Andréa Lira Ribeiro Pimenta

Segurança nos Contratos Internacionais de compra e venda na Internet: criptografia e assinatura digital

Monografia apresentada como requisito parcial para a conclusão do curso de bacharelado em Relações Internacionais do Centro Universitário de Brasília – UniCEUB.

Brasília – DF

2004

Andréa Lira Ribeiro Pimenta

Segurança nos Contratos Internacionais de compra e venda na Internet: criptografia e assinatura digital

Banca Examinadora:

Prof. Francisco Victor Bouissou
(Orientador)

Prof. Claudio Ferreira da Silva
(Membro)

Prof. Renato Zerbini Ribeiro Leão
(Membro)

Brasília – DF

2004

PIMENTA, Andréa Lira Ribeiro

Segurança nos contratos internacionais de compra e venda na Internet: criptografia e assinatura digital. Centro Universitário de Brasília – UniCEUB. Brasília, DF, Programa de Graduação em Relações Internacionais.Brasília, 2004..

Monografia: Graduação em Bacharel em Relações Internacionais.

59 p.

Orientador: Francisco Victor Bouissou .

1. História da Internet 2. Origem da criptografia 3.Comércio Eletrônico ou E-Commerce

I. Centro Universitário de Brasília – UniCEUB.

II. Título

AGRADECIMENTOS

Agradeço a Deus pelos momentos bons e ruins vividos nesses últimos quatro anos. Aos meus pais pela paciência, meu irmão pelo suporte nas horas difíceis, a minha família pelo apoio de sempre, ao Daniel pela extrema ajuda na elaboração deste trabalho, e o meu orientador Francisco Victor pela confiança depositada em mim.

RESUMO

Este trabalho tem como objetivo explicar a criação da Internet, suas formas de segurança onde é utilizada a criptografia e a assinatura digital. Assim como, a evolução dos contratos internacionais de compra e venda nos sites da Internet, como são celebrados, a lei aplicável que é utilizada nesse tipo de contrato.

ABSTRACT

This work as objectives to explain the creation of the InterNet, its forms os security where it is used the criptology and the digital signature. As well as, the evolution of international contracts of purchase and sites of sales of the InterNet, as are celebrated, the applicable law that is used in this type of contract.

LISTA DE SIGLAS

AC	Autoridade Certificadora
AR	Autoridade de Registro
ARPA	Advancced Research Projects Agengy
AUP	Acceptable Use Policy
CG	Comitê Gestor de Internet
DES	Data Encryption Standart
FAPESP	Fundação de Amparo e Pesquisa do Estado de São Paulo
FPGA	Field Programmable Gate Away
HD	Hard Drive (Disco Rigído)
HTML	Hyertexto
HTTP	Hyper Text Transfer Protocol
ICP	Infra Estrutura Chave Pública
IDEA	International Data Encryption Algorythm
IDS	Internet Detection System
IP	Internet Protocol
ITAR	International Traffic in Arms Registration
LNCC	Laboratório Nacional de Computaçao Cientifica
NCP	Network Control Protocol
NSF	National Science Foundation
ONG	Organizacao Não Governamental
ORA	Organizational Registration Authorities
PGP	Pretty Good Privacy
PSICA	Application Specific Inegrated Circuits

RNP	Rede Nacional de Pesquisas
RSA	Rivest, Shamin and Adleman
SET	Secure Eletronic Transactions
TCP / IP	Transfer Control Protocol / Internet Protocol
UFRJ	Universidade Federal do Rio de Janeiro
URL	Uniform Resource Protocol
VOL	Índice de Varejo on-line
WWW	World Wide Web

SUMÁRIO

INTRODUÇÃO

A Internet foi desenvolvida pelos militares americanos durante a Guerra Fria, com o objetivo de continuar se comunicando, mesmo que tivesse algum ataque nuclear. Antes de ser chamada de Internet, esta, teve outros nomes como ArpaNet e depois Arpa-Internet.

A Internet era utilizada no começo somente por militares, com o tempo a comunidade científica e universidades começaram também a ter acesso a rede, e algum tempo depois a sociedade tornou-se mais um membro à acessar a rede mundial de computadores.

Com a Internet veio a criação da *World Wide Web* para que documentos pudessem ser gerados a partir de uma tecnologia chamada Hipertexto (html), e com isso a possibilidade de qualquer usuário da Internet poder acessar o mesmo através do protocolo http (*Hipertext Transfer Protocol*).

A Internet chegou ao Brasil em 1995, pelo então Presidente Fernando Henrique Cardoso, antes esse acesso estava disponível somente para as universidades brasileiras ligadas às universidades americanas. Com a RNP (Rede Nacional de Pesquisa), houve a distribuição de redes nas principais capitais do país, para universidades e órgãos governamentais.

Com as privatizações ocorridas nos setor de telecomunicações, ficou decidido que empresas particulares seriam as responsáveis pelo acesso a Internet e o setor de telecomunicações ficaria responsável em dar a infra-estrutura e os recursos para se montar um provedor de acesso. No mesmo período houve a criação de um Comitê Gestor de Internet (CG), responsável pela rede mundial de computadores no Brasil.

A distribuição de domínios é de responsabilidade de cada país. No Brasil a responsável é a FAPESP, que institui o domínio BR para identificar as páginas brasileiras.

A Internet depois que passou a estar disponível a comunidade do mundo todo começou a ser fonte geradora de divisas, pois passou a comercializar produtos e serviços para seus usuários, tudo com comodidade e facilidade.

Para que um site possa estar disponível aos usuários, é necessário que exista uma política de uso aceitável, esta tem como objetivo dar segurança tanto a seus usuários quanto para os sites. Quando se aceita estas políticas ambos tem o dever de cumpri-las caso contrário poderá sofrer penalidades.

Com o avanço das tecnologias, hoje, consegue-se negociar contratos entre pessoas e sites ou entre empresas, mais para que isso ocorra sem Ter nenhum problema, é necessário que haja um nível de segurança bom para que as partes não possam ser prejudicadas, por uma invasão de *hackers* por exemplo. Alguns exemplos de segurança são: o uso de criptografia, assinaturas digitais, certificados digitais, *firewalls*, entre outros. Com todos esses métodos a serem utilizados dificilmente haverá algum problema durante a negociação.

As autoridades certificadoras são as responsáveis pela emissão de certificados digitais de chave pública, assim como renová-los, mantê-los atualizados, disponíveis para que as pessoas possam fazer eventuais consultas. As duas maiores empresas que emitem certificados digitais são a *VeriSign* e a *Thawte*, a *CertSing* é uma subsidiária da *VeriSign* no Brasil.

A criptografia existe desde o mundo romano, Júlio César foi o primeiro a usá-la, também foi muito utilizada na Segunda Guerra Mundial pêlos alemães, através da máquina *Enigma* . A criptografia é dividida em dois algoritmos: simétrica ou de chave privada e a assimétrica ou de chave pública. A criptografia de chave privada consiste na utilização de uma mesma chave para

codificar e descodificar uma mensagem. Os algoritmos mais utilizados na criptografia de chave simétrica são o DES e o IDEA. Na criptografia de chave pública são utilizadas as duas chaves pública e privada. Os algoritmos mais utilizados na criptografia assimétrica é o RSA e o *Diffie-Hellman*. A assinatura digital é feita através da criptografia assimétrica.

A segurança na criptografia depende do tamanho da chave e do algoritmo a ser utilizado. É aconselhável a utilização de chaves maiores que 1024 *bits*, pois quanto maior melhor será a segurança, pois é mais difícil de ser quebrada a não ser que se utilize um ataque de força bruta, fazendo com que demande tempo e dinheiro.

Com o avanço da Internet, surgiu o comércio eletrônico que é responsável pelo aumento nas vendas de produtos e bens de consumo em todo o mundo, por isso muitas empresas estão investindo no ambiente virtual. Apesar de ser um hábito recente o comércio eletrônico tem movimentado milhões só no mercado brasileiro.

Existem várias formas de pagamento de um produto ou serviço pela Internet, são eles: *digi-cash*, cheque eletrônico, cartões inteligentes e os mais utilizados no mundo todo, os cartões de crédito que são responsáveis por 90% do pagamento das compras via Web.

Para que o comércio eletrônico cresça mais ainda é necessário que as pessoas percam o medo de utilizar os cartões de crédito nas transações eletrônicas.

Um sub-item do comércio eletrônico são os contratos internacionais que podem ser celebrados entre empresas e usuários ou mesmo entre empresas. Quando se efetua um pedido de produto ou serviço em um site automaticamente está se realizando um contrato entre empresa e usuário.

Os contratos internacionais surgiram por causa das feiras italianas do século XI, dando origem a *Lex Mercatoria*. Algum tempo depois, veio a UNIDROIT (criada pela Liga das Nações), com o objetivo de criar regras de regulamentação de compra e venda de mercadorias, como não deu certo, foi criada a UNCITRAL (criada pela ONU), com o mesmo objetivo de criar normas universais dos contratos de compra e venda internacional. Com a UNCITRAL, veio a Convenção de Viena de 1980 sobre contratos de compra e venda internacional, onde seu objetivo principal é a proteção do comprador, permitindo que se possa realizar contratos entre pessoas em países diferentes.

Em muitos contratos internacionais de compra e venda na Internet vem sendo utilizada a Convenção de Viena de 1980, para solução de controvérsias já que não existe leis específicas sobre contratos internacionais via Internet.

Dentro da classificação dos contratos internacionais via Internet, existe os contratos de adesão, que consiste em clausulas pré-estabelecidas pelos *sites*, e que não há negociação entre as partes. A Amazon.com é um *site* de venda de livros, brinquedos, Cd's DVD's, programas de computador, entre outros. Quando se aceita a sua política de uso aceitável e seu termo de adesão automaticamente esta sendo celebrado um contrato de compra e venda. A partir do momento em que um produto é solicitado, deve-se cumprir com as obrigações que são explicitadas nos dois documentos, se uma das partes não cumprir, este sofrerá alguma penalidade que será julgada pela Associação de Arbitragem Americana, nos Estados Unidos.

CAPÍTULO I

1. A HISTÓRIA DA INTERNET

A Internet[1] surgiu nos Estados Unidos na década de 60, mais precisamente no ano de 1969, desenvolvida por militares americanos, com o objetivo de criar, proteger e dar segurança às informações em sua rede de comunicação de eventuais ataques nucleares, já que estavam no auge da Guerra Fria[2]. Os Estados Unidos usavam um Backbone[3] que passava por debaixo da terra, isso tornava mais difícil de ser interrompida a comunicação que ligava os militares a pesquisadores e organizações governamentais, sem ter que possuir um centro definido ou mesmo uma única rota para se ter acesso as informações. Essas conexões primeiramente ocorreram em quatro universidades dos Estados Unidos (Universidades da Califórnia em Los Angeles e Santa Barbara, Universidade de Utah e Instituto de Pesquisa de Stanford), essas instituições usavam um correio eletrônico para que houvesse a troca de informações estratégicas entre eles.

---

[1] Internet – É um conjunto de redes de computadores interligadas pelo mundo inteiro, que têm em comum um conjunto de protocolos e serviços, de forma que os usuários a ela conectados podem usufruir de serviços de informação e comunicação de alcance mundial. Guia Internet de conectividade (1999. p.13)

[2] Guerra Fria – Disputa pela hegemonia mundial entre as duas maiores super potências (Estados Unidos e União Soviética) após a Segunda Guerra Mundial (1939-1945), provocando assim uma corrida armamentista e tecnológica que se estendeu por 40 anos. O símbolo final da Guerra Fria é a queda do Muro de Berlim, em 1989, que separava a Alemanha Oriental da Ocidental. Almanaque Abril (1997. p. 417)

[3] Backbone – Estrutura central de uma rede composta por várias sub-redes. Linha (física) que é a base de conexão de alta velocidade dentro de uma rede, que, por sua vez, se conecta com linhas de menor velocidade. VIEIRA. (2003. p. 263). Atualmente os backbones são NFSNET nos Estados Unidos, EBONE na Europa. MURHAMMER, TCP/IP - Tutorial e técnico (2000. p. 4).

A Arpa[4] (Advanced Research Projects Agency), com a pressão constante de seus pesquisadores pela aquisição de computadores melhores e mais eficientes, sugeriu a esses pesquisadores que compartilhassem os computadores entre si, com isso a Arpa percebeu que poderia compartilhar e também conectar as máquinas, surgindo assim em 1969 um protótipo da rede chamada ArpaNet. Porém esse protótipo só começou a ser usado em 1972, por unidades militares e cerca de 20 universidades americanas. Com o passar do tempo, várias redes foram criadas, a ArpaNet foi desfeita, pois não atendia mais os requisitos de eficiência e segurança dos militares, e esses criaram uma rede privada chamada Milnet. Em 1983 houve a junção de novas redes entre elas a Csnet (para a comunidade científica) pertencente a *National Science Foundation* e a Bitnet (para comunidade não-científica) pertencente a IBM, essa rede ganhou o nome de Arpa-Internet e posteriormente passou a ser chamada somente de Internet.

Os pesquisadores da Arpanet fizeram estudos sobre a influência do crescimento da rede Arpanet nos seus usuários. Neste estudo foi constatado problemas com a velocidade de acesso, pois a mesma não foi alterada desde a implantação feita na época dos militares. Para solucionar este problema, foi necessária a mudança do protocolo utilizado (NCP[5] - *Network Control Protocol*) para o TCP/IP[6] (*Transfer Control Protocol/Internet Protocol*), propiciando uma maior escalabilidade e facilidade na implementação em diferentes hardwares[7].

Já se sabe que hoje com o crescimento contínuo da rede, está havendo a necessidade de novos endereços IP´s[8]. Deste modo a quantidade destes

---

[4] ARPA (Advanced Research Projects Agency) – Constitui um órgão dos Estados Unidos que tem por objetivo prover a segurança dos Estados Unidos.

[5] NCP (Network Control Protocol) – Foi o primeiro protocolo entre servidores, substituído pouco tempo depois pelo protocolo atual TCP/IP. MURHAMMER, TCP/IP – Tutorial e técnico (2000. p.4).

[6] TCP/IP (Transfer Control Protocol/Internet Protocol) - Família de protocolos que torna possível a comunicação de computadores de redes diferentes. VIEIRA**.** Os bastidores da Internet no Brasil (2003 p.267)

[7] Hardware – parte física dos computadores: CPU, monitor, teclado, circuitos. PEREIRA, Direito da Internet e Comércio Eletrônico (2001 p.476)

[8] IP (Internet Protocol) – é o protocolo responsável pela transferência de dados através da Internet. ANÔNIMO, Segurança máxima para linux (2000 p. 699).

IP's estão ficando escassos, por isso já está sendo usado em redes locais, ainda que em escala menor, mais já aceito na maioria dos sistemas operacionais, um padrão novo de endereços chamado Ipv6, possibilitando o endereçamento de um número muito maior de *hosts*[9].

Posição dos países por número de *hosts*

Posição	Pais	Hosts emJan/2003
1°	Estados Unidos	120 571 516
2°	Japão (.jp)	9 260 117
3°	Itália (.it)	3 864 315
4°	Canadá (.ca)	2 993 982
5°	Alemanha (.de)	2 891 407
6°	Reino Unido (.uk)	2 583 753
7°	Austrália (.au)	2 564 339
8°	Holanda (.nl)	2 415 286
9°	Brasil (.br)	2 237 527
10°	Taiwan (.tw)	2 170 233
11°	França (.fr)	2 157 628
12°	Espanha (.es)	1 694 601
13°	Suécia (.se)	1 209 266
14°	Dinamarca (.dk)	1 154 053
15°	Finlândia (.fi)	1 140 838
16°	México (.mx)	1 107 795
17°	Bélgica (.be)	1 052 706
18°	Polônia (.pl)	843 475
19°	Áustria (.at)	838 026
20°	Suíça (.ch)	723 243
21°	Noruega (.no)	589 621
22°	Argentina (.ar)	495 920
23°	Rússia (.ru)	477 380
24°	Nova Zelândia (.nz)	432 957
25°	Coréia (.kr)	407 318
26°	Hong Kong (.hk)	398 151

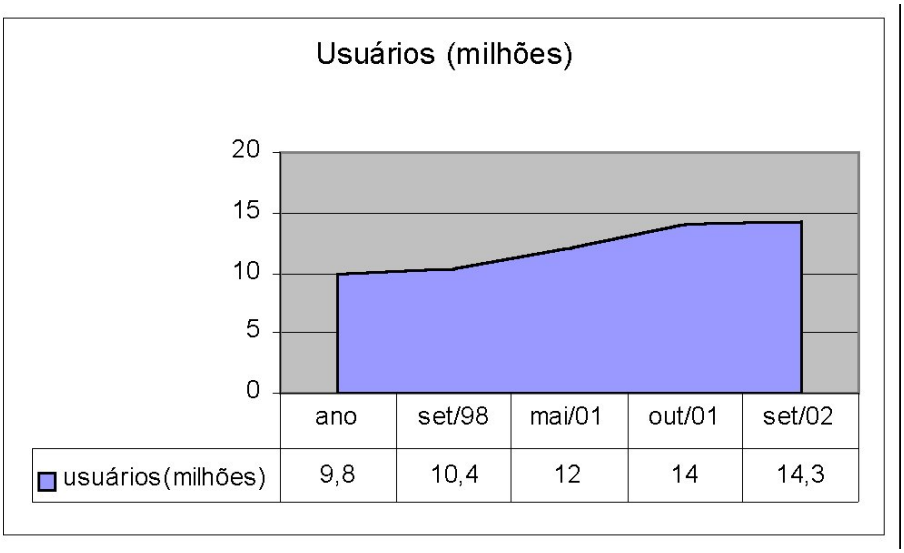
[9] Hosts – computador ligado a uma rede física. O tamanho de um host varia desde um computador pessoal até um supercomputador. Guia Internet de Conectividade (1999 p.133)

27°	Singapura (.sg)	338 349
28°	Portugal (.pt)	291 355
29°	Hungria (.hu)	254 462
30°	República Tcheca (.cz)	239 995

Fonte: Network Wizards, 2003

Com a eventual queda nos preços dos equipamentos além da facilidade dos *softwares*[10] para a navegação na rede, a Internet tornou-se acessível a uma quantidade crescente de usuários, caracterizando-a como a maior rede de computadores que temos acesso na atualidade. A Internet possui hoje uma variedade enorme de assuntos, pode-se encontrar e comprar de tudo desde livros até automóveis, tudo com a maior comodidade.

Evolução do número de usuários brasileiros



Fonte: Ibope eRatings

A fim de facilitar o acesso às informações disponíveis para os usuários da Internet, em 1990 um físico chamado Tim Berners-Lee criou a *World Wide*

[10] Software – É distribuído livremente, desde que seja mantido em seu formato original, sem modificações, e seja dado o devido crédito monetário ao seu autor. VIEIRA, Os Bastidores da Internet no Brasil (2003 p. 266)

Web[11] (www), esse espaço foi criado para armazenar as informações nos computadores através de documentos criados com uma tecnologia chamada hipertexto (html[12]) que permitia a ligação de textos e arquivos disponíveis na Internet de forma que seja possível visualizá-los de qualquer computador. Estes documentos são acessados através do protocolo http[13] (*Hipertext Transfer Protocol*), através de um endereço chamado URL[14] (*Uniform Resource Locator*), que é um identificador de hipertexto. Em meados de 1993, para que a Internet fosse vista além de uma tela preta e somente palavras escritas, foram desenvolvidos novas soluções tecnológicas (Modificações em especificações e *softwares*) que além de compartilhar textos e arquivos são capazes de gerar também imagens, sons e gráficos dando origem aos sites que conhecemos hoje.

1.1. A Chegada da Internet no Brasil

A Internet no Brasil chegou a sociedade brasileira por volta de 1995 no Governo do então Presidente Fernando Henrique Cardoso. Antes, a Internet era acessada somente por algumas universidades (UFRJ – Universidade Federal do Rio de Janeiro) e fundações de pesquisa (LNCC – Laboratório Nacional de Computação Científica) que tinham *links*[15] ligados a universidades americanas. O Governo Brasileiro, por meio do Ministério da Ciência e Tecnologia criou por volta de 1992 uma Rede Nacional de Pesquisa (RNP), que tinha o objetivo de criar e coordenar o oferecimento de serviços de acesso

[11] WWW – Baseada em hipertextos, é a interface gráfica da Internet que permite a navegação por arquivos através de hiperlinks e recursos multimídia. VIEIRA, Os Bastidores da Internet no Brasil (2003 p. 267)
[12] HTML é uma linguagem usada para criar documentos de hipertexto.
[13] HTTP (Hypertext Transfer Protocol) – É um protocolo projetado para permitir a transferência de documentos em HTML. MURHAMMER, TCP /IP – Tutorial e técnico (2000. p. 424)
[14] URL (Uniform Resource Locator) - Código para localização universal, que permite identificar e acessar um serviço na Web. VIEIRA, Os Bastidores da Internet no Brasil (2003 p.267)
[15] Link – Conexão que interliga computadores na rede. VIEIRA, Os Bastidores da Internet no Brasil (2003 p. 265).

a Internet no Brasil. Além disso, distribuiu para as principais capitais do país *backbones*, a partir de pontos de presença (POP – *Point of Presence*) que permitia o acesso a Internet em universidades, centros de pesquisa e órgãos governamentais.

Houve alguns impasses para saber quem seria o responsável em desenvolver a Internet brasileira. O Governo queria apoio dos Ministérios da Ciência e Tecnologia assim como o das Comunicações, e a Embratel queria explorar o novo mercado o que lhe daria o monopólio das telecomunicações e Internet. Como sabemos houve várias privatizações no governo de Fernando Henrique Cardoso e entre eles estava o setor de telecomunicações. Ficou decidido que somente empresas privadas é que poderiam fornecer o acesso à Internet, e que as operadoras poderiam fornecer somente a infra-estrutura e os recursos necessários para a montagem de um provedor de acesso.

Foi criado também nesse mesmo Governo um Comitê Gestor de Internet (CG), formados por representantes do Ministério das Comunicações, Ministério da Ciência e Tecnologia, Universidades, ONGS, e provedores de acesso[16], sendo de suma importância até hoje quando se trata da rede mundial de computadores. O comitê têm o objetivo de estabelecer as seguintes funções: estabelecer política de certificação e regras operacionais da autoridade certificadora, além de homologar, auditar e fiscalizar essas autoridades certificadoras.

O Governo Brasileiro editou uma Medida Provisória n° 2.200, de 24 de Agosto de 2001, estabelecendo os princípios para o uso de documentos eletrônicos e da criação da "Infra-Estrutura de Chaves Públicas Brasileiras – ICP-Brasil[17] , esse órgão tem o objetivo de reconhecer documentos eletrônicos e de dar-lhes legitimidade. O ICP-Brasil é um conjunto de técnicas, práticas e procedimentos elaborados para suportar um sistema criptográfico com base em

[16] Provedores de Acesso – são empresas comerciais que vendem à clientes o acesso para navegar na Internet. Almanaque Abril (1997 p. 488).
[17] LAWAND, Teoria geral dos contratos eletrônicos (2002 p. 64)

certificados digitais[18], ou seja, através do ICP-Brasil que poderá ser emitido assinaturas digitais, a partir da criptografia de chave pública. Este órgão será composto por um comitê gestor vinculado a Casa Cívil da Presidência da República, possuí onze membros, sendo quatro representantes da sociedade civil, e sete representantes de órgãos governamentais, entre esses órgãos estão, o Ministério da Justiça, Ministério da Fazenda, Ministério do Desenvolvimento, Indústria e Comércio Exterior, Ministério do Planejamento, Orçamento e Gestão e por último o Ministério da Ciência e Tecnologia[19].

Cada país possui um órgão ou entidade responsável pela distribuição de domínios[20] na Internet, estes podem ser institucionais ou geográficos, o primeiro consiste na identificação de instituições, e o segundo tem a função de identificar o país de origem da página. Aqui no Brasil a FAPESP (Fundação de Amparo a Pesquisa do Estado de São Paulo), é a responsável pela distribuição de domínios e endereços de redes cadastradas aqui no Brasil.

Ranking de Domínios

Domínio	Posição Fev/2003	Audiência fev/2003 (000)	Alcance fev/2003 (em %)	Audiência jan/2003 (000)	Audiência Dez/2002 (000)	Audiência Out/2002 (000)	Audiência jul/2002 (000)	Posição Jul/2002
Uol.com.br	1	4662	62,39	4927	4924	4972	4883	1
Ig.com.br	2	4601	61,58	4663	4734	4746	4666	2
Globo.com.br	3	3734	49,98	3807	3666	3825	4075	3
Terra.com.br	4	3441	46,05	3449	3597	3350	3149	6
Yahoo.com.br	5	3206	42,91	3194	3277	3402	3489	5
Bol.com.br	6	2485	33,26	2688	2680	2828	3565	4
msn.com	7	2436	32,60	2502	2407	2443	2483	7
Kit.net	8	2230	29,85	2553	2443	2068	-	-
Google.com	9	2183	29,21	2026	1989	1967	1850	11
Microsoft.com	10	1989	26,62	2034	1995	2499	2401	8

Fonte: Ibope eRatings/Nielsen/NetRatings

[18] http://www.certisign.com.br/companhia/icp_brasil.jsp. acessado em 07/06/04.
[19] LAWAND, Teoria geral dos contratos eletrônicos (2002 p. 65)
[20] Domínio – nome como determinada entidade ou computador é identificado pelo servidor de Internet (exemplo: em www.quidjuris.pt, o domínio é PT, pois esse domínio pertence a Portugal, BR pertence ao Brasil, UK, pertence a Inglaterra e assim por diante. PEREIRA, Direito da Internet e comércio eletrônico (2001 p.475).

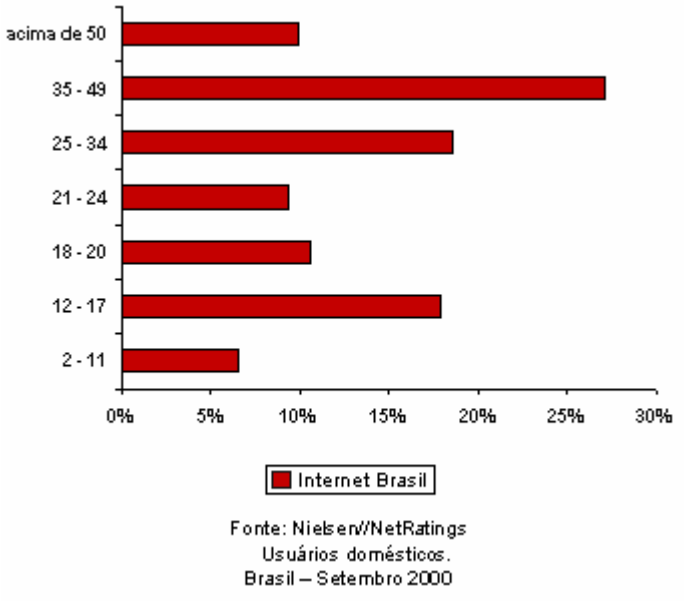
Percebe-se que a maioria dos domínios apresentados nessa tabela, são brasileiros e responsáveis pela formação de contas de acesso ao usuário da Internet, e os demais são domínios de sites especializados em *chats*[21] (msn.com*)*, de busca (google.com), e de informática (microsoft.com).

O Brasil possui 17,4 milhões de internautas[22] de idades variadas, e mais 6,6 milhões que acessam a Internet somente no trabalho, contabilizando 24 milhões de usuários que acessam a Internet. Dentro desse universo 10% são consumidores assíduos sendo que nos Estados Unidos está porcentagem chega aos 50%.[23]

[21] Chat – página que reúne usuários conectados simultaneamente no mesmo serviço para troca de mensagens em tempo real. Também conhecido como sala de "bate papo:. http://www.dicionarioecommerce.com. acessado em 07-06-04.

[22] Internautas – pessoa que navega (visita vários sites) na Internet. http://www.DICIONÁRIO E-COMMERCE.htm

[23] Cerca 80 a 85% dos pagamentos são feitos por cartão de crédito, 65% dos internautas que visitam uma loja não compram de imediato, apenas pesquisa preços, a maior parte dos compradores é formada por homens com idade entre 20 e 40 anos e integrantes das classes A e B, R$ 300 é o valor da compra. Este índice era de R$ 249 em Janeiro, o que representa um crescimento de 20,5%, 3,4 milhões de pessoas já compraram alguma coisa pela Internet, 2,1 milhões são consumidores assíduos, 1,3 milhão efetuaram apenas uma compra. Correio Braziliense (26-04-2004)



Fonte: Nielsen//NetRatings
Usuários domésticos.
Brasil – Setembro 2000

1.2. O Uso Comercial da Internet

Após virar um fenômeno mundial entre pesquisadores, organizações governamentais, militares e por último a sociedade civil, a Internet passou a ser vista como um grande potencial econômico. Dentre os serviços prestados atualmente estão: Provedores que oferecem hospedagem de conteúdo (páginas, aplicações), provedores de acesso, seus próprios sites[24] para prestação de serviços ou venda de produtos *on-line*[25].

Um exemplo de páginas bem sucedidas que faturam milhões durante o ano é a Americanas.com que está em primeiro lugar em lojas virtuais no Brasil, ela é responsável por 22% de todas as vendas realizadas pela Internet no país, em segundo lugar vêm a Submarino.com, que vendeu no ano passado cerca de R$ 211,6 milhões no ano de 2003, o Submarino é a única empresa de comércio eletrônico 100% pontocom[26] no Brasil.

[24] Sites – Servidor de informações acessado através de um endereço. Correio Braziliense (1996 p.21)
[25] On-line – conectado à Internet o que permite comunicação e transmissão de dados em tempo real. http://www.DICIONÁRIO E-COMMERCE.htm
[26] Correio Braziliense (26-04-2004)

As duas maiores do setor

Empresa	Faturamento	Fatia do mercado	Entrega/mês	Base de clientes
Americanas.com	R$ 267,6 milhões	22,3%	Não revela	1 milhão
Submarino	R$ 211,6 milhões	17,6%	100 mil	1,2 milhão

Fonte: Correio Braziliense (26-04--2004)

Tempo médio de navegação em residências

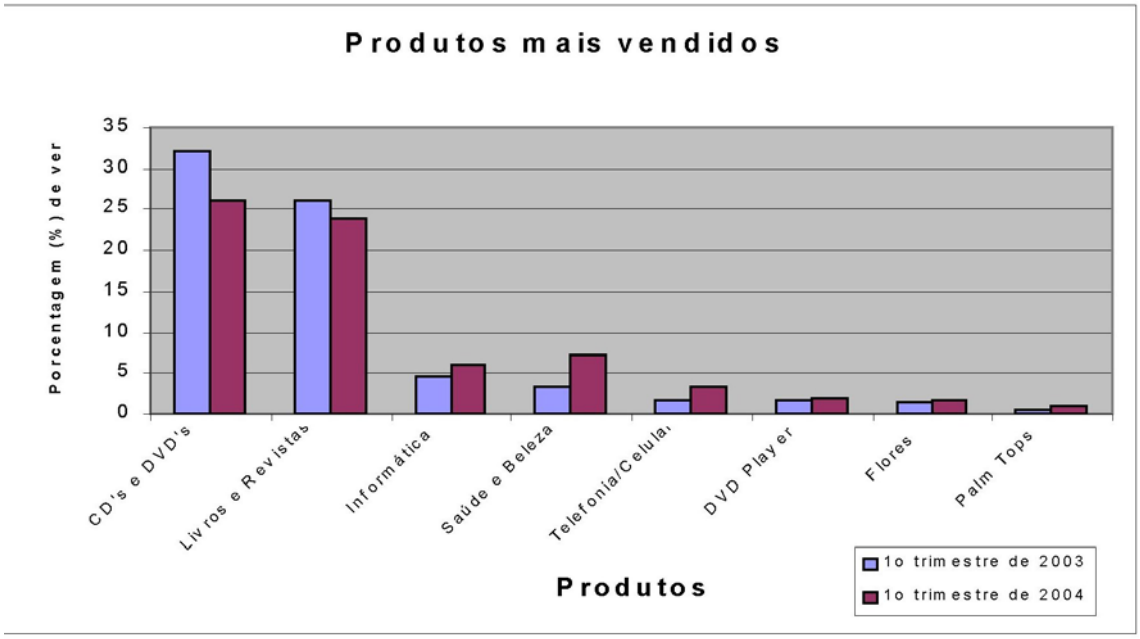
País	Horas de acesso por mês (jan/2003)
Hong Kong	16:12:45
Estados Unidos	13:17:47
Japão	12:25:50
Brasil	11:09:47
Alemanha	10:57:39
Suécia	10:48:55
França	10:37:20
Austrália	10:03:54
Espanha	09:47:27
Holanda	09:42:06

Reino Unido	08:52:41
Suíça	08:34:25
Itália	06:27:25

Fonte: Nielsen/NetRatings

A AUP (*Acceptable Use Policy* – política de uso aceitável), foi criada em 1992, com o objetivo de apoiar a pesquisa e a educação aberta, e não aceitava atividades que visavam lucro dentro do *backbone* NSFNET, porém este foi muito usado para transações comerciais. Por isso, em 1995 a AUP teve que mudar seus objetivos. Muitos provedores de acesso usam a AUP como uma forma de ter e prover segurança necessária a seus usuários, garantindo que as duas partes irão cumprir o que está escrito. O usuário a partir do momento que clica no “sim” na tela está sujeito à política de uso aceitável. .

Em 1994, a Internet ganhou mais uma função além da circulação de informações, ela começou a ser usada para a comercialização de produtos e serviços, seus primeiros produtos eram CD’s, Livros e programas de computador. Hoje em dia este perfil mudou, compra-se desde perfumes a geladeiras, isso mostra que os consumidores já estão mais confiantes para comprarem produtos que são caros utilizando cartão de crédito e boletos bancários.



Fonte: Correio Braziliense (26-04-2004)

Pela Internet circula diariamente vários tipos de informações e dados de diversas características, que vão desde trabalhos, lazer, operações bancárias e comerciais, a inúmeros contratos que são celebrados dentro da rede, e-mails pessoais ou até mesmo de negócios, são enviados de qualquer lugar do mundo ao outro extremo em questão de segundos, apenas com um *click*.

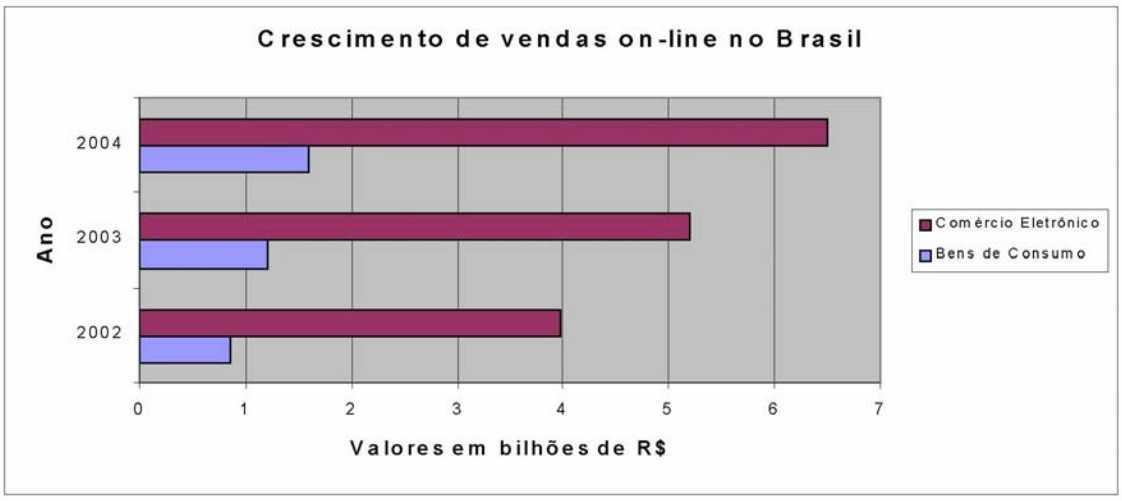
Quem oferece um produto ou serviço pela Internet, tem que ter a noção de que sua loja é acessível a todos os usuários do mundo, pois na Internet não há localização física e nem geográfica, basta somente ter computadores ligados a rede Internet para poder realizar negócios, pesquisar sobre determinado assunto, bate-papo, entre outras coisas. Sendo assim, o responsável pelo site precisa delimitar o seu público alvo, a fim de evitar transtornos aos seus usuários. Por exemplo, o site linuxmall.com.br entrega somente em território brasileiro, já a amazon.com ao contrário entrega em quase todo o mundo.

A Internet possui diversas vantagens tais como: conexão direta entre compradores e vendedores, apoio nas trocas de informações entre pessoas,

eliminação do tempo e lugar como foi dito no parágrafo anterior, capacidade de atualização imediata. A vantagem de se ter um comércio eletrônico são vários, entre eles pode se destacar, a redução de custos administrativos, prazo de distribuição curto, uma operação pode ser realizada em qualquer hora do dia ou da noite sem necessitar de um vendedor, entre outras.

O comércio eletrônico para o autor Alberto Luiz Albertin "é a realização de toda cadeia de valor dos processos de negócio num ambiente eletrônico, por meio de aplicação intensa de tecnologias de comunicação e de informação, atendendo aos objetivos de negócio"[27], ou seja, com o advento da revolução tecnológica da comunicação e da informação, tornou-se possível a realização de negócios dentro de um computador, em qualquer lugar, hora e principalmente com a segurança que o ambiente virtual proporciona.

O comércio eletrônico no Brasil cresceu cerca de 40,3% no ano de 2003, no ano de 2004 está projetado uma receita de R$ 6,5 bilhões, incluindo os negócios com automóveis e o setor de turismo. Isso se deve a duas explicações, a primeira é pelo chamado público-alvo, que são pessoas das classes A e B, e o segundo é que hoje têm uma média de 2,1 milhões de consumidores assíduos, e mais 10 milhões de consumidores que não compram com freqüência.



[27] LAWAND, Teoria geral dos contratos eletrônicos (2003 p. 32)

Fonte: Correio Braziliense (26-04-2004)

Desde o início da Internet, as tecnologias utilizadas vêm evoluindo, tornando possível a negociação de contratos entre empresas. Porém, este meio eletrônico, como em qualquer outro, possui inúmeras barreiras como problemas técnicos e até mesmo entidades e indivíduos de má fé, como por exemplo os hackers[28], que são os mais conhecidos por invadir sites realizando por exemplo transações bancárias com as senhas conseguidas através de vários métodos de invasão de sistema ou mesmo somente por diversão bagunçando todo o site de modo que ele fique algum tempo fora do ar, causando transtorno tanto para a empresa, quanto para os seus usuários. Assim, para que tais contratos sejam celebrados por meio eletrônico, via Internet, são necessárias tecnologias para que todas as partes envolvidas nestas negociações tenham um nível de segurança aceitável para a finalização dos negócios.

Para prover esta infra-estrutura, foram criados vários procedimentos e tecnologias, como comunicação segura através de canais de comunicação criptografado[29], assinaturas digitais[30], utilização de mecanismos de defesa dos sites comerciais como filtros de pacotes (*Firewalls*[31]), filtros de aplicativos

[28] Hackers - indivíduo que entra e utiliza os recursos protegidos da Internet, sem para tal estar autorizado, contudo não os altera, apaga ou introduz informações distintas. PEREIRA, Direito da Internet e comércio eletrônico (2001 p.476).

[29] Criptografia – processo de mistura de dados, para evitar que pessoas não autorizadas leiam as informações. PEREIRA (2001 p.474)

[30] Assinatura Digital - a assinatura digital não deve ser confundida com a imagem digitalizada de uma assinatura manual. É, na verdade, uma sequência de *bits* que foi gerada mediante uma função matemática unidirecional aplicada ao documento, com o uso de uma chave privada que é única e exclusiva do usuário. A sequência de *bits* que forma a assinatura digital só poderia ter sido gerada por aquele que detém a chave privada, o que permite atribuir-lhe a mesma exclusividade da assinatura manuscrita. MARCACINI, Direito e Informática – uma abordagem jurídica sobre a criptografia (2002 p. 185)

[31] Firewall – barreira de segurança baseada em hardware e software que protege a rede corporativa contra acessos externos não autorizados. É o ponto de conexão da rede com o mundo externo – tudo o que chega passa pelo

(*Proxys*[32]), IDS[33] (*Internet Detection System*), *Blowfish*[34], redes isoladas, utilização de senhas de identificação, todos esses procedimentos são para garantir a segurança tanto do site quanto dos seus usuários, evitando que algo aconteça e prejudique ambos.

Para contratos internacionais, as tecnologias mais utilizada são a assinatura digital e a criptografia, pois esses dois mecanismos de segurança permitem que o contrato não seja violado por outros, e somente as partes interessadas é que podem acessá-los e modifica-los a qualquer momento, a fim de torná-lo bom para ambas as partes. Para a comprovação das entidades participantes do contrato, é necessário a intermediação de uma entidade certificadora (Ex.: *VeriSign*, *Thawte*, *CertSign*), entre outras.

1.3 – Autoridades Certificadoras e Certificados Digitais

---

firewall, que decide o que pode ou não entrar, dependendo do nível de segurança criado pela entidade. PEREIRA (2001 p.476)

[32] Proxy – Em português, significa procuração. Um servidor proxy recebe pedidos de computadores ligados à sua rede e, caso necessário, efetua os pedidos ao exterior dessa rede usando como identificação o seu próprio número IP, e não o IP do computador que requisitou o serviço. http://www.DICIONÁRIO E-COMMERCE.htm

[33] IDS – é capaz de detectar diversos ataques e intrusões, auxilia na proteção do ambiente. Um IDS trabalha como uma câmera ou um alarme contra as intrusões, podendo realizar a detecção com base em algum tipo de conhecimento, como assinaturas de ataques, ou em desvios de comportamentos. O IDS é capaz de detectar e alertar os administradores quanto a possíveis ataques ou comportamentos anormais na organização. NAKAMURA & GEUS, Segurança de redes em ambientes cooperativos (2003, p. 251 e 253)

[34] Blowfish – é um esquema de criptografia de 64 bits desenvolvido por Bruce Schneier. Blowfish é frequentemente utilizado para criptografia de alto volume e alta velocidade. ANÔNIMO, Segurança máxima para linux. (2000 p. 687).

As autoridades certificadoras são as responsáveis pela emissão dos certificados digitais[35] de chave pública, esses certificados possuem vários níveis de segurança, e seus termos de adesão são bastante rígidos. Um certificado digital possui prazo de validade que pode ser renovado sempre que necessário.

É importante ressaltar que uma autoridade certificadora possui também como tarefa principal, receber a revogação da chave e dar-lhe publicidade, ou seja, é importante a divulgação *on-line* das chaves públicas certificadas, para que terceiros confiram se esta chave é valida e eficaz.

Existe três tipos de modelo de confiança das autoridades certificadoras, são elas: Modelo de autoridade central, onde essa autoridade certificadora é única e exclusiva; Modelo de autoridade hierárquica, na qual uma cadeia de autoridade emite certificados para as outras autoridades que estão no nível inferior da cadeia e assim por diante, e o Modelo *Web of Trust*, no qual a responsabilidade da confiança está no próprio usuário.

Um certificado digital, nada mais é do que a chave pública assinada digitalmente por uma autoridade certificadora confiável. A autoridade certificadora, os usuários, o sistema e seus certificados digitais são necessários para dar identificação, autenticação e acesso seguro aos sistemas.

Num certificado digital, além de possuir uma assinatura digital, inclui outras informações que determinam o nível de confiança do certificado. São elas: Nome, endereço e empresa do solicitante; Chave pública do solicitante; Validade do certificado; Nome e endereço da autoridade certificadora; e, Política de utilização (limites de transação, especificação de produtos, etc.).

[35] Certificado Digital – é um arquivo que liga uma identidade à chave pública associada. Esta ligação é validada por um terceiro participante confiável, o CA (*Certification Authority* – certificado de autoridade). Um certificado digital é assinado com a chave privada do certificado de autoridade, para poder ser autenticado. Ele é apenas emitido após uma verificação do requerente. MURHAMMER, TCP/IP – Tutorial e técnico (2000 p.271)

As duas maiores autoridades certificadoras do mundo são, a *Verisign* e a *Thawte*, primeiro e segundo lugar respectivamente. A *CertiSign* é a líder no mercado brasileiro de emissão de certificados digitais, a *CertiSign* é a única afiliada brasileira da *VeriSign*.

A *VeriSign* é a líder mundial na emissão de certificados digitais, além de prestar serviços de confiança no que tange a identificação, autenticação, validade e pagamento na Internet. A *VeriSign* permite que pessoas físicas e jurídicas de qualquer lugar do mundo comuniquem-se, troquem informações, realizem transações e comercializem na Internet com muita segurança.

Cerca de um milhão de *sites* usam o certificado digital assinado pela *VeriSign*, e mais de 10 milhões de pessoas físicas utilizam e-mails das empresas em que trabalham certificados pela *VeriSign*.

A *Thawte* foi criada em 1995, por um empresário chamado Mark Shuttleworth, para assessorar os negócios comerciais sul africanos, no que diz respeito a segurança na Internet. Em 1996, a *Thawte* se especializou em vender certificados SSL público fora dos Estados Unidos. A partir de 2000, a *Thawte* passou a pertencer a *VeriSign*, então a sua política de privacidade é a mesma da VeriSign.

A *CertiSign* foi criada em 1996, com o objetivo de emitir certificados digitais de projetos existentes no Brasil. Hoje, 98% dos certificados digitais emitidos no Brasil são da *CertiSign.* Desde 1999, a *CertiSign* vem usando a tecnologia de emissão de certificados digitais da *VeriSign*.

A *CertiSign* está credenciada pela ICP- Brasil para validar e emitir certificados digitais de todos os tipos, atuando como autoridade certificadora (AC) e autoridade de registro (AR), para as mais diferentes organizações brasileiras.

CAPÍTULO II

2. ORIGEM DA CRIPTOGRAFIA

A palavra Criptografia vem do grego que significa *Krypto* (oculto) e Graphia (escrita), então criptografia é ciência de manter dados e comunicações seguros. A criptografia tem como o objetivo criar mensagens que somente pessoas autorizadas consigam ter acesso, protegendo-as contra terceiros o seu significado. Na época dos romanos, os mensageiros utilizavam uma cifra de substituição, para que as mensagens somente fossem lidas pelos destinatários. Júlio César caracterizou essa cifra da seguinte forma: ele convertia o alfabeto em três posições a frente, assim a letra A tornava-se C, a letra B tornava-se D, e assim sucessivamente.

A criptografia continua com o mesmo objetivo de antigamente, porém com métodos diferentes de criptografar. Esses métodos foram muito usados na estratégia militar, pois havia a necessidade de se mandar mensagens às tropas que estavam em combate, mas que se caso caíssem nas mãos dos inimigos, estes não conseguiriam descobrir o que estava escrito. Paralelamente a isso verificou-se um grande desenvolvimento da "criptoanálise que é a arte de se quebrar o código e decifrar a mensagem alheia."[36]

A criptografia durante a Primeira Guerra Mundial não foi muito usada, pois era escrita a mão tornando-a trabalhosa de se fazer, além de ocupar muito tempo, então somente as mensagens mais importantes é que eram criptografadas. Porém durante a Segunda Guerra Mundial, houve um aumento considerável no uso de mensagens criptografadas pôr meio de máquinas, por sua vez muitos funcionários do serviço de inteligência fizeram uso da criptoanálise para decifrar as mensagens inimigas.

[36] MARCACINI, Direito e Informática – uma abordagem jurídica sobre a criptografia (2002 p.10)

Os alemães durante a Segunda Guerra Mundial, criptografavam suas mensagens através de uma máquina chamada *Enigma*[37] (software de codificação), isso levou a uma vantagem militar nazista no início da guerra, porém esse sistema foi quebrado pelos britânicos e acabou sendo de extrema importância para a vitória dos aliados. Depois da guerra essas máquinas foram apreendidas pelos EUA, e este as vendeu para países do chamado terceiro mundo, sem mencionar que seus códigos já haviam sido quebrados.

Com os computadores se desenvolvendo de maneira muito rápida ficou mais fácil criptografar mensagens e também decifra-lás, isso porque o computador consegue realizar cálculos muito complexos que um ser humano levaria anos para obter o resultado. Além disso, o computador trouxe grandes avanços à criptografia devido ao emprego de números binários[38], então, esse conjunto de números forma uma palavra, um texto, uma imagem, etc..

A criptografia hoje é usada não somente pelos militares, mais por toda sociedade, como por exemplo, ao acessar um site de banco, ao digitar a sua senha, o computador lança uma seqüência de números em que está inserida a senha, ou TV a cabo, codifica o seu sinal, para que somente os assinantes tenham acesso, para isso eles oferecem aparelhos decodificadores, todos esses processos em que se usa a criptografia servem para oferecer uma maior segurança a seus usuários e garantir que não serão usados por terceiros não autorizados.

Em algumas páginas da Internet em que se exige uma senha para se ter acesso, ou as que pedem dados pessoais, como por exemplo um número de cartão de crédito ou no próprio *webmail*[39] são usadas funções criptográficas

---

[37] MARCACINI, Direito e Informática – uma abordagem jurídica sobre a criptografia (2002 p.11)

[38] Números Binários ou Base Binária – Os computadores trabalham com base binária. Nesta, temos apenas dois algoritmos”0”e “1”, que significa “ligado” e “desligado”. MARCACINI, Direito e Informática – uma abordagem jurídica sobre a criptografia (2002 p186)

[39] Webmail – A palavra nasce da fusão de “World Wide Web” com “E-mail”. Trata-se de uma forma de utilização do correio eletrônico em que o envio e leitura de mensagens, dentre outras possíveis funções, é realizado no

dentro do programa navegador, esses utilizam chaves públicas e privadas. Isso tudo está visível para o usuário quando ao olhar no canto abaixo à direita da tela, perceberá um cadeado fechado, isso lhe garante que a página que está sendo acessada é segura e em cima da página mostra o endereço “https”, esse protocolo permite estabelecer uma comunicação segura com o servidor e também permite a sua identificação. O servidor envia a sua chave pública ao programa de navegador em que o usuário está conectado, criptografando assim as informações que são dadas naquele momento, de modo que não possa ser interceptado no meio do caminho.

Em alguns países existem leis que proíbem a distribuição de produtos criptográficos, um deles é os Estados Unidos que até 2000 proibia a exportação de soluções para criptografia além de outros produtos, através da lei *ITAR* (*International Traffic in Arms Regulation*)[40]. Também tentou-se estabelecer restrições da criptografia dentro dos Estados Unidos, porém sem sucesso, porque houve várias manifestações da comunidade contra essa lei.
Outro país que estabeleceu regras rígidas para o uso interno da criptografia foi a França. Até 1996, a criptografia estava sendo utilizada somente para a autenticação de documentos ou assegurar a integridade das mensagens transmitidas. A Rússia é outro país que, em 1995, proibiu o uso, o desenvolvimento e a produção de criptografia sem a prévia autorização da FAPSI, sucessora da KGB[41].

---

ambiente da World Wide Web. Ou seja, dispensa-se o uso de um software específico de correio eletrônico e sua correspondente configuração, na medida em que o acesso é feito por meio de uma página da WWW, com o uso do programa de navegação (browser). Assim, é facilitado ao usuário acessar sua caixa postal a partir de qualquer computador ligado à ele. MARCACINI, Direito e Informática – uma abordagem jurídica sobre a criptografia (2002 p192)

[40] MARCACINI, Direito e Informática – uma abordagem jurídica sobre a criptografia (2002 p13)

[41] KGB – Também conhecida dentro da ex-URSS como “Comitê de Segurança do Estado”, antes de ser conhecida por esse nome, teve três outros nomes Comissão Extraordinária, OGPU, NKVD (Comissariado do Povo dos Assuntos Internos). A KGB era responsável pela execução dos contra-revolucionários mais perigosos sem toda morosidade jurídica, dentro dos princípios da Revolução de Outubro. A KGB tivera sempre como missão fundamental a defesa do socialismo, da União Soviética e do Partido Comunista, dos

O software mais usado hoje em dia para a criptografia é o chamado PGP (*Pretty Good Privacy*) ou privacidade muito boa, ele é produzido pela *Network Associates Inc*. NAI. Em 1991, seu criador disponibilizou o programa e seu código fonte na Internet para que fosse acessado por qualquer usuário da rede mundial de computadores, afim de adquirirem a mais moderna tecnologia de criptografia, por meio da utilização no ambiente DOS, em 1997, o mesmo criador do PGP, lançou um software para o ambiente Windows.

O PGP, cifra as mensagens combinando o uso da criptografia simétrica e da criptografia assimétrica, ocorre da seguinte maneira: a mensagem é cifrada normalmente utilizando uma chave que foi gerada pelo programa que será utilizada uma única vez, em seguida essa chave é cifrada pela chave pública do destinatário, assim a mensagem que vai ser enviada fica composta por dois blocos, o primeiro fica com a mensagem cifrada convencionalmente e o segundo com a chave secreta do primeiro bloco que foi gerada pelo uso da criptografia assimétrica do destinatário.

Apesar de ser segura, o PGP já registrou falha em sua implementação. Por ter seu código fonte acessível a qualquer um, sendo que os hackers e a comunidade científica são os que mais acessam com a intenção de descobrir falhas e depois demonstrar como foi descoberta. Um cientista descobriu uma falha disponível em todas as versões posteriores do aplicativo que o cientista utilizou, logo em seguida a PGP consertou e a disponibilizou as correções em seu *site*.

Existem dois tipos de criptografia: simétrica, cuja principal característica é a rapidez na execução, e a desvantagem está na distribuição que não é

---

operários e camponeses não apenas da URSS, mas também de todo o mundo, ideal consagrado em seu símbolo, a espada e o escudo. Embora muitas vezes pintada com todos os tridentes e chifres, a KGB não foi uma “agência de terror e tortura”, foi sim uma arma de defesa do proletariado contra os contra-revolucionários e inimigos do povo, nacionais e estrangeiros, bem como uma força adicional de segurança. http://www.apaginavermelha.hpg.ig.com.br/kgbhist.htm

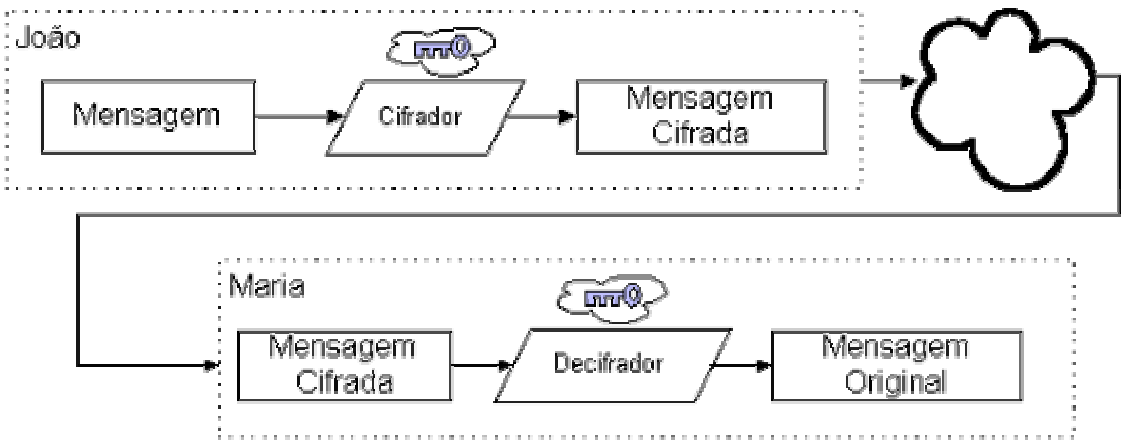
segura e no seu gerenciamento, e a criptografia assimétrica que é mais segura do que a simétrica, porém possui problemas de desempenho, pois exige maior poder de processamento.

Os processos criptográficos são usados somente para proteger os dados inseridos de modo que as informações pessoais do usuário não possam ser interceptadas e lidas por uma pessoa não autorizada.

2.1. Criptografia Simétrica ou Criptografia Convencional ou Criptografia de Chave Privada

A criptografia de chave privada ou simétrica consiste na utilização de uma mesma senha ou chave para codificar e descodificar uma mensagem, porém é necessário conhecer esta chave, mas esta deve ser mantida em sigilo para que a integridade da comunicação seja assegurada.

Criptografia de Chave Privada ou Simétrica



Fonte: Segurança de redes em ambientes cooperativos, NAKAMURA & GEUS (2003 p. 289)

Para conferirmos segurança à mensagem a ser criptografada é necessário que se crie um sistema capaz de criar um número enorme de senhas, para que qualquer pessoa que queira ter acesso a mensagem não

consiga acessá-la. O tamanho da segurança depende do grau de importância da mensagem. Por exemplo, se o emissor e o receptor querem proteger sua mensagem por uma semana, eles deverão utilizar um sistema de criptografia que resista aos ataques de hackers ou similares durante uma semana, já uma mensagem que nunca poderá se ter acesso exigirá um outro tipo de sistema criptográfico. Para que isso aconteça utiliza-se um sistema criptográfico proveniente de fórmulas matemáticas complexas ou também chamada de algoritmos[42].

A criptografia de chave privada possui algumas limitações quanto à sua segurança, pois ela garante segurança aos usuários que estão trocando mensagens entre si de pessoas não autorizadas que queiram ler a mensagem, pois ambos já decidiram qual senha irão usar. Outra limitação é que na criptografia simétrica não permite demonstrar para outra pessoa que a mensagem foi enviada pelo emissor, isso porque o próprio receptor pode encriptar a mensagem já que ele também sabe qual é a senha. Logo, conclui-se que não se pode criar assinaturas digitais na criptografia simétrica.

Existem dois algoritmos mais utilizados na criptografia simétrica são eles o DES (*Data Encryption Standard* – padrão de criptografia de dados), que foi criado pela IBM com o objetivo de produzir o texto cifrado do mesmo tamanho do original e o algoritmo de decifração sendo do mesmo tamanho da criptografia e o IDEA (*International Data Encryption Algorythm* – algoritmo de criptografia de dados internacionais), este foi desenvolvido na década de 90, com a função de substituir o algoritmo DES, apesar dessa nova solução, o DES continua sendo mais utilizado, pois o IDEA é muito recente, além de não ter sido testado adequadamente.

---

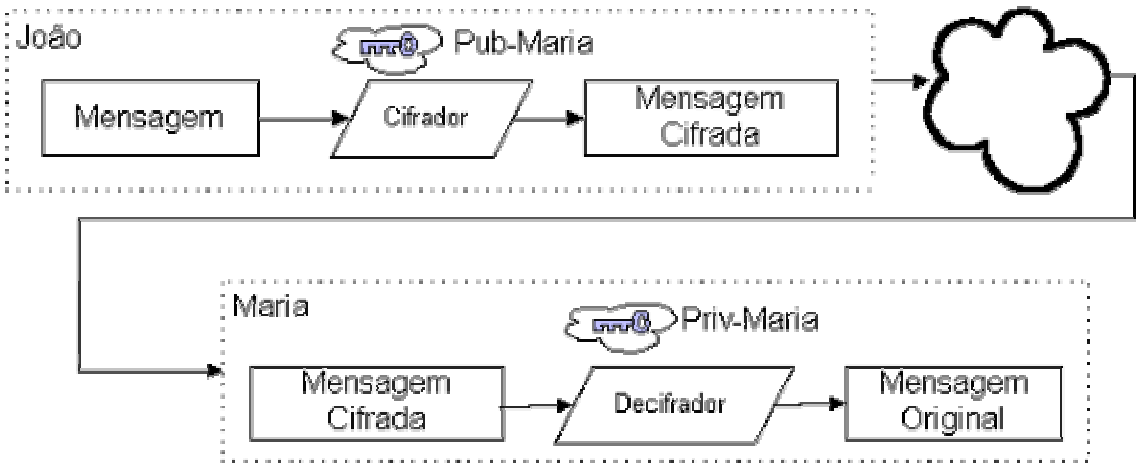
[42] Algoritmos – é uma sequência finita de instruções ou operações básicas (operações definidas sem ambiguidade e executáveis em tempo finito dispondo-se apenas de lápis e papel) cuja execução, em tempo finito, resolve um problema computacional, qualquer que seja a instância. A ordenação da sequência de instruções do algoritmo apoia-se na estratégia estabelecida durante a análise do problema. O desenvolvimento do algoritmo não pode perder de vista os tipos de dados considerados e a sua representação. SALVETTI & BARBOSA, Algoritmo (1998 p. 10)

2.2. Criptografia Assimétrica ou Criptografia de Chave Pública

Na criptografia assimétrica são utilizadas duas chaves: pública e privada, estas chaves são números que tem por objetivo complementar uma a outra, e que não podem ser escolhidas pelos usuários somente por computadores. A criptografia de chave pública é importante, pois possibilita a privacidade e a integridade das informações, além de autenticação das partes envolvidas.

Uma mensagem que foi encriptada por uma chave pública, só poderá ser decriptada por uma chave privada e o contrário também pode ocorrer, mensagem encriptada por uma chave privada só poderá ser decriptada pela chave pública correspondente. A criptografia assimétrica permite, proteger a integridade da seqüência de bits, fazendo com que esse não possa ser alterado.

Criptografia Assimétrica ou Criptografia de Chave Pública



Fonte: Segurança de redes em ambientes cooperativos, NAKAMURA & GEUS (2003 p. 290)

Existem dois algoritmos que são os mais usados na criptografia assimétrica que são o RSA (*Rivest, Shamir and Adleman*) e o *Diffie-Hellman*. O primeiro está baseado na dificuldade de se encontrar fatores primos de um grande número inteiro, e o segundo está baseado na dificuldade de se computar pequenos logaritmos gerados por grandes números primos. Por

esses códigos já terem sido estudados por vários cientistas, fica provado que ambos são confiáveis e seguros.

Se utilizarmos uma mesma chave para encriptar e decriptar uma mensagem, esta irá originar uma outra mensagem totalmente diferente da original, pois na criptografia assimétrica utiliza-se funções matemáticas que não tem retorno, ou seja, não existe operação inversa. Além disso, a criptografia assimétrica exige cálculos mais complexos do que na criptografia simétrica, de modo que a fórmula e escolha dos pares de chaves só podem ser feitos a partir desses cálculos.

É comum que a chave pública de uma pessoa esteja disponível para os usuários da Internet fazerem *download*,[43] enquanto que a chave privada só o dono é que pode ter acesso a ela. Para uma pessoa mandar uma mensagem cifrada a outra, esta poderá baixar em seu computador a chave pública da pessoa que se quer mandar a mensagem, então com a chave pública ele cifra a mensagem e a manda, o receptor então com a sua chave privada decodificará a mensagem e assim poderá acessá-la, esse processo garante que somente o emissor e o receptor é que terão acesso à mensagem eletrônica, protegendo-a de outras pessoas.

No Brasil existe um órgão denominado ICP- Brasil (Infra-Estrutura de Chaves Públicas Brasileiras), este é responsável pela regulação das empresas de certificação digital, e também pelo licenciamento de empresas para tornarem-se autoridades certificadoras,

[43] Download – significa “baixar” um arquivo armazenado em um computador remoto para o próprio computador. Isto é, copiar para o nosso computador um arquivo que se encontra em algum outro computador que acessamos pela Internet. MARCACINI, Direito e Informática – uma abordagem jurídica sobre a criptografia (2002 p.188)

2.3. Assinatura Digital

A assinatura digital não deve ser confundida com uma assinatura manual digitalizada, que nada mais é do que uma assinatura em papel que foi digitalizada em uma imagem no computador , ou seja, à assinatura digital é diferente de uma assinatura escrita[44], a assinatura digital se adapta com perfeição à todas as funções que podem ser atribuídas a uma assinatura manual, permitindo assim, identificar à autoria de um documento eletrônico. Outro erro que as pessoas cometem é confundir à assinatura digital com senha de acesso. Uma senha de acesso serve para acessar sistemas diferentes, por exemplo, provedores de acesso, e-mail, Intranet[45], entre outros.

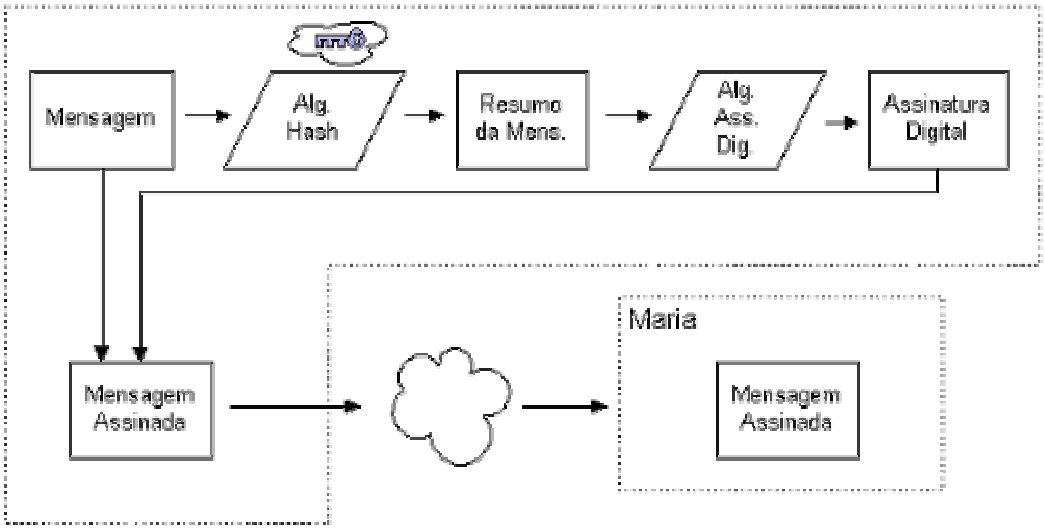
A assinatura digital é o resultado de uma operação matemática, utilizando algoritmos de criptografia assimétrica. Ela é produzida através de mensagem cifrada com a chave privada do emitente, o que permite que somente com a chave pública deste remetente seja possível abrir a mensagem. Assim qualquer pessoa pode ter acesso à assinatura e ao documento já que a chave pública pode ser repassada a qualquer interessado. Esse sistema de assinatura digital pode ser usado não só em textos, mas também em planilhas, arquivos executáveis, imagens, sons, vídeos e qualquer outro tipo de arquivo eletrônico, com o objetivo de proteger e autenticar qualquer um deles.

---

[44] Assinatura Escrita – é uma forma de expressar a vontade, em última análise, este significado simbólico decorre do fato de que a assinatura, é como um sinal único e exclusivo de uma dada pessoa, e permite identificar quem está preferindo aquela manifestação. MARCACINI, Direito e Informática – uma abordagem jurídica sobre a criptografia (2002 p. 83)

[45] Intranet – o conceito é o mesmo da Internet, mas o acesso não é aberto, ou seja, apenas pessoas autorizadas podem acessar uma Intranet. Normalmente, é usada por empresas ou instituições para comunicação entre os funcionários. http://www.dicionarioe-commerce.htm.

Processo de Assinatura Digital



Fonte: Segurança de redes em ambientes cooperativos, NAKAMURA & GEUS (2003 p. 291)

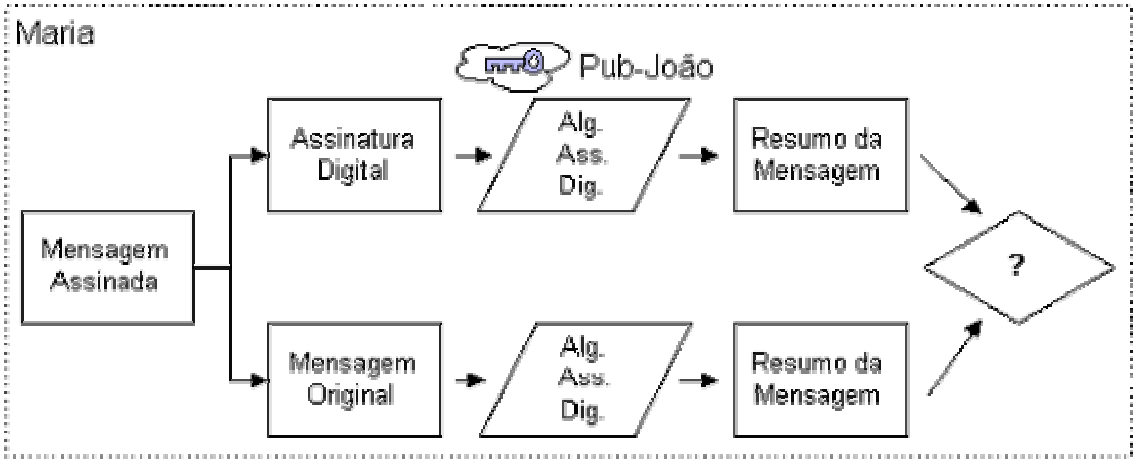
Quando uma assinatura digital é criada, o programa não aplica simplesmente a função de criptografia com chave pública (assimétrica) no documento, pois isto exigiria computadores muito sofisticados e chaves muito grandes, muitas vezes maior que a mensagem. Na verdade, é executada uma função digestora[46] no arquivo que disponibiliza um "resumo", e este resumo sim é assinado digitalmente.

Através do resumo da mensagem que é criptografado com a chave privada do emitente e da chave pública do destinatário é que dará origem a assinatura digital, com isso o documento ficará seguro contra pessoas não autorizadas. Para saber se realmente foi o destinatário que mandou a mensagem, é necessário que o resumo da mensagem seja igual aos caracteres decifrado da assinatura digital, isso provará que mensagem não foi modificada depois que se colocou a assinatura digital.

[46] Função Digestora – expressão em português para *Hash Function.* MARCACINI, Direito e Informática – uma abordagem jurídica sobre a criptografia (2002, p. 190)

A *hash function*[47] produz um número de controle geralmente de 128 *bits*[48], representado por um número de 39 casas decimais, fazendo com que seja impossível existir duas ou mais mensagens com mesmo número controle. Porém se alterarmos, por menor que seja o texto, isso alterará o número do controle do resultado final, alterando também a mensagem final.

Processo de Verificação de Assinatura Digital



Fonte: Segurança de redes em ambientes cooperativos, NAKAMURA & GEUS (2003 p. 292)

Quando é feita uma assinatura digital, e esta é vinculada a um documento, esta assinatura só será válida para tal documento, ou seja, para

[47] Hash Function - Função matemática sem retorno que, aplicada sobre arquivos eletrônicos de qualquer natureza ou tamanho, produz como resultado um número de tamanho sempre fixo, estatisticamente único, e diferente diante da menor alteração do arquivo. Com estas características, o número resultante da aplicação da *hash function* pode ser considerado um "resumo" do arquivo passado por esta função, representando- o. Por isso, as assinaturas digitais realizadas por criptografia assimétrica, ao invés de cifrarem o próprio documento eletrônico, cifram este "resumo". As mais utilizadas são a *Message Digest 5*, ou MD5, que produz um resultado de 128 bits, e a *Secure Hash Algorithm*, ou SHA, cujo resultado é um número de 160 bits. MARCACINI, Direito e Informática – uma abordagem jurídica sobre a criptografia (2002 p.190)

[48] Bits – É a menor unidade de informação. Um byte corresponde a oito bits. MARCACINI, Direito e Informática – uma abordagem jurídica sobre a criptografia (2002 p.187).

cada documento há uma assinatura diferente, mesmo que seja de uma mesma pessoa.

Como a mensagem é uma variável da fórmula para se criar uma assinatura digital, conclui-se que uma mesma pessoa pode ter várias assinaturas digitais e essas não podem ser reutilizadas, pois se mandarmos mensagens diferentes para uma ou várias pessoas, cada mensagem terá uma assinatura digital diferente, embora venha da mesma pessoa, pois esta foi gerada através de sua chave privada.

O autor Augusto Tavares Rosa Marcacini recomenda algumas dicas quando for salvar um documento que já foi assinado digitalmente, eis algumas dessas dicas:

- Manter mais de uma cópia do documento (CD, disquete, etc.,);
- Não corrigir algum erro de grafia que só tenha sido percebido após a assinatura digital ter sido gerada; e
- usuário não deverá gravar o documento, ao sair de um programa sem que fosse sua intenção[49]

Pois qualquer um desses erros, invalida a assinatura digital que foi produzida.

2.4. Segurança na Criptografia

A segurança na criptografia tanto na simétrica quanto na assimétrica, está relacionada ao tamanho da chave e a consistência do algoritmo. Ao empregar o algoritmo público em um programa de computador mostra-se que esse algoritmo é mais seguro e confiável do que se for utilizado um algoritmo que não foi divulgado, pois o primeiro já foi amplamente estudado e atacado de todas as formas, a fim de encontrar uma maneira para se quebrar o código e

[49] MARCACINI – Direito e Informática – uma abordagem jurídica sobre a criptografia (2002 p. 89)

para assegurar que não houve a instalação de uma "*back door*"[50] dentro do sistema, garantindo assim a sua segurança, e o segundo como não é divulgado não há como garantir se esse algoritmo é seguro e confiável.

Vale ressaltar que tanto na criptografia simétrica quanto na assimétrica, são necessários tamanho de chaves diferentes para que o nível de segurança seja igual, por exemplo, se usarmos um algoritmo de chave pública de 512 bits não significa que ela seja mais segura do que um algoritmo de chave privada de 128 bits.

É aconselhável o uso de chaves maiores de 1024 bits, pois quanto maior o número de bits em uma chave, maior será a sua segurança e consequentemente mais difícil de ser quebrada. Os algoritmos simétricos mais seguros são os IDEA, CAST, *Blowfish*, entre outros e algoritmos assimétricos mais seguros são os RSA, DES dentre outros, estes já passaram por vários ataques de cientistas, o que faz com que sejam considerados confiáveis e seguros.

Uma maneira de quebrar um determinado algoritmo é utilizar um Ataque de Força Bruta que consiste em tentar todas as combinações de chaves possíveis, até encontrar a chave certa, este ataque poder ser usado em qualquer sistema criptográfico, porém não é muito utilizado, já que demanda tempo e a utilização de computadores de última geração encontrado na maioria das vezes em grandes universidades ou centros de pesquisa.

Esses ataques de força bruta pode ser realizado usando computadores convencionais (PCs), ou pela tecnologia *Field Programmable Gate Away* (FPGA), que é um chip especial para a realização de cálculos, até o *Application-Specific Integrated Circuits* (PSICs), que é cerca de sete vezes

[50] Back Door – a expressão é utilizada para designar alguma fragilidade propositalmente inserida em um sistema criptográfico, que permite que alguém que a conheça decifrar as mensagens mesmo sem conhecer a chave utilizada pelo usuário para codificá-las. MARCACINI, Direito e Informática – uma abordagem jurídica sobre a criptografia (2002 p. 185)

mais rápido que o FPGA, porém, este necessita de um investimento maior em engenharia, e como conseqüência, possui um custo mais elevado.

De acordo com pesquisas realizadas, ao aplicarmos um ataque de força bruta em uma chave de criptografia simétrica de 128 bits (um número de 39 algarismos em base decimal), seriam necessários 10.790.283.070 anos para um bilhão de computadores com capacidade de processar 1 trilhão de chaves por segundo trabalhando 24 horas por dia para descobrir a chave correta.

Estimativas para ataques de "força bruta" em algoritmos simétricos

Custo	56 bits	64 bits	112 bits	128 bits
$ 100 K	3, 5 horas	37 dias	10^{13} anos	10^{18} anos
$ 1 M	21 minutos	4 dias	10^{12} anos	10^{17} anos
$ 10 M	2 minutos	9 horas	10^{11} anos	10^{16} anos
$ 100 M	13 segundos	1 hora	10^{10} anos	10^{15} anos
$ 1 G	1 segundo	5,4 minutos	10^{9} anos	10^{14} anos
$ 10 G	0,1 segundos	32 segundos	10^{8} anos	10^{13} anos
$ 100 G	0,01 segundos	3 segundos	10^{7} anos	10^{12} anos
$ 1 T	1 milissegundo	0,3 segundos	10^{6} anos	10^{11} anos

Fonte: Segurança de Redes em Ambientes Corporativos (2003 p.297)

Para garantir proteção a chave privada depois que foi gerada pela PGP, a mesma fornece algumas dicas, tais como:

- usuário deverá criar uma chave-senha, esta deverá ser longa e com várias palavras;
- jamais utilizar dados pessoais como, endereço, telefone, número de CPF, dentre outros;
- não utilizar frases famosas, ditos populares, trechos musicais;
- deve-se utilizar números, letras e símbolos, de preferência sem escrever palavra alguma, escrever uma frase absurda ou sem sentido, misturar palavras de diversos idiomas; e

- jamais anotar a frase-senha em algum lugar[51].

Essa proteção é feita através de uma criptografia simétrica forte, garantindo assim que, se caso a sua chave privada for descoberta, o invasor terá que descobrir a chave-senha para poder ter acesso a chave privada e fazer uso dela.

[51] MARCACINI, Direito e informática – uma abordagem jurídica sobre criptografia (2002 p. 49)

CAPÍTULO III

3. E- COMMERCE OU COMÉRCIO ELETRÔNICO

O E-commerce[52] ou comércio eletrônico[53] foi um dos primeiros tipos de negócios na forma digital que a Internet ofereceu aos seus usuários. É a mais nova forma que os empresários encontraram para vender bens de consumo e serviços através da rede mundial de computadores. Junto ao E-commerce existe outra categoria chamada E-business[54] que é responsável pela otimização do negócio, e pela melhor maneira de se divulgar uma marca, entre outros.

O comércio eletrônico consiste na realização de todas as formas de transações envolvendo pessoas e empresas, que se baseiam no processamento e na transmissão eletrônica de dados para vender e adquirir um produto ou serviço e pagar por ele.

Segundo o autor Daniel Amor, o comércio eletrônico não se baseia somente em segurança, criptografia, moedas e pagamentos eletrônicos, consiste também, na pesquisa e desenvolvimento, marketing, propaganda, negociação, vendas e suporte, ou seja, o comércio eletrônico sem esses fatores que são considerados de suma importância, estaria fadado ao fracasso.

---

[52] E-Commerce – expressão em inglês para comércio eletrônico.

[53] Comércio Eletrônico – é a realização de toda a cadeia de valor dos processos de negócios num ambiente eletrônico, por meio da aplicação intensiva das tecnologias de comunicação e da informação, atendendo aos objetivos de negócio. Outra definição para comércio eletrônico quando este está *on-line*, provê a capacidade de comprar e vender produtos e informações na Internet e em outros serviços *on-line*. AMOR, Comércio eletrônico (2004. p. 15)

[54] E-Bussiness – qualquer empreendimento baseado na Web, ou, as transações de negócio feitas entre empresas pela Internet. Normalmente é utilizado em seu lugar o termo e-commerce, embora não tenha a mesma abrangência. http://www.DICIONÁRIO E-COMMERCE.htm

O comércio eletrônico na Internet é feito através de uma infra-estrutura de comunicação e informação, possibilitando maior rapidez, flexibilidade e um custo reduzido dos produtos e serviços que serão oferecidos aos consumidores através dos *sites*.

Muitas empresas estão usando a Internet para comunicar-se com seus clientes e também com seus fornecedores para que haja uma melhor distribuição de seus produtos. A Internet desempenha funções importantes para seus clientes, tais como: distribuição de *software*, informações de suporte, capacidade de agir rápido quando solicitada pelo cliente, além de ser um novo canal de relacionamento cliente/empresa.

Um dos primeiros setores a utilizarem o comércio eletrônico foi o setor bancário, que permitia que seus clientes utilizassem todos os serviços que uma agência física, só que *on-line*, os bancos perceberam que esse método reduzia o custo das transações tradicionais.

Uma característica da Internet é a quantidade de informação disponível na rede, o que facilita ao consumidor decidir a quantidade e a qualidade do produto ou serviço que se deseja adquirir, assim como obter informações de uma empresa, verificando por exemplo, a sua idoneidade e confiabilidade. A Internet favorece a comunicação entre o mundo todo, sendo assim, quando se expõe um produto ou serviço através da Web, sabe-se que esse produto será visível a todos os usuários da Internet, por isso é importante, quando for expor um produto ou serviço, limitar quais os locais que poderão ser entregues, caso contrário, o *site* poderá ficar mau visto e perder futuros clientes.

O comércio eletrônico cresce no mundo todo, o que é diferente, é a intensidade com que ocorre esse crescimento. Em alguns países, como nos Estados Unidos, cerca de 50% dos internautas compram pela Internet, enquanto, no Brasil essa porcentagem chega a 10% de internautas que realizam compras pela Web[55].

O que faz o comércio eletrônico crescer continuamente, é o fato de seu público alvo possuir alto poder aquisitivo, isso faz com que as vendas e o valor total da compra cresça.

As compras *on-line* representam um hábito novo e que poucos usuários da Internet estão acostumados a utilizar, é um processo lento, mais que já está dando resultados para as empresas que estão atuando *on-line*. Para esse fenômeno crescer mais, é preciso que as pessoas percam o medo de comprar pela Internet. Quando uma pessoa efetua uma compra *on-line*, e esta percebe o quanto é cômodo e fácil, esta pessoa automaticamente estarão propagando esta modalidade de compra e venda a pessoas mais próximas a ela, e com isso o comércio eletrônico cresce. O melhor disso é que o comprador pode escolher qual forma de pagamento pretende usar: cartão de crédito, cheque eletrônico, dinheiro eletrônico[56]. Vendo isso as empresas conseguem ampliar e melhorar a qualidade de seus produtos e serviços oferecidos na Web e também melhorar o processo de comunicação e distribuição de seus produtos.

O VOL[57] (índice de varejo online), é o responsável pela divulgação dos valores arrecadados todos os meses no mercado *on-line* brasileiro. Ele foi

---

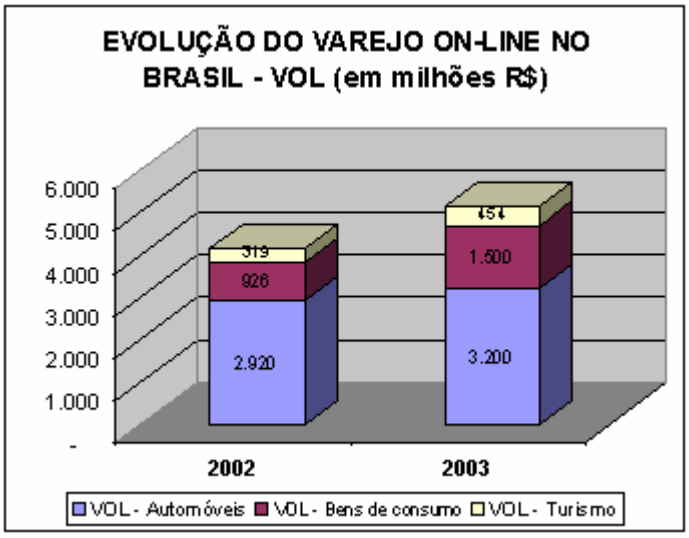
[55] Correio Braziliense (26-04-2004)

[56] Dinheiro eletrônico – é o valor armazenado em suporte eletrônico, como tarjeta-inteligante ou memórias de ordem. É outro meio de pagamento, sendo gerado com o objetivo de colocar-se à disposição dos usuários, como substituto eletrônico de moedas e ordens de pagamento bancárias e para realizar pagamentos de determinadas quantias por meios eletrônicos. FINKELSTEIN, Aspectos jurídicos do comércio eletrônico (2004 p.220).

[57] VOL - é o indicador oficial da Câmara Brasileira de Comércio Eletrônico, este indicador mede o montante de transações do B2C na ponta de venda incluindo automóveis, sites de leilão, bens de consumo e turismo online (cias aéreas e

criado para padronizar o sistema de medição do comércio *on-line*. Esse índice é divulgado sempre no primeiro dia útil de cada mês de acordo com dados levantados de dois meses antes, assim, por exemplo os dados de Março só serão apresentados no mês de Maio, e assim por diante. O VOL é dividido em três categorias: automóveis, turismo e bens de consumo, o primeiro se refere as vendas *on-line* de carros vindas diretamente dos *sites* das montadoras e das revendedoras, o segundo, corresponde as vendas de pacotes turísticos on-line das agências de turismo e das companhias aéreas, e o último trata de todos os bens e serviços adquiridos *on-line*.

O VOL em 2003 registrou, um aumento significativo no comércio eletrônico em relação ao mesmo período do ano de 2002 como mostra o quadro abaixo, todas as categorias em que houve a medição dos valores através do Índice Mensal de Varejo *on-line* brasileiro . Isso mostra que a tendência é que haja um crescimento gradual do comércio eletrônico brasileiro.



Fonte: http://www.e-commerce.org

agências). http://www.econsultingcorp.com.br/insider_info/indicadores.shtml. Acessado em 02/03/04

Segundo o índice de varejo online (VOL) divulgado pelo *site* http://econsultingcorp.com.br/vol/, o mercado brasileiro totalizou R$ 531,8 milhões no mês de Abril (2004), 43% a mais do que o mesmo período do ano passado[58], sendo que a VOL-Automóveis totalizou R$ 326,3 milhões cerca de 41% a mais que o mesmo período de 2003 e 61,4% do total da VOL do mês de Abril, a VOL-Turismo totalizou R$ 75,1 milhões, mais ou menos 14,1% do total do VOL e o VOL-Bens de consumo fechou o mês de Abril com R$ 130,4 milhões, 24,5% do total do VOL.

3.1. Sistemas de Pagamento Via Internet

Para que uma transação eletrônica tenha sucesso, é necessário que esse ambiente seja seguro, confiável e simples tanto para o comprador, quanto para o vendedor (*sites*). Algumas formas de pagamento na Internet não são aceitas, é o caso do cheque e do dinheiro, pois, para que haja o uso do cheque ou do dinheiro, deve haver a presença física do comprador e do vendedor o que leva o negócio para o ambiente fora da Internet. As formas de pagamento eletrônico mais usadas na Internet são: o dinheiro eletrônico (ou *digi-cash*, ou *e-cash*), cheque eletrônico, cartões inteligentes e o mais usado, o cartão de crédito.

O *digi-cash* ou dinheiro eletrônico, foi desenvolvido pela empresa do Dr. David Chaum, em Amsterdã. Esse sistema de pagamento é baseado em um sistema de sinais digitais chamada moedas digitais, essas moedas são criadas pelo consumidor e também assinadas digitalmente.

O pagamento de um produto ou serviço em que se utiliza o *digi-cash* ocorre da seguinte forma: o comprador criptografa com chave pública a quantidade de *digi-cash* que será necessário para pagar o produto ou o serviço, este envia para o vendedor através de um *e-mail* por exemplo, quando

o vendedor recebe o *e-mail*, ele o descriptografa, e depois o valor que foi colocado pelo comprador é enviado para uma instituição financeira que aceita o *digi-cash* e deposita o valor na conta do vendedor. O mais importante, o comprador dever ter uma conta nesta instituição. O *digi-cash*, não é a forma mais usada, pois muitos sites não aceitam essa modalidade de pagamento.

O cheque eletrônico envolve três agentes para realizar uma compra inclusive internacional via Internet, o comprador, o vendedor e o intermediário que geralmente é uma instituição financeira. Este pagamento funciona da seguinte forma: o comprador pede um produto ou serviço a um vendedor, o mesmo começa o processo de pagamento, o comprador obtém do intermediário uma certificação que é passada ao vendedor, este confirma o valor da compra e repassa novamente ao intermediário que deposita o valor na conta do vendedor que habilitou nesta instituição. O cheque eletrônico utiliza a assinatura digital baseada na criptografia de chave pública, assim como o uso do certificado eletrônico para autenticar o processo de pagamento.

O cheque eletrônico têm o objetivo de facilitar os serviços *on-line*, permitindo um melhor fluxo de pagamento, melhorar a segurança em cada etapa da transação, através da assinatura digital das partes envolvidas e facilitar o pagamento dos pedidos que foram realizados nos sites que aceitam esta forma de pagamento eletrônico.

Os cartões inteligentes ou também chamados *smart-cards*, se parecem muito com os cartões de crédito convencionais, porém, estes possuem algumas vantagens, como um armazenamento maior de informações, podendo ser usados para várias finalidades. Os cartões inteligentes são protegidos por senha, então se alguma pessoa se apoderar deste cartão, terá que saber a senha para poder utilizá-lo. Este mesmo cartão pode usar sistemas criptográficos RSA pública/privada, o usuário pode deixar somente a chave pública legível, garantindo que somente com o uso da chave privada é que

[58] www.e-commerce.org.br acessado em 26/05/2004

poderá decifrar uma mensagem que o usuário deseja manter em segredo, pois como foi dito, este cartão permite que se guarde qualquer tipo de informação.

Na Internet, o cartão inteligente é inserido em uma leitora de cartões e o usuário do cartão deverá fornecer o seu número de identificação, depois da identificação for concluída, poderá efetuar suas compras e o valor é debitado de seu cartão inteligente.

O responsável pela maioria dos pagamentos pela Internet é o cartão de crédito, cerca de 90%[59] dos consumidores utilizam esse sistema para efetuarem o pagamentos de suas compras internacionais no ambiente virtual.

Os vendedores de produtos e serviços na Internet estão experimentando três formas diferentes de se usar o cartão de crédito através da rede, a primeira é chamada *off-line*[60], onde o comprador após efetuar o pedido liga para o vendedor e transmite o seu número do cartão de crédito, a segunda é chamada de *on-line* com criptografia, onde o comprador transmite o número do cartão de crédito através de uma transação criptografada e a última é chamada de *on-line* sem criptografia, onde o comprador envia seu número do cartão de crédito por *e-mail*, contando apenas com a segurança do *e-mail* de não ser interceptado no caminho.

Existe um modelo de seguro para transações eletrônicas em que se utiliza os cartões de crédito é o chamado SET (Transações Eletrônicas Seguras – *Secure Eletronic Transactions*), o SET é baseado na tecnologia de criptografia de chave pública RSA, além do uso de assinaturas digitais, esse protocolo tem como objetivo, prover autenticidade ao dono do cartão de crédito, confidencialidade dos dados, além de proteger a integridade do pagamento.

---

[59] AMOR, Comércio eletrônico (2004 p. 204).
[60] Off-line – desconectado, não está ligado à Internet. http://www.DICIONÁRIO E-COMMERCE.htm

Para quem ainda não tem confiança de fornecer seu número de cartão de crédito em um *site*, esses podem usar uma outra forma de pagamento chamada de boleto bancário. Este só pode ser usado em compras realizadas no caso em território brasileiro. Funciona da seguinte forma, ao se fazer um pedido de um produto ou serviço em um determinado *site*, este lhe oferece algumas opções de pagamento, como cartão de crédito, cartão de débito ou boleto bancário, se caso a escolha for o boleto bancário, este será gerado pelo próprio *site* e impresso pelo comprador, então, o mesmo deverá se dirigir a uma agência bancária e pagar o valor da compra. O banco irá mandar o dinheiro para a conta do *site*, e assim que o *site* receber o pagamento, o mesmo irá liberar e enviar o produto ou fazer o serviço, que o comprador solicitou, dentro de um prazo estipulado pelo *site*.

Os sistemas de pagamentos são divididos em três categorias de acordo com as transações de negócio, são eles: sistema pré-pago (dinheiro eletrônico, cartões inteligentes), o sistema instantâneo (cartões de débito) e o sistema pós-pago (cartão de crédito, cheque eletrônico). Esses sistemas também possuem alguns requisitos que devem ser considerados na hora de decidir qual sistema usar na hora de realizar um pagamento na Internet. São eles:

- a aceitabilidade permite saber quais *sites* aceitam o sistema de pagamento que se deseja usar;
- o anonimato, os compradores procuram por privacidade na hora de se efetuar uma compra;
- a conversibilidade, esses sistemas, devem dar a possibilidade de se converter moedas;
- a eficiência é outro fator que deve se levar em consideração na hora de decidir qual forma de pagamento utilizar, pois o sistema não pode ter problemas operacionais;
- a flexibilidade é responsável pela adaptação nas mudanças de mercado que eventualmente acontecem;

- a integração deve estar unida aos sistemas tradicionais de pagamento, a confiabilidade que esses sistemas devem passar a seus compradores é de suma importância;
- a escalabilidade permitindo o aumento das compras em *sites* e um fluxo maior de capital;
- a segurança que é o componente mais importante para que uma compra eletrônica tenha êxito; e
- a facilidade que esses sistemas devem oferecer para seus compradores e vendedores.

Sistema Eletrônico de Pagamento e seus Requisitos

	Pré-Pago (e-cash, cartão inteligente)	**Instantâneo (cartões de débito)**	**Pós-Pago (cartão de crédito, cheque eletrônico)**
Aceitabilidade	Baixa	Baixa	Alta
Anonimato	Médio	Alto	Baixo
Convertibilidade	Alta	Alta	Alta
Eficiência	Alta	Alta	Baixa
Flexibilidade	Baixa	Baixa	Baixa
Integração	Média	Baixa	Alta
Confiabilidade	Alta	Alta	Alta
Escalabilidade	Alta	Alta	Alta
Segurança	Média	Alta	Média
Facilidade	Média	Média	Alta

Fonte: AMOR, Comércio eletrônico (2004 p.211)

3.2. Segurança e Privacidade no Comércio Eletrônico

A segurança na Web é feita através de um conjunto de procedimentos e tecnologias que são usadas para proteger os servidores, os usuários e os *sites*. Umas das principais preocupações de um cliente na hora em que ele decidir comprar pela Internet é a segurança e a privacidade do *site* que ele escolheu. Se esses dois fatores forem bem implementados pelos *sites*, poderá fazer com aumente as suas vendas, caso contrário poderá, levá-lo a desativar o *site* dentro de pouco tempo.

O que mais preocupa os usuários da Internet na hora de se efetuar uma compra *on-line*, são os vírus[61], os worm[62] e os cavalos de tróia[63], responsáveis pela destruição de programas, *software*, disco rígido (HD), entre outros além das fraudes que podem ocorrer ao utilizar o cartão de crédito, causados pelos hackers. Esses fatores devem ser levados em consideração para evitar que o *site* seja atacado por algum desses elementos, trazendo como conseqüência o ataque também a computadores dos usuários.

[61] Vírus – é um programa de computador mal intencionado que faz cópias de si mesmo e anexa estas cópias em outros programas. GARFINKEL & SPAFFORD, Comércio e segurança na Web (1999 p. 8).
[62] Worm – é similar a um vírus, exceto pelo fato de que ele envia cópias de si mesmo para outros computadores onde eles podem executar como programas autônomos. GARFINKEL & SPAFFORD, Comércio e segurança na Web (1999 p. 8).
[63] Cavalo de Tróia – é um programa que parece ter uma função útil, mas na verdade tem uma função maligna oculta. GARFINKEL & SPAFFORD, Comércio e segurança na Web (1999 p. 8).

Outro fator que preocupa os usuários da Internet são os chamados SPAMS[64], que na maioria as vezes não são autorizados pelos usuários, fazendo com que sua privacidade seja invadida. Geralmente o conteúdo desses e-mails são de produtos de interesse pessoal, pois foram escolhidos através de informações pessoais identificáveis (PII – *Personally Identificable Information*), fornecidos para alguns sites. O destino final dessas mensagens é a "lata de lixo".

Os *sites* protegem seus clientes através da criptografia, pois com ela o cliente pode enviar o número do seu cartão de crédito pelo seu computador até o *site*, sem correr o risco de ser pego por algum hacker, ou programas mal intencionados. Para o comércio via Internet o uso da criptografia é essencial, porém ela sozinha não garante a segurança de um *site*. Por exemplo, deve-se também proteger a rede, para que as informações não sejam lidas por outros, e ocultar as informações, mesmo aquelas que parecem não ter importância.

Outra opção de segurança é o uso de *Firewalls* nos *sites*, estes permitem que todas as conexões feitas sejam monitoradas , o que permite identificar com rapidez e eficiência, caso haja algum problema, ele detecta por exemplo, o ataque de um *cracker*. O *host*, é outro tipo de segurança que um servidor Web deve se preocupar em ter em seu *site*, pois todos os arquivos executáveis estão dentro do servidor Web, então quanto mais hosts, melhor será a segurança, pois poderá deixar cada host responsável por uma parte do servidor.

Como ainda não há nenhum tratado internacional especifico sobre comércio eletrônico e sobre compra e venda de produtos ou serviços pela Internet os sites estão usando a Convenção de Viena de 1980[65], nos contratos

[64] SPAM – é o envio de e-mails não solicitados. Normalmente é caracterizado quando se enviam muitos e-mails promovendo um produto ou serviço. ATHENIENSE, Internet e direito (2000 p.284).

[65] Convenção de Viena de 1980 – foi a primeira tentativa de uniformização substancial do regime de compra e venda internacional, com ampla aceitação

celebrados pela rede. Quando existe alguma controvérsia, cada país, tenta resolver individualmente a questão adaptando-a à Convenção de Viena de 1980. Como a Internet está ao alcance de todo o mundo, então, cada país fica responsável pela criação de suas leis. Nos Estados Unidos por exemplo, já existem leis federais e estaduais para crimes cometidos pela Internet. Cada estado dos Estados Unidos criou sua própria legislação a respeito de crimes cometidos pela Internet, se por exemplo, ao comprar um CD num site situado em Nova York, e este violar o contrato e não entregar, e o comprador morar em Seatlle, o caso será julgado de acordo com as leis de Nova York, pois provavelmente lá estará escrito que para qualquer conflito será usado as leis do estado em que foi constituído o *site*.

3.3. Evolução nos Contratos Internacionais

Os contratos internacionais[66] são usados desde a antigüidade com o objetivo de realizar trocas comerciais. O Direito Romano foi o responsável

---

na comunidade internacional, foi a Convenção das Nações Unidas sobre Contratos Internacionais de Compra e Venda de Mercadorias (*United Nations Convention on the International Sale of Goods*), mais conhecida como a Convenção de Viena de 1980. Esse documento representa moderno conjunto de regras materiais que reconhece a autonomia da vontade das partes e a obrigatoriedade dos usos e costumes do comércio internacional, abrangendo regras uniformes que vão da formação do contrato internacional até as obrigações das partes contratantes. BOUISSOU, Contratos internacionais e domésticos da Internet, Correio braziliense (2000 p. 5)

[66] Contratos Internacionais – é um acordo bilateral que pode ser produzido nos âmbitos interno e internacional. O contrato internacional ocorre quando, as partes contratantes tenham nacionalidades diversas ou domicílio em países distintos, quando a mercadoria ou o serviço objeto da obrigação seja entregue ou seja prestado além-fronteira, ou quando os lugares de celebração e execução das obrigações contratuais tampouco coincidam. VENTURA, Contratos internacionais empresariais (2002. p.23)

pelas primeiras regras comerciais, como por exemplo compra e venda de mercadorias, mercado de câmbio. Durante a Baixa Idade Média, mais precisamente no Séc. XI, houve o renascimento do comércio, que estava em crise até então. O homem daquela época começou a trocar sementes, fazendo assim um intercâmbio de trocas com novas rotas comerciais. Neste mesmo período surgem as primeiras feiras italianas que comercializavam vários produtos, desde produtos têxteis até especiarias do Oriente. Com essas feiras vieram o primeiros problemas jurídicos internacionais, pois haviam pessoas e medidas diferentes circulando por essas feiras, dando inicio então a "*Lex Mercatoria*[67]".

A *Lex Mercatoria* surgiu no século XII, para regulamentar os contratos internacionais comerciais que eram utilizados nas feiras. A *Lex Mercatoria* possui algumas características, como uso e costumes, onde os comerciantes desses mercados é que criavam os seus costumes, direito autônomo, que eram cumpridas foras da região, este era independente do direito interno e o direito costumeiro.

A nova *Lex Mercatoria*, ainda possui algumas características da *Lex Mercatoria* antiga, tais como:

- usos e costumes do comércio internacional; e
- arbitragem comercial internacional

No caso dos usos e costumes do comércio internacional houve a mudança no sentido de que existem associações fazendo com que houvessem novas regras e costumes que surgiram de forma espontânea, mais que deveriam ser considerados na hora de se celebrar o contrato. A arbitragem comercial internacional veio como um mecanismo alternativo de solução de

[67] Lex Mercatoria – é o conjunto de regras e institutos concernentes ao comércio internacional comumente aplicados pelos mercadores, conscientes de que se tratem de *regular iuris* (regras de direito) ou pelo menos de que os outros contraentes se comportem observando as mesmas regras. FINKELSTEIN, Aspectos jurídicos do comércio eletrônico (2004 p. 128).

controvérsias, onde o caso não é levado para o judiciário, tornando-se assim uma forma de solução mais rápida.

No início do século XX, houve uma retomada dos princípios consagrados da *Lex Mercatoria*, em 1926, foi criada pela Liga das Nações, a UNIDROIT (Instituto para a Unificação do Direito Privado), tinha como objetivo criar regras para a regulamentação de compra e venda de mercadorias e serviços.

A UNCITRAL[68] (Comissão das Nações Unidas para o Comércio Internacional), teve como responsabilidade a criação de normas universais e a harmonização das contratações avalizadas ao nível internacional. Sua principal legislação é Lei Modelo da UNCITRAL, que pode ser aplicada por todos os países que querem adotar normas jurídicas para o comércio eletrônico, a fim de regulamentar os contratos, sua formação, prova, propostos e outros elementos que são necessários para prover segurança jurídica nesse tipo de ambiente.

A finalidade da Lei Modelo da UNCITRAL, que teve iniciativa da Convenção de Viena de 1980, onde seu objetivo é ajudar aos usuários do e-commerce a descobrir possíveis soluções para as controvérsias jurídicas nos contratos celebrados pela rede mundial de computadores.

A Convenção de Viena de 1980, sobre compras e vendas internacionais de mercadorias e serviços é fruto da UNCITRAL. Sua característica principal, é a não substituição das regras internacionais que protegem o consumidor. A Convenção de Viena de 1980 é aplicada nos contratos de compra e venda em que o comprador e o vendedor residem em países diferentes ou quando as

[68] UNCITRAL – crida pela Assembléia Geral da Nações Unidas em 17/12/66, seguindo recomendações que havia sido apresentada pela delegação da Hungria junto à entidade, atendendo a um desejo de criação de um foro de debate sobre a matéria, no qual todas as regiões geográficas e os distintos sistemas jurídicos estivessem representados. BOUISSOU, Formação dos contratos internacionais e a Convenção de Viena de 1980; perspectiva de ratificação pelo Brasil (1996 p.36-37).

regras de conexão do Direito Internacional Privado de qualquer um dos dois assim permitir.

Como não existe Tratados Internacionais para regulação do comércio via Internet, as empresas (*sites*), vem usando a Convenção de Viena de 1980, como forma de regulação dos contratos estabelecidos via Internet.

A convenção de Viena de 1980 é usada nos contratos de compra e venda internacional de mercadoria por várias razões:

- sua flexibilidade permite que se possa ser usada nos contratos de compra e venda internacional pela Internet;
- a convenção é aplicada para bens tangíveis, ou seja, pode ser usada pois, na Internet os produtos comercializados são considerados bens tangíveis;
- em seu Art.11, diz que um contrato não precisa ser escrito para ter validade, em um contrato pela Internet, não existe assinatura escrita; e
- nas transações de comércio eletrônico na Internet é validada a oferta e a aceitação.[69]

Por isso é que muitos países utilizam a Convenção de Viena de 1980 para resolver controvérsias ocorridas na Internet, pois ela permite que pessoas de países diferentes consigam resolver seus problemas, até que todos os países adeqüem suas leis de acordo com esta convenção.

Com a evolução das obrigações e dos deveres jurídicos, os contratos passaram por várias mudanças, tanto de natureza familiar quanto de natureza comercial. Os contratos comerciais de compra e venda surgiram com o objetivo de facilitar a circulação de mercadorias ao redor do mundo, detalhando o preço, a forma de pagamento, e a modalidade de transporte.

[69] BOUISSOU, contratos internacionais e domésticos na Internet, Correio braziliense (2000 p. 5)

A intervenção do Estado sobre a economia foi refletida nos contratos, pois estes também tratavam de assuntos comerciais. Muitas cláusulas eram impostas ou proibidas pelo Estado, tornando as empresas privadas limitadas à estas imposições.

Para o autor Carlos Alberto Gonçalves o contrato " têm uma função social, sendo veículo de circulação de riqueza, centro da vida dos negócios e propulsor da expansão capitalista"[70], ou seja, com o uso de contratos para a realização de trocas comerciais, ficava mais fácil cobrar uma obrigação quando uma das partes não a cumprisse.

A maior transformação ocorrida nos contratos foi no século XX, com o surgimento da "sociedade de informação ou também chamada de sociedade pós-industrial"[71], nesta sociedade destaca-se a Internet, além de novas modalidades de transporte, fruto dos crescentes investimentos nas tecnologias de informação. Com a Internet, houve a possibilidade de se celebrar um contrato, sem que houvesse o documento impresso em um papel.

Para o autor Jorge José Lawand a Internet "é um elemento onde é possível manifestar a vontade, e as pessoas de lugares totalmente distintos têm acesso a comunicação de modo interativo, podendo encomendar e solicitar serviços e produtos, ou onde as empresas efetivam negócios com outras empresas fornecedoras e bancos, entre muitas outras facilidades"[72], em outras palavras, a Internet surgiu como um instrumento para a realização de contratos, onde não há presença física das partes, pôr se tratar de um meio virtual.

3.3.1. Contratos Internacionais na Internet

[70] LAWAND, Teoria geral dos contratos eletrônicos (2003 p. 15)
[71] LAWAND, Teoria geral dos contratos eletrônicos (2003 p. 19)
[72] LAWAND, Teoria geral dos contratos eletrônicos (2003 p. 21-22)

Hoje na Internet quem oferece um produto ou a prestação de um serviço qualquer ao usuário, sabe-se que não há a figura física do vendedor, o próprio site acaba fazendo o papel do vendedor. Esse tipo de procedimento é considerado como uma forma de contrato de compra e venda, pois existe a figura do vendedor (*site*) e a do comprador (usuário final).

Os contratos internacionais celebrados via Web contribuem significativamente para o desenvolvimento do comércio eletrônico mundial. Esses contratos eletrônicos são considerados formas jurídicas dentro da Internet, pois são comercializados produtos e serviços que podem ser incluídos dentro dos contratos de compra e venda.

Um contrato eletrônico[73], realizado entre usuário e *websites* são chamados de contratos eletrônicos interativos[74]. O usuário através do seu computador, adquire bens ou serviços que são oferecidos pelos *sites*. Nestas páginas, o usuário irá encontrar todas as informações sobre o produto ou serviço que se deseja adquirir, incluindo o preço e as formas de pagamento que são aceitas pelos *sites*.

Em um contrato internacional de compra e venda deve-se levar em consideração os sistemas jurídicos que serão utilizados, além, é claro, da definição da lei aplicável. Quando por exemplo, a pessoa está no Brasil e o produto que se deseja adquirir esta nos Estados Unidos, então se utiliza um processo chamado *Dépercage*[75] se caso ocorrer algum conflito nesse contrato.

---

[73] Contrato eletrônico – é um acordo manifestado por meio de computadores, tendente a criar, modificar ou extinguir obrigações que tenham por objeto bens e serviços. MONTENEGRO, A Internet em suas relações contratuais e extracontratuais. (2003 p.53).

[74] MONTENEGRO, A Internet em suas relações contratuais e extracontratuais (2003 p. 52).

[75] Dépecage – também chamada de fragmentação será usada quando presente dada situação jurídica passível de utilização de leis diferentes aplicáveis aos diversos aspectos do contrato. Isto decorre da limitação da autonomia da vontade que rege os contratos internacionais que implica então na decomposição do contrato em seus vários elementos, para a aplicação em cada uma de suas partes, da lei pertinente. http://www.alfa-redi.org/revista/data/28-8.asp, acessado em 02/06/04.

Um princípio importante a ser observado nos contratos internacionais de compra e venda pela Internet é o chamado “Princípio da Boa Fé”, que tem como objetivo dar confiabilidade, lealdade e veracidade nas relações entre comprador e vendedor, esses fatores são de suma importância para o direito internacional, pois de acordo com o autor Clóvis do Couto e Silva “a confiança do público é indispensável, o que se traduz na observância da boa-fé objetiva, que corresponde a um dever de conduta contratual, no tocante ao cumprimento da respectiva obrigação por cada qual das partes – tais quais a entrega da coisa vendida, o pagamento da compra, por exemplo, – e se soma a deveres secundários, laterais, anexos ou instrumentais de conduta, tais quais os de informação correta, esclarecimento, lealdade e assistência, dentre outros”[76], ou seja, todos esses fatores devem ser observados na hora de se fazer um contrato, pois são extremamente importantes para que um contrato tenha êxito.

Outro fator importante para a realização de um contrato internacional via Web, é a segurança. Na maioria dos casos o sistema de criptografia é a forma mais usada para dar segurança aos contratos que são realizados dentro das páginas da Web. Através da criptografia (“é usada para embaralhar as informações enviadas pela Internet e armazenadas em servidores de modo que invasores não possam acessar o conteúdo dos dados”[77]) pode-se usar cartões de crédito para efetuar o pagamento do produto, pois através da criptografia e de um programa como por exemplo, o protocolo SSL (*Secure Sockets Layer*)

da *Netscape*[78], estes não permitem que essa transação seja monitorada enquanto estiver em andamento. Outra estratégia de segurança é o uso de *Firewalls*, que tem como objetivo levar as conexões externas para um local bem monitorado e que detecte qualquer problema.

---

[76] LAWAND, Teoria geral dos contratos eletrônicos (2002 p. 51)
[77] GARFINKEL & SPAFFORD, Comércio & segurança na web (1999 p .209)
[78] SSL – programa criado pela Netscape que tem o objetivo de proteger as informações enquanto os dados estão em trânsito e dá aos usuários boas

3.4.2. Contratos de Adesão

Os contratos de adesão podem ser considerados como sendo contratos-tipo e também como condição geral de venda da Nova *Lex Mercatoria*, pois neste tipo de contrato, já existem clausulas pré-estabelecida por uma das partes portanto não tendo negociação, no caso os *sites* da Internet, e é uma condição geral para que um produto ou serviço possa ser adquirido

O contrato de adesão é constituído somente por uma das partes. Na Internet o contrato é feito pelos sites, e o usuário aceita todas as condições ou as rejeita completamente, ou seja, não há como negociar nenhuma das cláusulas.

No inicio do séc. XX, o autor Von Tuhr definiu o contrato de adesão como "um contrato por meio do qual se confere a uma das partes a faculdade de criar, por iniciativa própria , uma relação obrigacional já definida em seus pontos essenciais. Por meio de tal negócio jurídico, uma das partes tem apenas a liberdade de aceitar a proposta, completa e inalterável, da outra. A eficácia sugerida declaração de autuação, pois não há necessidade de outra manifestação de vontade, ou seja , já no começo do século existia esse tipo de proposta, a Internet a incorporou, ao fazer os contratos de adesão através dos sites que oferecem produtos e serviços.

Esse tipo de contrato utilizado nos sites é chamado de "clickwrap[79]", que são usados para mostrar que o usuário conhece os termos de uso do site, e

---

garantias que eles estão se comunicando com os sites com os quais acreditam estar. GARFINKEL & SPAFFORD, Comércio & segurança na web (1999 p. 15).

[79] Clickwrap – são contratos de adesão, escritos em um site, onde o leitor expressa a aceitação de seus termos apenas, com um click de mouse, marcando " I Agree", "eu concordo", "OK" ou algum termo equivalente. LAWAND, Teoria geral dos Contratos eletrônicos (2003 p.)

das penalidades que poderá sofrer se eventualmente descumprir alguma parte do termo.

Um *site* que pode ser dado como exemplo é o da Amazon.com. A Amazon começou numa garagem e realizava entregas bem pequenas. Com o tempo a Amazon começou a ter seus estoques de livros e hoje é uma das maiores lojas virtuais do mundo e entrega em qualquer parte do globo terrestre.

A Amazon começou somente com livros, e hoje vende além dos livros, CD, DVD, Programas de computador. Hoje a Amazon ocupa dois andares de um prédio em Seatlle[80] nos Estados Unidos.

A Amazon mantém alguns livros em estoque, geralmente os mais vendidos, o resto ela pede para seus distribuidores e para as editoras, isso faz com que o custo do produto seja reduzido e o preço final para o consumidor fique geralmente abaixo aos da concorrência, seja ela loja física ou virtual.

Para realizar uma compra na Amazon tem que se primeiro ler o termo e as condições desse contrato, além de se submeter a todas as regras dispostas no contrato. Existe um serviço de pagamento próprio da Amazon, porém só são aceitos cartões de crédito, este serviço está disponível sete dias por semana, vinte e quatro horas por dia, inclusive feriados. Além desse serviços, existe um serviço que é responsável por mandar notícias aos seus usuários cadastrados por *e-mail*, e outro, onde o consumidor pode deixar sua opinião a respeito do produto que foi adquirido.

O *site* também adverte as pessoas que queiram invadir o *site* com o intuito de prejudicar seus usuários, diz que irão descobrir quem realizou o delito e de acordo com a região, uma de suas filiadas avisará a polícia, e esta se encarregara de prender o culpado.

[80] AMOR, Comércio eletrônico (2004 p .64)

Os termos e condições do *site* da Amazon foram baseados nas leis do Estado de Washington nos Estados Unidos. Caso haja, alguma quebra do contrato por parte do usuário, a Amazon irá submeter a controvérsia internacional ao método alternativo da arbitragem comercial na cidade de Reno, que fica no Estado de Nevada nos Estados Unidos, através da Associação de Arbitragem Americana. Se caso houver uma quebra de contrato, por exemplo, por parte da Amazon, e o comprador é uma pessoa brasileira, está terá que se submeter as leis do Estado de Nevada.

CONCLUSÃO

A revolução tecnológica nas telecomunicações trouxe a Internet, para a sociedade com intuito de ligá-la ao mundo virtual, permitindo que as pessoas acessem diferentes *sites* situados em qualquer lugar do mundo com o preço de uma ligação local, além de conhecer vários lugares, pesquisar sobre determinado assunto, efetuar pagamentos pela Internet, fazer compras de produtos ou serviços sem sair de casa ou do trabalho, com a maior comodidade e receber o produto ou serviço em casa ou no trabalho. A Internet possui uma enorme quantidade de informações, o que faz com que seja considerada uma grande biblioteca virtual.

Com a descoberta da criptografia permitiu que bancos, TV´s a cabo, e *sites* por exemplo, utilizassem-a para prover segurança nas transações bancárias e na liberalização de canais com o intuito de proteger esses usuários de pessoas não autorizadas que queiram tirar proveito da situação e os *sites,* que permitem que se dê informações sigilosas, mais que não poderão ser descobertas . A assinatura digital permitiu dar proteção nos documentos gerados pela Internet, ficando mais fácil trocar informações seguras entre pessoas. Através dos algoritmos de chave pública e privada que são geradas por entidades especializadas nesse assunto, é que também ocorre essas trocas de informações seguras.

A segurança na criptografia depende do tamanho da chave a ser utilizada, pois quanto maior o número de bits, maior será a segurança da chave em eventuais ataques de força bruta, estes não são muito utilizados, pois demanda tempo e dinheiro. Estes ataques só poderiam ser realizados por comunidades científicas e universidades que possuem computadores de última geração.

Para saber se um *site* é seguro, basta olhar se este possui um cadeado fechado, se a resposta for sim, este está protegido por uma autoridade certificadora que garante que este *site* é seguro para receber informações pessoais, como por exemplo, digitar o número do cartão de crédito. Através também dos certificados digitais, pode-se também descobrir se um *site* está protegido, pois como esses expiram, a proteção desses têm prazo de validade, para que imprevistos não aconteçam, é necessário que este *site*, mantenha o seu certificado digital atualizado.

Com o preço dos computadores caindo, a tendência é que haja um aumento progressivo de pessoas que dispõe de acesso a Internet e com isso poderá haver um aumento do comércio eletrônico. Pois como somente pessoas com alto poder aquisitivo, é que dispõem de acesso a Internet, com a diminuição dos preços dos computadores, mais pessoas terão acesso e com isso o comércio eletrônico irá crescer, podendo ultrapassar o comércio tradicional.

A Internet permite que os consumidores decidam melhor quais produtos ou serviços que poderão ser adquirido, com facilidade e comodidade, a qualquer hora do dia ou da noite, sem ter a presença física do vendedor.

Apesar de ser um hábito novo para a sociedade, com tempo, as compras pela Internet serão consideradas parte do cotidiano das pessoas, o que ainda faz com que o comércio eletrônico ainda não faça parte deste cotidiano é o receio das pessoas em por exemplo, digitar o número do seu cartão de crédito. Mas, por exemplo, se algum conhecido fizer uma compra pela Internet, e tudo correr bem, a chance dessa pessoa comprar irá aumentar, e assim, passará para outras pessoas, fazendo com que o crescimento do comércio eletrônico evolua mais ainda.

Os sistema de pagamento mais utilizado para se pagar uma compra *on-line* é o cartão de crédito, como foi dito no capítulo anterior, este é responsável por 90% dos pagamentos *on-line*. Isso mostra, que a segurança nos *sites* vem sendo constantemente atualizadas. Existe outras formas de pagamento como *smart cards*, cheque eletrônico, porém não são muito utilizadas.

Com a evolução dos contratos internacionais ao longo do tempo, este chegou ao mundo virtual, trazendo grandes benefícios para os *sites* da Internet, como por exemplo, os contratos de adesão, que é a forma mais utilizada de contratos nos *sites* especializados em compra e venda de produtos e serviços, apesar de ser uma desvantagem para os consumidores, pois este tipo de contrato não permite que este possa ser negociado. Quem deseja adquirir um produto ou serviço, é necessário que se leia o contrato de adesão para efetuar o pedido, e seguir o contrato para evitar problemas futuros.

Um exemplo de *site* bem sucedido, é o da Amazon.com Esta é responsável por grande parte das vendas realizadas pela Internet. Sua especialidade é a venda de livros, CD´s, DVD´s e programas de computadores. Para fazer uma compra neste *site*, é necessário que se leia os termos de adesão e de políticas de privacidade, depois de lido, ainda se quiser realizar uma compra, qualquer problema será de responsabilidade de ambos, e serão resolvidos de acordo com as especificações do *site* da Amazon.

Concluindo, os contratos internacionais de compra e venda, estão sendo realizados através de compras em *sites* que oferecem produtos e serviços para o mundo todo. Graças a Internet, é que o comércio eletrônico vem crescendo de uma forma muito rápida, e daqui há algum tempo, poderá ultrapassar o valor de venda do comércio tradicional de todo o mundo.

REFERÊNCIAS BIBLIOGRÁFICAS

- ALBERTIN, Alberto Luiz – *Comércio Eletrônico*, São Paulo, Atlas, 2004.
- ANÔNIMO – *Segurança Máxima para Linux*, Rio de Janeiro, Campus, 2000
- AMOR, Daniel – *A (R) Evolução do E-business*, São Paulo, Makron Books, 2000.
- ARAUJO, Nadia de – Contratos Internacionais - autonomia da vontade, Mercosul e convenções internacionais, Rio de Janeiro, Renovar, 1997.
- ATHENIENSE, Alexandre – Internet e o Direito, Belo Horizonte, Inédita, 2000.
- BRASIL, Cyclades – *Guia Internet de Conectividade*, São Paulo, Cyclades, 1999.
- FINKELSTEIN, Maria Eugênia Reis – Aspectos Jurídicos do Comércio Eletrônico, Porto Alegre, Síntese, 2004.
- GARFINKEL, Simson & SPAFFORD, Gene – Comércio *e Segurança na Web*, São Paulo, Market Books, 1999.
- LAWAND, Jorge José – *Teoria Geral dos Contratos Eletrônicos*, São Paulo, Juarez de Oliveira, 2003.
- LUCCA, Newton de – Direito & Internet - aspectos jurídicos relevantes, São Paulo, Edipro, 2001
- MARCACINI, Augusto Tavares Rosa – *Direito e Informática, uma abordagem jurídica sobre criptografia*, Rio de Janeiro, Forense, 2002.
- MONTENEGRO, Antônio Lindberg – A Internet em suas Relações Contratuais e Extracontratuais, Rio de Janeiro, Lumen Juris, 2003.
- NAKAMURA, Emílio Tissato & GEUS, Paulo Lício de – *Segurança de Redes em ambientes cooperativos*, São Paulo, Futura, 2003.
- PEREIRA, Joel Timóteo Ramos – Direito da Internet e Comércio Eletrônico, Lisboa, Quid Juris, 2001.

- SALVETTI, Dirceu Douglas & BARBOSA, Lisbete Madsen – *Algoritmos*, São Paulo, Makron Books, 1998.
- VENTURA, Luiz Henrique – *Contratos Internacionais Empresariais*, Belo Horizonte, Del Rey, 2002.
- VIEIRA, Eduardo – *Os Bastidores da Internet no Brasil*, Barueri, Manole, 2003.

ARTIGOS E TESES

- BOUISSOU, Francisco Victor – Contratos Internacionais e Domésticos na Internet, Correio Braziliense, coluna Direito & Justiça, 13 de Novembro de 2000.

- Tese de Mestrado, BOUISSOU, Francisco Victor – A Formação dos Contratos Internacionais e a Convenção de Viena de 1980: perspectiva de ratificação pelo Brasil. Rio de Janeiro, 1996.

SITES CONSULTADOS

- http://www.e-commerce.org.br
- http://www.certisign.com.br/companhia/icp_brasil.jsp
- http://www.americanas.com
- http://www.submarino.com
- http://www.amazon.com
- http://www.thawte.com
- http://www.verising.com