COMÉRCIO ELETRÔNICO: SEUS ASPECTOS DE SEGURANÇA E PRIVACIDADE

Alberto Luiz Albertin
Professor do Departamento de Informática e Métodos Quantitativos da EAESP/FGV.
E-mail: albertin@eaesp.fgvsp.br

Rosa Maria de Moura
Aluna de pós-graduação na EAESP/FGV.

RESUMO: O comércio eletrônico, com suas aplicações inovadoras e revolucionárias, é tido como uma das tendências emergentes com maior poder potencial de inovação nos processos de negócio nos vários setores econômicos. Com a crescente utilização de comércio eletrônico, inclusive Internet, ficam cada vez mais críticos os aspectos de segurança e privacidade das informações que estão sendo utilizadas. Além disto, esses aspectos interferem significativamente na adoção dessa tecnologia. O artigo visa a apresentar estudos sobre os aspectos de segurança e privacidade, bem como a analisar o problema da resistência e as estratégias adotadas para a sua superação.

ABSTRACT: *The electronic commerce, with its innovative applications, is considered as one of the major emergent trends with the biggest contribution to the business processes, for all industries. With the crescent use of electronic commerce, including Internet, the aspect of security and privacy of information becomes critical. These aspects affect directly the adoption of this technology. The article has the objective to present studies about the aspects of security and privacy, as well as to discuss the problem of resistance and the strategy to overcome it.*

PALAVRAS-CHAVE: comércio eletrônico, segurança, privacidade.

KEY WORDS: *electronical commerce, security, privacy.*

O ambiente tradicional de negócio está evoluindo rapidamente, com consumidores e negócios procurando flexibilidade para mudar parceiros, plataformas, carreiras e redes. Muitas companhias estão olhando para fora de suas organizações quando estão elaborando suas estratégias de negócios. Essas atividades incluem estabelecer conexões eletrônicas privadas com clientes, fornecedores, distribuidores, grupos de indústria e mesmo com concorrentes. Estas conexões, caracterizadas como comércio eletrônico, visam incrementar a eficiência das comunicações de negócio, expandir a participação no mercado e manter a viabilidade de longo prazo no ambiente de negócio atual.

As aplicações de comércio eletrônico são muito variadas. Na sua forma mais comum, o comércio eletrônico também é utilizado para caracterizar a troca, sem papel, de informação de negócio, utilizando troca eletrônica de dados (*electronic data interchange – EDI*), correio eletrônico, *bulletin boards* eletrônicos, transferência eletrônica de fundos e outras tecnologias similares. Estas tecnologias são normalmente aplicadas em áreas de alto retorno, reconhecendo que as atividades de manipulação de papel usualmente aumentam as despesas sem adicionar valor.[1]

Por outro lado, o termo comércio eletrônico é utilizado para descrever um novo enfoque *on-line* para desempenhar funções tradicionais, tais como pagamentos e transferência de fundos, entrada e processamento de pedidos, faturamento, gerenciamento de estoque, acompanhamento de carga, catálogos eletrônicos e coleta de dados de ponto-de-venda. Mais recentemente, as companhias têm percebido que a propaganda, *marketing* e funções de suporte a cliente também fazem parte do domínio das aplicações de comércio eletrônico. Estas funções de negócio agem como iniciadores para um ciclo de gerenciamento de pedido completo, que incorpora as noções mais estabelecidas de comércio eletrônico.

Nesse ambiente, a utilização comercial da Internet tem um potencial ainda incalculável; entretanto, apesar da euforia geral, muitos administradores permanecem céticos. Vários artigos e outras publicações têm proclamado o valor da Internet, porém o número de compras realizadas ainda é muito baixo. Além disto, os casos, reais ou não, referentes a falta de segurança e a problemas de desempenho têm contribuído para o ceticismo.

Originalmente criada para servir como um *backbone* de comunicação nos tempos de crises nacionais, e mais tarde internacionais, e apoiar a pesquisa acadêmica nos tópicos relativos a defesa, a Internet não tem um ponto central de controle, pois, como seus criadores acreditavam, tal controle criaria um inaceitável risco de falha no sistema, no caso de um ataque hostil, desastre natural ou erro humano. Como resultado, o sistema cresceu como uma rede verdadeiramente distribuída e protocolos de rede foram desenvolvidos para criar um ambiente de sistema aberto, permitindo rotear mensagens e informações através de plataformas de rede largamente dispersas.

A adoção do comércio eletrônico ainda está associada à cultura e, principalmente, ao que esse sistema irá oferecer para que tais transações propostas, e que atualmente são realizadas de forma consolidada e conhecida, possam ser praticadas de forma segura. No momento, segundo pesquisas, uma das maiores preocupações dos executivos de TI é com relação a segurança.

SEGURANÇA NO COMÉRCIO ELETRÔNICO

Como uma das discussões atuais no ambiente de comércio eletrônico, a utilização comercial da Internet tem sido matéria de vários estudos e preocupações em várias organizações. Isto tem revelado que as empresas estão utilizando a Internet para correio eletrônico e envio e recepção de arquivos, mas ainda não estão utilizando todo o potencial da *information highway* como um meio de fazer negócios e atingir novos clientes. Uma das principais preocupações sobre essa utilização é referente aos aspectos de segurança.[2]

Os aspectos complexos de segurança, privacidade, autenticação e anonimato têm especial importância para o comércio eletrônico. Confidencialidade, confiabilidade e proteção das informações contra ameaças de segurança são um pré-requisito crítico para a funcionalidade do comércio eletrônico.[3]

Segundo pesquisas, o número de casos de violação da segurança de acesso aos compu-

1. KALAKOTA, R., WHINSTON, A. *Frontiers of electronic commerce*. New York: Addison-Wesley, 1996.

2. ALBERTIN, A. L. O comércio eletrônico na estratégia de globalização: um estudo do setor bancário privado nacional. *I Seminário de Administração* – FEA/USP, 1996.

3. KALAKOTA, R., WHINSTON, A. Op. cit.

tadores tem crescido 50% ao ano desde 1988, sendo que a maioria dos casos refere-se a violação de *e-mail* ou entrada nos computadores através dele.[4]

Ameaças de segurança

A ameaça de segurança é definida como uma circunstância, condição ou evento com potencial de causar danos em dados ou recursos de rede, na forma de destruição, exposição, modificação de dados, negação de serviço, fraude, perda ou abuso.[5]

As ameaças de segurança de mensagem podem ser divididas em três categorias:

- **Confidencialidade de mensagem:** a confidencialidade é importante para as utilizações que envolvem dados sensíveis, tais como números de cartões de crédito. Este requisito será ampliado quando outros tipos de dados, tais como registro de empregados, arquivos governamentais e números de seguro social começarem a ser tratados através da rede. A confidencialidade impede o acesso a tais informações ou a sua liberação para usuários não autorizados.
- **Integridade de mensagem e sistema:** as transações de negócio requerem que seus conteúdos permaneçam inalterados durante seu transporte. Em outras palavras, a informação recebida precisa ter o mesmo conteúdo e organização que a informação enviada. Enquanto a confidencialidade protege contra a monitoria passiva de dados, os mecanismos para integridade têm que prevenir os ataques ativos envolvendo a modificação de dados.
- **Autenticação/identificação do emissor da mensagem:** para comércio eletrônico é importante que os clientes se autentiquem para os servidores, que os servidores se autentiquem para os clientes e que ambos se autentiquem um ao outro. A autenticação é um mecanismo pelo qual o recebedor de uma transação ou mensagem pode ter certeza da identidade do emissor e/ou da integridade da mensagem. Em outras palavras, a autenticação verifica a identidade de uma entidade, um usuário ou um serviço, utilizando certas informações criptografadas transferidas do emissor para o destinatário.

A maioria das ameaças de segurança de executar *software* cliente resulta da natureza da Internet, que permite que estes programas interpretem dados carregados de servidores arbitrários. Na ausência de checagem destes dados, o risco é subverter programas rodando no sistema. As ameaças a clientes surgem, principalmente, de dados ou códigos prejudiciais, que se referem a:

- **Vírus:** um segmento de código que é replicado através da anexação de cópias de si mesmo nos executáveis existentes. A nova cópia do vírus é executada quando o usuário ativa o programa hospedeiro.
- **Cavalo de Tróia:** um programa que desempenha uma tarefa desejável mas também inclui funções inesperadas e indesejáveis.
- ***Worm*:** um programa auto-replicante que é autocontido e que não necessita de um programa hospedeiro. O programa cria uma cópia de si mesmo e causa sua execução, não requerendo a intervenção do usuário.

A ADOÇÃO DO COMÉRCIO ELETRÔNICO AINDA ESTÁ ASSOCIADA À CULTURA E, PRINCIPALMENTE, AO QUE ESTE SISTEMA IRÁ OFERECER PARA QUE AS TRANSAÇÕES PROPOSTAS, E QUE ATUALMENTE SÃO REALIZADAS DE FORMA CONSOLIDADA E CONHECIDA, POSSAM SER PRATICADAS DE FORMA SEGURA.

Uma outra ameaça de segurança que está surgindo no mundo do comércio eletrônico é o código móvel, agente de *software*, que em muitas maneiras pode ser comparado com as tradicionais ameaças de vírus. O código móvel é um programa executável que tem a habilidade de mover-se de máquina para máquina e também se invoca sem influência externa. Estas ameaças podem ser divididas em

4. MARTINS, I., GUROVITZ, H. Ilusão de privacidade. *Exame*, ano 30, n.7, março 1997.

5. KALAKOTA, R., WHINSTON, A. Op. cit.

duas categorias:

- ameaças para o ambiente computacional local de *software* móvel;
- controle de acesso e ameaças a servidores que incluem imitação, bisbilhotice, negação de serviço, substituição e modificação de pacotes.

As ameaças a servidores consistem em modificações não autorizadas de dados do servidor, bisbilhotice ou modificação não autorizada de pacotes de dados de entrada e comprometimento do sistema servidor pela disseminação de falhas no *software* e atuação dos *hackers*. Alguns exemplos:

- acesso potencial a um grande número de sistemas;
- utilização de programas *UNIX* populares, como *Finger*, *rsh* ou *rush*, para descobrir nomes de contas e então tentar adivinhar senhas simples, utilizando um dicionário ou métodos mais sofisticados;
- utilização de bisbilhotice eletrônica para capturar nomes de usuários e senhas não criptografadas enviadas pela rede;
- poder burlar, ou configurar, um sistema para mascará-lo como um outro sistema, ganhando acesso não autorizado a recursos ou informações.

As tecnologias de segurança se protegem desses riscos através dos protocolos de segurança do tipo *SSL* ou *S-HTTP*. O primeiro deles usa um grupo de regras que diz aos computadores os passos a serem seguidos para melhorar o nível de segurança das comunicações. Essas regras são:

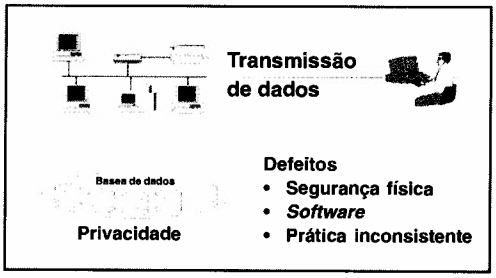
- criptografia, que protege contra espreita;
- integridade de dados, que protege contra manipulação;
- autenticação, que protege contra personificação.

Contudo, esses efeitos protegem os dados somente durante a transmissão. Ou seja, os protocolos de segurança de rede não protegem os dados antes de serem enviados ou depois de recebidos. Da mesma forma como se confia nos comerciantes em não divulgarem as informações dos cartões de crédito, deve-se confiar nos receptores dos seus dados *on-line*.

Preocupações com segurança

As preocupações com segurança no comércio eletrônico, como mostra a Figura 1, podem ser divididas em três categorias.

Figura 1 – Preocupações com segurança



1. **Segurança em cliente-servidor:** utiliza vários métodos de autorização para ter certeza de que somente os usuários e programas válidos terão acesso a recursos de informações, tais como bases de dados. Mecanismos de controle de acesso precisam ser estabelecidos para assegurar que os usuários apropriadamente autenticados terão acesso a somente aqueles recursos previamente a eles autorizados. Tais mecanismos incluem proteção de senha, cartões inteligentes criptografados, *biometrics* e *firewalls*.
2. **Segurança de dados e transmissão:** assegura a privacidade e a confidencialidade em mensagens eletrônicas e pacotes de dados, incluindo a autenticação de usuários remotos nas transações em rede para atividades, tais como pagamentos *on-line*. O objetivo é invalidar qualquer tentativa de assumir uma outra identidade quando correio eletrônico ou outras formas de comunicação de dados estão envolvidos. Medidas preventivas incluem criptografia de dados utilizando vários métodos.
3. Os problemas de segurança de rede cliente-servidor podem se manifestar de três maneiras:

- **defeitos de segurança física:** originam-se quando indivíduos ganham acesso físico não autorizado de um computador;
- **defeitos de segurança de *software*:** originam-se quando programas escritos de forma ruim ou *software* privilegiado são comprometidos em fazer coisas que eles não deveriam;
- **defeitos de prática inconsistente:** originam-se quando um administrador de sistema agrupa uma combinação de *hardware* e *software* de tal forma que o sistema é seriamente violado do ponto de vista de segurança.

As organizações têm que utilizar produ-

tos destinados a segurança dos sistemas e precisam de:[6]

- medidas de segurança e ferramentas de avaliação de produtos;
- estratégias para tratar os problemas identificados, considerando os pontos fortes e fracos dos produtos;
- estratégias de diversificação e redundância, como proteção contra ataques localizados;
- estratégias de adaptabilidade, permitindo que os sistemas se reconfigurem quando atacados;
- diagnósticos de segurança e gerenciamento automatizados.

A PROTEÇÃO DE REDE MAIS COMUMENTE ACEITA É UMA BARREIRA, UM *FIREWALL*, ENTRE A REDE CORPORATIVA E O MUNDO EXTERNO.

Existem muitas razões para ficar atento às propostas atuais de criar uma nova forma de proteção legal para os conteúdos das bases de dados.[7] Até o momento, existe um consenso geral, pelo menos entre os profissionais ligados à propriedade intelectual, sobre a necessidade de alguma proteção legal adicional para os conteúdos das bases de dados. Mas, uma vez que essa lei mudaria profundamente as regras existentes sobre a extração e reutilização de dados, existe a necessidade de ter um cuidado considerável para que não passe inadvertidamente de um estado de pouca proteção de conteúdos de bases de dados para um estado de superproteção.

Considera-se que no momento deve-se construir, na comunidade internacional de criação de políticas sobre a propriedade intelectual, um tratado que proteja as bases de dados comercialmente significativos do surgimento de mercados, nos quais os piratas de dados poderiam minar a habilidade dos produtores de bases de dados de reajustar seus grandes investimentos para compilar e manter os dados. Dada a natureza global da Internet e outros elementos da infra-estrutura de informação emergente, o argumento de alguns autores é que o melhor enfoque é adotar uma norma geral neste momento e redefinir os detalhes de sua aplicação no futuro.

MÉTODOS DE PROTEÇÃO

Alguns métodos de proteção, também chamados de autorização ou controle de acesso, têm sido desenvolvidos para resolver os problemas de segurança, como por exemplo:

- **Segurança baseada na confiança:** significa confiar em todo mundo e não fazer nada extra para proteção.
- **Segurança através de obscuridade:** utiliza a noção de que qualquer rede pode ser segura, uma vez que ninguém de fora do grupo de administração poderia ter acesso a informações operacionais e que os usuários são providos apenas de informações necessárias para suas atividades.
- **Esquemas de senha:** provêm uma barreira em primeiro nível para a intrusão acidental, sendo que estes esquemas fazem pouco no caso de ataques deliberados, especialmente quando palavras comuns ou nomes próprios são selecionados como senhas.
- **Sistemas biométricos:** são considerados como o nível mais seguro de autorização, envolvendo alguns aspectos únicos da pessoa, incluindo comparação de impressão digital, impressões da palma da mão, padrões de retina, verificação de assinatura e reconhecimento de voz. Estes sistemas são muito caros.

Uma solução de segurança para processamento de transação deve satisfazer os seguintes requisitos fundamentais de segurança:[8]

- **Confiabilidade:** todas as comunicações entre as partes estão restritas às partes envolvidas na transação. A confiabilidade é um componente essencial na privacidade do usuário, assim como na proteção da informação proprietária e na inibição de roubo de serviços ou informação.
- **Autenticação:** ambas as partes têm que se sentir seguras de que elas estão se comunicando com a parte com a qual

6. LUNT, T. Securing the information infrastructure. *Communications of the ACM*. v.39, n.6, p.130, June 1996.

7. SAMUELSON, P. Legal protection for database contents. *Communications of the ACM*. v.39, n.12, p.17-23, December 1996.

8. BHIMANI, A. Securing the commercial Internet. *Communications of the ACM*. v.39. n.6, p.29-35, June 1996.

elas pensam que estão fazendo negócio. A autenticação é usualmente provida através de assinaturas e certificados digitais.

- **Integridade de dados:** o dado enviado como parte de uma transação não deve ser modificável em trânsito. Similarmente, não deve ser possível modificar um dado enquanto armazenado.
- **Reconhecimento:** nenhuma parte pode ser capaz de negar ter participado de uma transação após o fato.
- **Aplicação seletiva de serviços:** pode ser desejável que parte de uma transação seja escondida, enquanto o restante da mesma transação fique a vista.

Os principais aspectos referentes a segurança para os sistemas interorganizacionais,[9] e que foram adaptados por Applegate, McFarlan e McKenney,[10] estão apresentados no Quadro 1.

A seguir serão descritas algumas das soluções adotadas para tratar do problema de segurança.

Firewalls

A proteção de rede mais comumente aceita é uma barreira, um *firewall*, entre a rede corporativa e o mundo externo. O *firewall* é um método de proteção que visa a colocar equipamentos, um computador ou um roteador, entre a rede e a Internet, a fim de controlar e monitorar todo o tráfego entre o mundo externo e a rede local. Tipicamente, o equipamento permite que os usuários internos da organização tenham acesso total a serviços do lado externo, enquanto fornece acesso seletivo para quem estiver acessando de fora da organização. Para isto, permite acesso através de identificação, senha, endereço de *IP* e outros identificadores.

Os *firewalls* abrangem desde simples sistemas de trilhas, que registram todo o tráfego de rede que passa através do *firewall*, através do registro num arquivo ou base de dados para finalidade de auditoria, até métodos mais complexos, tais como *IP packet screening routers*, ou seja, um serviço de

Quadro 1 – Aspectos de segurança

PROBLEMA	ASPECTO DE NEGÓCIO	SOLUÇÃO
Autorização	O usuário tem a permissão de acessar o computador específico ou o conjunto de informações?	Nome do usuário e senha, ou outro tipo de mecanismo de controle de acesso.
Autenticação	O usuário é verdadeiramente quem ele diz ser?	Sistema de *hardware* e *software* específico gera um número randômico, o qual o usuário irá usar para autenticar a identidade.
Integridade	A pessoa mandou a mensagem como foi recebida? O destinatário pode ter certeza de que a mensagem não foi alterada?	Assinatura digital.
Privacidade	A conversação, ou transação de negócio, é privada? Tem alguém espionando?	Algoritmos de criptografia de chave pública ou privada.
Fraude/Furto	Tem alguém roubando?	Políticas e procedimentos de gerenciamento de sistemas, *log* e auditoria.
Sabotagem	Alguém pode entrar no sistema e destruir ou alterar uma informação?	*Firewalls* e *firebreaks*.

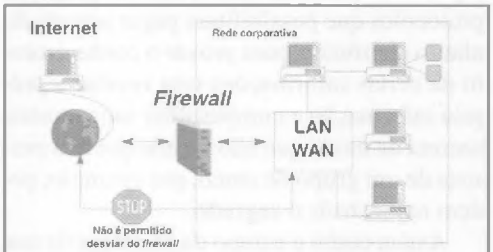
Fonte: APPLEGATE, L. M., McFARLAN, F. W., McKENNEY, J. L. *Corporate information systems management:* texts and cases. Boston: Irwin, 1996, adaptado de APPLEGATE, L. M., GOGAN, J. *Paving the information superhighway:* an introduction to the Internet. Boston: Harvard Business School Publishing, 1995.

9. APPLEGATE, L. M., GOGAN, J. *Paving the information superhighway:* an introduction to the Internet. Boston: Harvard Business School Publishing, 1995.

10. APPLEGATE, L. M., McFARLAN, F. W., McKENNEY, J. L. *Corporate information systems management:* texts and cases. Boston: Irwin, 1996.

roteamento estático de tráfego colocado entre o roteador do provedor de serviço de rede e a rede interna; *hardened firewall hosts*, máquina *stripped-down* que tem sido configurada para aumentar a segurança; e *proxy application gateways*, um servidor especial que tipicamente roda nas máquinas de *firewall*. A Figura 2 apresenta uma estrutura de conexão com a Internet utilizando segurança por *firewall*.

Figura 2 – Conexão com a Internet utilizando *firewall*



Fonte: KALAKOTA, R., WHINSTON, A. *Frontiers of electronic commerce.* New York: Addison-Wesley, 1996.

O método de proteção baseado em *firewall* vive em permanente conflito entre facilidade de uso e paranóia de segurança. Antes de colocar um *firewall*, o administrador que tem a responsabilidade de projetar, especificar, implementar ou supervisionar a instalação precisa considerar alguns aspectos gerenciais:

- **Política de segurança da organização.** O *firewall* instalado é para negar todos os serviços, exceto aqueles necessários para atender a missão de conectar a Internet ou o *firewall* instalado é para prover um método medidor e auditor para regular o acesso de maneira não ameaçadora?
- **Qual é o nível de monitoria, redundância e controle?** Tendo estabelecido o nível de risco aceitável para resolver o primeiro aspecto, um *checklist* é feito com o que deve ser monitorado, permitido ou negado.
- **A política de *firewall*** deve refletir realisticamente o nível de segurança na rede como um todo.

As empresas geralmente designam um ou mais computadores como servidores de rede e procuram proteger cuidadosamente os sistemas internos com a implantação de um *firewall*. Em alguns casos, em que é requerida segurança em alto nível, as empresas instalam *firebreaks*, que são barreiras físicas através das quais não existem conexões eletrônicas entre o servidor e os sistemas de informações internos da empresa.

Senhas

Em adição aos *firewalls* e *firebreaks* (espaços protegidos entre dois *firewalls*), as senhas podem selecionar os usuários prospectivos e garantir que somente aqueles pertencentes a uma lista pré-aprovada possam entrar no sistema. Certamente, isso requer um custo administrativo adicional e às vezes se torna inconveniente para certas áreas de comércio eletrônico.

Os benefícios de abrir uma loja eletrônica, por exemplo, são muito reduzidos se for necessário restringir o acesso somente àqueles que já são conhecidos. Por outro lado, pode ser mais apropriado marcar eletronicamente as mercadorias; assim, poderia ser dado um sinal de alerta se alguém tentar deixar a loja com uma mercadoria que não tenha sido comprada ou que não é para venda.

Mas até mesmo estes esquemas de autorização podem ser violados. As senhas podem ser criptografadas, mas também podem ser facilmente interceptadas num ambiente de computação em rede, no qual existem usuários tecnologicamente sofisticados. Além disso, em muitas empresas as senhas não são tratadas como propriedade privada e alienável, e há a possibilidade de as pessoas divulgarem suas senhas para outras. Quando isso não acontece, ainda existe o problema do usuário usar senhas de fácil adivinhação, como nome de familiares, seqüência de números ou letras etc.

Em algumas situações, as empresas podem desejar solicitar aos indivíduos que comprovem que eles são quem dizem ser. Um enfoque para autenticar usuários de rede combina *hardware* e *software* especiais. Os usuários autorizados a acessar um servidor específico ou a passar pelo *firewall* da empresa recebem um equipamento especial a ser guardado, na forma de um cartão magnético que contém um algoritmo de criptografia.

Quando o usuário autorizado tenta conectar-se a outro computador da empresa ele recebe um número de cinco dígitos, gerado randomicamente, como um pedido de senha de autenticação. O usuário alimenta o número no equipamento, recebe um outro

número de cinco dígitos e, então, responde com este número como a chave para o pedido de senha. Se o sistema remoto ficar satisfeito com a resposta, o usuário terá permissão de acessar o servidor.

OS BENEFÍCIOS DE ABRIR UMA LOJA ELETRÔNICA SÃO MUITO REDUZIDOS SE FOR NECESSÁRIO RESTRINGIR O ACESSO SOMENTE ÀQUELES QUE JÁ SÃO CONHECIDOS.

Criptografia

Criptografia para a maioria das pessoas refere-se a manter as comunicações privadas. De fato a proteção de comunicações sensíveis tem sido a ênfase da criptografia durante boa parte da sua história. Contudo, hoje em dia esta é apenas uma parte da criptografia.

A encriptação é a transformação de dados em uma forma não possível de ser lida. O seu propósito é de assegurar privacidade mantendo a informação escondida de qualquer pessoa a quem ela não é destinada, mesmo àqueles que podem tê-la encriptado. A decriptação é o reverso da encriptação: é a transformação dos dados encriptados de volta a uma forma inteligível.

A encriptação e a decriptação requerem o uso de informação secreta, referida usualmente como chave. Dependendo do mecanismo de encriptação usado, a mesma chave pode ser usada para ambos, encriptação e decriptação, enquanto para outros mecanismos as chaves usadas para encriptação e decriptação podem ser diferentes.

Mas a criptografia usada hoje em dia é mais do que escrita secreta, mais do que encriptação e decriptação. Autenticação é uma parte tão fundamental da vida como privacidade. Normalmente, a autenticação é usada no dia-a-dia, quando se assina o nome para algum documento, por exemplo, e como se está movendo para um mundo em que as decisões e contratos são comunicados eletronicamente.

A criptografia provê mecanismos para tais procedimentos. Uma assinatura digital junta um documento ao possuidor de uma determinada chave, enquanto um carimbo digital junta um documento à sua criação em um determinado momento. Esses mecanismos de criptografia podem ser usados para controlar acesso a um *drive* compartilhado, a uma instalação de alta segurança ou a um canal de TV *pay-per-view*.

Com apenas poucas ferramentas básicas é possível construir elaborados esquemas e protocolos que possibilitam pagar usando dinheiro eletrônico, para provar o conhecimento de certas informações sem revelar a própria informação e compartilhar uma quantia secreta de modo que não menos que três pessoas de um grupo de cinco, por exemplo, podem reconstruir o segredo.

Assim como o campo da criptografia tem avançado, as linhas divisórias para o que é e o que não é criptografia têm começado a ficar confusas. Criptografia hoje pode ser sumariada como o estudo de técnicas e aplicações que dependem da existência de problemas difíceis. Um criptologista balanceia mecanismos criptográficos, e criptologia (do grego *kryptós lógos*) é a disciplina de criptografia e criptoanálise combinadas.

As informações sensíveis que precisam viajar através de canais públicos, tal como a Internet, podem ser protegidas pela sua criptografia. A criptografia é a mutação de informação em qualquer forma (texto, vídeo ou gráficos) em uma representação não legível por qualquer pessoa sem uma chave de criptografia. Genericamente, existem dois métodos de criptografia: com chave secreta (*secret key*) e com chave pública (*public key*).

A criptografia com chave secreta envolve o uso de uma chave compartilhada para a criptografia pelo transmissor e a decriptografia pelo destinatário. As técnicas de chaves compartilhadas sofrem com o problema de distribuição de chave, uma vez que as chaves compartilhadas precisam ser seguramente distribuídas para cada par das partes da comunicação. A distribuição segura de chave torna-se um incômodo nas grandes redes.

Uma implementação amplamente adotada de criptografia de chave secreta é o *Data Encryption Standard* (*DES*), que foi introduzido em 1975 pela IBM, National Security

Agency (NSA) e National Bureau of Standards (NBS, que passou a ser chamado de NIST). O *DES* é um sistema de criptografia de chave secreta simétrico, ou seja, o emissor e o destinatário precisam conhecer a mesma chave secreta, que é utilizada para criptografar e decriptografar a mensagem. Atualmente, os *softwares* que utilizam o *DES* estão prontamente disponíveis e sem custo para qualquer um que acesse a Internet.

A criptografia com chave pública é uma forma mais forte e envolve o uso de chaves públicas. As técnicas de chave pública envolvem um par de chaves, uma chave privada e uma chave pública associadas com cada usuário. A informação criptografada pela chave privada pode ser decriptografada somente utilizando a chave pública correspondente.

A chave privada, usada para criptografar a informação transmitida pelo usuário, é mantida secreta. A chave pública é utilizada para decriptografar no destinatário e não é mantida secreta. Uma vez que somente o autor legítimo de uma mensagem criptografada tem conhecimento da chave privada, uma decriptação com sucesso, utilizando a chave pública correspondente, verifica a identidade do autor e assegura a integridade da mensagem.

A criptografia com chave pública pode ser utilizada para autenticação de emissor, conhecida como assinatura digital. O *RSA* é um sistema de chave pública para criptografia e autenticação desenvolvido em 1977 por Ron Rivest, Adi Shamir e Leonard Adleman. O sistema de *RSA* utiliza um par casado de chaves de criptografia e decriptografia, cada uma desempenhando uma transformação de uma direção dos dados. O *RSA* está também desenvolvendo assinaturas digitais, que são algoritmos matemáticos que criptografam um documento inteiro e que podem ser usados para autenticar documentos eletrônicos da mesma forma que as assinaturas manuscritas são usadas para autenticar documentos em papel.

Algumas aplicações têm utilizado a combinação de *RSA* e *DES* para tornar a comunicação mais segura num ambiente de canais não seguros.

Um *chip*, denominado Clipper, foi desenvolvido para desempenhar as funções de criptografia de forma mais segura. Este *chip* pode ser utilizado da mesma maneira que o *DES*, mas, devido ao seu projeto, prevê a utilização de chaves de 80 *bits* e trata os dados em 32 passos (o *DES* utiliza 56 *bits* e 16 passos).

Considera-se que a criptografia seja a solução para os problemas de segurança. No entanto, apesar de a criptografia ser necessária para uma segurança forte, ela não é suficiente. Na Internet, a maioria das criptografias é utilizada em aplicações tais como *e-mail* e *browsers* da Web. Mas ataques comuns aos sistemas operacionais podem superar as aplicações de criptografia e mesmo a autenticação de sistema operacional. O uso de criptografia isoladamente não aumenta a resistência à invasão dos sistemas.

AS INFORMAÇÕES SENSÍVEIS QUE PRECISAM VIAJAR ATRAVÉS DE CANAIS PÚBLICOS, TAL COMO A INTERNET, PODEM SER PROTEGIDAS PELA SUA CRIPTOGRAFIA.

Além disto, é importante mencionar que o custo de recuperação de uma informação criptografada é alto. A empresa precisa controlar a chave de criptografia, ou seja, a custódia da chave. Cada uma das chaves pessoais de criptografia usadas na empresa tem uma cópia em lugar seguro e acessível apenas ao administrador do sistema. Para se ter uma relação do custo deste sistema podemos dizer que para cada máquina o investimento é dez vezes maior do que uma cópia de um programa de correio eletrônico.

Assinatura digital

No caso de transações de negócio, recomenda-se o uso de assinaturas digitais, que desempenham uma função para documentos digitais similar àquela desempenhada pelas assinaturas manuscritas para documentos impressos. A assinatura digital permite verificar se um documento transmitido eletronicamente por uma pessoa foi realmente enviado por esta pessoa e permite a possibilidade de se provar posteriormente.

Uma assinatura digital é usada no lugar de uma assinatura manual. Essas assinaturas digitais são usadas como prova de intenção quando atividades como comércio eletrônico são envolvidas e apresentam algumas características como:

- não são forjáveis;
- provêm autenticação ao documento, identificando o autor ou originador;
- provêm integridade ao documento, que não pode ser alterado sem que a alteração seja detectada;
- previnem que o documento não seja repudiado, ou seja, o assinante não pode alegar posteriormente que não assinou.

A FALTA DE SEGURANÇA DE DADOS E MENSAGENS NA INTERNET TEM SE TORNADO UM PROBLEMA CRÍTICO DEVIDO AO CRESCENTE NÚMERO DE EMPRESAS QUE ESTÃO TENTANDO COLOCAR SEUS NEGÓCIOS COMERCIAIS NA REDE.

A tradução da prova de autoria e intenção na forma digital requer as seguintes salvaguardas:

- *software* para suportar assinatura digital;
- autenticação e identificação convencional, código de identificação e senha, para proteger uma chave privada de indivíduo ou organização;
- um processo que forneça uma autêntica e confiável assinatura digital, que é única para o indivíduo ou organização.

As assinaturas digitais devem ser implementadas em um sinal físico (*floppy disk*, *PC Card*, *Smart Card* etc.) que pode ser removido do computador e da rede quando não estiver em uso. A proteção do código de assinatura deve incluir criptografia de forma que não seja possível para um indivíduo usar a assinatura digital de outro indivíduo.

SEGURANÇA NA INTERNET

A falta de segurança de dados e mensagens na Internet tem se tornado um problema crítico devido ao crescente número de empresas que estão tentando colocar seus negócios comerciais na rede. Esta situação é uma das maiores preocupações das organizações comerciais, especialmente para a alta gerência. Pela conexão com a Internet, uma rede local de uma organização pode tornar-se exposta para a população inteira da Internet. Segundo alguns *hackers* americanos, a Internet brasileira é muito frágil, podendo ser comparada apenas às redes do Chile e da Rússia.[11]

A Internet é inerentemente insegura. Nenhum método de segurança pode reivindicar impenetrabilidade. A segurança de qualquer conexão de rede depende dos dois lados da conexão, ou seja, o lado do cliente (*browser*) e o lado do servidor (*http://www.servidor.com*). Os seguintes passos são recomendados para aumentar a proteção dos usuários da Internet:

- Usar sempre as últimas versões de *software*, independentemente do fabricante. A descoberta de falhas de segurança é uma das mais significativas razões para os fabricantes lançarem novas versões de *software*.
- Usar a versão de mais alta segurança do *software* utilizado. Existem *softwares* que possuem versões com chave de 40 *bits* e de 128 *bits*.

Os riscos básicos de segurança nas comunicações via Internet são:

- **espreita:** intermediários escutando conversa privada;
- **manipulação:** intermediários mudando a informação em conversa privada;
- **personificação:** um remetente ou receptor se comunicando sob falsa identificação.

A situação é análoga a compras feitas por telefone a serem entregues pelo correio. Os compradores querem certificar-se de que nenhum terceiro irá ouvir o número de seu cartão de crédito (**espreita**), de que ninguém pode inserir informação adicional ao pedido ou mudar o endereço de entrega (**manipulação**) e de que é realmente a empresa vendedora que está do outro lado da linha e não um impostor de cartão de crédito (**personificação**).

11. MARTINS, I., GUROVITZ, H. Op. cit.

Algumas das maneiras pelas quais os problemas de segurança na Internet comercial se manifestam são:[12]

- Os ataques de bisbilhoteiros na rede podendo resultar no roubo de informações de contas, tais como números de cartões de crédito, número de contas de clientes ou informações sobre saldo e extrato de contas. Similarmente, tais ataques podem resultar no roubo de serviços, normalmente limitados a subscritores, tais como produtos baseados em informação.
- Os ataques de espionagem de senha podendo ser utilizados para obter acesso em sistemas nos quais informações proprietárias são armazenadas. O uso crescente de algoritmos fortes de criptografia tem inibido este tipo de ataque.
- Os ataques de modificação de dados podendo ser utilizados para alterar os conteúdos de certas transações, por exemplo, alterar o sacador em um cheque eletrônico ou alterar o valor que está sendo transferido para uma conta bancária. Tais ataques também podem ser utilizados para modificar certos pedidos através da rede.
- Os ataques de falsificação podendo ser utilizados para permitir que uma das partes no processo possa ser mascarada. Em tal situação, um indivíduo mal intencionado pode estabelecer uma "loja de fachada" e coletar milhares e às vezes milhões de números de cartões de crédito, números de contas e outras informações de clientes sem levantar suspeitas.
- O não-reconhecimento de transações podendo causar maiores problemas com sistemas de faturamento e acordos de processamento de transações. Por exemplo, se uma parte não cumprir um acordo após o fato, a outra parte pode incorrer no custo de processamento de transação sem se beneficiar da transação.

A manutenção da segurança e integridade de informação através das fronteiras interorganizacionais é sempre um desafio na Internet, entretanto, que ainda se configura como um pesadelo. Lembrando que a Internet cresceu de uma maneira não controlada, qualquer pessoa em praticamente qualquer país pode conectar-se à Internet com um computador pessoal, um *modem*, um endereço na rede e uma conexão com um servidor da Internet. Em analogia ao problema de quantas fechaduras se coloca na porta de uma residência, o nível de segurança depende de como o sistema é utilizado se existem algumas ligações diretas entre a Internet e os sistemas de informações das empresas.

Para reduzir estas ameaças de segurança, vários métodos de proteção são utilizados. O problema no caso do comércio eletrônico é muito simples: se consumidores e clientes conectam um computador na Internet, eles podem se conectar facilmente a qualquer lugar que a rede alcance. Esta é a boa notícia. A má notícia é que, sem um controle de acesso apropriado, qualquer pessoa pode fazê-lo também.

OS ADMINISTRADORES QUE SÃO CONTEMPLADOS COM A CONDUÇÃO DE COMÉRCIO ELETRÔNICO ATRAVÉS DA INTERNET PRECISAM ASSUMIR QUE QUALQUER PESSOA NO MUNDO PODE VIR E BATER À SUA PORTA.

Não existe, atualmente, nenhum padrão de segurança para a Internet. Existem várias empresas, como Netscape, EIT/Terisa, Spyglass e outras, propondo várias soluções de segurança. A Netscape tem uma proposta de protocolo submetida ao *Consórcio W3*, chamado *Secure Sockets Layer* (*SSL*), que foi provido para a comunidade Internet na forma de implementação de referência. Um outro exemplo de protocolo é o *S-HTTP*, da empresa EIT/Terisa, mas nenhum deles é um padrão oficial de segurança definido pelo *W3C*.

O *W3C* é um consórcio de empresas cuja missão é desenvolver e distribuir *software* da próxima geração para a WWW. O desenvolvimento de tecnologia pelo *W3C* vai ajudar na expedição de processos de estabelecimento de padrões Internet na *IEFT* (*Internet Engineering Task Force*) para a WWW. A *IEFT* é o braço de engenharia e

12. BHIMANI, A. Op. cit.

desenvolvimento de protocolo da Internet. Ela é uma grande e aberta comunidade internacional de desenvolvedores de rede, operadores, fabricantes e pesquisadores preocupados com a evolução da arquitetura da Internet e sua suave operação.

Os administradores que são contemplados com a condução de comércio eletrônico através da Internet precisam assumir que qualquer pessoa no mundo pode vir e bater à sua porta. Eles precisam preservar as redes corporativas internas contra elementos externos não desejados.

Em relação a compras pela Internet, a forma mais comum de pagamento eletrônico é através de cartões de crédito. Isto levou as administradoras de cartão de crédito Visa e Mastercard a elaborarem um modelo padrão de segurança, denominado *SET* (transação eletrônica segura).

PRIVACIDADE

Um outro problema grave com o comércio eletrônico é proteger a privacidade das informações pessoais. Por exemplo, uma empresa criou uma aplicação Web interna para permitir o compartilhamento de informação entre os empregados internos. Apesar do fato de o servidor estar protegido por um *firewall* e de o fornecimento de uma senha ser requerido, a empresa achou que alguém poderia quebrar a segurança, entrar no sistema e roubar informações altamente confidenciais. As transações financeiras eletrônicas são também uma grande preocupação.

Muitas empresas, incluindo a Microsoft Corporation e a Visa International, têm anunciado parcerias para prover segurança adequada para as transações financeiras *on-line*. Algumas estão utilizando assinaturas digitais e chaves de criptografia para autenticar dados de transações financeiras, outras requerem que as informações de cartão de crédito sejam enviadas por telefone, criando, desta forma, um *firebreak*.

O mundo *on-line* do comércio eletrônico também levanta muitos novos aspectos sobre a privacidade de informação. Quando se compra um livro publicado, assume-se que a proteção de direito autoral e os direitos de propriedade intelectual tenham sido tratados pelo autor e pela editora. Cada livro é encadernado para garantir que todas as partes do livro sejam consideradas e protegidas como um todo.

Contrastantemente, no mundo *on-line* a informação é transmitida em pequenos *bits* e pedaços que podem ser reconstruídos por muitos diferentes usuários em diferentes formas. Leis de direito autoral ainda têm que ser escritas para acomodar esta situação, e manter a propriedade intelectual e os direitos de privacidade torna-se um pesadelo de logística.

O aumento do número de usuários de computadores, aplicações e interconexão de sistemas, juntamente com o aumento da complexidade das capacidades tecnológicas como um todo, significam uma grande chance para que a privacidade do correio eletrônico (*electronic mail* ou *e-mail*) fique comprometida.[13]

As invasões de privacidade de *e-mail* são caracterizadas por duas dimensões: fontes de invasão e tipos de invasão. As comuni-

Quadro 2 – Tipos de invasão de privacidade de correio eletrônico

FONTES DE INVASÃO	**Interceptação interna**	**Monitoração de desempenho de empregado**	**Bisbilhotice**
	Interceptação externa	**Investigação legal**	***Hackers***
		Interceptação autorizada	**Interceptação não autorizada**

Fonte: SIPIOR, J. C., WARD, B. T. The ethical and legal quandary of email privacy. *Communications of the ACM.* v.38, n.12, p.48-54, December 1995.

13. SIPIOR, J. C., WARD, B. T. The ethical and legal quandary of email privacy. *Communications of the ACM.* v.38, n.12, p.48-54, December 1995.

A precificação de uma opção torna-se particularmente complexa quando se pretende aplicar o modelo de *Black-Scholes* a situações particulares, em que as hipóteses iniciais não são verificadas. Daí surge a necessidade de alterar a fórmula, de modo a acomodá-la às características reais da operação. Entre os modelos que surgiram, relaxando as hipóteses de *Black-Scholes*, podem-se destacar o trabalho de Cox, Ross & Rubinstein,[8] que apresentam um modelo de avaliação de opções para tempo discreto (Modelo Binomial).

O CONCEITO DE OPÇÕES REAIS É UMA EXTENSÃO DO CONCEITO DE FLEXIBILIDADE, SENDO QUE COM AS OPÇÕES REAIS PROCURA-SE MENSURAR A FLEXIBILIDADE QUANTITATIVAMENTE.

Os métodos numéricos de solução envolvem uma abordagem de programação dinâmica para a determinação do valor de uma opção. Trabalha-se na solução de sistemas de equações que determinam o valor de uma opção a qualquer momento em termos do valor da opção no próximo período. O método inicia-se por cálculos na data de vencimento da opção e vai voltando no tempo cronologicamente, período por período, para estimar o valor da opção em cada estágio. Ele inicia-se na data de vencimento do contrato de opção, pois é nesse momento que o valor "justo" da opção é idêntico ao seu valor intrínseco.

Genericamente,[9] existem dois tipos de métodos numéricos de cálculo do valor de uma opção: (1) aqueles que procuram intuitivamente aproximar-se do processo estocático subjacente ao valor de uma opção e (2) aqueles que se aproximam pela resolução de equações diferenciais parciais.

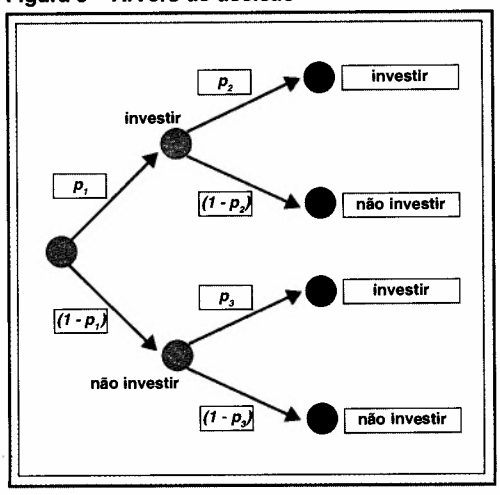
ANALISANDO A APLICABILIDADE DA PRECIFICAÇÃO DE OPÇÕES NA ANÁLISE DE INVESTIMENTOS (*REAL OPTIONS*)

A maioria das organizações utiliza critérios quantitativos para capturar o custo estimado e os benefícios associados com determinado projeto. Os métodos mais populares são a taxa interna de retorno, o valor presente líquido e o *payback*. Entretanto, esses métodos partem de premissas incorretas, assumindo uma posição passiva da administração diante das contingências durante a vida esperada do projeto. Acrescente-se que esses métodos também ignoram os efeitos sinérgicos que um projeto de investimento pode proporcionar. Em síntese, os instrumentos tradicionais não avaliam corretamente a flexibilidade gerencial.

O VPL tradicional estima o valor de um projeto por meio de estimativas do fluxo de caixa futuro de um determinado projeto, sendo esse fluxo posteriormente descontado por uma taxa apropriada que mensure o risco ajustado pelo custo de oportunidade do capital. Entre as dificuldades desse método está a previsão com exatidão e antecedência de qual será o fluxo de caixa futuro, bem como a definição da taxa de desconto a ser utilizada. Na prática, o fluxo de caixa descontado (DCF) subavalia investimentos, na medida em que ignora aspectos estratégicos na tomada de decisões, bem como a existência de determinadas flexibilidades operacionais.

As árvores de decisão garantem uma maior flexibilidade sobre os mecanismos tradicionais na medida em que as decisões são definidas com um maior grau de flexibilidade. Nas árvores uma série de eventos pode ser mapeada ao longo dos diversos ramos, envolvendo várias decisões de seqüenciamento. Como exemplo de uma árvore de decisão apresentamos simplificadamente o modelo a seguir (Figura 3):

Figura 3 – Árvore de decisão



8. COX, J., ROSS, S., RUBINSTEIN, M. Option pricing: a simplified approach, *Journal of Financial Economics*. 7, p. 229-63, 1979.

9. Uma revisão ampla das técnicas de mensuração de uma opção pode ser encontrada no artigo: GESKE, R., SHASTRI, K. Valuation by approximation: a comparison of alternative option valuation techniques, *Journal of Financial and Quantitative Analysis*. p.1511-24, March 1985.

cações de *e-mail* correm o risco de intercepção de fontes internas e externas da organização. As fontes internas são pessoas empregadas pela organização, incluindo executivos, gerentes e colaboradores. As fontes externas são pessoas com as quais a organização interage, através de relacionamentos formais e informais. Os relacionamentos formais podem ligar provedores de serviços, consultores, fornecedores e clientes. A interação pode também ocorrer na ausência de relacionamentos informais, com concorrentes, espiões corporativos e *hackers*.

A invasão pode ser autorizada ou não autorizada, isto é, ela pode ser justificada por uma autoridade interna, tal como um gerente, uma autoridade externa, tal como uma investigação legal, ou ela pode ser uma violação de privacidade totalmente não autorizada. Essas combinações são organizadas em quatro células, conforme apresentado no Quadro 2, que mostra os tipos de invasão de privacidade no correio eletrônico.

Considera-se que os avanços rápidos da TI obrigam que os sistemas legais resolvam conflitos para os quais não há precedentes.

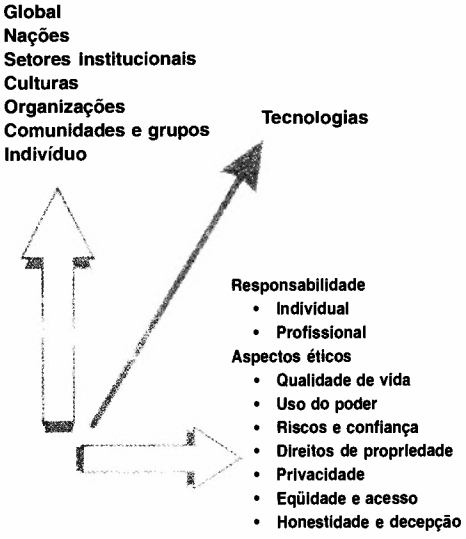
ÉTICA

O estudo dos aspectos éticos e sociais na computação tem uma natureza interdisciplinar. Éticos, historiadores, analistas sociais, sociólogos, antropólogos e psicólogos têm contribuído nas pesquisas dessa área. Ao invés de sugerir que se estude cada disciplina separadamente, sugere-se que, da perspectiva da ciência da computação, todo aspecto ético esteja localizado em um nível particular de análise social.

Somente a análise que considera pelo menos três dimensões – técnica, social e ética – pode representar os aspectos como eles afetam a ciência de computação na prática. Considerar cada dimensão separadamente provê alguma visão, mas somente sua interação revela a complexidade desses aspectos. A análise de qualquer aspecto também tem que especificar e examinar a análise social e o conteúdo técnico relacionados.[14]

A Figura 3 apresenta a definição de duas dimensões – análise social e aspectos éticos associados com tecnologia. Uma terceira dimensão é indicada, mas não especificada por incluir as várias tecnologias que requerem análise de alguma parte das primeiras duas dimensões. Uma vez que as mudanças de tecnologia ocorrem muito rapidamente, especificar as tecnologias limitaria a utilização do esquema conceitual.

Figura 3 – Análise social e aspectos éticos



Fonte: HUFF, C., MARTIN, D. Computing consequences: a framework for teaching Ethical Computing. *Communications of the ACM*, v.38, n.12, p.75-84, December 1995.

CONCLUSÃO

Enquanto assinaturas digitais, *firewalls*, algoritmos de criptografia e senhas podem auxiliar a proteger nossos direitos, eles não são suficientes. Procedimentos e práticas atuais de segurança, privacidade e integridade de informação precisam ser examinados e as políticas de informação e comunicação interorganizacionais precisam ser estabelecidas. Regulamentações governamentais e aspectos legais precisam ser tratados.

Embora todas essas adaptações ainda devam ser feitas, atualmente os progressos conseguidos com as técnicas de segurança e privacidade permitem que as empresas passem, cada vez mais, a utilizar comércio eletrônico, inclusive como forma de obter vantagem competitiva. ❑

14. HUFF, C., MARTIN, D. Computing consequences: a framework for teaching Ethical Computing. *Communications of the ACM*. v.38, n.12, p.75-84, December 1995.