

INTERNET E COMÉRCIO ELETRÔNICO UMA VISÃO GERAL

Wilson M. Yonezawa^(*)

Sidnei Bergamaschi^(**)

RESUMO

A prática de atividades comerciais na Internet vem crescendo em ritmo acelerado e despertando o interesse nos mais diversos segmentos. A perspectiva de atingir um grande volume de usuários, trabalhar com custos significativamente menores e ainda utilizar uma forma de comunicação ainda pouco convencional, são características que colocam este assunto em destaque.

O objetivo deste trabalho é apresentar as questões básicas relacionadas ao comércio eletrônico na Internet, tais como os fundamentos do Comércio Eletrônico, sua expansão, a questão da segurança e privacidade e os métodos de pagamento eletrônico.

(*) Doutorando do Programa de Pós-Graduação em Administração da Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo. Professor do Departamento de Computação da UNESP-Bauru. Mestre e graduado em Ciências da Computação pela UNESP-Bauru. E-mail: yonezawa@dco.bauru.unesp.br.

(**) Mestrando do Programa de Pós-Graduação em Administração da Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo. Professor da Universidade do Sagrado Coração - Bauru. Bacharel em Ciências da Computação pela UNESP-Bauru. E-mail: gamaschi@usp.br.

INTRODUÇÃO

O cenário mundial vem passando por grandes transformações nos últimos anos, em diversos aspectos, mais especificamente no que se refere aos aspectos de mercados globais, surgimento de novos mercados e disseminação de informações.

O fator tecnologia tem estado presente a todo momento, como um dos elementos que possibilita e favorece esse processo, atuando como elemento de difusão, disseminação e compartilhamento de informações, de maneira e velocidade não possíveis até então, atingindo as mais diversas partes do planeta. Segundo Drucker (1993) “não existem mais fronteiras nacionais para a informação” (p. 105).

Hoje, o mercado global é caracterizado por agilidade e transformação. Essa é uma era, segundo Odenwald e Matheny (1996), em que a informação é comunicada e o trabalho é conduzido sobre fronteiras, culturas, companhias, indústrias, lugares e funções com novas demandas emergentes em relação a trabalhadores e corporações em todo o mundo.

O que estamos vivendo, segundo Negroponte (1995) “é uma era da pós-informação, com menor significância do espaço e do tempo, e com um público constituído, cada vez mais, de uma única pessoa” (p.157). Ou seja, além da informação ultrapassar as barreiras e fronteiras físicas ao redor do mundo, estar disponível 24 horas por dia, ela ainda passa a ser extremamente personalizada, adequada às necessidades de cada indivíduo.

Neste contexto, os mais diversos aspectos da atividade humana são e serão afetados, desde comunicação pessoal, surgimento de novas atividades até a alteração na forma como os negócios são feitos. O objetivo deste trabalho é fornecer uma visão geral sobre algumas questões relacionadas com a prática de Comércio Eletrônico através da Internet.

A Internet

O surgimento e disseminação da Internet, a rede mundial de computadores, tem sido um dos pilares tecnológicos para a sustentação de todo este processo. A Internet está presente em mais de 150 países e, apesar da não exatidão dos

dados a seu respeito, estima-se que atinja atualmente mais de 150 milhões de pessoas. A partir de julho de 1995, já haviam mais de 6 milhões de computadores ligados permanentemente na rede, com um índice de crescimento anual de 100% (Lynch & Lundquist, 1996, p.7)

A definição dada pelo FNC (Federal Networking Council) para a Internet é a seguinte:

“Internet” refere-se ao sistema de informações globais que – (i) é logicamente conectado entre si por um espaço de endereçamento global único baseado no Protocolo Internet (IP) ou suas subseqüentes extensões/prosseguimentos; (ii) é capaz de fornecer comunicações usando o conjunto Protocolo de Transmissão e Controle/Protocolo Internet (TCP/IP) ou suas subseqüentes extensões/prosseguimentos, e/ou outro protocolo IP-compatível; e (iii) fornece, usa ou torna acessível, tanto de forma pública ou privada, serviços de alto nível baseados em comunicações e na referida infra-estrutura descrita acima. (Leiner et al., 1997)

A Internet sofreu, desde seu surgimento, uma grande mudança, seja em sua velocidade e amplitude, seja nos recursos e serviços disponíveis, em pouco mais de 20 anos. Ela é, hoje, um elemento fundamental para a criação da superestrada de informações (*information highway*) é defendida pelo próprio presidente dos EUA, Bill Clinton e o seu vice, Al Gore, quando a consideram nada menos do que uma “ferramenta fundamental para manter os Estados Unidos competitivos em termos econômicos, educacionais e de saúde pública” (Sullivan-Trainor, 1995, p. 56)

As origens da evolução da Internet podem ser observadas por vários ângulos, quer seja da evolução tecnológica na área de redes e telecomunicações, quer nos serviços disponíveis através da rede e do seu próprio gerenciamento, quer ainda de seu impacto na sociedade. Em linhas gerais, a evolução da Internet pode ser observada a partir de alguns fatos importantes que marcaram sua formação.

A Internet não surgiu repentinamente, na forma como é conhecida atualmente, mas passou por um processo de evolução a partir dos trabalhos de muitos pesquisadores e instituições, que foram desenvolvendo e moldando-a. Os primeiros textos envolvendo os conceitos que permitiriam o surgimento da Internet reportam a 1961, com o artigo de Leonard Kleinrock, do Instituto de Tecnologia de Massachussetes (MIT) (Leiner *et al.*, 1997), sobre sua teoria de comutação de pacotes, que permitiria a comunicação entre computadores utilizando pacotes de dados ao invés de circuitos. Isso viria a ser o primeiro passo importante na tecnologia da comunicação de redes.

De 1962 a 1966, J.C.R. Licklider e Lawrence G. Roberts, trabalharam juntos na Agência de Pesquisa Avançada em Projetos de Defesa (DARPA¹), órgão do Departamento de Defesa dos EUA, no conceito de redes de computadores e produziram um projeto para a criação de uma rede chamada ARPANet, que foi apresentado em 1967. Outros dois trabalhos sobre o assunto também foram apresentados na época: o primeiro deles por Paul Baran, da RAND Corporation, e o segundo pelos ingleses Donald Davies e Roger Santlebury, do PNL. (Leiner *et al.*, 1997)

O Departamento de Defesa tinha particular interesse em uma tecnologia de rede de computadores que operasse de forma não hierárquica, pois, durante o período da chamada Guerra Fria era grande a preocupação com ataques nucleares que pudessem destruir centros de controle e comando. Dessa forma, buscavam-se formas de comunicação que continuassem a funcionar e permitir troca de informações mesmo com alguns nós da rede eventualmente destruídos. Em 1968, tiveram início os trabalhos para desenvolvimento da ARPANet com o trabalho dividido em diversos grupos para os vários aspectos da implementação da rede. (Banta, 1996, p. 62)

Em setembro de 1969, o primeiro computador foi conectado e estava instalado o primeiro nó da rede, na Universidade da Califórnia Los Angeles (UCLA). O segundo foi instalado um mês após no Instituto de Pesquisa Stanford (SRI), quando a primeira mensagem trafegou pela rede entre dois computadores. Em seguida foram adicionados os nós na Universidade da Califórnia em Santa Bárbara (UCSB) e na Universidade de Utah. No final de 1969, estavam conectados 4 *hosts*, formando o início da ARPANet. (Lynch & Lundquist, 1996, p. 5)

Em meados de 1973, a ARPA identificou a necessidade de melhorar e padronizar a forma de comunicação entre os computadores da rede, e Bob Khan e Vint Cerf, de Stanford, iniciaram o desenvolvimento de um novo protocolo chamado Protocolo de Controle de Transmissão/Protocolo Internet (TCP/IP), que permitiria que diferentes redes de computadores se comunicassem, através de uma arquitetura aberta. A idéia geral era de uma rede não voltada para uma única e exclusiva aplicação, mas de uma estrutura de permitisse que novas aplicações fossem desenvolvidas. (Banta, 1996, p. 62; Leiner *et al.*, 1997)

Durante a década de 80, ocorreu um crescimento progressivo da rede com a entrada de novas instituições, provocando problemas em seu uso e gerenciamento. Este fato levou ao desenvolvimento do Sistema de Nomes de Domínios (DNS), que permite que os endereços dos computadores da rede sejam convertidos em nomes, como por exemplo, www.usp.br. Como o Departamento de Defesa vinha manifestando uma grande preocupação, por questões de segurança nacional, em razão do aumento das mais diferentes organizações na rede, com a padronização com o TCP/IP pode ser criada uma solução para este problema, com a separação da ARPANet em duas redes distintas: a ARPANet, para fins de pesquisa e a MilNet, para uso operacional do governo. (Banta, 1996, p. 62; Leiner *et al.*, 1997)

Com a utilização da MilNet para fins exclusivamente governamentais, o Departamento de Defesa passou, em 1986, a administração da ARPANet para a Fundação Nacional pela Ciência (NSF), que transformou a antiga ARPANet em uma rede de alta velocidade,

¹ A ARPA (Advanced Research Projects Agency) mudou seu nome para DARPA (Defense Advanced Research Projects Agency) em 1971, voltou para ARPA em 1993 e novamente para DARPA em 1996. Esse texto utiliza seu nome atual.

São muitas as diferenças entre os números da Internet, também os que dizem respeito a sua demografia. Hoffman, Kalsbeek e Novak desenvolveram uma pesquisa sobre a demografia na Internet após a constatação das enormes divergências entre as informações divulgadas sobre a demografia na Internet. Essas diferenças podem ser mostradas nos resultados de pesquisa obtidos para, por exemplo, o número de pessoas maiores de 16 anos que usam a Internet, nos EUA e Canadá. Segundo a Nielsen são 37 milhões; para O'Reilly & Associates são 5,8 milhões; para a FIND/SVP são 8,4 milhões; já para o Times Mirror são 25 milhões. (1996, p.37)

Segundo esses autores essas diferenças dizem respeito, além do viés de pesquisa normalmente existente, principalmente aos diversos empregos do conceito “uso da Internet”. Em trabalho desenvolvido por eles os resultados apontaram um número de 28,8 milhões de indivíduos, maiores de 16 anos, nos EUA com acesso à Internet, sendo que destes, 16,4 milhões usam a Internet; 11,5 milhões usam a Web e 1,5 milhões já utilizaram a Web para comprar alguma coisa. (Hoffman et ali, 1996, p.43). Entretanto, o que se sabe, com certeza, é que o número de “usuários” da Internet é grande e cresce rapidamente.

Comércio Eletrônico

De acordo com dados da Organização Mundial do Comércio (OMC), somente 30 países movimentam anualmente 10 trilhões de dólares, o que representa 88.5% (5,25 trilhões de dólares) e 82.5% (5,39 trilhões de dólares) de todas as exportações e importações mundiais, respectivamente. Desse montante, o comércio por meio eletrônicos (TV, telefone, Fax, Internet, etc), movimenta, apenas, entre 4,5% e 5%. Entretanto, a OMC estima um crescimento para 16% a 17% do total., o que representa um movimento de 1,6 e 1,7 trilhões de dólares anuais, ou seja, um crescimento de quase 400%.

Nos últimos 500 anos, o comércio passou do comércio da era colonial para o comércio da era industrial. Atualmente, observamos a passagem do comércio da era dos blocos econômicos para o comércio da era da informação, e é neste cenário que surge o Comércio Eletrônico.

Comércio Eletrônico é um conjunto de transações comerciais conduzidas através do uso de computadores e redes de telecomunicações. As transações podem ocorrer entre empresas ou entre empresas e seus consumidores na forma de compra e venda, assistência técnica ou divulgação de produtos e/ou serviços. Existem, basicamente três classes de aplicações em Comércio Eletrônico:

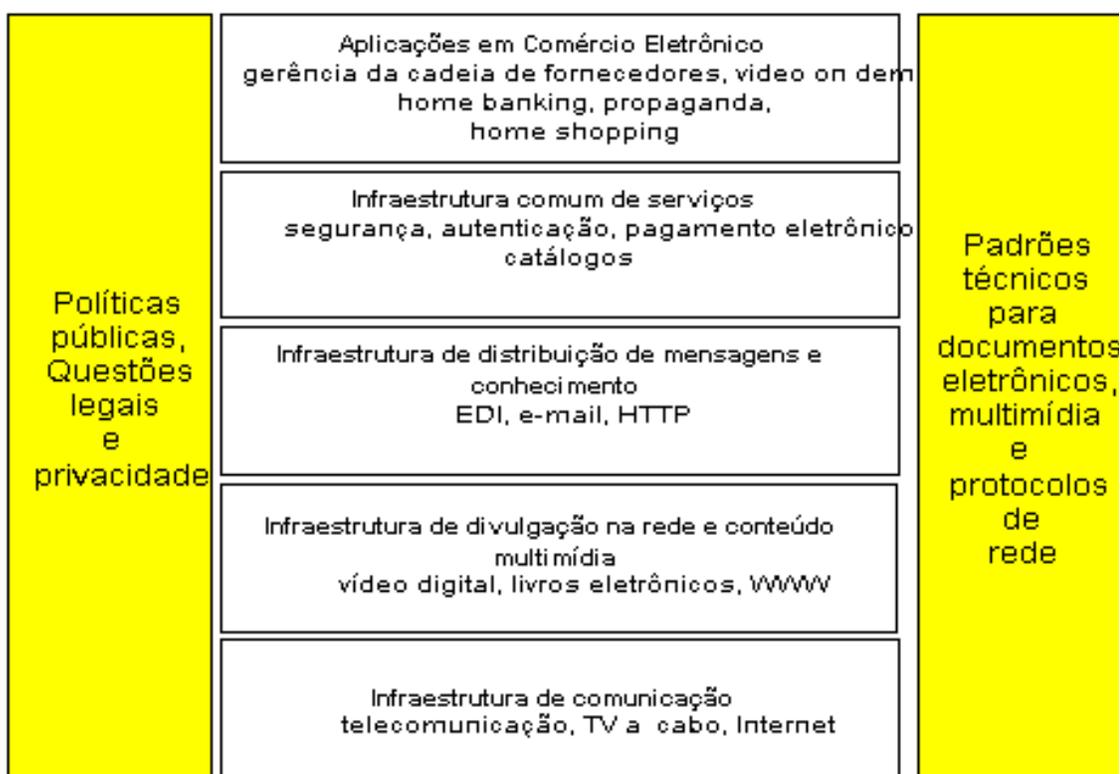
- a) Transação “*Customer-to-Business*” ou transações entre o cliente e empresa. Os exemplos mais comuns nessa classe são as aplicações de compra *on-line* na Internet ou mesmo aplicações de *home banking*. Nesse tipo de aplicação a empresa oferece os produtos/serviços diretamente aos clientes por meio da tecnologia da informação.
- b) Transação “*Business-to-Business*” ou transações entre empresas. Nesta classe de aplicações as transações comerciais entre empresas são conduzidas eletronicamente, utilizando-se de um protocolo comum. O protocolo mais comum para troca de informações comerciais entre empresas é o EDI (Electronic Data Interchange).
- c) Transação “*Intra-organizacional*”. Aplicações nesta classe caracterizam-se pela divulgação/promoção de informações dentro da organização, por meio de redes Intranet ou Extranet – ou seja, redes com características da Internet, mas com âmbito reduzido.

As principais vantagens na adoção do Comércio Eletrônico são: a melhoria dos processos de negócio; a redução dos custos de operação; a redução de papel; e a possibilidade de se explorar novos mercados. Como exemplo da redução de custo, o Quadro 1 mostra os custos de uma transação bancária com a utilização de três diferentes tecnologias.

Transações bancária	Custo por transação
No caixa	\$2 a 3 R\$ 2,30 a R\$ 3.50
ATM	35 a 45 cents R\$ 0,70
Internet	2 a 3 cents R\$ 0,08 a R\$ 0,13

Quadro 1 - Custo da Transação Bancária

O Quadro 2 apresenta o Modelo de Kalakota (1996), com os principais elementos que compõe o cenário do Comércio Eletrônico. Este modelo é baseado em níveis de serviços (também conhecido como Modelo de Camadas). Cada nível de serviço oferece ao nível superior uma infra-estrutura de apoio. As aplicações de Comércio Eletrônico representam o mais alto nível de serviço. O nível mais baixo representa a infra-estrutura de comunicação existentes. Essa infra-estrutura oferece os serviços básicos de transmissão e recepção de dados. Esse nível depende das tecnologias de telecomunicações existentes.



Quadro 2 - Infra-Estrutura do Comércio Eletrônico

Fonte: Kalakota (1996, p. 4)

Os níveis intermediários entre a infra-estrutura básica de comunicação e as aplicações de Comércio Eletrônico representam os mais diferentes veículos de transporte para as aplicações ou os serviços adicionais para as aplicações. Por exemplo, uma aplicação de Comércio Eletrônico pode divulgar informações utilizando vídeo digital ou a World Wide Web (WWW), que é a arquitetura de divulgação mais conhecida e utilizada no momento.

Vídeo digital ou WWW são tecnologias suportadas pela infra-estrutura de divulgação na rede e conteúdo multimídia. Essa camada fornece mecanismos para especificar o conhecimento relacionado aos produtos e um meio para comunicá-los aos usuários.

O nível imediatamente superior à infra-estrutura de divulgação na rede e conteúdo multimídia oferece os serviços de distribuição de mensagens. Os serviços de distribuição são formas padronizadas para troca de dados. Os

meios mais conhecidos são EDI (Electronic Data Interchange) e e-mail (correio eletrônico). Essa camada inclui os vários significados para envio e recuperação do conhecimento. Os serviços de mensagem oferecem soluções para troca de dados formatados e não formatados. Dados não formatados são documentos do tipo carta, memorando ou relatórios. Dados formatados são documentos do tipo fatura, pedido, nota fiscal.

O nível imediatamente inferior ao nível de aplicação é a infra-estrutura de segurança. Essa camada garante segurança para o conteúdo das informações e inclui vários métodos para facilitar os processos de negócio *on-line*, tais como, compra, venda e mecanismos de transferência eletrônica de fundos. O nível de segurança oferece os serviços de identificação e autenticação de informações envolvidas em uma transação.

No modelo de Kalakota o funcionamento de todos os serviços depende, basicamente, de dois pontos: as questões legais e questões sobre privacidade; e padrões técnicos para os documentos eletrônicos e redes de computadores.

O comércio eletrônico tornou-se viável graças à evolução da tecnologia da informação e a Internet é o campo atualmente mais explorado. A Internet está se consolidando, cada vez mais, como a base para o Comércio Eletrônico, se tornando rapidamente a maior infra-estrutura de multimídia interativa, e que deverá, em um futuro próximo, ameaçar algumas mídias tradicionais.

Muitas empresas estão descobrindo este potencial da Internet para negócios, utilizando-a em diferentes atividades ligadas ao seu negócio, como por exemplo, propaganda, venda, assistência técnica e outros. Estima-se que os gastos com publicidade na Internet foram de US\$ 220 milhões em 1996 e devem atingir US\$ 2.2 bilhões até o ano 2000, o que demonstra o quanto as empresas estão investindo, e esperam investir, nesse segmento (Murphy, 1997, p. 8).

Também no Brasil diversas empresas têm iniciado atividades na Internet, atentando para as possibilidades que a mesma oferece. Após a liberação da Internet no Brasil, em 1995 -

anteriormente ela somente estava disponível para universidades e instituições de pesquisa - o número de usuários vem crescendo 30% ao mês, com um potencial estimado de 5 milhões de usuários (Martins, 1996, p. 27).

Segundo o instituto de pesquisas americano Yankee Group, “no ano 2000 o volume de negócios gerado com transações, usando a Internet, alcançará a cifra de US\$ 144 bilhões por ano” (“O EDI se integra a teia mundial”, p. 22).



Figura 2 - Produtos/Serviços Comprados On-Line

Fonte: www.e-land.com (14/05/98)

De acordo com a empresa eMarketer os produto/serviço comercializados *on-line* são:

- Os que possuem maior valor agregado para os serviços *on-line*, isto é, disponibilidade de informações e de fácil entendimento para o comprador.
- Sejam de fácil transação, isto é, a decisão de compra não seja complexa.

No seu estágio atual, a Internet ainda pode não ser um concorrente ao varejo - ou outra forma de comércio tradicional - mas o que chama atenção é a rapidez de seu crescimento e as novas possibilidades de relacionamento e marketing criadas pela mesma. O gráfico, a seguir, mostra o aumento da representatividade que espera-se do Comércio Eletrônico até o ano 2005.

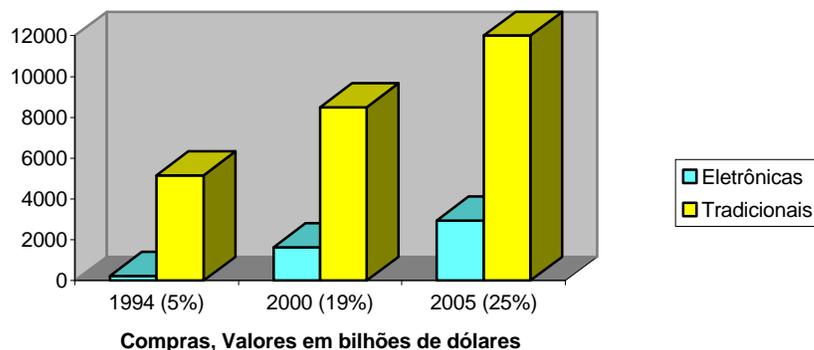


Figura 3 - Previsão de Vendas do Varejo Tradicional em Relação ao Comércio Eletrônico

Fonte: Lynch & Lundquist, p.2

A Internet, e conseqüentemente sua utilização comercial, vem se expandindo muito mais depressa que outros meios de comunicação tinham feito até então. Segundo o U.S. Investment Research Report, da empresa de consultoria Morgan Stanley, nos EUA, para

atingir 50 milhões de usuários o rádio levou 38 anos, a TV 13 anos e a TV a cabo, 10 anos. Acredita-se que a Internet o fará em apenas 5 anos. A curva, abaixo, demonstra esta comparação.

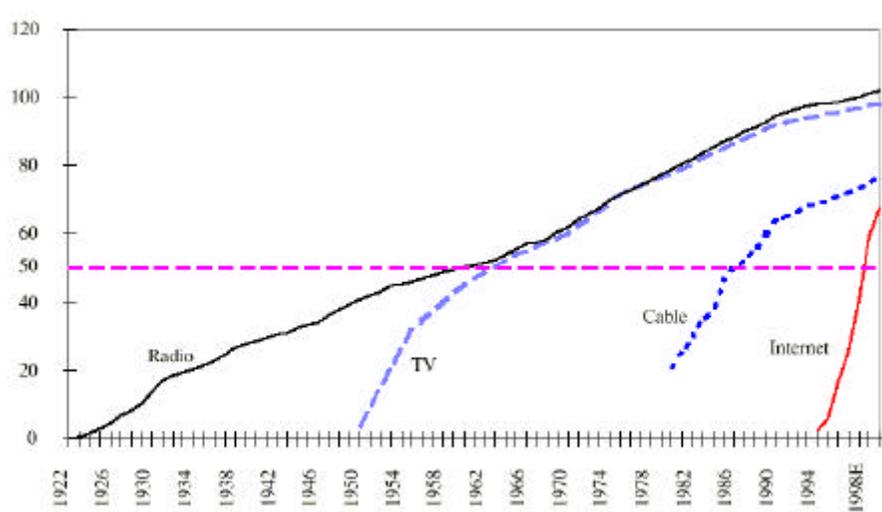


Figura 4 - Curva da Adoção de Diversas Mídias

Fonte: Morgan Stanley, U.S. Investment Research Report (1997, p.2-2)

Segurança em Comércio Eletrônico

Em qualquer tipo de transação comercial a questão segurança é um ponto essencial. A criptografia é uma das técnicas usadas para garantir segurança nas transações eletrônicas. Dois são os processos básicos da criptografia:

criptografar e “descriptografar”. Criptografar significa disfarçar uma mensagem de modo a ocultar o seu conteúdo; enquanto que “descriptografar” significa recuperar o conteúdo de uma mensagem criptografada.

Os sistemas criptográficos são muitas vezes classificados entre fortes e fracos. A força de um

sistema criptográfico é expressa em cinco princípios básicos (Lynch & Lundquist, 1996, p. 57): identificação (verifica se o remetente da mensagem é realmente quem diz ser), autenticação (verifica o remetente e se o texto da mensagem não sofreu alteração), impedimento da rejeição (diz respeito à qualidade do sistema que evita que alguém possa negar ter enviado certos dados, quando de fato o tenha feito), verificação (identifica e autentica, com segurança, uma comunicação criptografada específica) e privacidade (capacidade do sistema de ocultar efetivamente a comunicação dos outros não envolvidos no processo).

Tradicionalmente, utiliza-se o conceito de chave secreta, também conhecida como criptografia simétrica na criptografia, isto é, o remetente e o destinatário conhecem e usam uma mesma chave secreta para a codificar e decodificar mensagem, respectivamente. O principal problema neste caso, é conseguir que o remetente e o destinatário concorram com uma chave sem que ninguém mais a descubra. A questão aqui é que ambos precisam confiar no mensageiro para receber ou trocar as chaves. Neste caso, alguém mais pode interceptar o mensageiro e descobrir a chave (Lynch & Lundquist, 1996, p. 60). A criptografia por chave pública é a outra alternativa.

O conceito de chave pública foi introduzido em 1976 por Whitfield Diffie e Martin Hellman para resolver o problema de gerenciamento de chaves. Neste novo conceito, cada pessoa recebe um par de chaves, uma chamada de chave pública e a outra de chave privada. A chave pública é publicada, enquanto a chave privada é mantida em segredo, com isso, a necessidade do remetente e do destinatário em compartilhar informações secretas é eliminada. Toda comunicação envolve apenas chaves públicas, as chaves privadas nunca são transmitidas ou compartilhadas. Não mais é necessário confiar na segurança do canal contra escutas (RSA Laboratories, 1998).

O DES (Data Encryption Standard) é o método mais conhecido de criptografia por chave privada e o RSA (RSA Laboratories) o mais conhecido para criptografia de chave pública.

O DES foi aprovado, como padrão pelo governo americano, em 1977. Sua segurança se

baseia no segredo da chave usada para criptografar a mensagem. O DES é baseado em um algoritmo desenvolvido, na IBM, na década de 70.

Já o RSA é um sistema criptográfico baseado em chave pública, desenvolvido em 1977, por Ron Rivest, Adi Shamir e Leonard Adleman para cifrar e autenticar. Ele funciona da seguinte forma: cada usuário precisa de um par de chaves formado por dois grandes números primos, p e q . Dados p e q , descubra o seu produto n que é chamado de módulo. Escolha um número e , menor que n é primo de $(p-1)(q-1)$, isto é, ele não possui fatores comuns entre eles. Depois descubra o inverso de e , chame-o de d , $mod (p-1)(q-1)$ de modo que $ed = 1 mod (p-1)(q-1)$. O par (n, e) torna-se a chave pública, e a chave privada é d . Os dois grandes números primos p e q devem ser mantidos em segredo ou então destruídos.

Muitos órgãos de padrões (ANSI, ITU, Internet PEM e PKCS) têm desenvolvidos padrões na área da criptografia com chave pública, tais como: ANSI X9.F1, ITU X.500 e Internet PEM RFC 1421). Outros algoritmos importantes de criptografia são PGP (Pretty Good Privacy) de domínio público, o IDEA (International Data Encryption Algorithm), MD5, Capstone, Clipper, Skipjack e DSA (Digital Signature Algorithm).

Os sistemas de criptografia podem e devem ser incorporados às aplicações de Comércio Eletrônico, pois tratando-se de uma transação comercial, mais do que o sigilo, a segurança da mesma é essencial. Somente com transações seguras o Comércio Eletrônico pode garantir aos seus usuários tranquilidade em sua utilização.

Existem no mercado diversos produtos para segurança de dados na Internet. Em geral, a segurança na Internet segue o modelo cliente/servidor, isto é, uma parte do mecanismo de segurança fica na aplicação do cliente e a outra no servidor. Do lado do cliente, a segurança está incorporada ao programa navegador (*browser*), do tipo Netscape ou Internet Explorer. No servidor a segurança está incorporada ao *software* que controla os acessos às páginas Web do *site*.

Um dos padrões mais conhecidos de segurança e privacidade na Internet é o SSL (Secure Socket Layer). O SSL é um programa

incorporado ao navegador que garante a segurança das mensagens transmitidas na rede. O SSL utiliza o sistema de criptografia de chave pública-privativa da RSA Laboratories. O SSL representa a camada do serviço de segurança para serviços Internet (WWW, FTP –

transferência de arquivos e correio eletrônico), conforme mostra a Figura 5.

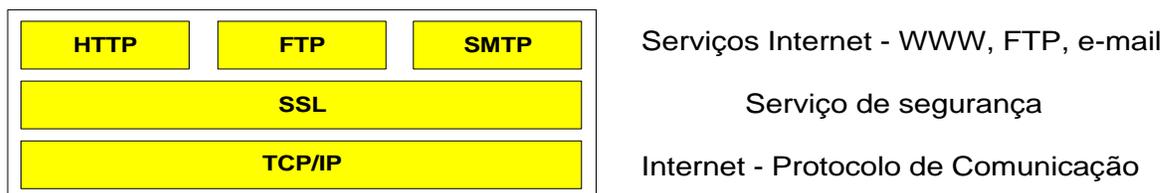


Figura 5 - Protocolo de Segurança SSL e a Internet”

Fonte: Adaptado de Bhimani, 1996, p. 31

Outro protocolo de segurança na Internet é o S-HTTP (Secure Hypertext Transfert Protocol). O S-HTTP é uma extensão do HTTP (Hypertext Transfer Protocol), e foi projetado para oferecer confiabilidade, autenticidade, integridade enquanto suporta mecanismo de gerenciamento de chaves múltiplas e algoritmos de criptografia, via opções de negociações entre as partes envolvidas na transação.

prestam serviços financeiros, uma vez que o número de compras com cartão de crédito na Internet está crescendo; diversos bancos estão planejando oferecer autorização de cartão diretamente na Internet; e diversas empresas estão testando métodos de pagamento eletrônicos com moedas ou dinheiro eletrônico (SET Secure Electronic Transaction LLC, 1998).

Sistema de Pagamento Eletrônico

O crescimento dos negócios que envolvem o Comércio Eletrônico afetarão as empresas que

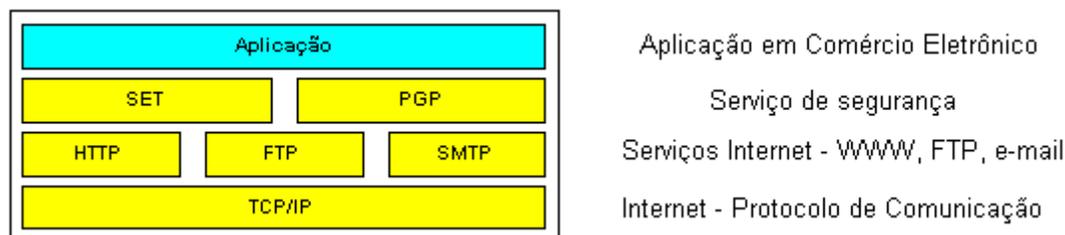


Figura 6 - Protocolo de segurança SET e a Internet”

Fonte: Adaptado de Bhimani, 1996, p. 31

Um sistema de pagamento eletrônico deve oferecer confidencialidade na transmissão; autenticar as partes envolvidas; assegurar a

integridade do pagamento e autenticar a identidade do comprador e do vendedor para ambos.

Duas foram as principais iniciativas para criação de sistemas de pagamento eletrônico: o SEPP (Secure Electronic Payment Protocol) desenvolvidas pela Mastercard, IBM e Netscape; e o STT (Secure Transaction Technology) promovida pela Visa e Microsoft.

Em 1996, a Mastercard International e a Visa anunciaram o desenvolvimento de um padrão técnico simples de proteção de compras com cartão de crédito em redes abertas. O padrão foi chamado de SET (Secure Electronic Transaction). A especificação do SET inclui: certificados digitais que são formas de verificação de informações do proprietário do cartão no ato da compra; meios seguros para instituições financeiras, vendedores e

comerciantes de obter mais do emergente mercado do comércio eletrônico. O SET oferece confidencialidade, integridade na transação e diminui a oportunidade de fraude em todos os pontos da transação. O processo envolve uma série de verificações de segurança por meio de certificados digitais que são emitidos aos participantes.

Atualmente, diversas empresas oferecem serviços relacionados a pagamento eletrônico na Internet. Os serviços oferecidos variam de compras com cartão de crédito até o oferecimento de transações envolvendo alguma forma de dinheiro digital. O quadro abaixo mostra algumas empresas e seus serviços:

Empresa	Principal Cliente	Serviço Diferencial
Checkfree	Consumidores	Pagamento de Contas
Cybercash	Bancos	Transações comerciais e bancárias
Digicash	Consumidores	Anonimato
First Virtual	Empresas de Informações	Microtransações para vendas de informações
OMI	Negócios	Vitrines seguras

Quadro 3 - Empresas e serviços de pagamento eletrônico

Fonte: Lynch e Lundquist (1996, p. 31)

CONCLUSÃO

O desenvolvimento da Internet foi, sem dúvida, uma das maiores mudanças na área de Tecnologia dos últimos anos. Porém, seu maior impacto diz respeito às alterações que ela provocou nos mais diversos meios, surgindo como uma nova forma de comunicação e criando grandes expectativas em relação ao seu futuro. No ambiente econômico, acima de tudo, a presença da Internet promoveu mudanças substanciais, desde a forma para se relacionar com clientes e consumidores até a sua utilização para transações bancárias e comerciais.

A padronização de comunicação gerada pela Internet – independente do *hardware* ou *software* utilizado – foi um grande avanço, pois o intercâmbio de informações é conseguido graças à padronização da forma de transporte dos dados, no caso o protocolo TCP/IP, que representa a verdadeira base da sua estrutura de comunicação. Além desta base, estão construídos e definidos alguns serviços básicos, como o WWW (World Wide Web) via protocolo

HTTP, a transferência de arquivos via FTP (File Transfer Protocol) e o envio de mensagens (correio eletrônico), que permitiram o surgimento de diversas tecnologias e propostas para novos serviços. É exatamente neste campo que proliferam as idéias sobre o Comércio Eletrônico.

Entender os conceitos e a estrutura do Comércio Eletrônico na Internet é o primeiro passo no desenvolvimento de aplicações que envolvem compra e venda nas redes abertas. Embora nenhuma empresa ou padrão de serviço de segurança tenha sido adotado amplamente, é possível identificar os sinais no horizonte para se preparar para o que está por vir.

BIBLIOGRAFIA

Answer to Frequently Asked Questions About Today's Cryptograph, [on-line] <http://www.rsa.com/rsalabs/newfaq/>, - versão 3.0, [site] *RSA Laboratories*, em 20/07/98.

- BANTA**, Glen. *Internet pipe schemes: the evolution of Internet bandwidth*. *Internet World*, v. 8, n. 10, p. 62-70, Oct. 1996.
- BHIMANI**, Anish. Securing The Commercial Internet. *Communications of the ACM*, vol. 39, nº 6, p. 29-35, June, 1996.
- DRUCKER**, P.F. *Sociedade pós-capitalista*. 5ª ed. Tradução de Nivaldo Montigelli Jr. São Paulo: Pioneira, 1993.
- EDI se integra à teia mundial*. *LanTimes Brasil*, vol. 3, ed. 9, p. 22-23, 25/08/97.
- HAMILTON**, Scott. E-Commerce for the 21-st Century. *IEEE Computer*, vol.30, nº 5, p. 44-47, May, 1997.
- HOFFMAN**, Donna L., **KALSBECK**, William D., **NOVAK**, Thomas P.. *Internet and Web use in the US*. *Communications of the ACM*, vol. 39, nº 11, p. 36-46, December 1996.
- KALAKOTA**, Ravi, **WHISTON**, Andrew B. *Frontiers of Electronic Commerce*. New York: Addison-Wesley, 1996.
- KANBIL**, Ajit. Doing Business in the Wired World. *IEEE Computer*, vol.30, nº 5, p. 56-61, May, 1997.
- KROL**, Ed. *The whole Internet guide user's guide*. 2. ed. Sebastopol, CA: O'Reilly & Associates, 1995.
- LINER**, Barry M., **CERF**, Vinton G., **CLARK**, David D., **KAHN**, Robert, E., **KLEINROCK**, Leonard, **LYNCH**, Daniel C., **POSTEL**, Jon, **ROBERTS**, Larry G., & **WOLFF**, Stephen. *A brief history of the Internet*. [on-line] <http://www.isoc.org/internet-history>, versão 3.1, de 20/02/97, [site] *The Internet Society*, em 24/08/97.
- LYNCH**, Daniel C. & **LUNDQUIST**, Leslie. *Dinheiro digital - O comércio na Internet*. Rio de Janeiro: Campus, 1996, 251 p. Traduzido por Follow-Up Traduções e Assessoria de Informática.
- MARTINS**, I. O império da rede. *Exame*. Ano 29, Nº 2, 17-Jan-1996, pp. 24-30.
- MURPHY**, K. Calculando o potencial da publicidade na Web. *Web Week*. Vol. 1, Nº 8, mar/1997, p.8.
- NEGROPONTE**, N. *A vida digital*. 2ª ed. Tradução de Sérgio Tellaroli. São Paulo: Companhia das Letras, 1995.
- ODENWALD**, S.B. & **MATHENY**, W.G. *Global Impact*. New York: Irwin Professional Publishing, 1996.
- SET** *Secure Electronic Transaction Specification – Book 1: Business Specification*. [on-line] http://www.setco.org/set_specifications.html, versão 1 , de 31/05/97, [site] SET Secure Electronic Transaction LLC, em 20/07/98.
- SULLIVAN-TRAINOR**, Michael. *Information superhighway: toda a verdade sobre a super-rodovia da informação*. Tradução de Lenke Peres Alves de Araújo. São Paulo: Makron Books, 1995, 289 p. Do original: *The Truth about the Information Superhighway*.
- U.S. INVESTMENT RESEARCH REPORT**. Morgan Stanley. New York, May, 28, 1997.
- What's selling on-line – an overview*. [on-line] <http://www.e-land.com/estats/welcome.html>, [site] eMarketer, 1997.