia, já há projetos de lei no Congresso Americano no sentido da liberação da exportação dos programas o que seria bastante interessante em decorrência da própria necessidade do comércio virtual internacional em transacionar com maior segurança.

A cada chave privada de criptografia existe uma e uma só chave pública associada e, obviamente, cada par de chaves estará associada a apenas um usuário, a apenas uma pessoa como "proprietária".

Antes de aprofundar no tema da assinatura digital, deve-se precisar o que vem a ser a “mensagem de dados” trocada entre os usuários. Para as pessoas, pode ser um contrato de compra e venda, um acordo de compra de ações, ou mesmo uma confissão de dívida, ou até mesmo um "título de crédito virtual". Para o computador, trata-se de um arquivo de dados transmitido por via digital, também conhecido como EDI (Electronic Data Interchange). Por ser um arquivo de dados digital, transmitido através de computador e utilizado, conforme certo padrão, pelo comércio eletrônico, trata-se de um recurso da maior relevância para a viabilização

das transações comerciais, como se pode concluir do texto abaixo que se refere especificamente ao tema:

> *“Uma grande parte do comércio eletrônico, atualmente, é realizado entre as grandes empresas. As transmissões usam, tipicamente, os protocolos uniformizados desenvolvidos por grupos que cuidam da padronização dos "EDI's", como "UN/EDIFACT" ou "ANSI x 12" ("American National Standards Institute Committee x 12").*
>
> *Em virtude de a situação legal de todos os casos não estar perfeitamente definida, em relação ao comércio eletrônico, tornou-se prática comum entre aqueles que utilizam os "EDI's" a adoção de um contrato especial que resolve as questões legais mais importantes, pelo menos aquelas com as quais os contratantes estão mais familiarizados. “Tais contratos são conhecidos como “EDI Agreements” (Acordos “EDI’s”)”.*

Retornando ao tema da criptografia, percebe-se que cada pessoa deve ter uma chave privada de criptografia que somente ela conhece e uma chave pública, utilizada para "abrir" os documentos digitais criptografados pela chave privada. A grande vantagem dessa idéia é que a chave privada de criptografia não é do conhecimento de terceiros(não circula pela rede), garantindo, assim, maior segurança para o seu dono contra eventuais fraudes.

O funcionamento prático da assinatura digital envolve, ainda, a necessidade de uma terceira parte desinteressada que faz a certificação de que a chave privada utilizada é mesmo do assinante do documento digital (o que pode ser, ainda, por exemplo, do emitente da "nota promissória virtual"). Esta terceira parte é a Autoridade de Certificação. Veja-se o conceito trazido pelo Prof. FROOMKIN em recente artigo:

> *"Uma Autoridade de Certificação (CA) é um órgão, público ou privado, que procura preencher a necessidade de uma terceira parte de confiança no comércio eletrônico que fornece certificados digitais, atestando algum fato acerca do sujeito do certificado".*

A própria legislação alemã supracitada traz um conceito bastante didático da Autoridade de Certificação:

> *"(2) Para os propósitos desta Lei, Autoridade de Certificação significa uma pessoa natural ou jurídica que certifica a atribuição de chaves públicas de assinatura para as pessoas e para tal possui uma licença conforme o § 4º desta Lei."*

A Autoridade de Certificação desempenha, pois, a tarefa de comprovar, através da emissão de um certificado, que o assinante daquele documento digital é efetivamente a pessoa com quem a outra parte espera estar negociando. Em resumo, se o credor recebe uma confissão de dívida virtual e o CA emitir o certificado, não restarão dúvidas de que os aspectos formais do documento digital estarão sendo respeitados. Há, pois, garantia jurídica para o credor.

Um pequeno detalhe que não deve passar despercebido é o conceito de certificado. Recorre-se, mais uma vez, à lição do Prof. FROOMKIN:

> *"Um certificado é uma afirmação emitida por uma Autoridade de Certificação que provê a confirmação independente de um atributo afirmado por uma pessoa titular de assinatura digital".*

Do conceito acima, conclui-se que o certificado pode assegurar não só quem é a pessoa que assinou digitalmente o EDI, bem como outros parâmetros. Conseguem-se assim certificados de hora, de residência, de maioridade, dentre outros. Deve-se ater, todavia, ao certificado que atesta a identidade do emissor do EDI, do "assinante digital".

Também a legislação alemã pertinente à matéria em discussão elenca, de forma taxativa, os elementos que devem estar contidos nos certificados.

Uma pergunta pode ficar do estudo dos CA's: Teria um emissor de certificado funções análogas às de um cartório? Seria o CA uma espécie de "cartório virtual"?

A analogia não é de toda absurda. Tanto não o é que a própria American Bar Association e a United States Arm of the International Chamber of Commerce estão estudando a possibilidade da criação de uma nova espécie de notário, o "Cyber Notary", o cibernotário.

Retornando, pois, à assinatura digital, pode-se dizer que ela nada mais é do que um identificador acrescido a um determinado pacote de dados digitais, gerado por uma chave privada de assinatura do assinante e que só será decodificado por uma chave pública associada àquele assinante e garantida por uma autoridade de certificação (CA), que faz a identificação das partes e a posterior certificação, emitindo certificados de autenticidade da chave pública utilizada.

Uma vez recebido o certificado de autenticidade emitido pela autoridade competente, não restam dúvidas de que do outro lado está realmente o dono da assinatura

digital, o que possibilita, não só o fechamento de contratos virtuais, mas, também, o crédito através das redes de computadores, daí a origem dos "títulos de crédito virtuais".

Um problema evidente que surge é o risco de o proprietário de uma chave privada perdê-la. Uma pessoa passaria a ter acesso à "assinatura" de outra. O mau uso pode ocorrer. Daí surge a inevitável pergunta: haveria responsabilidade do CA em certificar uma assinatura utilizada por outrem? E, ainda: estaria o dono da chave privada, indevidamente utilizada por outrem, sujeito a adimplir eventual contrato que não tem sua efetiva participação?

Antes de responder a tais questões, julga-se da maior importância considerar duas situações distintas: na primeira, o usuário comunica ao CA a perda da chave privada e pede seu conseqüente cancelamento; na segunda, não ocorre tal providência.

Entende-se que na primeira hipótese, o CA deverá proceder ao cancelamento da chave privada perdida e da chave pública associada. Surgirá, assim, para o CA a obrigatoriedade de manter uma lista de certificados revogados, contendo as chaves inválidas. Trata-se da proposta legal contida no modelo alemão. É claro que após tal comunicado, se o CA certificar uma operação que utilizou uma chave cancelada, sua responsabilidade será patente, estando o antigo proprietário da chave isento de qualquer responsabilidade.

O problema surge para o particular quando este é desapossado de sua chave privada e não comunica o fato ao CA. Ora, sem tal comunicação, o CA poderá certificar eventualmente uma operação não efetuada pelo legítimo dono da chave. Uma vez que a assinatura digital, devidamente certificada, gera uma presunção de que do outro lado está o dono da assinatura associada ao conjunto de chaves privado-pública, entende-se que o ônus da prova desloca-se para o particular. E, mais, a situação ainda se complica quando se pensa na possibilidade da presença de um terceiro de boa-fé que poderia estar eventualmente envolvido. Há que prevalecer tal posição, pois, do contrário, a segurança jurídica estaria comprometida, visto que o certificado emitido pelo CA estaria sujeito a contestações judiciais, cabendo ao credor o ônus de provar que, embora tenha recebido a certificação de um CA, que aquele certificado corresponde a uma assinatura digital gerada por uma chave privada não desapropriada. Como "o Direito não socorre aqueles que dormem", cabe ao dono da chave privada, mantê-la a mais bem protegida possível e comunicar qualquer furto ou perda com a maior brevidade. A legislação de Utah

baseia-se neste esquema, ou seja, impõe ao consumidor o ônus de comunicar a perda da chave privada.

Nota-se que há duas questões distintas relacionadas à assinatura digital. A primeira refere-se à eficácia probatória dos contratos celebrados através dos computadores e a segunda está mais próxima da discussão acerca da segurança e privacidade dos usuários dessa nova tecnologia.

Como se pode perceber, o tema ainda é novo e vem despertando movimentos em todo o mundo, culminando com a proposta de lei uniforme da UNCITRAL. Trata-se de uma matéria de grande interesse não só para o advogado como para o público que, em breve, há de ter disponível uma poderosa ferramenta destinada a agilizar e facilitar o comércio virtual com maior segurança.

Um ponto que não se pode perder de vista é o aspecto internacional do comércio virtual, associado ao fato de que a Internet estar bastante difundida pelos mais variados países. Embora seja intuitivo que uma rede de computadores, espalhada por todo o mundo, ligada em tempo real, e a baixo custo, cria um ambiente global, ainda assim torna-se importante lembrar tal característica das redes amplas de computadores a fim de que sempre seja possível pensar em soluções propostas para o Direito Comercial Virtual em termos mais amplos possíveis. Devem ser lembradas as palavras de Roberta Cooper Ramo, presidente da American Bar Association, que conceituou, em recente artigo, a Internet como sendo criadora de "uma comunidade ao longo do mundo, operando em tempo real".

É exatamente nesse sentido que se entende que a legislação deve, a exemplo do modelo alemão, reconhecer a validade dos certificados emitidos por CA’s de outros Estados, que só teremos certeza com as aprovações dos inúmeros projetos de lei em trâmite. No caso brasileiro, tome-se a situação do Mercosul, por exemplo. Não há motivos para se criarem barreiras à validade de um certificado emitido nos demais países do bloco. É claro que se trata de mais um tema para discussão nos tratados internacionais.[82]

3.3 – SISTEMÁTICA DE FUNCIONAMENTO

[82] E-SEC: Tecnologia em Segurança de Dados . Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > . Acesso em 02 jul. 2007.

Com o objetivo de exemplificar o funcionamento técnico do sistema de leitura da Assinatura Digital, sendo que o foco principal da monografia é o debate da parte jurídica da Assinatura Digital, utilizarei da transcrição do estudo feito pela e-Sec Tecnologia em Segurança de Dados, informações estas obtidas através do acesso feito em 02 de julho de 2.007 e disponível no site http://www.digitrust.com.br/AssinaturaDigital.doc:

> *"Suponhamos que alguém deseja enviar uma mensagem a você e quer ter a certeza de que mais ninguém poderá ler a mesma. Independente das medidas que se tome, existe sempre a possibilidade de que alguma outra pessoa possa abrir a correspondência (papel ou eletrônica), para dela tomar conhecimento. Para alcançarmos uma condição de sigilo da mensagem, podemos contar com as ferramentas da Criptografia (a ciência que trata deste tipo de problema) para "embaralhar" a mensagem de tal forma que somente o destinatário autorizado possa recuperá-la.*
>
> *Na terminologia da Criptografia a mensagem original é chamada "texto claro", ou simplesmente "mensagem". O processo de embaralhar a mensagem de forma a ocultar seu conteúdo de outrem é denominado "cifração", se constituindo de transformações matemáticas adequadas sobre a mensagem. A mensagem embaralhada, ou seja, cifrada, é denominada "texto cifrado" ou "criptograma". Claro que devemos ter o processo inverso de recuperar a mensagem a partir do criptograma, e este processo é denominado "decifração". Os processos de cifração e decifração se utilizam de um algoritmo (o processo de codificação/embaralhamento) e de um parâmetro de controle denominado "chave criptográfica", de forma que a decifração, em princípio, somente é possível conhecendo-se a chave apropriada para decifrar, mesmo que se conheça o algoritmo utilizado.*
>
> *Enquanto a Criptografia trata de manter mensagens secretas, por outro lado existe também a "Criptoanálise", que é a arte de "quebrar" os criptogramas, recuperando-se as mensagens, mesmo sem se conhecer a chave apropriada para a decifração. Por isto, os algoritmos criptográficos devem satisfazer a uma série de critérios de forma a garantir, no maior grau possível, que seja impraticável quebrar o sistema.*

A Criptografia trata não apenas dos problemas estritos de sigilo de mensagens, como também de problemas de autenticação, assinatura digital ou eletrônica, dinheiro eletrônico, e outras aplicações.

Quanto aos Algoritmos Criptográficos, existem duas classes de algoritmos criptográficos: simétricos (ou de chave-secreta) e assimétricos (ou de chave-pública). Os algoritmos simétricos utilizam uma mesma chave tanto para cifrar como para decifrar (ou pelo menos a chave de decifração pode ser obtida trivialmente a partir da chave de cifração), ou seja, a mesma chave utilizada para "fechar o cadeado" é utilizada para "abrir o cadeado". Nos algoritmos assimétricos temos chaves distintas, uma para cifrar e outra para decifrar e, além disso, a chave de decifração não pode ser obtida a partir do conhecimento da chave de cifração apenas. Aqui, uma chave é utilizada para "fechar" e outra chave, diferente, mas relacionada à primeira, tem que ser utilizada para "abrir". Por isso, nos algoritmos assimétricos, as chaves são sempre geradas aos pares: uma para cifrar e a sua correspondente para decifrar.

Pela sua característica no uso da chave, os algoritmos simétricos exigem que a chave seja mantida secreta, do conhecimento exclusivo dos dois interlocutores. Este fato traz complexidade ao manuseio destas chaves, o que dificulta um pouco a utilização destes algoritmos isolada-mente. É requerido um canal seguro que permita a um usuário transmitir a chave ao seu interlocutor (um canal seguro pode ser, por exemplo, um portador de confiança). A figura 1 ilustra a forma de operação de um algoritmo criptográfico simétrico, onde Bob envia uma mensagem cifrada para Alice, tendo antes que enviar a chave que vai utilizar, secretamente, para Alice.

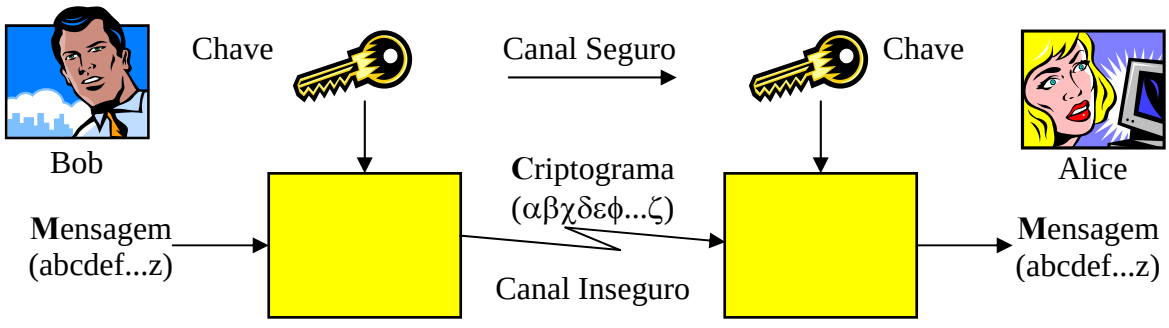

Figura 1: Uso de algoritmo criptográfico simétrico (chave secreta).

Os algoritmos assimétricos permitem que a chave de cifração possa ser tornada pública, por exemplo, disponibilizando-a em um repositório de acesso público ("canal público"), e por isso denominada chave-pública, retirando aquele problema existente nos algoritmos simétricos. Qualquer um pode cifrar mensagens com uma dada chave-pública, contudo somente o destinatário, detentor da correspondente chave de decifração (denominada chave-privada, ou secreta), poderá decifrá-la. A chave-privada não precisa e nem deve ser dada a conhecer a ninguém, devendo ser guardada em segredo pelo seu detentor apenas, que deve também ter sido o responsável pela geração do seu par de chaves, enquanto a chave-pública pode ser publicada livremente. Na figura 2 temos uma ilustração da operação de um algoritmo assimétrico. Aqui, Alice gera seu par de chaves, e envia (publica) sua chave-pública para Bob. Este cifra a mensagem com a chave-pública de Alice ($K_{Pública}$), a qual, e somente ela, será capaz de decifrá-la, utilizando sua chave-privada ($K_{Secreta}$).

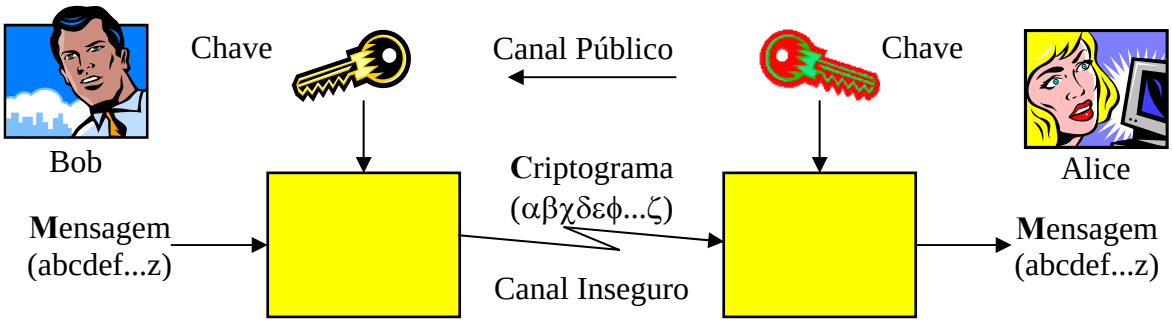

Figura 2: Uso de algoritmo criptográfico assimétrico (chave pública).

Geralmente os algoritmos simétricos são mais eficientes computacionalmente que os assimétricos, podendo ser bastante rápidos em sua execução, permitindo altas taxas de cifração (até da ordem de gigabits/s – 10^9 bits/s). Os algoritmos assimétricos são geralmente menos eficientes, e normalmente a tendência é a utilização dos dois tipos de algoritmos em conjunto, tal que um algoritmo de chave-pública é utilizado para cifrar uma chave criptográfica, gerada aleatoriamente, para ser então utilizada para cifrar a mensagem através de um algoritmo simétrico. O destinatário então primeiro decifra a chave simétrica utilizando sua chave-privada no sistema de chave-

pública, e após decifra a mensagem utilizando a chave recuperada no sistema simétrico. Desta forma não há o problema de "compartilhar o segredo da chave" com ninguém. A cada nova mensagem pode-se sempre repetir todo o processo. Nesta situação, se Bob deseja enviar uma mensagem para Alice, ele primeiro escolhe uma chave K, e a envia através do algoritmo de chave-pública cifrada com a $K_{Pública}$ de Alice. Esta recupera K decifrando o criptograma recebido com sua chave privada $K_{Secreta}$. Agora Bob pode enviar a mensagem real através do algoritmo simétrico, mais eficiente para isto, cifrando-a com a chave K, que Alice já dispõe, e enviada a ela de forma segura.

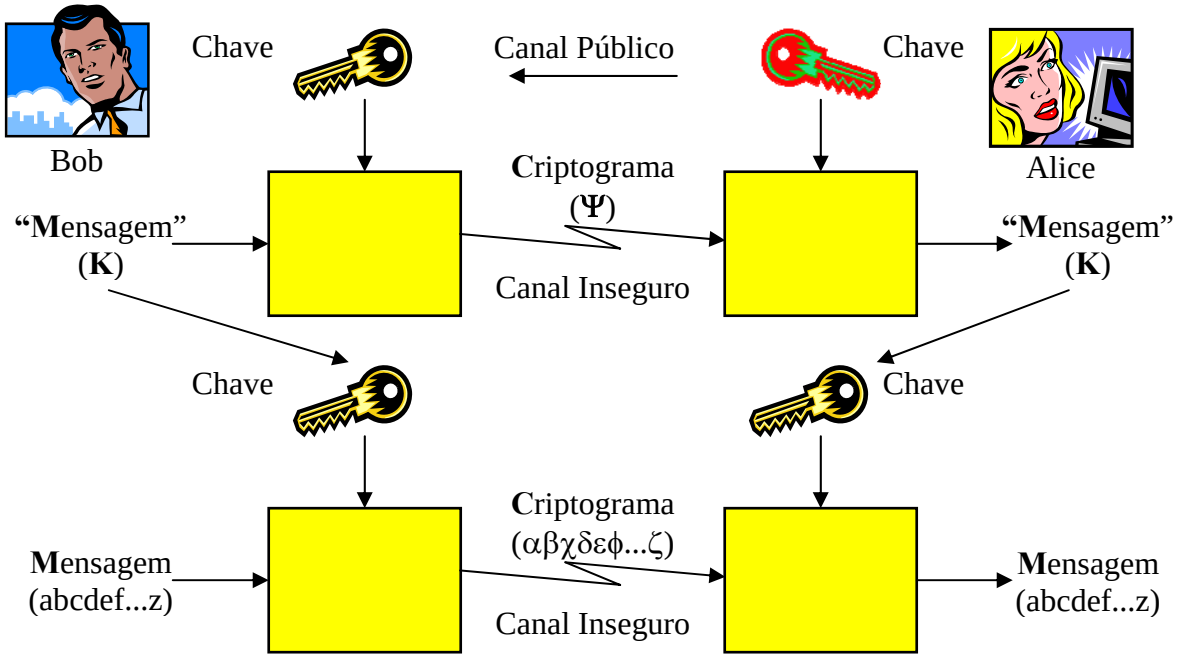

Figura 3: Uso de misto de algoritmo criptográfico assimétrico e simétrico.

Em relação as Assinaturas Digitais, alguns algoritmos criptográficos de chave-pública permitem que estes sejam utilizados para gerar o que se denomina de assinaturas digitais. Estes algoritmos têm a característica de, além da operação normal de cifrar com a chave-pública e decifrar com a chave-privada, eles permitem também que, "cifrando-se" com a chave-privada, a "decifração" com a chave-pública resulta na recuperação da mensagem. Obviamente esta forma de uso não assegura o sigilo da mensagem, uma vez que qualquer um pode "decifrar" o criptograma, dado que a chave-pública é de

conhecimento público. Entretanto, se esta operação resulta na "mensagem esperada" podemos ter a certeza de que somente o detentor da correspondente chave-privada poderia ter realizado a operação de "cifração". Assim, uma assinatura digital é o criptograma resultante da cifração de um determinado bloco de dados (documento) pela utilização da chave-privada de quem assina em um algoritmo assimétrico. A verificação da assinatura é feita "decifrando-se" o criptograma (assinatura) com a suposta chave-pública correspondente. Se o resultado for "válido", a assinatura é considerada "válida", ou seja, autêntica, uma vez que apenas o detentor da chave-privativa, par da chave-pública utilizada, poderia ter gerado aquele criptograma. Na figura 4 ilustramos este procedimento.

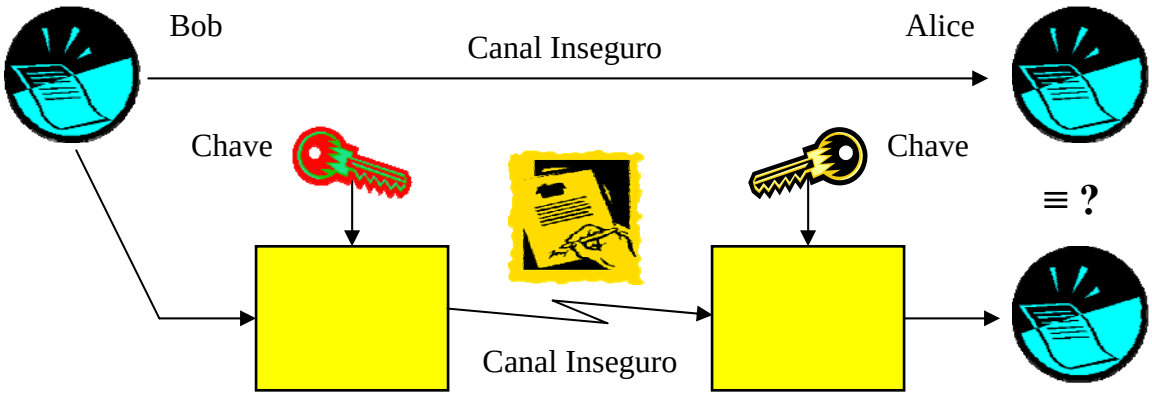

Figura 3: Geração de Assinatura Digital de um documento.

Aqui, Bob assina um "documento", cifrando-o com <u>sua</u> chave-privada e enviando tanto o documento original quanto a "assinatura" para Alice. Esta "verifica a assinatura "decifrando-a" com a chave-pública de Bob (de conhecimento público), e comparando o resultado com o documento recebido. Se estiverem de acordo, a assinatura "confere", caso contrário a assinatura é considerada inválida, significando que ou não foi Bob quem assinou, ou o documento foi adulterado após a assinatura. Observe-se que este procedimento é capaz de garantir tanto a origem (autenticação do emissor), tendo em vista que supostamente somente Bob conhece sua chave-privada e portanto somente ele é capaz de gerar uma assinatura que possa ser verificada com sua chave-pública, como também a integridade do documento, já que, se o mesmo for alterado, a verificação da assinatura irá indicar isto, caso tenha vindo efetivamente do pretenso emissor.

Usualmente, face à ineficiência computacional dos algoritmos simétricos, os métodos para assinatura digital empregados na prática não assinam o documento que se deseja autenticar em si, mas uma súmula deste, obtida pelo seu processamento através do que se denomina uma função de Hashing. Uma função de hashing é uma função criptográfica que gera uma saída de tamanho fixo (geralmente 128 a 256 bits) independentemente do tamanho da entrada. A esta saída se denomina de hash da mensagem (ou documento ou o que quer que seja a entrada). Para ter utilidade criptográfica, a função de hashing deve ser tal que:

-é simples (eficiente, rápido) se computar o hash de dada mensagem;

-é impraticável se determinar a entrada a partir de seu hash;

-é impraticável se determinar uma outra entrada que resulte no mesmo hash de uma dada entrada;

-os valores de hash possíveis são estatisticamente equiprováveis.

A operação de assinatura utilizando hashing é feita então da seguinte forma, como ilustrado na figura 4:

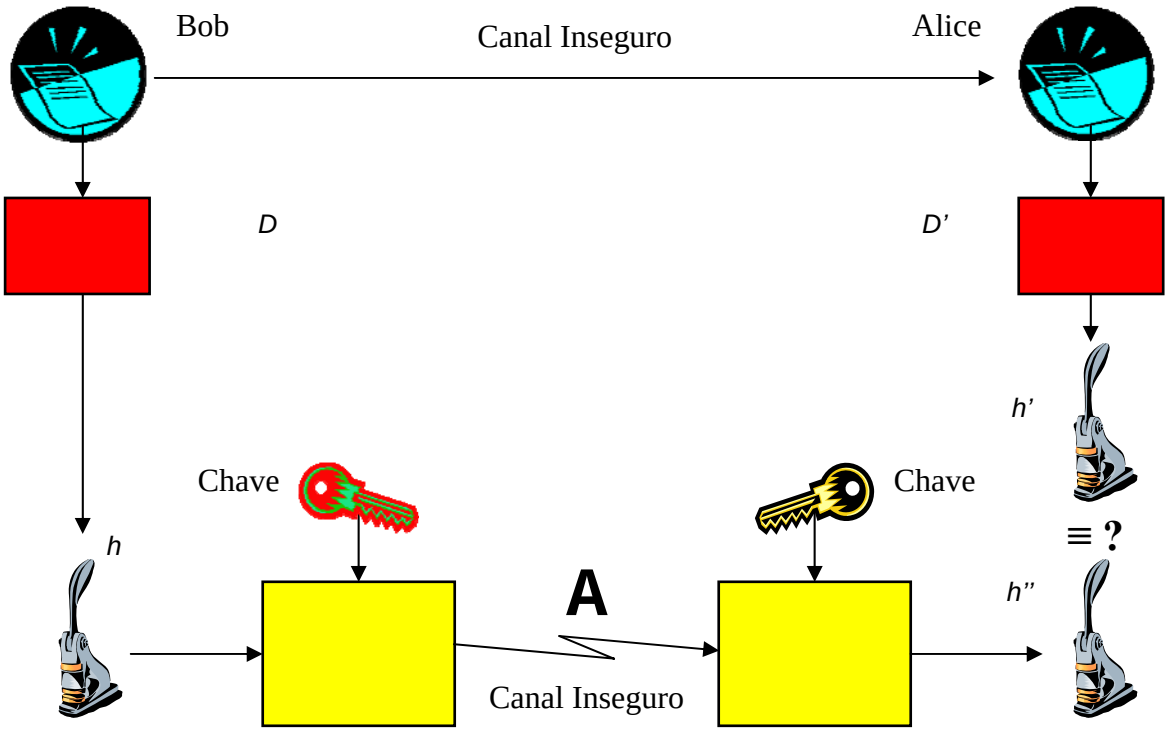

figura 4: Assinatura utilizando funções de hashing.

Bob computa o hash do documento D que deseja assinar, obtendo h;

Bob assina o hash obtido, cifrando-o com sua chave-privada, obtendo A;

Bob envia o documento original, D, e sua assinatura, A, para Alice;

Alice recalcula o hash do documento recebido, D', (é fácil fazer este cálculo e a função de hashing é de domínio público), obtendo h';

Alice "decifra" a assinatura recebida com a chave pública de Bob, obtendo h'';

Se h' ≡ h'', então a assinatura confere e, com elevadíssimo grau de certeza, Alice sabe que foi Bob que enviou o documento, e o documento recebido é cópia fiel do original. Caso contrário, ou não foi Bob que o enviou (assinou), ou o documento foi adulterado após a assinatura, ou ambos."

4 – CERTIFICADO DIGITAL

Resta um problema em relação às chaves públicas: como confiar que determinada chave efetivamente pertence ao seu suposto proprietário? Para resolver este problema, foi criada uma aplicação especial para as assinaturas digitais – os Certificados Digitais.

Um certificado digital nada mais é que um documento (eletrônico) contendo a chave pública de um usuário (ou processo) e dados de identificação do mesmo. Este documento deve ser assinado por uma *autoridade confiável*, a Autoridade Certificadora, atestando sua integridade e origem. Usualmente, certificados digitais são utilizados para garantir a integridade e origem de chaves públicas depositadas em bases de dados de acesso público. O padrão mais comumente utilizado para certificados digitais é o denominado X-509, o qual prevê, entre outras informações possíveis, os seguintes dados de identificação:

a) chave pública do usuário;

b) nome do usuário proprietário da chave;

c) nome da organização associada;

d) data de emissão do certificado;

e) período de validade da chave.

Desta forma, obtendo-se uma chave pública de um usuário associada a tal certificado, confiando-se na autoridade certificadora e verificando-se sua assinatura no certificado, pode-se ter certeza de que a chave realmente pertence ao alegado usuário, e que, pretensamente, somente ele dispõe da correspondente chave secreta que o capacita a decifrar mensagens cifradas com aquela chave pública, ou assinar documentos com a correspondente chave secreta.

A certificação digital pode abranger um escopo que foge em muito àquele atribuído aos tabeliães. Tal atribuição de exclusividade aos tabeliães, a diferenciação entre os serviços a serem prestados pelos tabeliães públicos e outras entidades certificadoras privadas, além de representar uma concentração significativa de poder junto aos mesmos, pode também representar um atraso significativo no desenvolvimento econômico.[83]

Na esfera pública, chaves e certificados podem servir tanto para a segurança da transmissão de mensagens internas corriqueiras como de informações de segurança máxima, ou ainda, para atribuir autenticidade a documentos públicos. O Decreto Lei nº 3.587/00 define finalidades e os efeitos que os documentos eletrônicos poderão produzir.[84]

Portanto, o certificado digital é um documento eletrônico firmado digitalmente pela Autoridade Certificadora, que vincula uma chave pública a uma pessoa determinada, confirmando sua identidade. Tem o condão de unir a tecnologia com o Direito, deixando clara a possibilidade, em face do nosso ordenamento jurídico, de se legitimar o documento eletrônico como meio de prova.[85]

A Medida Provisória 2.200-2, de 24 de agosto de 2001 instituiu a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil", para garantir a autenticidade , a integridade e a validade jurídica de documentos em forma eletrônica.

---

[83]SILVA JUNIOR, Ronaldo Lemos Da e Ivo Waisberg (organizadores) . Comércio eletrônico . São Paulo: Editora Revista dos Tribunais, 2001, p. 155.

[84] MARCACINI, Augusto Tavares Rosa . Direito e Informática: Uma abordagem jurídica sobre a criptografia . Rio de Janeiro: Forense,2002- p. 97.

[85] FINKELSTEIN, Maria Eugênia . Aspectos jurídicos do comércio eletrônico . Porto Alegre: Síntese, 2004 ,p. 180.

4.1 – AUTORIDADES CERTIFICADORAS

Um dos pontos críticos da assinatura digital é o processo verificação. O processo em si é bem simples como demonstrado acima. Porém, como ter certeza de que a chave pública usada para verificar é realmente do assinante da mensagem? Num grupo pequeno, um pode trocar, pessoalmente, sua chave pública com o outro e assim todos do grupo têm condições de verificar a assinatura um do outro.

Porém, numa rede grande esse processo se torna inviável, pois fica muito difícil encontrar todas as pessoas para receber as chaves públicas delas. Se estivermos falando de relações comerciais isso se torna mais complicado ainda, pois nesse tipo de relação milhares de pessoas são atendidas e muitas vezes a comunicação é entre máquinas e não mais entre pessoas. A solução é trabalhar com delegação de confiança. Nesse processo, uma pessoa aceita a chave pública de outra, desconhecida para ela, porque uma terceira pessoa que ela conhece e confia garantiu para ele que aquela chave pública é realmente da pessoa cuja assinatura se deseja verificar. Na verdade encarar esse processo como um reconhecimento de firma digital, visto que é exatamente isso que acontece no processo tradicional de reconhecimento de firma. Quando uma pessoa vai a um cartório reconhecer a assinatura de outra, ela o faz por confiar na entidade cartório. E o que o cartório faz é apor a sua assinatura junto à assinatura do terceiro garantindo que aquela assinatura é verdadeira. A pessoa aceita a assinatura como verdadeira por confiar na instituição que dá a chancela. No mundo digital acontece a mesma coisa. Uma entidade confiável (chamada comumente de Autoridade Certificadora – AC) assina eletronicamente um documento (chamado de Certificado Digital) contendo os dados pessoais de uma pessoa além da sua chave pública. Assim o certificado digital tem a chave pública da pessoa e a assinatura da AC. De posse da chave pública da AC qualquer um pode verificar a assinatura do certificado digital e ter certeza que a chave pública contida nele pertence à pessoa nominada no mesmo. Veja que nesse processo há uma hierarquia de confiança da AC para o proprietário do certificado. Uma vez tendo certeza de que a chave pública do certificado é verdadeira qualquer pessoa pode verificar a assinatura do proprietário do certificado em qualquer documento eletrônico.

Qual a vantagem desse processo? A AC agora é responsável por identificar pessoalmente a pessoa, receber a sua chave pública e emitir um certificado para ela. Assim, para verificar a assinatura de alguém somente é necessário guardar a chave pública da AC e sempre que a assinatura de alguém tiver de ser verificada em um documento, a pessoa que verifica precisa apenas do certificado do assinante emitido pela AC. Agora, em vez de guardar um grande número de chaves públicas no seu computador, somente é necessário guardar a chave pública da sua AC de confiança.[86]

Surge a figura do "cibernotário" que é a pessoa ou entidade que atua como uma autoridade certificadora – AC, expedindo certificados de autenticidade de forma organizada. Devem ser consideradas as finalidades ou as intenções das partes, o certificador e o titular da chave certificada, bem como a posição que estas partes ocupam no cenário jurídico. Uma empresa pode, ela própria, certificar seus clientes. Empresas têm expedido certificados eletrônicos como sua atividade principal. Neste caso, os certificados têm o valor de uma declaração pública à praça, para afirmar que realmente pertencem ao titular nela indicado. Para maior segurança há fixação precisa dos termos e responsabilidades com que os certificados são emitidos. As certificações privadas, enfim, são frutos de relações contratuais.

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.[87]

Certificado Digital e a Autoridade Certificadora são as respostas tecnológicas atual para o problema de autenticação de usuários na crescente demanda por segurança nos serviços oferecidos via Internet, desde *home banking*, passando por compras *on-line*, indo até serviços de informação por assinatura. Eles podem ser vistos como um *Passaporte Eletrônico*, onde estão

[86] E-SEC: Tecnologia em Segurança de Dados - Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital .doc > – Acesso em 02 jul. 2007.

[87] FINKELSTEIN, Maria Eugênia . Aspectos jurídicos do comércio eletrônico . Porto Alegre: Síntese, 2004 , p.181.

contidas as informações e garantias necessárias sobre a identidade do portador, além de sua chave pública.

4.2 – QUEM PODE SER UMA AC

Dentre as mais conhecidas identificamos a SERASA, a OAB e a CERTSIGN.

Conforme a orientação do 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.[88]

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 subseqüente 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, ditribuir, 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.

[88] Ministério da Justiça, Ministério da Fazenda, Ministério do Desenvolvimento, Indústria e Comércio exterior, Ministério don Planejamento, Orçamento e Gestão, Ministério da Ciência e tecnologia, Casa Civil da Presidência da República e Gabinete de segurança Institucional da Presidência da República.

Já as autoridades de Registro deverão identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às autoridades Certificadoras e manter registro de suas operações. As autoridades de registro serão sempre vinculadas a uma determinada Autoridade Certificadora.[89]

5 – ATUALIDADES

5.1 – E-SELO: SISTEMA DE ASSINATURA DIGITAL E REGISTRO DE DOCUMENTOS ELETRÔNICOS

O comércio eletrônico aumenta a eficiência dos negócios, permitindo que informações eletrônicas sejam armazenadas, acessadas e transmitidas com grande facilidade. Apesar disso, faz-se necessário uma comunicação mais eficiente das informações eletrônicas, com o mesmo nível de confiança e valor que o público se habituou ao trocar informações no ambiente físico.

O Sistema de Assinatura Digital e Registro de Documentos Eletrônicos (*e-Selo*) foi concebido para possibilitar a troca de informações entre sistemas comerciais, financeiros e governamentais, de uma maneira segura, fortalecendo a privacidade e a produtividade das comunicações eletrônicas através do uso da tecnologia de assinatura digital.

5.1.1 - Objetivos

O *e-Selo* é um sistema de segurança, baseado na web, que inclui suporte à certificados digitais e carimbos de tempo, viabilizando a utilização da assinatura digital de conteúdos eletrônicos em ambientes corporativos.

O *e-Selo* implementa todos os recursos e ferramentas necessárias para permitir o armazenamento e o controle de fluxo entre as partes envolvidas no processo de assinatura digital de documentos eletrônicos.

[89] FINKELSTEIN, Maria Eugênia . Aspectos jurídicos do comércio eletrônico . Porto Alegre: Síntese, 2004, p.183.

O *e-Selo* garante a privacidade das informações, fornecendo todas as evidências necessárias para garantir o Não-Repúdio de transações eletrônicas, prevenindo e detectando alterações ou manipulações fraudulentas de conteúdos eletrônicos.

5.1.2 – Aplicabilidade

O *e-Selo* garante a integridade, a autoria e a validade jurídica de conteúdos eletrônicos, podendo ser aplicado a e-mails, formulários web, contratos, procurações, relatórios, imagens, mandatos, notificações, balanços, declarações, resultados de exames, prontuários médicos, propostas e apólices de seguros, arquivos eletrônicos transferidos entre empresas (*EDI*), viabilizando a eliminação do uso do papel e a diminuição dos custos de emissão, armazenamento e descarte destes documentos.

5.1.3 – Confiabilidade

Um documento eletrônico assinado e registrado pelo *e-Selo* é confiável porque:

Verifica validade dos certificados digitais no ato das assinaturas, incluindo consultas às Listas de Certificados Revogados (*LCR*);

Os dados manipulados pelo *e-Selo* ficam armazenados em Bancos de Dados corporativos, criptografados, podendo ser acessados somente pelas partes contratadas ou previamente autorizadas pelo criador do documento;

Pode adicionar a cada assinatura, por solicitação do cliente, um carimbo confiável de tempo, garantindo a irretroatividade da assinatura de um documento eletrônico, sendo um elemento fundamental ao Não-Repúdio da operação;

5.1.4 - Principais Funcionalidades

Possibilita o registro de documentos eletrônicos em um servidor corporativo, funcionando como um repositório seguro de documentos eletrônicos (Cofre Eletrônico) que

poderão ser visualizados, assinados, impressos ou exportados, a qualquer momento, pelas pessoas autorizadas;

Mantém os documentos eletrônicos armazenados pelo período tempo determinado pela lei aplicável a cada tipo de documento ou operação;

Implementa um mecanismo de *workflow*, notificando e permitindo o acompanhamento, pelas partes envolvidas, de todas as etapas do processo de aprovação e assinatura de documentos eletrônicos;

Permite a visualização e verificação da autenticidade de documentos eletrônicos, possibilitando a consulta das informações das pessoas que assinaram um determinado documento.

5.1.5 - Benefícios

Assinatura e verificação do documento independente da localização física das partes envolvidas, pois a operação é realizada via *Internet;*

Diminuição do tempo necessário para o recebimento e envio dos documentos para obter as assinaturas;

Redução de custos operacionais decorrentes da eliminação dos documentos em papel

Não é necessário recolher assinaturas nem papel;

É desnecessária a verificação manual de assinaturas, que além de tomar tempo, exige mão de obra específica;

Eliminação de recursos de gerenciamento eletrônico de documentos (*GED*), pois não há papel a escanear;

Eliminação da necessidade de armazenamento dos documentos físicos (papel), pois eles não existem;

Aumento natural de capilaridade da rede de captação.

Diminuição do custo da captação, sem perda da segurança e com aumento da produtividade.

5.1.6 - Integração com Sistemas Legados

O *e-Selo* pode ser integrado a qualquer sistema legado previamente existente ou customizado de acordo com as necessidades de cada empresa. O *e-Selo* possui um *kit* de desenvolvimento de *software* (*SDK*) para que os desenvolvedores possam construir novas aplicações ou alterar aplicações já existentes, incorporando funcionalidades do *e-Selo* ou de assinaturas digitais (*PKI*).

5.1.7 - Garantias Adicionais

a) Controle de Acesso & Autenticação de Usuário

O *e-Selo* já incorpora toda a infra-estrutura necessária para garantir o melhor nível de segurança na assinatura de conteúdos eletrônicos, assegurando que somente as pessoas que tiverem o perfil e alçada adequados terão acesso às informações e serviços oferecidos. A autenticação dos usuários pode ser feita de várias formas, incluindo a autenticação biométrica ou através de Certificados Digitais armazenados em *Tokens* ou *Smart Cards*, ou Serviços de Diretórios (*AD*).

b) Controle de Limites, Poderes e Alçadas (Políticas de Aprovações)

Opcionalmente, o controle de limites, poderes e alçadas dos usuários pode ser garantido através da integração do *e-Selo* com o QualiFP - Sistema de Administração de Firmas, Documentos e Poderes, ou com a Procuração Eletrônica, ambas da *QualiSoft*, ou ainda com outros sistemas já existentes na empresa. Uma vez integrado, o *e-Selo* obtém automaticamente a lista de pessoas que podem assinar um determinado tipo de documento e também verifica, em tempo real, no ato de cada assinatura, se a pessoa que assinou eletronicamente o documento tinha poderes para tal.

c) Validade Jurídica, Normas e Recomendações

No Brasil, a validade jurídica do *e-Selo* está embasada na medida provisória 2200-2, de 24 de Agosto de 2001, que estabelece que todo documento em forma eletrônica tenha assegurada a autenticidade, integridade e validade jurídica desde que utilize certificados digitais.

O *e-Selo* é tecnológica e funcionalmente aderente às recomendações da *American Bar Association PKI Assessment Guidelines 2001*, *E-SIGN* (*Electronic Signatures in Global and National Commerce Act* / Junho 2000), ao Comunicado FB-074/2004 da FEBRABAN, à Circular 277/04 da SUSEP e às Circular e Carta-Circular 3.234 e 3.134 respectivamente, do Banco Central do Brasil, que garantem a assinatura digital de contratos de câmbio.

O *e-Selo* também está em conformidade com o *Manual de Condutas Técnicas, Volume IV*, do *ITI – Instituto Nacional de Tecnologia da Informação*, que estabelece os requisitos mínimos de certificação digital para os processos de assinatura digital, sigilo e autenticação para softwares *ICP-Brasil*.

O *e-Selo* é compatível com todos os certificados digitais padrão *X.509*, incluindo o *e-CPF* e o *e-CNPJ*, documentos digitais oficiais da *SRF* do Brasil.[90]

5.2 – PROTEÇÃO AO CONSUMIDOR

A proteção ao consumidor é um dos assuntos mais delicados na falta de regulação. É imediatamente perceptível que a proteção do consumidor sofre diretamente com os problemas de jurisdição e lei aplicável na Internet. Um exemplo é a compra de um produto em um site americano através de cartão e o produto não é entregue. Em face dessa situação, difícil fica a determinação do mecanismo para ressarcimento e perante qual foro e sob qual direito deverá ser proposta eventual ação. O consumidor teria de se submeter ao direito do local da oferta, ou seja, ao direito norte-americano, tendo que ajuizar a ação nos Estados Unidos. Porém o código de defesa do Consumidor expressamente prevê que os consumidores brasileiros têm o direito de promover quaisquer ações fundadas na responsabilidade do fornecedor perante o foro de seu próprio domicílio. Assim, o consumidor poderia promover a ação no Brasil, mas o direito a ser aplicado pela corte brasileira teria de ser o direito norte-americano. A aplicação do direito estrangeiro por parte dos tribunais brasileiros traz insegurança para as partes e para o judiciário. A tendência seria aplicar a *lex fori*, a lei brasileira, porém traria grande problema na decisão da corte brasileira para que seja acatada nos Estados Unidos. Para solucionar estes conflitos foram

[90] ICP-BRASIL . Disponível em: < http://www.qualisoft.com.br/produtos/e-selo/e-selo.asp>.

criados “Mecanismos Alternativos de Resolução de Disputas” (ADR), a institucionalização de determinados órgãos internacionais para estas questões. A tendência é de que em um futuro muito próximo, todos os sites de e-commerce filiem-se a algum órgão de resolução de disputas.

Outra solução imediata adotada na prática quanto à proteção do consumidor on-line foram dadas pelas próprias empresas de cartões de crédito. Várias empresas de cartão de crédito oficializaram uma diretriz própria de que os consumidores seriam responsabilizados por fraudes relacionadas ao uso indevido de seus cartões de créditos somente até 50 dólares, em casos em que a fraude não tivesse sido comunicada à empresa em até 2 dias após sua ocorrência.[91]

O Projeto de Lei nº 4.906/01 que tramita no Congresso Nacional prevê que será aplicado as normas de defesa do consumidor ao comércio eletrônico em seu art. 30.

5.3 – AUTORIDADE CERTIFICADORA – CERTSIGN

A Certsign é uma das empresas mais atuantes neste ramo no Brasil, embora a OAB esteja utilizando cada vez mais a Certificação da Assinatura Digital. A CertSign celebra um contrato para a emissão de assinaturas digitais registrado em um Registro de Títulos e Documentos, com o fim de dar publicidade ao mesmo. A pessoa que deseja receber um certificado digital deverá aderir a esse contrato. A CertSign enviará ao interessado um termo de adesão ao seu contrato padrão. Neste termo estará mencionado o número da identificação digital a ser utilizada em meio eletrônico. Em havendo interesse, a parte deverá dirigir-se a um ofício de notas para o reconhecimento de firma por autenticidade da assinatura aposta no termo de adesão, bem como tirar cópia autenticada de alguns documentos de identificação. Uma vez concluída tal tarefa, o interessado deverá enviar via correio o termo e as cópias relacionadas para a CertSign, que se encarregará de levar tais documentos para arquivo junto a um Registro de Títulos e Documentos. Após isto a CertSign enviará para o interessado a chave que o identificará no meio eletrônico. Nesse sentido, quando duas pessoas identificadas em meio eletrônico pela autoridade Certificadora iniciarem uma troca de documentos, haverá uma presunção de que aquelas pessoas

[91]SILVA JUNIOR, Ronaldo Lemos Da e Ivo Waisberg (organizadores) . Comércio eletrônico . São Paulo: Editora Revista dos Tribunais, 2001 , p. 161.

são de fato as que efetivamente contrataram. Além disso, a Autoridade Certificadora deve deixar claro o termo de validade da Certificação Digital auferida.[92]

5.4 – ESTUDO SOBRE A EVOLUÇÃO DA LEGISLAÇÃO NO BRASIL

No que se refere ao plano legislativo, o primeiro marco pode ser encontrado, na década de 70, no artigo 100 da Lei sobre as Sociedades por Ações nº 6.404, de 15 de dezembro de 1976, que prevê a possibilidade, nas companhias abertas, de substituição dos tradicionais livros sociais por registros magnetizados ou eletrônicos.

Houve, em seguida, mais algumas manifestações isoladas, mas só a prtir da década de 90 é que a legislação deu mostras mais efetivas de compreensão da importância do avanço tecnológico, primeiramente com as Leis nºs 8.934 e 8.935, ambas de 18 de novembro de 1994, que dispuseram, respectivamente, sobre o Registro Público de empresas Mercantis e atividades afins, onde o artigo 57 estabelecia que os atos de empresas, após microfilmados ou preservada a sua imagem por meios tecnológicos mais avançados, poderiam ser devolvidos pelas juntas Comerciais, conforme dispusesse o regulamento, e sobre os serviços notariais e de registro, onde o artigo 41 incumbia aos notários e aos oficiais de registro praticar, independentemente de autorização, todos os atos previstos em lei necessários à organização e execução dos serviços, podendo, ainda, adotar sistemas de computação, microfilmagem, disco ótico e outros meios de reprodução. E, posteriormente, com as Leis nº 9.099, de 26 de setembro de 1995, que disciplina os Juizados Especiais Cíveis e Criminais, onde o parágrafo 3º do artigo 13 dispõe que apenas os atos considerados essenciais serão registrados resumidamente, em notas manuscritas, datilografadas, taquigrafadas ou estenotipadas, e os demais atos poderão ser gravados em fita magnética ou equivalente, que será inutilizada após o trânsito em julgado da decisão e Lei nº 9.610 de 19 de fevereiro de 1.998 que disciplina os Direitos Autorais, onde o artigo 5º considerou ser transmissão ou emissão: a difusão de sons ou de sons e imagens, por meio de ondas radioelétricas; sinais de satélite; fio, cabo ou condutor; meios óticos ou qualquer outro processo eletromagnético; enquanto o artigo 29 previu a necessidade de autorização prévia e

[92] FINKELSTEIN, Maria Eugênia . Aspectos jurídicos do comércio eletrônico . Porto Alegre: Síntese, 2004 , p.174.

expressa por parte do autor para a utilização da obra, qualquer que seja a modalidade desta, incluindo-se, a distribuição para oferta de obras ou produções mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para percebe-la em um tempo e lugar previamente determinados por quem formula a demanda, e nos casos em que o acesso às obras ou produções se faça por qualquer sistema que importe em pagamento pelo usuário.

Merece referência também, a Lei nº 9.457/97, relativamente à nova redação, por ela determinada, do parágrafo 1º do artigo 289 da Lei nº 6.404, possibilitando que as publicações exigidas para as sociedades por ações pudessem ser feitas, com autorização da Comissão de Valores Mobiliários, em jornal de grande circulação nas localidades em que os valores mobiliários da companhia fossem negociados em bolsa ou em mercado de balcão, ou disseminadas por algum outro meio que assegurasse sua ampla divulgação e imediato acesso às informações. A Lei nº 9.755, de 16 de dezembro de 1.998, que dispôs sobre a criação de uma homepage na internet, pelo tribunal de Contas da União, para a divulgação dos dados e informações relevantes relacionados às contas públicas. A Lei nº 9.800, de 26 de maio de 1.999, que permitiu às partes a utilização de sistema de transmissão de dados para a prática de atos processuais.[93]

A Lei nº 9.800, de 26 de maio de 1.999, permitiu às partes a utilização de sistema de transmissão de dados para a prática de atos processuais.[94]

Quanto aos Projetos de Lei em andamento, novamente destacamos:

Projeto de Lei 2161/91 – que dispõe sobre o arquivamento e eliminação de processos judiciais.

Projeto de Lei 5067/91 – trata do Mandado de Segurança e de procedimentos eletrônicos.

Projeto de Lei 1713/96 – trata de documentos eletrônicos e da possibilidade de arquivos digitais.

---

[93] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.45.

[94] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.115.

Projeto de Lei 1233/99 – trata do interrogatório à distância e se encontra apensado ao Projeto de Lei 2504/2000.

Projeto de Lei 1532/99 – dispõe sobre o arquivamento de dados judiciais em meios eletrônicos.

Projeto de Lei 1589/99 – dispõe sobre comércio eletrônico e define o que venha a ser documento eletrônico.

Projeto de Lei 3475/2000 – acrescentou o parágrafo único ao artigo 154 do CPC.

Projeto de Lei 6896/2002 – altera a Lei do Fax, para inserir o envio de dados processuais por meio eletrônico.

Projeto de Lei 6965/2002 – armazenamento de dados processuais em meio eletrônico.

Projeto de Lei 7316/02 – do Executivo, para utilizar nomenclatura internacional sobre assinatura eletrônica.

Projeto de Lei 1237/2003 – interrogatório à distância.

Um dos mais importantes é o Projeto de Lei 4906/01 – apensados os Projetos de Lei 1483/99 e 1589/99 - 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.

Não poderia deixar de citar também:

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 Orgãos 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.

E as Leis e Decreto Leis:

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

2 – Lei 9800 de 26 de maio de 1999 – Sistema de transmissão de dados para prática de atos processuais.[95]

3 - 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. [96]

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

Se, porém, a exemplo do que se viu em outras legislações, houver a previsão legal específica conferindo efeitos probantes às mensagens eletrônicas, o quadro atual poderá se positivamente alterado a fim de que um meio tão prático, rápido e barato, já de uso correntio pela sociedade brasileira, possa oferecer maior segurança às relações jurídicas entre as pessoas. Foi o que ocorreu com a edição da já referida Medida Provisória 2.200-2, de 24 de agosto de 2.001, cujo art. 10 estabeleceu que seriam considerados documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos por ela tratados. Fica claro, portanto, que o e-mail e o documento digital, no Brasil, desde que certificados digitalmente de acordo com as normas da ICP-Brasil, terá o mesmo efeito que o documento original, consoante apregoa o parágrafo 2º do art. 10.[97]

Um grande marco dentre os Projeto de Lei em trâmite ainda é a Lei nº 1.589/99, que foi elaborado através do anteprojeto elaborado pela Comissão de Informática da Ordem dos Advogados do Brasil, Seccional São Paulo, que hoje está apensado aos Projetos de Lei nºs

[95] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.46.

[96] ITAU. Disponível em <www.itaubank.com.br/popups/ contratos_digitais /legislacao.asp> Acesso em: 20 ago.2007.

[97] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p119.

672/99 e 1.483/99, dando origem ao Projeto de Lei nº 4.906, de 26 de setembro de 2.001.[98] Importante ressaltar que este Projeto de Lei no seu art. 30 prevê que aplicam-se ao Comércio Eletrônico as normas de defesa do consumidor vigentes no País, naquilo que não conflitar com esta Lei.[99]

Outra novidade é a criação da Portaria nº 1.017, de 7 de julho de 2.003, pelo Ministério da Justiça. Esta Portaria criou a Comissão de Proteção ao Consumidor no Comércio Eletrônico e com a ajuda do Departamento de Proteção e Defesa do Consumidor – DPDC, foi possível a elaboração de uma cartilha (tira-dúvidas), em linguagem simples e didática, a fim de orientar aos consumidores que pretendam adquirir produtos ou utilizar serviços através da Rede.

5.4.1 – QUANTO A VALIDADE JURÍDICA DO MEIO ELETRÔNICO

O nosso velho Código Comercial já previa na época imperial que os contratos comerciais poderiam ser provados, entre outros meios, pela chamada correspondência epistolar (art. 122, inciso IV). O meio de prova chamada correspondência epistolar é o papel. Já o meio de prova na Internet será o suporte eletrônico. Diz o art. 332 do Código de processo Civil:

"Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa."[100]

Ao lado do art. 332 do CPC, há de se considerar, igualmente, a disposição constante do art. 131 do mesmo código, relativamente ao livre convencimento motivado:

---

[98] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.32.

[99] FINKELSTEIN, Maria Eugênia . Aspectos jurídicos do comércio eletrônico . Porto Alegre: Síntese, 2004 , p.490.

[100] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.80.

"O juiz apreciará a prova livremente, atendendo aos fatos e circunstâncias constantes dos autos, ainda que não alegados pelas partes; mas deverá indicar na sentença os motivos que lhe formaram o convencimento."[101]

Já o art. 335 do CPC prevê:

"Em falta de normas jurídicas particulares, o juiz aplicará as regras de experiência comum subministradas pela observação do que ordinariamente acontece a ainda as regras de experiência técnica, ressalvado, quanto a esta, o exame pericial."[102]

Expressou, com a propriedade de sempre, quanto a evolução da informática na época, o eminente Ministro Sálvio de Figueiredo (STJ, 4º turma, embargos de Declaração no REsp 62.529-RS, DJU 2.9.1996):

"O judiciário, conservador por tendência e carências bem conhecidas, não pode fechar os olhos a instrumento tão eficaz e hoje amplamente utilizado no plano mundial. Recomenda-se, para melhor segurança do sistema, inclusive para fins de aferição da tempestividade, a colocação de aparelho receptor nas dependências do protocolo."[103]

Destaque-se, em tal sentido, a seguinte ementa:

"Processo Civil – embargos de Declaração – Oposição por fax – apresentação dos originais após o prazo recursal – Irrelevância. À luz dos princípios modernos do Processo Civil, que prestigiam o uso dos instrumentos de documentação e os recursos da informática, esta egrégia Corte tem proclamado o entendimento no sentido de ser admissível a admissão de recurso manejado por meio de aparelho de fax, remetido e recebido no prazo legal, não constituindo obstáculo para o seu conhecimento a apresentação dos originais após o decurso do lapso referenciado. Embargos de Declaração rejeitados."(EREsp 0093944, 6º Turma, Rel. Ministro Vicente Leal, j. em 24.2.1997, DJ de 17.3.1997, p. 7573).

---

[101] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.88.

[102] SILVA JUNIOR, Ronaldo Lemos Da e Ivo Waisberg (organizadores) . Comércio eletrônico . São Paulo: Editora Revista dos Tribunais, 2001, p. 310.

[103] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.113.

A legislação superveniente viria acompanhar, como era de se esperar, a evolução representada por esse último Acórdão, tendo sido editada a Lei nº 9.800, de 26 de maio de 1.999, que permitiu às partes a utilização de sistema de transmissão de dados para a prática de atos processuais.

Pelo art. 371, inciso I do Código de Processo Civil:

"Reputa-se autor do documento particular:

I – aquele que o fez e assinou.

O art. 219 do Código Civil dispõe que:

"as declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários".

O art. 10, da MP 2.200-2/01 dispôs:

"*consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos digitalmente assinados".*

O parágrafo 2º do art. 10 da MP 2.200-2/01 deixou aberta a possibilidade de validação de documentos eletrônicos certificados por outros meios de comprovação de autoria e integridade, mesmo que não emitidos na forma da ICP-Brasil, desde que o emitente os tenha aceito como válidos. Essa disposição está de acordo com a sistemática estabelecida pelo Código civil para a validade do negócio jurídico, quando o art.107 estabelece que :

"a validade da declaração de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir".

Essa diretriz está em linha com a filosofia recomendada pela Lei Modelo da UNCITRAL quando estabelece, no art. 7º , que se considera satisfeito o requisito legal de assinatura quando um documento eletrônico utilizar um método fiável para identificar o autor e a aceitação do conteúdo, incluindo a existência de um acordo nesse sentido.[104]

Atualmente o problema da identificação e da integridade dos documentos eletrônicos foi solucionado pela assinatura digital, conforme todo o exposto nesta monografia e que mostra a

[104] LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros . Direito & Internet : aspectos jurídicos relevantes . São Paulo: Quartier Latin, 2º. Edição, 2005, p.445.

grande tecnologia que acompanha o desempenho preciso da tecnologia para a validade jurídica dos contratos eletrônicos, que antes era duvidoso e que necessariamente deve acompanhar a evolução da tecnologia na mesma velocidade das suas mudanças para que o mundo jurídico não fique a quem do amanhã.

PARTE III – CONSIDERAÇÕES FINAIS

1 - COMENTÁRIOS

Este tema, ao contrário do que pensávamos, de que seria restrito, no desenvolvimento da monografia percebemos a necessidade de abranger ao máximo os conceitos técnicos, para o perfeito entendimento, afinal a intenção e objetivo maior é focar, depois de embasado em inúmeras informações da área de informática, na tese a respeito da validade jurídica da Assinatura Digital no Contrato Eletrônico. Em muitos trechos foram incluídos vários entendimentos doutrinários para ter o entendimento majoritário do tema. Uma grande dificuldade sentida, por isso da grande preocupação em manter informações obtidas pela Internet, do próprio computador que é o tema desta discussão, em relação ao avanço da tecnologia e a necessidade da segurança nas informações, foi a desatualização de várias doutrinas, onde observava-se que a grande maioria foram escritas em meados de 2000 a 2003, e é inevitável que devido a rapidez na evolução da informática, preocupação dos legisladores na atualização das Leis, devido as tendências mundiais, os inúmeros Projetos de Lei e o próprio Código Civil de 2002 que entrou em vigor só em 2003, fato que apenas as doutrinas escritas em 2004 estão atualizadas. Em busca de livros recentes, percebi a dificuldade em trabalhar com um tema novo e constantemente em atualização, que está ainda, inclusive se solidificando no Brasil.

2 – RECOMENDAÇÕES

O tema é extenso, porém procurei abordar os principais pontos de forma a apresentar ao leitor, mesmo leigo no assunto informático, de entender a sistemática da Assinatura digital e sua importância no contrato eletrônico, sem muito se ater a tipos de contratos, que não é o foco de estudo. Juntei todas as informações mais importantes para a compreensão e embasamento de minha tese e ao leitor que tiver interesse no prosseguimento ao estudo do tema, utilize-se da grande ferramenta que temos hoje, que é uma das fontes doutrinárias mais atualizadas, a Internet e as empresas de buscas de informações, que muito me auxiliou, mas respeite a autoria de quem nos ajuda a completar e solucionar nossas dúvidas, tanto nos Sites quanto na doutrina atual.

3 – CONCLUSÃO

Portanto há validade jurídica da assinatura digital no Contrato eletrônico? A resposta é sim.

Fiz um levantamento de todas as informações disponíveis, procurei trazer o entendimento de várias doutrinas para poder justificar a minha tese em relação a Validade Jurídica da Assinatura Digital no Contrato Eletrônico, até mesmo em função do novo Código Civil de 2002 e do Código de Processo Civil de 1973. Atualmente o problema da identificação e da integridade dos documentos eletrônicos foi solucionado pela assinatura digital, conforme todo o exposto nesta monografia e que mostra a grande evolução da tecnologia para a validade jurídica dos contratos eletrônicos, que antes era duvidoso e que foi superado. Isto graças ao acompanhamento da estrutura jurídica internacional e o acompanhamento nacional da evolução da tecnologia. O uso da criptografia assimétrica e simétrica, chave pública e privada, da Certificação digital e da Autoridade Certificadora no Brasil, praticamente nos garante a certeza de sua validade jurídica. Para gerar assinaturas digitais cria-se um vínculo entre a assinatura e o corpo do documento, impedindo a sua alteração posterior. A assinatura digital se torna inforjável, sendo dessa forma mais segura que a assinatura convencional. Portanto, graças a tecnologia, a possibilidade de validade jurídica do Contrato Eletrônico através da utilização da Assinatura Digital é a realidade hoje.

Fazendo um resumo de tudo que estudei trago algumas outras conclusões:

1 - A primeira dúvida que surgiu foi a confusão entre assinatura eletrônica e assinatura digital. Após estes estudos percebe-se claramente que a assinatura eletrônica não se confunde com a assinatura digital. A assinatura eletrônica seria qualquer método ou símbolo baseado em meios eletrônicos utilizado por uma parte com a intenção de autenticar um documento, cumprindo todas as funções de uma firma manuscrita. A assinatura digital seria uma forma específica de assinatura eletrônica, em que há um processo criptográfico que dá segurança àquele que assina o documento, através de uma chave privada de assinatura e da integridade dos dados com o uso de uma chave pública de assinatura sustentada por um certificado de chave de assinatura utilizada, fornecida por uma autoridade de certificação.

2 - Nota-se que há duas questões distintas relacionadas à assinatura digital. A primeira refere-se à eficácia probatória dos contratos celebrados através dos computadores, já concluído acima e a segunda é a discussão acerca da segurança e privacidade dos usuários dessa nova tecnologia.

2.1 - Quanto a primeira questão:

O documento eletrônico assinado digitalmente é dotado de um maior grau de confiabilidade que o próprio documento tradicional. A verdadeira assinatura digital, legitimamente gerada pelo seu titular, não tem como ser falseada. No fundo, inexiste falsidade a ser apurada no próprio documento eletrônico. O problema se resume exclusivamente na verificação da autenticidade da chave pública. Sabendo ser autêntica a chave pública, com um simples uso do programa de criptografia que utiliza tais chaves, pode-se conferir a autenticidade e veracidade do documento eletrônico, como também auferir com segurança a origem e a integridade do documento.

As Assinaturas Digitais assim produzidas ficam de tal sorte vinculada ao documento eletrônico “subscrito” que, ante a menor alteração, a assinatura se torna inválida. A técnica não só permite demonstrar a autoria do documento, como estabelece uma “imutabilidade lógica” do seu conteúdo. A verificação positiva de uma assinatura digital enseja um elevado grau de certeza jurídica da autenticidade da autoria e da integridade da mensagem ou outro tipo de documento, pois se prova com certeza substancial que o documento não foi alterado. E que provém do seu emissor.

Não há como por meio da chave pública, desvendar os segredos da chave privada devido às operações matemáticas que são utilizadas para a confecção da chave privada. As operações são de tal forma intrincada que a segurança delas pode ser considerada total e impedem que a chave pública possa descobrir os segredos numéricos da chave privada. Esta é como uma complicada senha.

Portanto um documento eletrônico instrumentalizado por técnica cuja eficácia e segurança possam ser comprovadas, além de atestar a sua autenticidade, dentro do contexto de liberdade probatória, deve ser aceito como válido e, assim, obrigar as partes a ele relacionadas. A MP 2200-2/01 e a Assinatura Digital de Chave Pública vieram para facilitar o reconhecimento da legalidade desse tipo de documento, liberando as partes de recorrerem a meios externos e excepcionais para fazer a prova da sua validade. Portanto, o certificado digital é um documento eletrônico firmado digitalmente pela Autoridade Certificadora, que vincula uma chave pública a uma pessoa determinada, confirmando sua identidade. Tem o condão de unir a tecnologia com o Direito, deixando clara a possibilidade, em face do nosso ordenamento jurídico, de se legitimar o documento eletrônico como meio de prova.

2.2 - Quanto a segunda questão:

Deve-se observar a necessidade da garantia jurídica do vendedor de que está negociando com a pessoa certa bem como de eventuais exigências legais quanto à obrigatoriedade da presença da assinatura das partes. Um documento digital com assinatura digital deve ser aceito como se fora um documento escrito se atende as formalidades legais.

Um problema evidente que surge é o risco de o proprietário de uma chave privada perdê-la. Uma pessoa passaria a ter acesso a assinatura digital de outra. Há duas questões distintas: na primeira, o usuário comunica ao CA a perda da chave privada e pede seu conseqüente cancelamento; na segunda, não ocorre tal providência.

Entende-se que na primeira hipótese, o CA deverá proceder ao cancelamento da chave privada perdida e da chave pública associada. Surgirá, assim, para o CA a obrigatoriedade de manter uma lista de certificados revogados, contendo as chaves inválidas. Trata-se da proposta legal contida no modelo alemão. É claro que após tal comunicado, se o CA certificar uma operação que utilizou uma chave cancelada, sua responsabilidade será patente, estando o antigo proprietário da chave isento de qualquer responsabilidade.

Entende-se que na segunda hipótese que o ônus da prova desloca-se para o particular. E, mais, a situação ainda se complica quando se pensa na possibilidade da presença de um terceiro de boa-fé que poderia estar eventualmente envolvido. Há que prevalecer tal posição, pois, do contrário, a segurança jurídica estaria comprometida, visto que o certificado emitido pelo CA estaria sujeito a contestações judiciais, cabendo ao credor o ônus de provar que, embora tenha recebido a certificação de um CA, que aquele certificado corresponde a uma assinatura digital gerada por uma chave privada não desapropriada. Como "o Direito não socorre aqueles que dormem", cabe ao dono da chave privada, mantê-la a mais bem protegida possível e comunicar qualquer furto ou perda com a maior brevidade.

3 - A grande vantagem do contrato Eletrônico é que o documento em si, ainda pode ser alterado, sem deixar vestígios no meio físico, mesmo assinado digitalmente, mas se isto for feito, perderá o vínculo que mantém com a assinatura, perdendo todo seu valor probante, mas esta modificação seria em comum acordo entre as partes. Isto trouxe um aspecto prático na flexibilidade de mudanças do texto contratual, de onde partirá nova assinatura digital para reafirmar a mudança ocorrida.

Além disso, a assinatura digital pode ser remetida pela rede e verificada remotamente através de uma cópia da mesma. Essa característica não é válida para a assinatura tradicional.

4 - Um ponto que não se pode perder de vista é o aspecto internacional do comércio virtual, associado ao fato de que a Internet estar bastante difundida pelos mais variados países. Embora seja intuitivo que uma rede de computadores, espalhada por todo o mundo, ligada em tempo real, e a baixo custo, cria um ambiente global, ainda assim torna-se importante lembrar tal característica das redes amplas de computadores a fim de que sempre seja possível pensar em soluções propostas para o Direito Comercial Virtual em termos mais amplos possíveis. A legislação brasileira deveria então familiarizar-se com as nomenclaturas americanas que inevitavelmente deverão ser utilizadas, pois o mundo deve falar a mesma linguagem para se comunicar e se não acompanhar esta tendência o Brasil ficará novamente desatualizado com os países desenvolvidos. Isso se verifica até no momento de uma entrevista de emprego onde quem não tem fluência na língua inglesa está fora da concorrência.

5 - Ao final de toda esta discussão, mais uma vez nos leva a crer que surge a necessidade urgente de uma legislação específica, embasada principalmente na doutrina americana e alemã, onde possuem mais experiências práticas que nós, sendo o primeiro passo a aprovação de projetos que estão aguardando tantos anos o seu trâmite, sob pena de uma paralisação na economia do país que não acompanhar de forma rápida a evolução tecnológica mundial e a realidade do mundo virtual. A Medida Provisória 2.200-2, já foi um grande passo para garantir a autenticidade , a integridade e a validade jurídica de documentos em forma eletrônica e inegável a importância da OAB, secção São Paulo com o Projeto de Lei n 1589/99.

4 – BIBLIOGRAFIA

ASCENÇÃO, José de Oliveira. Direito da Internet e da sociedade da informação. Rio de Janeiro: Forense, 2002;

BLUM, Renato M. S. Opice (coordenador) e outros. Direito Eletrônico: A Internet e os Tribunais. Bauru,SP : EDIPRO , 2001;

BRASIL. MINISTÉRIO DA CIÊNCIA E DA TECNOLOGIA. Livro Verde da Sociedade da Informação no Brasil. Brasília: Ministério da Ciência e Tecnologia, 2000;

CASSEB, Paulo Adib. Democracia na Sociedade da Informação. Revista do Curso de Direito da UniFMU, São Paulo, UniFMU, v. 28, p.5-12, 2005;

CASTELLS, Manuel. A era da Informação: economia, sociedade e cultura. Volume I, a sociedade em rede. 5 ed., São Paulo: Paz e Terra, 2001;

CORRÊA, Gustavo Testa. Aspectos jurídicos da Internet. 2 ed. rev., São Paulo: Saraiva, 2002;

DEL NERO, Patrícia Aurélia. Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil. São Paulo: Atlas, 2000;

DE LUCCA, Newton. Aspectos jurídicos da contratação informática e telemática. São Paulo: Saraiva, 2003;

FINKELSTEIN, Maria Eugênia. Aspectos jurídicos do comércio eletrônico. Porto Alegre: Síntese, 2004;

GLANZ, Semy. Internet e Contrato Eletrônico, Revista dos Tribunais, volume nº 757, nov.1998;

LORENZETTI, R. L. Comercio Eletrónico. Buenos Aires: Abeledo Perrot, 2000;

LUCCA, Newton De e Simão Filho, Adalberto (coordenadores) e outros. Direito & Internet: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2º. Edição, 2005;

MARCACINI, Augusto Tavares Rosa. Direito e Informática: Uma abordagem jurídica sobre a criptografia. Rio de Janeiro: Forense,2002;

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

PAESANI, Liliana Minardi (coordenadora) e outros. O direito na Sociedade da Informação. 1. ed. São Paulo : Atlas, 2007;

PAESANI, Liliana Minardi Paesani. Direito de Informática: Atlas, 2000;

PAESANI, Liliana Minardi; BAPTISTA, Ézio Carlos S. A privacidade na Sociedade Sociedade da Informação: breves reflexões. Revista do Curso de Direito da UniFMU, São Paulo, UniFMU, v. 28, p. 13-24, 2005

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

Sites:

BRASIL, Angela Bittencourt. Assinatura digital . Jus Navigandi, Teresina, ano 4, n. 40, mar. 2000. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=1782;

ICP-BRASIL . Disponível em: <http://www.qualisoft.com.br/produtos/e-selo/e-selo.asp>;

E-SEC : Tecnologia em Segurança de Dados . Disponível em: <http://www.digitrust.com.br/ AssinaturaDigital.doc>;

ROHRMANN, Prof. Carlos Alberto. A Assinatura Digital. Disponível em: <http://www. direitodarede.com.br/ AssDg.html>;

ITAU. Disponível em: <www.itaubank.com.br/popups/ contratos_digitais /legislacao.asp>;

WIKIPEDIA. Disponível em: <http://pt.wikipedia.org/wiki/Orkut>;

.