CURSO DE ADMINISTRAÇÃO

ÉTICA EM SISTEMAS DE INFORMAÇÃO: QUESTÕES DE PRIVACIDADE E DE SEGURANÇA

DIEGO FELIPE BORGES DE AMORIM

Sapucaia do Sul
2013

DIEGO FELIPE BORGES DE AMORIM

ÉTICA EM SISTEMAS DE INFORMAÇÃO:
QUESTÕES DE PRIVACIDADE E DE SEGURANÇA

Trabalho de conclusão apresentado ao Curso de Administração das Faculdades Equipe, como requisito parcial para obtenção do grau de Bacharel em Administração, sob a orientação do professor Ms. Sandro Celestino da Rosa Wollenhaupt

Sapucaia do Sul

2013

DIEGO FELIPE BORGES DE AMORIM

ÉTICA EM SISTEMAS DE INFORMAÇÃO: QUESTÕES DE PRIVACIDADE E DE SEGURANÇA

Esta monografia foi julgada adequada à obtenção do grau de Bacharel em administração e aprovada pelo Curso de Administração das Faculdades Equipe - FAE, Sapucaia do Sul.

Banca Examinadora:

_____

Orientador – Prof. Ms. Sandro Celestino da Rosa Wollenhaupt
Faculdades Equipe

_____

Profª Ms. Eliane de Mello
Faculdades Equipe

_____

Prof. Ms. Walmir Güintzel
Faculdades Equipe

RESUMO

O referido trabalho tem seu foco na ética, correlacionando o tema sobre segurança e privacidade na utilização de sistemas de informação e internet. Este trabalho, através de uma pesquisa descritiva, procurou sintetizar o assunto ao relacionar como a conduta ética e as questões sobre segurança e privacidade de dados individuais, através da rede, são vistos pela sociedade moderna. Os resultados do estudo permitiram uma reflexão sobre as relações entre usuários do sistema e como os dilemas éticos surgem a partir dessas interações. A conclusão indica que, com o surgimento de muitas regras de governança e conformidade, todos os usuários devem entender questões éticas em torno da informação. Como recurso organizacional chave, a informação deve ser protegida contra danos e utilização indevida. Isso envolve a abordagem das questões éticas sobre a coleta, o armazenamento e o uso da informação; a proteção da privacidade da informação; e a garantia de que as informações estejam seguras contra ataques e acesso não autorizado.

Palavras-chave: Ética, Segurança, Privacidade.

ABSTRACT

Such work focuses on ethics, correlating the theme issues on security and privacy in the use of information systems and internet. This paper, through a descriptive research sought to synthesize the matter relating to ethical conduct and the issues on security and privacy of individual data across the network are seen by modern society. The results of the study led to a reflection on the relationship between users of the system and how ethical dilemmas arise from these interactions. The conclusion indicates that the emergence of many governance rules and compliance, all users must understand the ethical issues surrounding information. As a key organizational resource, information must be protected from damage and misuse. This involves addressing the ethical questions about the collection, storage and use of information, the protection of information privacy, and the assurance that the information is secure against attacks and unauthorized access.

Keywords: Ethics, Security, Privacy.

LISTA DE ABREVIAÇÕES E SIGLAS

AOL - America OnLine

CIO - Chefe Oficial de Informação

CPF - Cadastro de Pessoa Física

Epolicies - Políticas Eletrônicas

ERP – Planejamento de Recursos Empresariais

EUA - Estados Unidos da América

IBGE - Instituto Brasileiro de Geografia e Estatística

IP - Protocolo de Internet

MEC - Ministério da Educação e Cultura

MI - Mensagem Instantânea

P3P - Plataforma de Preferências de Privacidade

PA74 - Lei de Privacidade de 1974

PDAs - Assistentes Pessoais Digitais

PGP - Privacidade Bastante Boa

PKE - Criptografia de Chave Pública

PL - Projeto de Lei

PNAD - Pesquisa Nacional por Amostra de Domicílios

RFID -Identificação por Radiofrequência

SI - Sistema de informação(ões)

TI - Tecnologia da Informação

TSE - Tribunal Superior Eleitoral

TV - Aparelho Televisor

LISTA DE FIGURAS

Figura 1: Componentes de um sistema de informação 16
Figura 2: Estrutura de um sistema de informações 18
Figura 3: Custo associado a crimes na internet 20
Figura 4: Agir eticamente e agir legalmente nem sempre são a mesma coisa 25
Figura 5: Políticas corporativas de privacidade 31
Figura 6: Principais ameaças à segurança e à privacidade de dados.....34
Figura 7: Criando um plano de segurança da informação.....35
Figura 8: Deletar uma mensagem de e-mail do computador do receptor 42
Figura 9: O e-mail como alvo principal de mensagens indesejadas.....46
Figura 10: Processo de criptografia.....52
Figura 11: Etapas, fases e passos de um processo de pesquisa científica 56

SUMÁRIO

1 INTRODUÇÃO 10
1.1 O Cenário da Ética em Sistemas de Informação.....10
1.2 Identificação do Problema.....12
1.3 Objetivos 12
1.4 Justificativa.....13
1.5 Estrutura do Trabalho.....13
2 FUNDAMENTAÇÃO TEÓRICA.....15
2.1 Sistemas de Informação.....15
2.2 Ética 22
2.2.1 Ética em Sistemas de Informação.....27
2.3 Políticas de Gerenciamento da Informação.....30
2.4 Segurança e Privacidade 32
2.5 A Privacidade e Algumas de suas Implicações no Uso da Internet.....36
2.5.1 Direito à Privacidade 36
2.5.2 Privacidade no Trabalho.....39
2.5.3 Privacidade do E-mail e Mensagem Instantânea 40
2.5.4 Dispositivos Pessoais Sensíveis e Privacidade.....43
2.5.5 Privacidade e Internet.....43
2.6 Tratamento de Bases de Dados e Privacidade 47
2.6.1 O Mercado de Bases de Dados 47
2.6.2 O Tratamento de Bases de Dados na Lei Brasileira 50
2.7 Transmissão de Informações e Privacidade.....51
3 METODOLOGIA.....54
3.1 Componentes da Pesquisa Científica 54
3.2 Classificação da Pesquisa Científica.....57
3.2.1 Pesquisa Bibliográfica 57
3.2.2 Pesquisa de Campo 57
3.2.3 Pesquisa Experimental.....58
3.2.4 Estudo de Caso.....59
3.3 Encaminhamento Metodológico da Pesquisa.....60
4 CONCLUSÃO.....61

5 LIMITAÇÕES E SUGESTÕES PARA ESTUDOS FUTUROS.....67
REFERÊNCIAS BIBLIOGRÁFICAS.....68

1 INTRODUÇÃO

1.1 O Cenário da Ética em Sistemas de Informação

Desde quando foi inventado, até o final da década de 80, o computador era usado em poucos nichos de aplicações militares, acadêmicas e comerciais. Nas empresas, o uso era restrito e isolado, permitindo pouco contato entre os profissionais de computação e os usuários e também entre os usuários e o próprio computador. Essa situação começou a mudar a partir do final da década de 80, em razão de vários avanços tecnológicos, entre os quais estão a invenção do computador pessoal, as redes de computadores (Internet) e as aplicações e serviços que surgiram em decorrência da disponibilidade desse ambiente tecnológico. Como consequência dessa mudança, os computadores são hoje um produto de consumo em massa. (MASIERO & BIGONHA, 2008)

Neste contexto, o acesso à rede Internet em escala global possibilitou um grande avanço. Hoje, as organizações estão em rede, bem como o cidadão comum. Comprar ou mesmo se relacionar com outras pessoas é possível através de redes sociais. O usuário precisa, apenas, informar alguns dados pessoais como nome, endereço e telefone para fazer um cadastro que dará acesso a uma aquisição, por exemplo. Muitas vezes, não damos a importância necessária sobre o que farão com essas informações, as empresas ou pessoas que terão acesso aos nossos dados, como utilizarão e para que fim. Se quisermos corrigir nossos dados cadastrais ou, simplesmente, apagá-los, poderemos fazê-lo? São questões que trazem à tona dilemas éticos com relação à nossa privacidade na rede.

Diante disto, o tema da ética começa a chamar a atenção da sociedade a partir da reflexão de vários fatos de condutas antiéticas na política, na economia, como também no uso indevido de informações privadas através da internet. Stair & Reynolds (2011), indicam que, basicamente, a questão da privacidade trata do direito de ser deixado só ou de ser afastado da visão pública. Com os sistemas de informação, a privacidade lida com o conjunto e o uso ou mal uso de dados. Dados são constantemente coletados e armazenados sobre cada um de nós. Esses dados são frequentemente distribuídos em redes facilmente acessíveis e sem nosso conhecimento ou consentimento.

Muitos países possuem legislação própria sobre o assunto. A União Europeia possui uma diretriz para a proteção de dados que exige que as empresas que transportam dados através das fronteiras nacionais tenham instalados certos procedimentos de privacidade. Nos Estados Unidos, por exemplo, existe a *lei Gramm-Leach Billey de 1999* que exige que as instituições financeiras protejam e garantam os dados não públicos dos consumidores quanto a acesso e uso não autorizado (STAIR & REYNOLDS, 2011). No Brasil, a lei denominada M*arco Civil da Internet*, criada em 2009, e ainda em tramitação no Congresso, define os princípios, garantias, direitos e deveres de quem usa a rede e determina as diretrizes de atuação do Estado. O Marco Civil foi apresentado como um Projeto de Lei do Poder Executivo à Câmara dos Deputados, sob o número PL 2126/2011 (atualmente apensado ao PL 5403/2001). O texto do projeto trata de temas como neutralidade da rede, *privacidade*, retenção de dados, a função social da rede e responsabilidade civil de usuários e provedores.

Enquanto nada está definido, temos a sensação de inseguridade em relação aos nossos dados junto a empresas públicas e privadas através da rede, a última, em especial, web sites de vendas e rede de relacionamentos. Tais empresas possuem uma clara política de privacidade? Quantas têm? Antes de nos cadastrarmos, lemos sobre tais políticas de privacidade? Quando preenchemos um cadastro e informamos alguns dados pessoais aparentemente pouco relevantes, esses mesmos dados cruzados com outros já existentes se tornam informações valiosas a nosso respeito. Se nos cadastramos junto a uma empresa, supostamente, nossos dados estariam resguardados somente àquela empresa. É isso mesmo que ocorre?

Os atuais acontecimentos mostram o contrário. Numa certa ocasião, uma empresa aérea que abriu falência foi adquirida por uma terceira não pela frota de aviões sucatas que detinha, mas pelo seu banco de dados relacionados a sua carteira de clientes. Em um programa televisivo recente, uma apresentadora declarou: *informação é poder e dinheiro*. Essa verdade se tornou tão banal nos tempos de internet e redes sociais que esquecemos sua importância até sermos acordados novamente pelos fatos.

O caso mais recente foi o contrato do Tribunal Superior Eleitoral para fornecer dados de cerca de 141 milhões de eleitores para a Serasa Experian, empresa conhecida pelo seu banco de dados de maus pagadores. O negócio causou

perplexidade até mesmo nos ministros do TSE – onde foi suspenso pela presidente, Carmen Lúcia – e mostrou como são vulneráveis a privacidade e as informações pessoais dos cidadãos. Mas, para uma das mais altas cortes de Justiça do país, negociar seu banco de dados parece um feito inédito.

Nesse sentido, o presente trabalho busca identificar os tipos de privacidade através da rede e suas implicações nas relações em sociedade, considerando as vulnerabilidades que expõem o usuário da rede e questões éticas envolvidas.

1.2 Identificação do Problema

A privacidade na rede é a principal questão a respeito do uso legal das novas tecnologias digitais. Esse tipo de privacidade se refere à possibilidade de uma pessoa utilizar redes de acesso, como a internet, mantendo sigilo a respeito de suas informações pessoais, bancárias e profissionais, revelando somente informações de uso público.

O surgimento das redes sociais e sites de compartilhamento aumentaram os riscos de um indivíduo ter a privacidade violada na sociedade atual, principalmente pela divulgação direta e indireta de dados pessoais. A partir dessas redes sociais e de sites de compartilhamento, as empresas buscam informação sobre os usuários e oferecem produtos e serviços de acordo com as preferências deduzidas através das informações colhidas.

As empresas mais valiosas do mundo faturam bilhões usando as informações que deixamos cotidianamente nas redes sociais e na internet. Diante disso, surge a questão: Qual a importância da ética nos sistemas de informação e no uso da internet e como as questões de segurança e privacidade de dados individuais são vistas pela sociedade atual?

1.3 Objetivos

A pesquisa buscou realizar um estudo descritivo por meio de pesquisa bibliográfica, para identificar práticas relacionadas à ética em sistemas de informação com relação à privacidade na rede e fornecer contribuições ao estudo do

tema, por meio da caracterização de um cenário sobre a ética e sua utilização através do sistema de informação internet.

O objetivo geral desse trabalho é apresentar a importância da conduta ética nas relações entre usuários, através da rede, e os dilemas éticos relativos à privacidade dos indivíduos. Os objetivos específicos visam analisar:

- o que é e como se estrutura um sistema de informações (SI);
- o que é ética e a importância dos valores, princípios e conduta éticos que envolvem um sistema de informações (SI);
- a relação entre segurança e privacidade na rede, bem como o surgimento de dilemas éticos quanto à utilização de tecnologias da informação (TI) no âmbito pessoal e no âmbito do trabalho; e
- o tratamento de bases de dados, seu armazenamento e transmissão segundo a legislação brasileira.

1.4 Justificativa

A principal justificativa para a realização da pesquisa residiu na necessidade de identificar a relação da ética em sistemas de informação com o tema da privacidade na rede nos termos social, econômico e político. Nesse sentido, o trabalho visa contribuir para um processo de conscientização sobre a importância do tema privacidade nas relações entre usuários, principalmente cidadão/empresa considerando os aspectos legais envolvidos na disposição de informações de caráter privado.

Por fim, destaca-se a importância do trabalho de pesquisa, pelo fato de existir pequena quantidade de estudos científicos relacionados ao tema da ética nos sistemas de informação, o que permite divulgar o referido tema que está em plena ascensão e possibilitar novas pesquisas científicas.

1.5 Estrutura do Trabalho

Para atender aos objetivos propostos, o trabalho de pesquisa foi dividido em capítulos e subcapítulos. O capítulo 1 abrange 5 subcapítulos que remontam à

introdução sobre o tema de pesquisa, destacando uma breve apresentação do tema, a identificação do problema, os objetivos da pesquisa e a justificativa adotada.

O capítulo 2 abrange 15 subcapítulos que fundamentam o referencial teórico utilizado, discriminando os sistemas de informação, tópicos sobre ética, políticas e termos que relacionam o tema proposto. Ainda, apresentam-se algumas implicações com relação ao uso das novas tecnologias e os impactos na sociedade, emergindo alguns dilemas éticos associados ao trabalho e ao lazer.

O capítulo 3 reflete a metodologia utilizada para o alcance dos objetivos do presente trabalho. O capítulo 4 e o capítulo 5 incluem a conclusão e as limitações e sugestões para estudos futuros, respectivamente.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Sistemas de Informação

Pessoas e organizações usam informações e interagem com os sistemas todos os dias. Usamos caixas eletrônicos automáticos em bancos para verificar saldos, retirar extratos ou mesmo sacar/depositar dinheiro. Podemos utilizar o home ou internet banking (acesso remoto ao banco) para fazer movimentações financeiras em nossa conta pessoal, bem como consultar saldos e autorizar débito automático. Graças à internet, acessamos e selecionamos informações diversas que nos permitem comparar preços de produtos e serviços de empresas, por exemplo. Através da rede, temos acesso às lojas virtuais e podemos encontrar praticamente de tudo, desde alimentos típicos a dispositivos de tecnologia de última geração.

Para tanto, quando queremos comprar algum produto ou adquirir um tipo de serviço o comum é pagarmos por ele, ainda que haja alguns serviços ou mesmo produtos “gratuitos” como a abertura de uma conta de e-mail, por exemplo. Antes é necessário que nos cadastremos junto à empresa ofertante, a qual devemos repassar alguns de nossos dados pessoais (como nome, data de nascimento, telefone e endereço residencial, entre outros) para que tenhamos acesso ao que queremos. Muitas vezes, não reparamos na importância que está relacionada a cada informação que repassamos para essas empresas e o que elas fazem ou poderão fazer com todos esses dados. Uma política de privacidade adotada pela empresa deve esclarecer aos futuros usuários (clientes) sobre o que será feito com suas informações pessoais, em termos de uso e temporalidade. Nem todas as empresas possuem uma política de privacidade clara; outras tantas, nem a possuem.

Vivemos hoje em uma economia informatizada. A informação por si possui valor, e o comércio muitas vezes envolve a troca de informações em vez de bens tangíveis. Os sistemas computacionais são cada vez mais utilizados para criar, armazenar e transferir informações (STAIR & REYNOLDS, 2011). Nesse sentido, o valor da informação se relaciona ao modo como ela pode auxiliar os tomadores de decisão a alcançar seus objetivos. Se empresa, como essa informação poderá ser utilizada para aumentar o volume de vendas ou satisfazer um novo nicho de

mercado, por exemplo. Se usuário (cliente), como essa informação poderá ser utilizada para fechar a aquisição de um produto ou ser a fonte confiável de uma pesquisa acadêmica, por exemplo.

No entanto, não vamos entrar num detalhamento profundo sobre as características das informações em um sistema de informações e nem sobre os tipos de sistemas existentes que detalham o funcionamento de um SI, pois esse não é o objetivo. Ao invés disso, identifiquemos apenas os conceitos básicos sobre o sistema, que devam gerar o entendimento necessário para a compreensão do funcionamento de um SI e sua relação com o tema privacidade na rede. O primeiro passo é conceituá-lo.

Segundo os autores O'Brien & Marakas (2012), um sistema é definido como um conjunto de componentes inter-relacionados com limites claramente definidos, que colaboram para a realização de um conjunto comum de objetivos, admitindo subsídios e produzindo resultados em um processo de transformação organizado.

Para Stair & Reynolds (2011), um sistema de informação (SI) é um conjunto de componentes inter-relacionados que coleta, manipula, armazena e dissemina dados e informações e fornece um mecanismo de realimentação para atingir um objetivo. Ainda, segundo Rosini & Palmisano (2003), o conceito básico de sistema de informações estabelece que todo o sistema é um conjunto de elementos interdependentes em interação, visando atingir um objetivo comum.

Definido o conceito de sistema de informações, podemos interpretá-lo segundo o esquema abaixo:

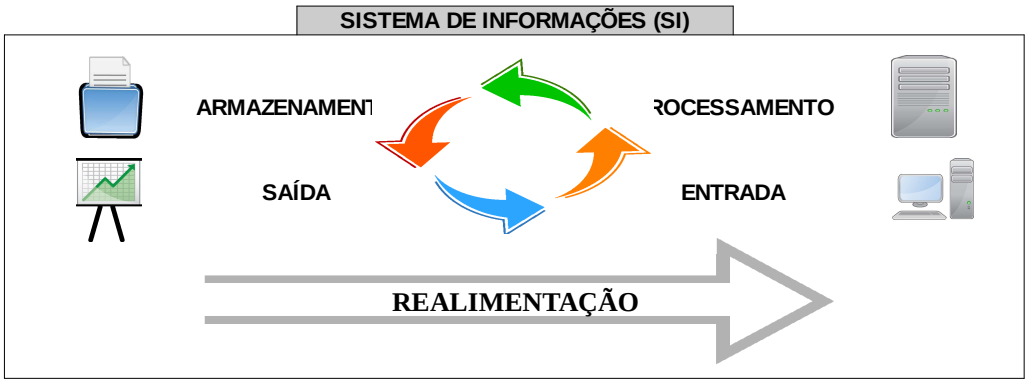

Figura 1: Componentes de um sistema de informação
Fonte: adaptado de Stair & Reynolds, 2011

A figura 1 representa o conjunto de componentes associados a um sistema de informações com base em computador. O primeiro componente é a **entrada** que é caracterizada pela *atividade de captar e reunir os dados brutos* (STAIR & REYNOLDS, 2011). A entrada, ou subsídio, envolve a captura e a montagem dos elementos que entram no sistema para serem processados (O'BRIEN & MARAKAS, 2012). O segundo componente, o **processamento**, significa converter ou transformar dados em resultados úteis. O processamento pode envolver a realização de cálculos, comparação de dados e execução de ações alternativas (STAIR & REYNOLDS, 2011). O processamento abrange os processos de transformação que convertem a entrada no resultado (O'BRIEN & MARAKAS, 2012). O terceiro componente, o **armazenamento**, envolve guardar os dados e as informações disponíveis para utilização futura (STAIR & REYNOLDS, 2011). O armazenamento é o ato ou efeito de armazenar, guardar, juntar os dados em um banco de dados para que seja possível seu resgate, consulta ou uso posterior. O quarto componente, a **saída**, envolve a produção de informações úteis, normalmente na forma de documentos e relatórios (STAIR & REYNOLDS, 2011). O resultado ou saída envolve a transferência dos elementos que foram produzidos por um processo de transformação ao seu destino final (O'BRIEN & MARAKAS, 2012). O quinto componente, a **realimentação**, é a informação originada no sistema que é utilizada para fazer mudanças na entrada ou nas atividades de processamento (STAIR & REYNOLDS, 2011). A realimentação ou *feedback* é o nome dado ao procedimento através do qual o processo de saída de um sistema é transferido para a entrada deste mesmo sistema, com o objetivo de aumentar, reduzir e/ou reavaliar a saída através de um ciclo contínuo.

O sistema de informações está tão difundido que torna fundamental sua utilização pelas empresas e a sociedade moderna, apesar de ainda haver um número relevante de exclusão digital no país. Segundo dados do IBGE (extraídos da pesquisa *pnad* em 16/05/2013), cerca de 53% dos brasileiros não têm acesso à internet. O que não quer dizer que todas essas pessoas não possuam alguns de seus dados pessoais registrados em algum banco de dados do governo, como o banco de dados da previdência social e o banco de dados do ministério da saúde, por exemplo. Isso ascende dilemas éticos que envolvem questões de segurança e liberdade. A segurança está relacionada ao destino e à utilização de dados pessoais, enquanto a liberdade está relacionada à vontade ou não em fazer parte do

sistema. Alguns especialistas discutem se haveria possibilidade ou não de um indivíduo escolher entre participar ou não do sistema, uma vez que o sistema está em todo lugar.

As pessoas utilizam um SI em muitas das suas rotinas, em casa, na rua ou no trabalho. Os sistemas estão inseridos em quase todos os aparatos tecnológicos disponíveis. Telefones celulares são os mais utilizados e não são apenas aparelhos para receber e fazer chamadas telefônicas. Os modelos mais simples incluem acesso à internet entre outros aplicativos. Os mais modernos já estão substituindo os velhos cartões de crédito em transações financeiras.

Entretanto, um sistema de informação não é apenas um software e/ou hardware isolado. A estrutura de um sistema de informações é mais abrangente. Um sistema de informação baseado em computador é um conjunto único de hardwares, softwares, banco de dados, telecomunicações, pessoas e procedimentos que são configurados para coletar, manipular, armazenar e processar dados em informações. Essa infraestrutura de tecnologia é um conjunto de recursos compartilhados do sistema de informação (SI) que forma a base de cada sistema de informação baseado em computador (STAIR & REYNOLDS, 2011). A figura 2 esquematiza a estrutura de um SI.

Figura 2: Estrutura de um sistema de informações
Fonte: Adaptado de Stair & Reynolds, 2011

A figura 2 ilustra o modelo de um sistema de informação que mostra uma estrutura conceitual fundamental para os principais componentes e atividades dos sistemas de informação. Um sistema de informação depende de recursos de *pessoas* (usuários finais e especialistas de SI), *hardware* (máquinas e meios de armazenamento de dados), *software* (programas e *procedimentos*), *dados* (base de dados e conhecimento) e *redes* (meios de comunicação e suporte de rede) para realizar entrada, processamento, saída, armazenamento e para controlar as atividades que convertem os recursos de dados em produtos de informação (O'BRIEN & MARAKAS, 2012).

A informação é um conjunto de dados organizados que possuem relação entre si. Não devemos confundir os dados com informações. Segundo Stair & Reynolds (2011), os dados são constituídos de fatos crus, pois são números isolados que por si só não possuem significância. Informação é um conjunto de fatos organizados de tal maneira que possuem valor adicional, além do valor dos fatos individuais.

Transformar os dados em informação é um processo, ou um conjunto de tarefas logicamente relacionadas realizadas para alcançar um resultado definido. O processo de definir relações entre os dados para criar informações úteis requer conhecimentos. Conhecimento é a consciência e a compreensão de um conjunto de informações e os modos como essas informações podem ser úteis para apoiar uma tarefa específica ou para chegar a uma decisão. Ter conhecimento significa entender as relações na informação (STAIR & REYNOLDS, 2011).

Os sistemas de informação têm sido desenvolvidos para atender as necessidades de todos os tipos de organizações e pessoas. A velocidade e a ampla utilização dos sistemas de informação, no entanto, abrem aos usuários uma variedade de ameaças de pessoas sem ética. Embora os sistemas de informação possam oferecer benefícios enormes, eles também apresentam inconvenientes. Alguns inconvenientes são menores, como estar sempre conectado ao trabalho e ao seu chefe por meio da internet, reduzindo o tempo livre. Outros podem ser mais graves, como no caso em que os dados pessoais, incluindo os dados do cartão de crédito, podem ser perdidos ou roubados, resultando em fraude e arruinando o crédito pessoal (STAIR & REYNOLDS, 2011).

Casos e mais casos de roubo de informações pessoais, principalmente, aquelas alocadas em banco de dados de esfera pública são anunciados a cada dia.

Além de transtornos pessoais, eles também causam danos financeiros para empresas e cidadãos. No Brasil, por exemplo, os chamados cibercrimes (aqueles realizados através de um computador) causam prejuízos na ordem de 16 bilhões de reais, segundo estudo realizado pela empresa Norton/Symantec no ano de 2012. Os cibercrimes incluem fraude por roubo, principalmente, de informações bancárias. A figura 3 ilustra o custo associado a crimes realizados através da internet.

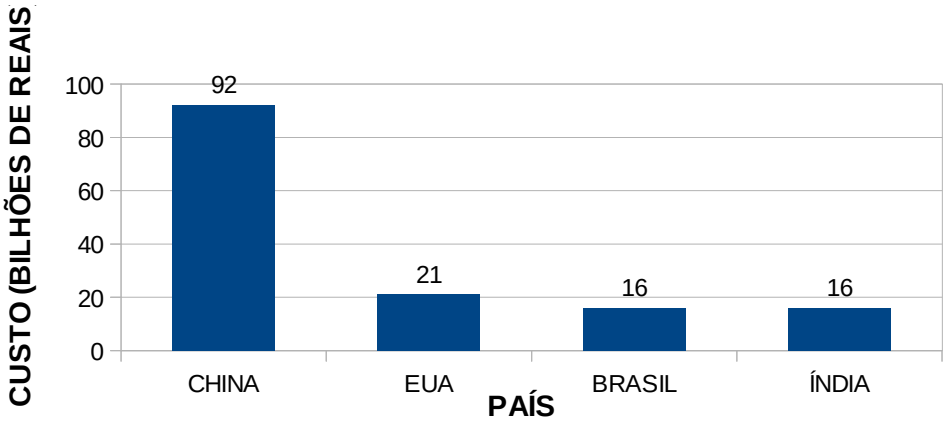

Figura 3: Custo associado a crimes na internet
Fonte: Adaptado do jornal NH, *cibercrimes: danos incluem fraude por roubo de informações bancárias*, 05/10/2012

A reportagem de um jornal local revela o custo associado ao roubo e as fraudes feitas por computador. Os danos causados por meio da internet no país incluem fraude e roubo de informações bancárias, usando vírus e representa 7% do prejuízo mundial originado pelo chamado cibercrime. E, segundo o estudo, 75% dos brasileiros que usam a Internet, de alguma forma, já foram lesados (Jornal NH, 05/10/2012).

Além dos prejuízos financeiros que as empresas e os usuários (clientes) enfrentam, há prejuízos intangíveis como, perda de confiabilidade do cliente perante a empresa e a perda de credibilidade da organização e seus reflexos na imagem corporativa. O vazamento de informações privadas pode levar a empresa a ser processada judicialmente, além de perder seus clientes. Evidentemente que uma política de segurança deve ser adotada por toda empresa para garantir que todas as informações que estão sob seu domínio e sejam de caráter privado não sejam dispostas ao público. No entanto, são recorrentes as falhas dos sistemas que permitem que terceiros acessem tais informações e cometam crimes variados como

a emissão de cheques roubados, documentos de identificação falsos e cartões de crédito clonados, entre outros.

Uma das razões pelas quais a preocupação com a privacidade é tão forte é que os dados muitas vezes são colhidos sem que o consumidor explicitamente os forneça. Uma pessoa que visita um web site pode ter esse fato registrado (no mínimo, seu endereço IP), bem como quais partes do site foram visitadas, que informações foram solicitadas, que links foram acessados e assim por diante, sem consentimento nem conhecimento. Outras informações podem ser colhidas de modo mais direto. As informações de diversos sites e fontes podem ser combinadas para desenvolver perfis individuais (HAWKINS, MONTHERSBAUGT & BEST, 2007).

No Brasil, embora previsto na constituição, a proteção à informação ainda carece de leis e regulamentações robustas. O Ministério da Justiça criou um blog no endereço <http://culturadigital.br/dadospessoais>, com o objetivo de receber contribuições de entidades, de especialistas e da população em geral sobre o tema da segurança à informação. O debate ficou aberto até abril de 2011 e agora serve de subsídio para a futura confecção de um projeto de lei sobre o assunto (BALTZAN & PHILLIPS, 2012). O *marco civil da internet* é um projeto de lei que promete normatizar e regulamentar a utilização da internet no país, incluindo temas de neutralidade, retenção, responsabilidade e privacidade de dados na rede. Tal projeto, que tramita no Congresso, foi iniciado em meados de 2009.

Outro motivo de preocupação que envolve o tema da privacidade na rede e que serviu de subsídio para desenvolver o projeto de lei, denominado marco civil da internet, diz respeito ao modo como os dados são tratados através do sistema. O fluxo de dados através da rede é enorme e cresce em volume exponencial. Um dos problemas típicos do tratamento de dados pessoais em grande volume é que a chance de algo dar errado e estes dados *vazarem*, ou serem difundidos indevidamente, tende a ser considerável. Não é por outro motivo que o tema do vazamento de dados pessoais é uma das principais questões enfrentadas ao se vislumbrar modelos normativos para tratar da matéria (DONEDA, 12/03/2011).

O vazamento de dados é geralmente consequência de ineficiências operacionais, onde pessoas superestimam as suas capacidades de controlar o sistema devido à facilidade de se registrar um volume cada vez maior de informações. A administração destes grandes volumes de informação é algo problemático, e os reflexos de uma má política de administração da informação

dentro de corporações são visíveis, para além das questões envolvendo dados pessoais, e abrangem o vazamento de segredos industriais e comerciais, planos de negócios, estruturas organizacionais e tantos outros dados que tenham caráter privado. A necessidade de manipular informações em grande volume faz com que seja comum que eles sejam manipulados sem o cuidado devido, em quantidades excessivas, por pessoas não qualificadas ou por qualquer outro procedimento que facilite uma eventual difusão pública, seja acidental ou mesmo intencional (DONEDA, 12/03/2011).

O cidadão brasileiro vem tomando conhecimento da gravidade do problema do vazamento de dados da pior maneira possível, ou seja: assistindo a reiterados casos de vazamento de dados pessoais, com frequência cada vez maior e cuja publicidade vem sendo sensivelmente intensificada (DONEDA, 12/03/2011). Assim ocorreu com os recentes casos de vazamento de dados pessoais da Receita Federal (2010), do MEC (2012), da Petrobras (2013). Consideremos a tentativa absurda de comercialização de dados privados de eleitores brasileiros por parte do Tribunal Superior Eleitoral, ainda este ano.

O conhecimento público sobre casos de vazamento de dados pessoais provoca, justificadamente, uma grande desconfiança do cidadão em relação à corporação que os deixou vazar, seja esta privada, seja esta estatal. Vazamentos de dados costumam deixar marcas que, por vezes, são difíceis de apagar e, resgatar o respeito e a confiança do cidadão ou do consumidor pode ser um desafio para estas empresas.

Na batalha para proteger informações valiosas e privadas on-line, todos os níveis de gerenciamento dos negócios e dos governos estão ou devem estar totalmente envolvidos (STAIR & REYNOLDS, 2011). Os desvios aumentam a partir de pessoas que procuram se beneficiar financeira ou politicamente, o que acarreta o surgimento de dilemas éticos sobre a utilização de informações privadas.

2.2 Ética

A tecnologia da informação exerce um papel fundamental nas relações em sociedade, colaborando para a evolução de suas interações. Reduz fronteiras, aumenta o fluxo de informações, gera comodidade, acelera negócios, propicia a

inovação, etc. Muitos pontos positivos podem ser creditados aos sistemas e aos meios tecnológicos que, realmente, transformam as relações em sociedade.

Por outro lado, os sistemas e os meios tecnológicos podem ter alguns pontos negativos, como, por exemplo, serem utilizados de forma inadequada por pessoas que queiram obter vantagens ou por pura imperícia, inclusive por não aceitação. Para que as tecnologias possam ser efetivas, se faz necessário que os usuários as compreendam e aceitem utilizá-las. Os sistemas e os meios tecnológicos por si só raramente são culpados por desvios que possam ocorrer, pois para que eles sejam funcionais as pessoas precisam operá-los segundo padrões preestabelecidos.

Portanto, quando falamos em sistemas e meios tecnológicos falamos, também, de pessoas. Segundo os autores Stair & Reynolds (2011), as pessoas podem ser o elemento mais importante na maioria dos sistemas de informação com bases em computador; elas fazem a diferença entre o sucesso e o fracasso para a maioria das organizações. O pessoal dos sistemas de informação inclui todas as pessoas que gerenciam, administram, programam, mantêm e rodam o sistema. Ainda, segundo os autores, os *usuários* são pessoas que trabalham com sistemas de informação para conseguir resultados; incluem executivos financeiros, equipe de marketing, operadores da produção e muitos outros. Certos usuários de computador também são a própria equipe de SI.

Nesse contexto, a tecnologia da informação tem um papel fundamental que muitas vezes tem sido negligenciado, ou mesmo tem passado despercebido, na maioria das empresas. As competências essenciais e o conhecimento coletivo se baseiam em informações de negócio: conhecimento e experiência. O papel a ser desempenhado pela TI é estratégico: ajudar o desenvolvimento coletivo e o aprendizado contínuo, tornando mais fácil para as pessoas na organização compartilharem problemas, expectativas, ideias e soluções. Neste cenário competitivo do mundo contemporâneo, o principal desafio das organizações está em estabelecer os padrões éticos nas relações entre pessoas e empresas (PALETTA & PALETTA, 2002).

Mas, afinal, o que é ética? A ética é uma característica inerente a toda ação humana e, por essa razão, é um elemento vital na produção realidade social. Todo homem possui um senso ético, uma espécie de consciência moral, estando constantemente avaliando e julgando suas ações para saber se são boas ou más, certas ou erradas, justas ou injustas (PALETTA & PALETTA, 2002).

O termo ética deriva do grego *ethos -comportamento* (MARQUES, 2010). A ética é formada pelos princípios morais, valores e crenças internos que as pessoas usam para analisar ou interpretar uma situação e, então, decidir qual é a forma "certa" ou adequada de se comportar. Ao mesmo tempo, a ética também indica o que é um comportamento inadequado e como uma pessoa deve se comportar para evitar prejudicar a outra (JONES & GEORGE, 2008).

Segundo Ferreira (2005), a ética pode ser definida como "O estudo dos juízos de apreciação referentes à conduta humana, do ponto de vista do bem e do mal". Ou ainda, segundo o mesmo autor, um "Conjunto de normas e princípios que norteiam a boa conduta do ser humano".

Dubrin (2003) define a ética como: as escolhas morais que uma pessoa faz e o que essa pessoa deveria fazer. É o que ela considera como certo e errado ou como bom ou mau. É transformar valores em ação.

Os dilemas éticos surgem, segundo Jones & George (2008), a partir do impasse em que as pessoas se encontram quando têm de decidir se devem agir de determinada maneira que possa ajudar outra pessoa ou grupo, e esta é a coisa "certa" a fazer, embora agir desse modo possa ir contra seus próprios interesses. Um dilema pode surgir ainda quando uma pessoa precisa decidir entre duas ações diferentes, sabendo que, qualquer que seja a ação escolhida por ele ou ela, isso resultará em danos para uma pessoa ou grupo, embora possa beneficiar outro. O dilema ético aqui é decidir qual é o "menor dos males".

Jacomino (2000), apud Paletta & Paletta (2002, p. 4), associa a ética ao sucesso profissional, mencionando o seguinte:

> Hoje, mais do que nunca, a atitude dos profissionais em relação às questões éticas pode ser a diferença entre o seu sucesso ou fracasso. Ser ético nada mais é do que agir direito, proceder bem, sem prejudicar os outros. Ser ético é, também, agir de acordo com os valores morais de uma determinada sociedade. Essas regras morais são resultado da própria cultura de uma comunidade. Elas variam de acordo com o tempo e sua localização no mapa. A regra ética é uma questão de atitude, de escolha. Já a regra jurídica não prescinde de convicção íntima – as leis têm de ser cumpridas independentemente da vontade das pessoas. A ética não é algo superposto à conduta humana, pois todas as nossas atividades envolvem uma carga moral.

O problema essencial ao lidar com questões éticas e resolver dilemas morais é que não há regras ou princípios absolutos ou inquestionáveis que possam ser

desenvolvidos para decidir se uma ação é ética ou antiética. Em termos simples, pessoas ou grupos diferentes podem disputar quais ações são éticas ou antiéticas dependendo de seu próprio interesse e atitudes, crenças e valores específicos (JONES & GEORGE, 2008).

Jacomino (2000), apud Paletta & Paletta (2002, p. 4), menciona: “a empresa que almeje ser ética deve divulgar declarações precisas definindo as regras e deve criar procedimentos de verificação para assegurar que todos na organização as estão cumprindo”.

Como dito anteriormente, as pessoas precisam entender o que se espera delas e como suas interações podem afetar a coletividade. Entretanto, como salientam os autores Baltzan & Phillips (2012), agir eticamente e agir legalmente nem sempre são a mesma coisa.

A figura 4 representa um quadro de comportamento ético e legal. A meta ideal para as organizações é tomar decisões dentro do quadrante I, que são legais e éticas.

	SISTEMA DE INFORMAÇÕES (SI)	
	LEGAL	**ILEGAL**
ÉTICO	**I**	**II**
NÃO ÉTICO	**III**	**IV**

Figura 4: Agir eticamente e agir legalmente nem sempre são a mesma coisa
Fonte: Extraída de Baltzan & Phillips, 2012, p. 94

Ao estudar a relação entre ética e lei, é importante entender que nem as leis nem a ética são princípios fixos, gravados na pedra, que não mudam com o tempo. Crenças éticas alteram-se e mudam com o passar do tempo, e assim as leis mudam para refletir as crenças éticas em transformação de uma sociedade (JONES & GEORGE, 2008).

A internet tem modificado o comportamento humano, incentivando a paixão pelo conhecimento, educação e cultura. A sociedade contemporânea valoriza comportamentos que praticamente excluem qualquer possibilidade de cultivo de relações éticas. É fácil verificar que o desejo obsessivo na obtenção, possessão e consumo da maior quantidade possível de bens materiais é o valor central na nova ordem estabelecida no mundo e que o prestígio social é concedido para quem consegue esses bens. Esse desejo se tornou mais evidente e de acesso mais fácil depois da ascensão do comércio eletrônico na internet. Um dos campos mais carentes, no que diz respeito à aplicação da ética, é o das novas tecnologias e nisso inclui-se a internet (PALETTA & PALETTA, 2002).

Não existe uma legislação prevendo condutas ou regras, com isso fica muito perto o limite da ética no trabalho e exercício profissional. Uma das principais e mais evidentes realidades da internet é o individualismo extremo, esse fator, muitas vezes associado à falta de ética pessoal, tem levado alguns profissionais a defender seus interesses particulares acima dos interesses das empresas em que trabalham, colocando-as em risco (PALETTA & PALETTA, 2002).

Ética, além de ser a ciência que estuda o comportamento moral das pessoas na sociedade, é um investimento. Um investimento que traz bons frutos em longo prazo. É importante entender que o conceito de que estender benefícios à sociedade é um meio concreto de abraçar a ética e criar uma boa imagem para a empresa. Na internet, é extremamente necessário se ter credibilidade para que a empresa possa sobreviver no comércio eletrônico (PALETTA & PALETTA, 2002).

Jacomino (2000), apud Paletta & Paletta (2002, p. 4), alerta: “quando falamos de empresa ética, estamos falando de pessoas éticas. Uma política interna mal definida por um funcionário de qualquer nível pode atingir em cheio dois dos maiores patrimônios de uma empresa: a marca e a imagem”.

Nesse sentido, percebe-se que a conduta ética é de vital importância para as relações em sociedade, pois deriva de normas e princípios que regem os comportamentos em coletividade. Portanto, as empresas e os profissionais devem sempre considerar suas decisões sob o aspecto da ética, medindo valores e seus reflexos e agindo de forma responsável, priorizando o bem coletivo ao invés do individual.

Além da ética geral que foi abordada até agora, existe a aplicação da ética de uma maneira mais específica: a ética em sistemas de informação. O avanço das

novas tecnologias e o aumento da utilização de computadores, seja para o desempenho do trabalho profissional, seja para o desenvolvimento de relações sociais, despertou o surgimento de novos paradigmas e dilemas éticos com relação ao comportamento virtual por parte de seus usuários. Tal assunto será tratado a seguir.

2.2.1 Ética em Sistemas de Informação

A ética da informação diz respeito às questões éticas e morais decorrentes do desenvolvimento e utilização das tecnologias da informação, bem como a criação, coleta, duplicação, distribuição e processamento da informação em si (com ou sem o auxílio das tecnologias de informática). Os indivíduos determinam como utilizar essa informação e como ela os afeta. Como os indivíduos se comportam em relação aos outros e como lidam com a informação e a tecnologia são questões amplamente influenciadas pela ética de cada um deles. Os dilemas éticos geralmente não surgem em situações simples e bem definidas, mas de um confronto de metas concorrentes, responsabilidades e lealdades. Inevitavelmente, o processo de decisão tem mais de uma decisão “correta” socialmente aceitável (BALTZAN & PHILLIPS, 2012).

Ética e segurança são dois pilares fundamentais para todas as empresas. Nos últimos anos, eventos como os escândalos da Enron e de Martha Stewart, acompanhado do 11 de setembro, lançaram uma nova luz sobre o significado de ética e segurança. Quando o comportamento de alguns indivíduos pode destruir empresas de bilhões de dólares, o valor da ética e da segurança torna-se evidente (BALTZAN & PHILLIPS, 2012).

Ainda, segundo os autores, as questões éticas envolvendo a violação de direitos autorais e a propriedade intelectual estão consumindo o mundo do e-business. Os avanços na tecnologia facilitam copiar tudo, da música às imagens. A tecnologia levanta novos desafios para a nossa ética – os princípios e as normas que guiam o nosso comportamento em relação a outras pessoas.

Nesse sentido, os valores e os princípios éticos também estão inseridos nos sistemas de informação, pois as interações sociais ganharam nova forma a partir do desenvolvimento dessas tecnologias. As fronteiras desapareceram. Por exemplo,

redes sociais como facebook e linkedin tornaram possível o relacionamento e novas formas de comunicação entre pessoas através da grande rede. Um habitante do Brasil pode se comunicar em tempo real com outro habitante de algum país da Ásia, utilizando mensagens de texto, dispositivos de áudio e vídeo, por exemplo.

Muitas das tecnologias existentes hoje foram desenvolvidas, num primeiro momento, para atender as necessidades das empresas, como sistemas ERP, PDAs e os aparelhos celulares. Com a difusão dessas tecnologias na sociedade, elas foram adaptadas para a utilização de massa, ou seja, para uso das pessoas físicas.

Na sociedade atual, que usa intensivamente a informação, o uso de dados pessoais para fins comerciais tornou-se prática corrente, que permite a fornecedores e produtores de todo tipo de mercadoria ou serviço alcançar vantagens sobre seus concorrentes. Assim, perfis de consumidores bem elaborados, consolidando informações diversificadas, são de grande valia para todo tipo de empresa (LINS, 2000).

A informação não tem ética. A informação não se importa em como será usada. Ela não vai parar, por conta própria, de enviar spam aos clientes, de compartilhar seu conteúdo eventualmente confidencial ou pessoal, ou de revelar detalhes a terceiros. A informação não pode se excluir ou se preservar. Portanto, recai sobre os ombros daqueles que possuem a informação o estabelecimento de diretrizes éticas sobre a forma de gerir a informação (BALTZAN & PHILLIPS, 2012).

Um computador pode ser usado como uma ferramenta para obter acesso a informações valiosas e como meio para roubar muito dinheiro. Talvez seja uma questão de motivação – muitas pessoas que cometem crimes por computador justificam que o fazem pelo desafio, não pelo dinheiro. A fraude do cartão de crédito – pela qual um criminoso obtém ilegalmente acesso à linha de crédito de outra pessoa com números de cartões de créditos roubados – é a principal preocupação dos bancos e instituições financeiras hoje (STAIR & REYNOLDS, 2011).

Em geral, segundo os autores, os criminosos precisam de duas habilidades para cometer a maioria dos crimes por computador. Primeiro, o criminoso precisa saber como obter acesso ao sistema computacional. Algumas vezes, obter acesso requer conhecimento de um número de identificação e uma senha. Em segundo lugar, o criminoso precisa saber como manipular o sistema para produzir o resultado desejado. Com frequência, uma senha crítica de computador foi discutida com uma pessoa, uma prática chamada de *engenharia social*. Ou os agressores

simplesmente buscam no lixo – *mergulho no lixo* – importantes peças de informações que podem ajudar a invadir os computadores ou a convencer alguém da empresa a dar-lhes mais acesso. Além disso, mais de 2 mil web sites oferecem ferramentas digitais – gratuitamente – que permitem que as pessoas encontrem informações privadas, invadam computadores, assumam os controles de uma máquina ou recuperem uma cópia de cada tecla digitada.

A privacidade é um dos maiores problemas éticos enfrentados pelas empresas. A privacidade é o direito de ser deixado sozinho quando você quiser, de ter controle sobre seus próprios bens pessoais e não ser observado sem o seu consentimento. A privacidade está relacionada à *confidencialidade*, que é a garantia de que as mensagens e informações estão disponíveis apenas para aqueles que estão autorizados a vê-las. Algumas das decisões mais problemáticas enfrentadas pelas organizações estão situadas nas águas turvas e turbulentas da privacidade. A carga vem do conhecimento de que a cada vez que um funcionário toma uma decisão sobre questões de privacidade, o resultado poderia afundar a empresa (BALTZAN & PHILLIPS, 2012).

Nos últimos dez anos, o assunto da privacidade ganhou novas facetas, em virtude da disseminação das tecnologias de tratamento da informação. São essencialmente três os fenômenos que vêm contribuindo para uma maior preocupação com o tema: primeiramente, a estruturação de bases de dados, que abriu a possibilidade de se cruzar informações com grande facilidade, construindo perfis detalhados de praticamente qualquer pessoa, a um custo baixo, até mesmo sem a ciência do interessado; em segundo lugar, a disseminação da informática, que culminou com a ampla utilização da Internet, estimulando praticamente a todos a manterem em forma digital as suas informações, facilitando a sua coleta; e, finalmente, a padronização de equipamentos e sistemas, o que facilitou a aquisição de informações mantidas por usuários de informática, inclusive sem o seu conhecimento (LINS, 2000).

Cate (1997, p. 2), apud Lins (2000), relaciona alguns exemplos de dados pessoais que são coletados e cruzados a partir das nossas atividades usuais:

> a) Cartórios, hospitais, seguradoras e bancos detêm informações sobre o nosso histórico familiar, financeiro e de saúde.
> b) Empresas telefônicas mantêm cadastro dos números mais usados e da frequência de ligações.

> c) Editoras mantêm informações sobre hábitos de leitura e procuram elaborar perfis econômicos dos assinantes.
> d) Operadoras de cartão de crédito elaboram perfis de consumo e histórico de compras.
> e) Mercados e lojas mantêm histórico de consumo de alimentos, bebidas, vestuário, automóveis, aparelhos elétricos e outros bens e serviços.
> f) Provedores na Internet mantêm registro de acesso a *sites*, envio e recebimento de e-mails e preferências de material acessado.

O cruzamento de informações permite a criação de retratos que mostram os nossos principais hábitos e práticas, revelando facetas das quais o próprio indivíduo muitas vezes não se apercebe. Podem ser elaborados por empresas privadas, para fins comerciais, ou por órgãos do governo, inclusive para fins de investigação criminal (LINS, 2000).

Ainda, segundo o autor, tais práticas constituem um problema social e jurídico de grande interesse, uma vez que é preciso determinar até que ponto e de que forma poderão ser exercidas, se é que o podem, sem constituir uma violação da privacidade pessoal.

Infelizmente, há poucas regras rígidas e rápidas para determinar sempre o que é e o que não é ético. Conhecer a lei nem sempre ajuda, porque o que é legal pode não ser sempre ético, e o que poderia ser ético nem sempre é legal (BALTZAN & PHILLIPS, 2012). Políticas e procedimentos rígidos que garantam redes, funcionários e parceiros operando da maneira mais segura possível é o caminho.

2.3 Políticas de Gerenciamento da Informação

Embora as leis de privacidade para as organizações privadas não sejam muito restritivas, a maioria das organizações é muito sensível às questões de privacidade e de justiça. Elas percebem que as invasões de privacidade podem prejudicar seus negócios, afastar consumidores e reduzir dramaticamente suas receitas e lucros (STAIR & REYNOLDS, 2011).

Tratar informações corporativas confidenciais como um recurso valioso reflete uma boa administração. Formar uma cultura empresarial baseada em princípios éticos que os funcionários possam entender e implementar é gestão responsável (BALTZAN & PHILLIPS, 2012).

Considere uma importante empresa internacional de cartões de crédito. Se a empresa vender informações financeiras confidenciais de milhões de consumidores para outra empresa, os resultados podem ser desastrosos. Em questão de dias, os negócios e as receitas da empresa podem ser reduzidos drasticamente. Portanto, a maioria das organizações mantém políticas de privacidade, embora elas não sejam exigidas por lei. Algumas empresas podem até possuir um estatuto de direitos que especifica como a privacidade dos funcionários, clientes e consumidores será protegida. As políticas corporativas de privacidade devem definir o conhecimento do consumidor, o controle, o aviso e o consentimento sobre o armazenamento e o uso de suas informações. Elas também podem estabelecer quem tem acesso aos dados privados e quando podem ser usados (STAIR & REYNOLDS, 2011).

As empresas devem registrar sua política, estabelecendo orientações aos funcionários, procedimentos de pessoal e regras de organização da informação. Essas políticas definem as expectativas dos funcionários sobre as práticas e as normas da organização e protegem a organização da má utilização dos sistemas de informática e recursos de TI. Se os funcionários de uma empresa utilizam computadores no trabalho, a organização deve, no mínimo, implementar políticas eletrônicas. As políticas eletrônicas (epolicies) são políticas e procedimentos que visam o uso ético dos computadores e da internet no ambiente de negócios (BALTZAN & PHILLIPS, 2012).

A figura 5 apresenta alguns exemplos de políticas de privacidade dispostas por algumas empresas em seus web sites:

EMPRESA	URL (ENDEREÇO ELETRÔNICO)
extra.com	http://www.extra.com.br/CentraldeAtendimento/politica-privacidade.aspx#info
americanas.com	http://www.americanas.com.br/estatica/politica-de-privacidade
fnac.com	http://fnac.neoassist.com/?action=answer&id=13086417&match_number=4&question=Pol%C3%ADtica+de+Privacida
Google	https://www.google.com.br/intl/pt-BR/policies/privacy/
GVT	http://www.gvt.com.br/PortalGVT/Atendimento/Area-Aberta/Documentos/Politica-de-Privacidade
Anuntis	http://www.infojobs.com.br/ajuda/aviso_legal__1902.aspx

Figura 5: Políticas corporativas de privacidade
Fonte: adaptado de Stair & Reynolds, 2011

Todas as empresas listadas acima possuem sua própria política de privacidade, que pode ser identificada de forma clara em seu web site. Os usuários devem sempre buscar essas informações antes de repassar dados pessoais através da internet para que estejam cientes do que será feito a partir de suas informações que serão coletadas pela empresa. As empresas que possuem sua política de privacidade geralmente as que possuem certificações e são auditadas periodicamente por instituições certificadoras.

Instituições certificadoras como Ebit, Truste e Certisign, são empresas que garantem a “blindagem” do site, prevenindo ataques de hackers e vulnerabilidades relativas à segurança do sistema de informações. Os sites que possuem essas credenciais podem ser considerados seguros em seu ambiente de navegação.

2.4 Segurança e Privacidade

A privacidade está relacionada com a segurança da informação. Logo, quando falamos de privacidade na rede, também estamos falando de segurança na rede. Um ambiente virtual seguro diminui as chances de que desvios ocorram principalmente àqueles associados ao roubo ou vazamento de dados privados. Para tanto, tecnologia e pessoas devem estar alinhadas no sentido de proporcionar um ambiente virtual seguro para navegação.

Existem diversos tipos de desvios que podem ocorrer no ambiente virtual. O roubo de identidade é o mais recorrente. Ele é um crime pelo qual um impostor obtém importantes informações sobre identificação pessoal, como os números do seguro social ou da carteira de motorista, para se passar por outra pessoa. As informações são usadas para obter crédito, mercadoria e/ou serviços no nome da vítima ou para fornecer falsas credenciais ao ladrão (STAIR & REYNOLDS, 2011).

Ainda, segundo os autores, em alguns casos, o ladrão de identidade usa informações pessoais para abrir novas contas de crédito, estabelecer um serviço de telefone celular ou abrir uma nova conta bancária para obter cheques em branco. Em outros casos, o ladrão de identidade usa informações pessoais para obter acesso às contas reais das pessoas. Em geral, o ladrão altera o endereço de

correspondência de uma conta e faz uma enorme compra antes que a pessoa, cuja identidade foi roubada, perceba que há um problema. A internet tornou mais fácil para um ladrão de identidade usar as informações roubadas porque as transações podem ser realizadas sem qualquer interação pessoal.

Inúmeros são os casos anunciados diariamente pelos veículos de comunicação. No Brasil, o mais comum é a venda de cheques em branco que podem ser negociados por 150 ou 200 reais nas grandes metrópoles, como Porto Alegre, por exemplo. Golpes do cartão de crédito clonado e de abertura de contas bancárias em nome de terceiros também são recorrentes.

Do ponto de vista do usuário comum, a segurança e a privacidade do ambiente virtual pode, muitas vezes, passar despercebida. Do ponto de vista do usuário empresa, a segurança e a privacidade dos dados que estão sob seu domínio em seu ambiente virtual é questão de sobrevivência. Portanto, a manutenção de um ambiente virtual seguro é fundamental para evitar danos financeiros, na imagem e reputação da empresa.

A informação organizacional é o capital intelectual. Assim como as empresas protegem seus ativos – mantendo seu dinheiro em um banco ou proporcionando um ambiente de trabalho seguro aos funcionários –, elas também devem proteger seu capital intelectual. O capital intelectual de uma empresa inclui tudo, desde patentes até informações transacionais e analíticas. Com falhas de segurança em ascensão e hackers de computador em todo lugar, uma empresa deve colocar em prática medidas fortes de segurança para sobreviver (BALTZAN & PHILLIPS, 2012).

Os dados e informações são ativos valiosos de uma corporação. O uso intencional de programas ilegais e destrutivos para alterar ou destruir dados é tão criminoso quanto destruir bens tangíveis. Os mais comuns desses programas são os vírus e os worms, programas de software que, quando carregados em um sistema computacional, destruirão, interromperão ou causarão erros no processamento. Tais programas são chamados de malware e o índice de crescimento desses programas é epidêmico. A empresa de segurança da internet McAfee calcula que a cada dia surgem de 150 a 200 programas malware (STAIR & REYNOLDS, 2011).

A figura 6 elenca os principais softwares (programas) utilizados para práticas ilícitas que ameaçam a segurança e a privacidade de dados através do uso da internet.

PROGRAMA	DESCRIÇÃO
Vírus	É um programa de computador capaz de unir-se aos discos ou outros arquivos e reproduzir-se repetidamente, em geral, sem o conhecimento ou permissão do usuário. Alguns vírus se anexam aos arquivos, de modo que quando o arquivo infectado é executado, o vírus também é. Outros vírus ficam na memória de um computador e infectam os arquivos quando o computador é aberto, modifica ou cria arquivos.
Worms	São programas parasitas que se reproduzem, mas, diferente dos vírus, não infectam outros arquivos de programas computacionais. Os worms podem criar cópias no mesmo computador ou podem enviar as cópias para outros computadores via rede. Os worms frequentemente se espalham via Internet relay Chat (IRC).
Cavalo de Troia	É um programa malicioso que se disfarça de uma aplicação útil ou jogo e faz deliberadamente algo que o usuário não espera. Os cavalos de Troia não são vírus porque não se reproduzem, mas podem ser igualmente destrutivos.
Bomba lógica	É um tipo de cavalo de Troia que se executa quando ocorrem condições específicas. Os disparadores para as bombas lógicas podem ser uma mudança em um arquivo por uma série determinada de batidas no teclado ou em um momento ou data específicos.
Rootkit	É um conjunto de programas que permite que seus usuários obtenham acesso em nível de administrador a um computador ou uma rede. Uma vez instalado, o atacante pode obter controle total do sistema e até ocultar a presença do rootkit dos legítimos administradores do sistema.
Variante	É uma versão modificada de um vírus produzido pelo autor do vírus ou por outra pessoa que altera o código do vírus original. Se as mudanças forem pequenas, a maioria dos antivírus detectará as variantes. No entanto, se as mudanças forem significativas, a variante pode passar despercebida pelo software antivírus.
Worm Storm	É um calo de Troia que infecta computadores pessoais que executam os sistemas operacionais da Microsoft. Ele infecta mensagens de e-mail. O e-mail contém um anexo que, se aberto, carrega vários programas malware em um computador pessoal. O resultado é que o computador fica comprometido e age como um computador "zumbi" sob o controle de outros computadores.
Spyware	É um software instalado em um computador pessoal para interceptar ou assumir controle parcial sobre a interação do usuário com o computador sem o seu conhecimento ou permissão. Algumas formas de spyware secretamente entram nas batidas do teclado para que o nome do usuário e as senhas possam ser capturados. Outras formas de spyware registram informações sobre os hábitos de navegação na Internet do usuário e sites visitados.

Figura 6: Principais ameaças à segurança e à privacidade de dados
Fonte: Adaptada de Stair & Reynolds, 2011

A segurança da informação é um termo amplo que abrange a proteção da informação contra mau uso acidental ou intencional por pessoas dentro ou fora da empresa. A segurança talvez seja a mais fundamental e essencial de todas as tecnologias/disciplinas que uma empresa deve ter diretamente no local de suas operações para executar sua estratégia de negócios (BALTZAN & PHILLIPS, 2012).

Isso demonstra a importância da adoção de normas e procedimentos de segurança alinhados às estratégias de negócio da organização. As políticas de segurança da informação identificam as regras necessárias para manter a segurança da informação. Um plano de segurança da informação detalha como a empresa implementará as políticas de segurança da informação (BALTZAN & PHILLIPS, 2012). A figura 7 exemplifica os passos para adoção de um plano de segurança da informação.

CINCO PASSOS PARA A CRIAÇÃO DE UM PLANO DE SEGURANÇA DA INFORMAÇÃO	
1. Desenvolva as políticas de segurança da informação	Identifique quem é responsável e confiável para projetar e implementar as políticas de segurança da informação da empresa. Simples, mas tipos de políticas de segurança da informação altamente eficazes incluem: exigir que os usuários façam log off de seus sistemas antes de sair para almoço ou reuniões; nunca compartilhar senhas; e mudar as senhas pessoais a cada 60 dias.
2. Comunique as políticas de segurança da informação	Ensine as políticas a todos os funcionários e estabeleça claras expectativas de cumprimento das políticas. Por exemplo, deixe todos os funcionários cientes de que irão receber uma advertência formal caso deixem um computador desprotegido.
3. Identifique os principais ativos e riscos associados da informação	Exija o uso de identificação (ID) de usuário, senhas e softwares antivírus em todos os sistemas. Certifique-se de que qualquer sistema que contenha links para redes externas tenha as devidas proteções técnicas, tais como firewalls ou softwares de detecção de intrusos. Um firewall é um hardware e/ou software que protege uma rede privada por meio da análise de informações que entram e saem da rede. Um software de detecção de intrusos (IDS) procura por padrões no tráfego de informações e da rede para indicar os ataques e responder rapidamente a eles para evitar qualquer dano.
4. Teste e reavalie os riscos	Realize revisões contínuas de segurança, auditorias, verificação de antecedentes e avaliações de segurança.
5. Obtenha apoio das partes interessadas	Obtenha a aprovação e o apoio das políticas de segurança da informação, do conselho de administração e de todas as partes interessadas.

Figura 7: Criando um plano de segurança da informação
Fonte: Extraída de Baltzan & Phillips, 2012, p. 108

Assim como o usuário empresa, o usuário comum também precisa estar atento às ameaças que cercam o ambiente virtual. Ter em mente que utilizar software antivírus e mantê-lo atualizado, bem como ativar o software/hardware firewall são medidas importantes para assegurar um ambiente de navegação mais seguro, preservando sua privacidade. Outro ponto é visitar somente web sites que iniciem com https:// em sua barra de endereço eletrônico. O “s” significa que as informações transmitidas entre o browser e o site visitado estão sendo criptografadas.

A criptografia codifica a informação de uma forma alternativa, que requer uma chave ou senha para descriptografar as informações. Se houver uma violação da segurança da informação, e esta estivesse criptografada, a pessoa que a roubou não conseguirá vê-la. A criptografia pode alternar a ordem dos caracteres, substituir caracteres por outros, inserir ou remover caracteres ou usar uma fórmula matemática para converter a informação em algum tipo de código. As empresas que transmitem informações confidenciais de clientes pela internet, como número de cartões de crédito, frequentemente fazem uso da criptografia (BALTZAN & PHILLIPS, 2012).

Ainda, segundo os autores, algumas tecnologias de criptografia utilizam chaves múltiplas, como a criptografia de chave pública. A criptografia de chave pública (PKE, Public Key Encryption) é um sistema de criptografia que utiliza duas chaves: uma pública, que todos podem ter; e outra privada, apenas para o receptor. Ao implementar a segurança usando chaves múltiplas, a empresa fornece a chave pública para todos os seus clientes (consumidores finais e outras empresas). Os clientes utilizam a chave pública para criptografar suas informações e enviá-las pela internet. Quando as informações chegam ao seu destino, a empresa deve usar a chave privada para decifrar as informações criptografadas.

Outro ponto importante a se destacar quando navegamos pela internet é observar o desenho de um “cadeado fechado” junto à barra de endereço do web site. Este cadeado representa que a conexão é segura; se o cadeado estiver aberto, significa que a conexão não é segura. Ao clicar sobre o cadeado, será exibida uma tela que permite verificar as informações referentes ao certificado emitido pela instituição que mantém o site, bem como informações sobre o tamanho da chave utilizada para criptografar os dados. Quanto maior a chave, maior a proteção.

2.5 A Privacidade e Algumas de suas Implicações no Uso da Internet

2.5.1 Direito à Privacidade

O direito à privacidade no uso da internet já faz parte de legislações adotadas por países, como Estados Unidos. A primeira lei de privacidade foi promulgada em

1974, intitulada PA74 – Privacy Act 0f 1974 -. Segundo Stair & Reynolds, o objetivo da lei é fornecer certas salvaguardas para pessoas contra a invasão de privacidade pessoal ao exigir que as agências federais, entre outras coisas:

> – Permitam que os indivíduos determinem quais registros pertencentes a eles serão coletados, mantidos, usados ou disseminados por essas agências.
> – Permitam aos indivíduos impedir que registros pertencentes a eles sejam usados ou disponibilizados para outros fins sem o seu consentimento.
> – Permitam aos indivíduos acessar as informações pertencentes a eles nos registros das agências federais, terem uma cópia de todas ou parte dessas informações e corrigir esses registros.
> – Garantam que as informações de identificação pessoal sejam coletadas, mantidas, usadas ou disseminadas para garantir que essas ações sejam para fins necessários e legais, que as informações sejam atualizadas e precisas para o uso previsto e que salvaguardas adequadas sejam oferecidas para evitar o mau uso dessas informações.
> – Permitam exceções apenas em casos em que exista uma necessidade pública importante de exceção, conforme determinado pela autoridade legislativa específica.
> – Estejam sujeitas a processos civis por danos que possam ocorrer como resultado de ações intencionais que violam os direitos individuais sob essa lei.

Segundo Lins (2000), o direito à privacidade nasceu da mudança de hábitos e costumes decorrente da ascensão da burguesia no século XVIII. Com a modernização do espaço urbano e a criação de várias facilidades domésticas, inúmeras atividades que eram exercidas comunitariamente, ou ao menos sem qualquer intimidade, passaram a fazer parte da vida particular das pessoas, dando a noção de um direito à privacidade. Este, embora seja um direito não escrito em muitos países, é hoje considerado parte essencial da liberdade.

Segundo o autor, a nossa Constituição Federal estabelece, como direito básico da pessoa o direito à privacidade:

> (…)Art.5º .....
> .....
> .
> X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> .....(...)

Como já mencionado, uma legislação já se encontra em tramitação no Congresso Nacional à espera de validação. No Brasil, o projeto de lei intitulado *marco civil da internet* dispõe entre outras coisas:

> (…) Art. 1º Esta lei tem por objetivo garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa, particularmente em relação à sua liberdade, igualdade e privacidade pessoal e familiar, nos termos do art. 5º, incisos X e XII da Constituição Federal.
> Art. 2º Toda pessoa tem direito à proteção de seus dados pessoais.
> …….....(...)
> (…) Art. 9º O tratamento de dados pessoais somente pode ocorrer após o consentimento livre, expresso e informado do titular, que poderá ser dado por escrito ou por outro meio que o certifique, após a notificação prévia ao titular das informações constantes no art. 11.....
> .....(...)
> (…) Art. 11. No momento da coleta de dados pessoais, o titular será informado de forma clara e explícita sobre:
> I – a finalidade para a qual os seus dados pessoais estão sendo coletados e de que forma serão tratados;
> II – a identidade e o domicílio do responsável pelo tratamento;
> III – a natureza obrigatória ou facultativa do fornecimento dos dados;
> IV – as consequências de uma eventual negativa em fornecê-los;
> V – os sujeitos para os quais os dados podem ser comunicados e o seu âmbito de difusão; e
> VI – os seus direitos, em particular da possibilidade de negar-se a fornecer os dados pessoais e sobre o seu direito de acesso e retificação gratuitos.....
> .....(...)

Stair & Reynolds (2011) destacam que as preocupações com a privacidade dos dados precisam ser levadas em conta, quando tais dados são constantemente coletados e armazenados sobre cada um de nós quando navegamos através da internet.

Ainda, segundo os autores, com os computadores atuais o direito à privacidade é um problema especialmente desafiador. Mais dados e informações são produzidos e utilizados hoje do que antes:

> Quando alguém nasce, faz alguns exames no ensino médio, inicia um trabalho, matricula-se em um curso universitário, candidata-se à obtenção de carta de motorista, compra um carro, faz o serviço militar, casa-se, compra seguro, recebe um cartão de biblioteca, candidata-se a um cartão de débito ou crédito, compra uma casa ou simplesmente adquire certos produtos, os dados são coletados e armazenados em algum lugar em bancos de dados de computadores. Uma questão difícil de responder é: “A

> quem pertencem essas informações e conhecimentos?". Se uma organização pública ou privada gasta tempo e recursos para obter dados sobre você, a organização é proprietária desses dados e pode usá-los da maneira que desejar? A legislação do governo responde a essas perguntas até certo ponto para as agências federais, mas as perguntas permanecem sem respostas para as organizações privadas.

Portanto, as questões de privacidade envolvem muito além da segurança e da confidencialidade. Elas envolvem o exercício da liberdade de cada indivíduo em exercer o controle sobre sua própria vida. Com o surgimento de novas formas de comercialização e relacionamento social, a citar o comércio eletrônico e as redes sociais, onde usuários do sistema trocam diversas informações através da rede cotidianamente, novos dilemas éticos surgem diante desta nova forma de interação social através da utilização de novas tecnologias.

2.5.2 Privacidade no Trabalho

O direito à privacidade no trabalho é também uma questão importante. Atualmente, existe um conflito entre os direitos dos funcionários que querem privacidade e os interesses das empresas que exigem conhecer mais sobre seus funcionários.

Por exemplo, as tecnologias estão em todo lugar, inclusive no ambiente de trabalho. Muitas empresas contam com essas tecnologias para realizar o monitoramento sobre as atividades exercidas por cada um de seus funcionários. Esses sistemas, tal como o sistema SAP, controlam as atividades de cada colaborador, discriminando sua produtividade em algum monitor de TV, geralmente situado no centro de algum setor produtivo. Cada funcionário é caracterizado por um número, que é sua identificação. Cada um desses "números" encontra-se organizado em forma de *escore* que define sua posição em relação aos demais colaboradores. Detalhe: qualquer pessoa da empresa tem acesso a essas informações.

Segundo Stair & Reynolds (2011), uma recente pesquisa revelou que 78% das empresas monitoram seus funcionários no trabalho, de uma forma ou de outra. De acordo com outro estudo recente, quase um terço das empresas demitiram um funcionário por violar as políticas de e-mail da empresa. Estatísticas como essa

aumentam as preocupações dos funcionários. Por exemplo, os funcionários podem acreditar que são monitorados de perto pela tecnologia computacional. Esses sistemas de monitoramento computacional são diretamente ligados às estações de trabalho e programas computacionais especializados podem rastrear cada toque no teclado feito pelo usuário. Esse tipo de sistema pode determinar o que os funcionários fazem enquanto estão diante do teclado. O sistema também sabe quando o funcionário não usa o teclado ou o sistema computacional. Esses sistemas podem calcular o que as pessoas fazem e quantos intervalos fazem. Desnecessário dizer que muitos funcionários consideram essa supervisão cerrada muito desumana.

Segundo Baltzan & Phillips (2012), está crescendo entre os funcionários a preocupação de que infrações em relação às políticas das empresas, mesmo acidentais, venham a ser motivo para ação disciplinar. O site Whitehouse.gov exibe o site oficial do presidente dos Estados Unidos e atualiza assinaturas de leis e novas políticas. O endereço Whitehouse.com, porém, leva a um site falso que capitaliza por meio do nome famoso do verdadeiro. Um simples erro de digitação de .gov para .com poderia custar o emprego de alguém, caso a empresa tenha uma política de rescisão para a visualização de sites ilegais. Monitorar os funcionários é um dos maiores problemas que os CIOs enfrentam quando estão desenvolvendo políticas de gestão da informação.

Segundo os autores, precedentes legais que sustentam as empresas financeiramente responsáveis pelas ações de seus funcionários dirigem a decisão de monitorar ou não o que os funcionários fazem no horário de expediente com os recursos corporativos. Cada vez mais o monitoramento do funcionário não é uma escolha, é uma obrigação de gestão de risco.

2.5.3 Privacidade do E-mail e Mensagem Instantânea

O e-mail também levanta algumas questões interessantes sobre a privacidade do trabalho. Leis federais permitem que os empregadores monitorem os e-mails enviados e recebidos pelos funcionários. Além do mais, mensagens de e-mail apagadas dos discos rígidos podem ser recuperadas e usadas em processos legais porque as leis da descoberta (obrigação de apresentar os dados na fase de prejulgamento) exigem que as empresas revelem todos os documentos relevantes

do negócio. Por outro lado, o uso de e-mail entre funcionários públicos pode violar as leis de “open meeting” (que se aplicam quando há reuniões em que se deliberem e tomem decisões). Essas leis, aplicadas a muitas agências locais, estaduais e federais, impedem que os funcionários públicos se reúnam privadamente para deliberar sobre matérias que afetam o estado ou a área local (STAIR & REYNOLDS, 2011).

O e-mail é um dos meios de comunicação mais utilizados pelas empresas. Sua operacionalidade é muito simples e sua comunicação é bem efetiva. Ágil e direto, ele proporciona uma comunicação sem fronteiras e em tempo hábil. Pelo fato de ser tão difundido, ele também é alvo de mensagens não solicitadas. Essas mensagens podem ser enviadas para o e-mail do usuário sem que o mesmo tenha solicitado. Esta mensagem não solicitada é um spam.

O spam é a mensagem não solicitada e também uma praga que atinge todos os níveis de funcionários dentro de uma empresa, de recepcionistas a CEOs. Estimativas indicam que o spam representa de 40% a 60% do tráfego de e-mail da maioria das empresas (BALTZAN & PHILLIPS, 2012).

A maioria das pessoas que utilizam a internet possui uma conta de e-mail. Possuir uma conta de e-mail não é luxo, é necessidade. O problema reside em como gerenciamos nossa conta de e-mail e como somos gerenciados pelo provedor de e-mail. O fato é que ninguém está livre de mensagens indesejadas, pois de alguma forma o sistema permite o fluxo dessas informações através da rede.

Segundo Baltzan & Phillips (2012), identificam que o e-mail é tão difundido nas empresas que exige a sua própria política específica. Em uma pesquisa recente, 80% dos trabalhadores profissionais identificaram o e-mail como o modo preferencial de comunicação corporativa. As tendências também mostram um aumento drástico na taxa de adoção de mensagens instantâneas (MI) no local de trabalho. Apesar de o e-mail e as MI serem ferramentas de comunicação de negócios comuns, existem riscos associados ao seu uso. Por exemplo, uma mensagem fica armazenada em, pelo menos, três ou quatro computadores diferentes (ver figura 8). Simplesmente apagar uma mensagem de um computador não a exclui dos outros computadores. As empresas podem atenuar muitos dos riscos do uso de sistemas de mensagens eletrônicas mediante implementação e adoção de uma política de privacidade de e-mail.

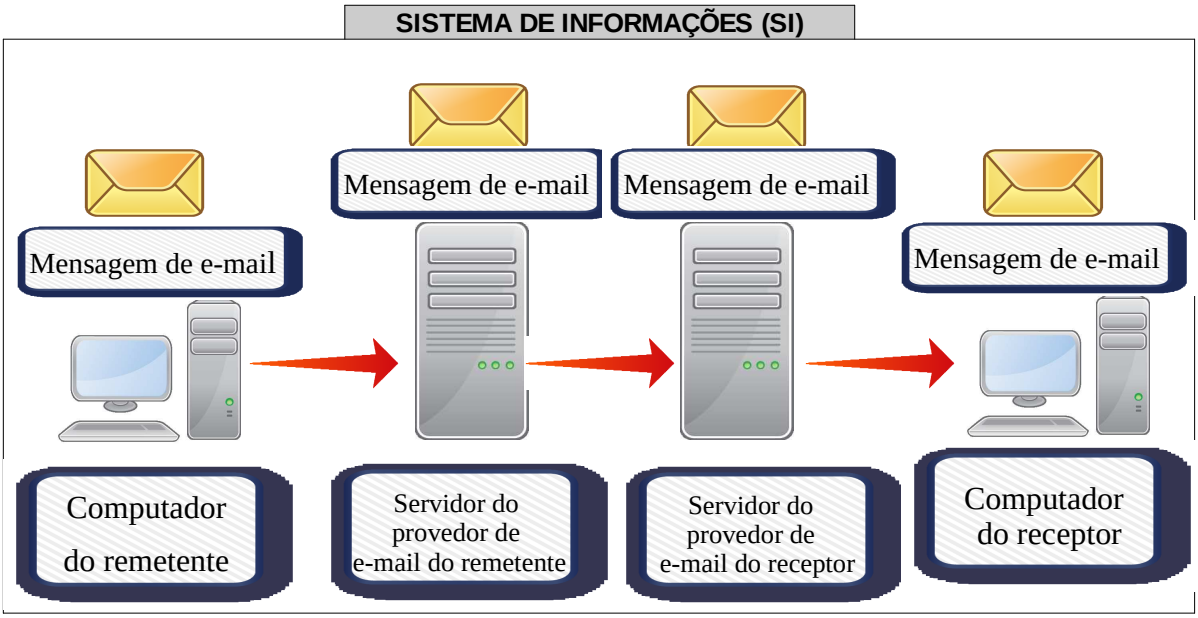

Figura 8: Deletar uma mensagem de e-mail do computador do receptor não a deleta do computador do remetente ou do computador do provedor
Fonte: Adaptada de Baltzan & Phillips, 2012

Segundo os autores, um dos maiores problemas do e-mail são as expectativas de privacidade por parte do usuário. Geralmente, a empresa que possui o sistema de e-mail pode operá-lo tão aberto ou restrito quanto queira. Isso significa que, se a empresa quer ler as mensagens de todos, pode fazê-lo. Se ela optar por não ler nenhuma, isso também é permitido. Assim, cabe à empresa decidir quantas mensagens de e-mails, se houver, ela vai ler. Então, quando ela decidir, deve informar os usuários, de modo que eles possam consentir esse nível de intrusão. Em outras palavras, uma política de privacidade de e-mail detalha em que medida as mensagens de e-mails podem ser lidas por terceiros.

Usar programas de mensagem instantânea (IM – instant messaging) para enviar e receber mensagens, arquivos e imagens, introduz as mesmas questões sobre privacidade associadas com o e-mail.

De acordo com Stair & Reynolds (2011), da mesma forma que o e-mail, a lei federal norte-americana permite que os empregadores monitorem mensagens instantâneas enviadas e recebidas pelos funcionários. Não envie mensagem instantânea pessoal ou privada no trabalho. Outras questões significativas de privacidade dependem do programa de mensagem instantânea que se usa. Por exemplo, certa vez AOL e o ICQ declararam, em sua política de privacidade, que

“Você abre mão de qualquer direito à privacidade” e que eles podem usar suas mensagens instantâneas da maneira que acharem apropriado.

2.5.4 Dispositivos Pessoais Sensíveis e Privacidade

Os marcadores RFID, essencialmente microchips com antena, são embutidos em muitos dos produtos que compramos, como caixas de remédios, roupas, impressoras, chaves de carros, livros de biblioteca e pneus. Os marcadores RFID geram transmissões de rádio que, se não forem tomadas medidas apropriadas, podem levar a preocupações potenciais com a privacidade. Uma vez que esses marcadores são associados com o indivíduo que adquire o item, alguém pode potencialmente rastreá-lo pelo identificador único associado com o chip RFID (STAIR & REYNOLDS, 2011).

Segundo os autores, vários Estados norte-americanos reagiram ao potencial para abuso dos marcadores RFID, indo tão longe quanto passar uma legislação proibindo a implantação de chips de RFID sob a pele das pessoas sem sua aprovação.

Apesar de parecer filme de ficção científica, não é. A tecnologia por trás destes marcadores permite o rastreamento de qualquer artigo que os contenha. E com o avanço dessa tecnologia, já existem chips cada vez menores, alguns do tamanho de um grão de areia e que são utilizados em intervenções cirúrgicas. Outros marcadores de RFID podem ser identificados em tornozeleiras eletrônicas utilizadas em detentos sob regime condicional.

2.5.5 Privacidade e Internet

A privacidade na internet relaciona-se, de forma análoga à imprensa, à revelação de fatos privados embaraçosos e ao uso de métodos questionáveis para coleta de informações. No primeiro caso, a similaridade com o veículo de imprensa é clara: será violação à privacidade a divulgação, através da Internet, de dados ou fatos que atentem contra a intimidade, a vida privada, a honra e a imagem de uma

pessoa. Tal divulgação poderá ser feita por um “site”, por correio eletrônico ou por arquivo disponível para cópia (LINS, 2000).

Segundo o autor, no entanto, a internet traz um agravante: a rede é mundial e o fato poderá ser divulgado em escala nunca antes alcançada por outros meios de comunicação de massa. Tal circunstância levanta, inclusive, aspectos de natureza técnica: os fatos podem ser divulgados a partir de países que, por não dispor de legislação para tal, não punirão a ocorrência, dando um caráter de impunidade à atitude delituosa. Já o uso de métodos questionáveis encontra amplas variações na internet, em virtude da diversidade dos recursos de informática hoje existentes. Podem ser classificados nas seguintes categorias:

> a) Coleta de informações no computador do usuário, sem o seu consentimento: trata-se de um procedimento mais comum e viável do que se imagina. Pode ocorrer através do uso de programas invasivos ou através da identificação dos acessos feitos pelo computador.
> b) Monitoramento da linha de comunicação ou do teclado do computador do usuário através de programas invasivos: trata-se de uma variante mais grave do procedimento anterior.
> c) Coleta ou compra de informações sobre o usuário em outros computadores, tais como o servidor que o atende ou os computadores de empresas cujos serviços a pessoa tenha utilizado: nesse caso, os dados podem estar sendo repassados sem o consentimento do interessado.
> d) Cruzamento das informações sobre a pessoa, obtidas em sites diversos, sem o seu consentimento explícito: às vezes o usuário, por exemplo, consente que o seu e-mail ou seus dados sejam repassados a terceiros para recebimento de correspondência. No entanto, essa autorização não se estende à elaboração do seu perfil.
> e) Violação da comunicação através de dispositivos externos de escuta: trata-se de procedimento incomum, em vista da complexidade dos protocolos de transmissão de dados adotado na Internet, mas viável.
> f) Uso do codinome, da senha ou de outros dispositivos de segurança do usuário, para entrar na rede em seu lugar e obter, dessa forma, informações a seu respeito.

Ainda, conforme o autor, as duas últimas modalidades ilustram casos extremos do uso de métodos questionáveis, que se configuram quando estes se encontram associados à ocorrência criminal. Em tais casos, o infrator adota procedimentos considerados ilegais. Estes, por sua vez, dependem, para a sua caracterização, de uma tipificação criminal clara, o que a legislação brasileira ainda não oferece.

Segundo Stair & Reynolds (2011), algumas pessoas supõem que não há privacidade na internet e que você a usa por sua própria conta e risco. Outras acreditam que as empresas com web sites devem possuir procedimentos de

privacidade rígidos e sejam responsáveis pela invasão de privacidade. Independente de sua visão, o potencial para invasão da privacidade na internet é enorme. As pessoas que querem invadir sua privacidade podem ser quaisquer pessoas, desde hackers criminosos a empresas de marketing e chefes corporativos. Suas informações pessoais e profissionais podem ser colocadas na internet sem seu conhecimento ou consentimento. O e-mail é o alvo principal, como discutido anteriormente (ver figura 9). Enviar uma mensagem pelo e-mail é como ter uma conversa aberta em uma grande sala – as pessoas podem ouvir suas mensagens. Quando você visita um web site na internet, informações sobre você e seu computador podem ser capturadas. Quando essas informações são combinadas com outras informações, as empresas podem saber o que você lê, quais produtos você compra e quais são seus interesses.

A maior parte das pessoas que compra produtos na web diz que é muito importante que um site tenha uma política explicando como as informações pessoais são usadas. A declaração da política deve fazer com que as pessoas se sintam confortáveis e ser extremamente clara sobre quais informações são coletadas e o que será feito ou não com esses dados. No entanto, muitos web sites não expõem em destaque a sua política de privacidade ou implantam práticas completamente inconsistentes com essa política. A questão real com a qual os usuários da internet devem estar preocupados é: “o que os provedores de conteúdo querem com suas informações pessoais?”. Se um site pede que você forneça nome e endereço, você tem todo o direito de saber por que e o que será feito com isso. Se você compra algo e fornece um endereço para entrega, ele será vendido para outros varejistas? Se assim for, você deve perceber que não é diferente das listas compiladas dos pedidos que você coloca em catálogos de varejistas. Você tem o direito de ser tirado de qualquer lista de mala direta (STAIR & REYNOLDS, 2011).

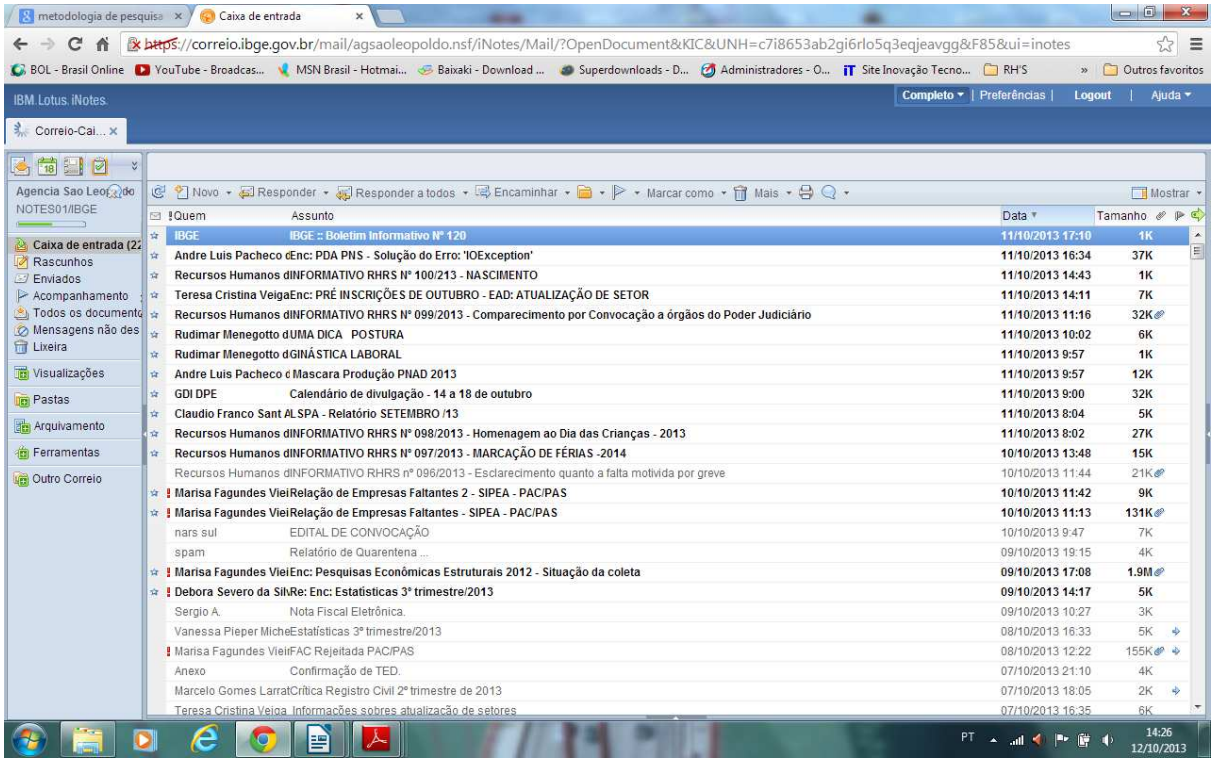

Figura 9: O e-mail como alvo principal de mensagens indesejadas
Fonte: Adaptada de Stair & Reynolds, 2011

Uma solução potencial para algumas preocupações com a privacidade do consumidor é a tecnologia de varredura chamada **plataforma de preferências de privacidade** (P3P), que é proposta para proteger os usuários de sites que não oferecem o nível de proteção de privacidade desejado. Em vez de forçar os usuários a encontrar e ler a política de privacidade de cada site visitado, o software P3P no navegador de uma empresa baixará a política de privacidade de cada site, varrê-la, e notificará o usuário se a política está de acordo com as suas preferências. (Naturalmente, sites não éticos podem colocar políticas de privacidade que não refletem exatamente a maneira pela qual os dados são tratados). O World Wide Web Consortium, grupo internacional de empresas cujos membros incluem Apple, Commerce One, Ericsson e Microsoft, fornece suporte para desenvolvimento de P3P (STAIR & REYNOLDS, 2011).

Ainda, segundo os autores, um serviço de rede social emprega a web e software para conectar pessoas por qualquer motivo. Há milhares dessas redes que se tornaram populares entre os adolescentes. Algumas das redes sociais mais populares incluem facebook, Orkut, Linkedin, MySpace e Instagram. A maioria desses web sites permite que se crie facilmente um perfil de usuário que fornece

detalhes pessoais, fotos e mesmo vídeos que podem ser vistos por outros visitantes do site. Alguns dos web sites possuem restrições de idade ou exigem que os pais registrem seu pré-adolescente, fornecendo um cartão de crédito para validar a identidade. Os adolescentes podem fornecer informações sobre onde moram, a escola que frequentam, sua música favorita e interesses na esperança de encontrar novos amigos. Infelizmente, eles podem encontrar estranhos mal-intencionados nesses sites. Muitos encontros documentados envolvem adultos disfarçados de adolescentes tentando encontrar jovens para propósitos ilícitos. Os pais são aconselhados a discutir os perigos potenciais, checar o perfil de suas crianças e monitorar suas atividades em tais web sites.

2.6 Tratamento de Bases de Dados e Privacidade

2.6.1 O Mercado de Bases de Dados

Bases de dados são coleções de dados, estruturadas e organizadas com o uso de recursos de informática, de modo a facilitar a seleção e recuperação das informações armazenadas. A tecnologia para o tratamento de bases de dados foi desenvolvida simultaneamente com o computador e bases mantidas para fins comerciais existem desde os anos sessenta (LINS, 2000).

Destacado pela grande imprensa nos últimos tempos, o roubo de dados confidenciais de aposentados, donos de automóveis, clientes de banco dentre outros infelizmente se tornou um mercado negro no Brasil. O comércio de dados confidenciais de cidadãos brasileiros torna-se cada vez mais uma prática altamente lucrativa seja pela internet ou nas esquinas do país (ATHENIENSE, 2013).

De acordo com o autor, numa rápida pesquisa no Google, é possível encontrar empresas que anunciam a venda de informações confidenciais de diversos bancos de dados do Brasil, como os dos Detrans (Departamentos Estaduais de Trânsito) e de empresas privadas, como seguradoras de veículos e operadoras de telefonia. Na região central de São Paulo, é possível comprar por 250 reais um cadastro com lista telefônica e registros do INSS.

Comercializar um conjunto de dados privados ou uma base inteira de dados privados é, no mínimo, antiético. Ianotta (1987), apud Lins (2000), descreve que o direito à privacidade do indivíduo em face ao uso de bases de dados pode ser definido como a expectativa de que este possa determinar por si próprio quando, como e em que medida informações sobre si sejam comunicadas a terceiros. Tal direito fundamenta-se nos seguintes parâmetros:

> a) informações pessoais devem ser coletadas segundo procedimentos legítimos, com o prévio conhecimento e consentimento da pessoa a quem as informações se referem;
> b) as informações armazenadas em bases de dados não devem ser utilizadas para quaisquer fins distintos daqueles para os quais a base de dados foi criada;
> c) o indivíduo tem o direito de saber o que há sobre ele armazenado em uma base de dados;
> d) o indivíduo tem o direito de corrigir ou de solicitar a correção ou retirada de dados pessoais incorretos armazenados em bases de dados.

Embora um banco de dados forneça os fundamentos essenciais para o sistema de informações e apoio ao sistema de decisão de uma organização (STAIR & REYNOLDS, 2011), ele também possibilita o uso inadequado por parte de pessoas que queiram extrair vantagens ilícitas de sua utilização.

Conectar os bancos de dados à internet é uma das razões da popularidade da internet. Uma grande porcentagem dos bancos de dados corporativos é acessada por meio da internet por um browser padrão da web. Ser capaz de acessar os dados de uma conta bancária, matrícula escolar, contas de cartão de crédito, catálogos de produtos e um hospedeiro de outros dados online não apenas é conveniente para os usuários individuais. O Google está introduzindo um DBMS (Sistema de Gerenciamento de Banco de Dados) que fornecerá aos pacientes e médicos um sistema para armazenar todos os registros médicos, acessado por um navegador da web. Acessar informações médicas privadas em um sistema de rede pública levanta alguma preocupação para os defensores da privacidade (STAIR & REYNOLDS, 2011).

Segundo uma reportagem de um jornal local, após a denúncia de venda de informações pessoais sigilosas de cidadãos, o secretário de Segurança do Rio Grande do Sul, Airton Michels, disse que o governo não tem como prever esse tipo de crime. No estado, pelo menos 58 juízes tiveram informações acessadas a partir

da senha de um policial militar. Ele afirmou que o Estado tem o compromisso de investigar e que não existe tecnologia que supere ações de má-fé. "Não é falha do sistema, é má-fé humana. Ações criminosas existem com ou sem sistema dessa natureza", afirmou. “Se será bem ou mal usado, dependerá da conduta de alguém” (JORNAL G1RS, 12/08/2013).

Se, por um lado, a segurança e a privacidade de dados dependem da conduta daqueles que manipulam o sistema, conforme indicam os autores Stair & Reynolds (2011): as pessoas podem ser o elemento mais importante na maioria dos sistemas de informação com bases em computador […], por outro lado, procedimentos devem ser adotados para minimizar as possibilidades do mau uso dos sistemas. Segundo os autores, os procedimentos incluem as estratégias, políticas, métodos, e regras para utilizar o CBIS, incluindo a operação, manutenção e segurança dos sistemas.

É recomendável que as empresas redobrem suas atenções para a segurança dos dados armazenados, não só investindo em sistemas de proteção, monitoramento e auditoria de acessos. Importante também a implantação de uma política de segurança da informação entre colaboradores, funcionários, prestadores de serviços e o público em geral, pra criar regras claras e punir infratores que possam vazar a informação (ATHENIENSE, 2013).

Ainda, segundo o autor, para enfrentar estes incidentes, não bastará ao cidadão ter controle sobre a divulgação excessiva de dados pessoais pelo meio eletrônico, caso as entidades que hospedam esta informação não tomarem medidas que possam assegurar o monitoramento dos dados armazenados e a punição para os infratores.

Tais parâmetros tornam-se mais importantes na medida em que já existe, hoje, capacidade de armazenamento de dados suficiente para se elaborar, em nível governamental, um cadastro único contendo informações relevantes sobre boa parte dos habitantes de um país. Códigos como o número de CPF no Brasil ou o número de seguridade social nos EUA e na França poderiam, nesse contexto, ser usados como um número de identificação nacional, facilitando a tarefa. Nesse caso, “a perda de privacidade torna-se uma possibilidade factível, com a qual deveremos conviver cada vez mais” (Oliveira, 1977, apud Lins, 2000, p.9).

2.6.2 O Tratamento de Bases de Dados na Lei Brasileira

No Brasil, a realização de pesquisa para estruturação e comercialização de cadastros, bem como para outras finalidades comerciais, não se encontra regulamentada. Lins (2000) relata que algumas disposições foram consagradas na Lei nº 8.078, de 11 de setembro de 1990, que "dispõe sobre a proteção do consumidor e dá outras providências", no que diz respeito aos cadastros de compradores, estruturados para efeito de cobrança. Esse diploma dispõe, no art. 43:

> Art. 43 O consumidor, sem prejuízo do disposto no art. 86, terá acesso a informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> § 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
> § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
> § 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
> § 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
> § 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos sistemas de proteção ao crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

Para o autor, entre os aspectos não regulamentados, cabe destacar a revenda de cadastros de pessoas físicas sem prévia autorização, hoje prática corrente. Também não há regulamentação quanto ao cruzamento de cadastros para fins de levantamento de perfis socioeconômicos e de consumo. É preciso estabelecer, ainda, a quem será atribuída a responsabilidade pela retificação da informação junto às bases de dados.

Concluindo, no Brasil ainda não há uma legislação específica que regule o gerenciamento de bases de dados, sua utilização, armazenamento e disseminação. O projeto de lei denominado marco civil da internet, que atualmente tramita no Congresso Nacional, tenta regulamentar essa situação.

2.7 Transmissão de Informações e Privacidade

A transmissão de dados é outro mecanismo pelo qual é possível obter-se dados de forma questionável. O procedimento consiste em monitorar externamente uma conexão de computadores, interceptando as informações enviadas e recebidas, ou em usar uma rede pública, como a internet, para colocar-se no lugar de um usuário e receber as informações a ele destinadas (LINS, 2000).

A transmissão de informações ocorre quando há a troca de mensagens entre emissor e receptor. Segundo Stair e Reynolds (2011), a interceptação de informações confidenciais por indivíduos não autorizados pode causar um comprometimento de informações particulares sobre funcionários ou consumidores, revelar marketing ou planos de desenvolvimento de um novo produto ou ainda causar constrangimento organizacional.

Segundo Lins (2000), há inúmeras alternativas técnicas para executar tais procedimentos. Dentre as alternativas, sob o ponto de vista da segurança, é preferível destacar a criptografia.

Conforme Stair & Reynolds (2011), a criptografia de dados é uma abordagem utilizada para proteger a segurança das comunicações por meio das redes com fio e sem fio. A criptografia é o processo de converter uma mensagem original em uma forma em que se pode ser entendida apenas pelo receptor a quem é dirigida (ver figura 10).

Lins (2000) afirma que, tradicionalmente, a criptografia dos dados transmitidos era feita através de um sistema de senhas, que eram usadas para codificar e decodificar a mensagem. Essas senhas eram armazenadas em ambos os computadores envolvidos na transmissão ou deveriam ser enviadas junto com a mensagem.

Nobre (1999), apud por Lins (2000, p. 11), relata que se os computadores não estivessem ligados a uma rede, a segurança das senhas envolveria apenas aspectos de proteção física contra o acesso aos equipamentos, e a segurança contra acessos ao sistema de senhas, em geral uma tabela ou um programa. Quem quisesse invadir o computador deveria primeiramente obter acesso a um terminal do mesmo e, então, violar a segurança do seu sistema.

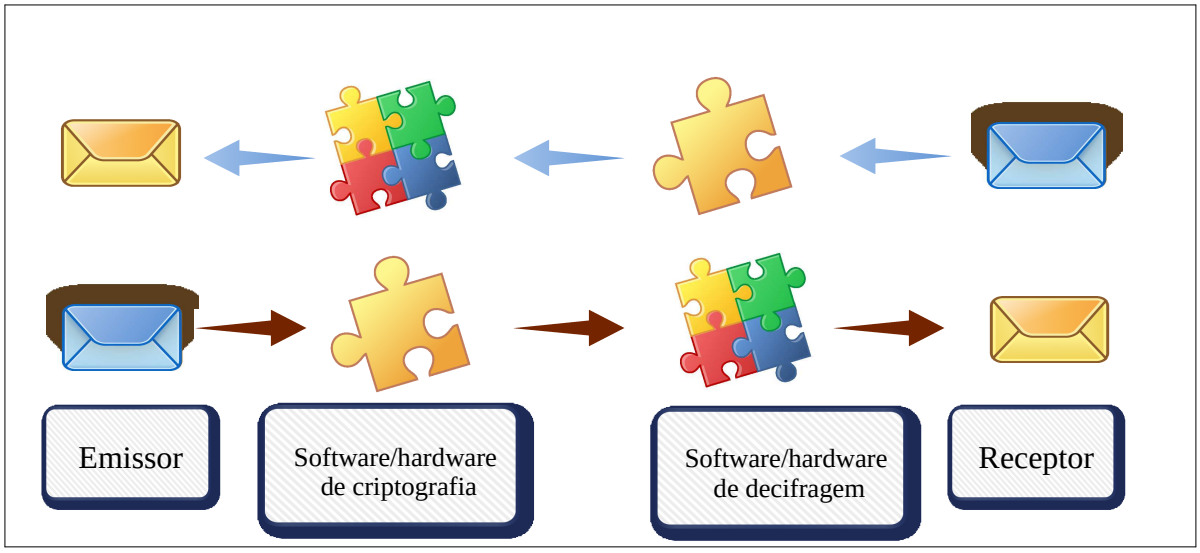

Figura 10: Processo de criptografia
Fonte: Adaptada de Stair & Reynolds, 2011

Hoje, no entanto, os computadores encontram-se conectados em rede, podendo ser acessados por todo tipo de “hacker” disposto a invadi-lo. Conforme Lins (2000), nesse contexto, a solução encontrada foi a de se usar um sistema de duas chaves. Uma chave é pública, sendo usada por qualquer um que queira enviar um arquivo para um certo destinatário. Este, por sua vez, dispõe de uma chave pessoal ou privada, a única forma de descriptografar a informação.

Uma chave é um valor variável que é aplicado (utilizando um algoritmo) para um conjunto de texto não criptografado para produzir texto criptografado ou para decifrar um texto criptografado. A chave é escolhida entre um grande número de chaves de criptografia possíveis. Quanto mais longa a chave, maior o número de chaves possível (STAIR & REYNOLDS, 2011).

O processo pode ser usado em sentido inverso, para certificar um certo documento. Esse procedimento, comercialmente denominado de assinatura digital, consiste em enviar o documento ou arquivo em forma legível, acompanhado de uma “arrumação” dos dados feita por um processo de codificação pela chave privada. Qualquer um poderá ler o documento e, se estiver de posse da chave pública do remetente, autenticá-lo. Se o documento tiver sido modificado, não será autenticado (LINS, 2000).

Segundo o autor, o sistema de chave dupla já é usado, de forma simplificada, nas páginas seguras na Internet. Várias versões do mesmo, desenvolvidas a partir

do sistema original – o PGP – estão incorporadas em programas comerciais, tais como os “browsers”.

O sistema de chave dupla PGP, do inglês *Pretty Good Privacy* (privacidade bastante boa), é um programa de computador de encriptação e descriptografia de dados (criptografia de chave pública) que fornece autenticação e privacidade criptográfica para comunicação de dados. É frequentemente utilizado para assinatura, criptografia e descriptografia de textos, e-mails, arquivos, diretórios e partições inteiras de disco para incrementar a segurança de comunicações via e-mail (REBÊLO, 2009).

Conforme Stair & Reynolds (2011), um protocolo de criptografia baseado em uma chave de 56 bits, por exemplo, possui 2^{56} diferentes chaves possíveis, enquanto um protocolo com base em uma chave de 128 bits possui 2^{128} chaves diferentes possíveis. Naturalmente, é essencial que a chave seja mantida em segredo dos possíveis interceptadores. Um hacker que obtém uma chave mediante quaisquer meios pode recuperar a mensagem original dos dados criptografados.

Segundo Lins (2000), o processo descrito é um sistema de proteção de dados seguro. No entanto, coloca diversas questões de natureza jurídica ainda não tratadas na legislação brasileira. Primeiramente, a segurança depende de uma adequada proteção da chave privada e de sua configuração. Em segundo lugar, um mecanismo eficaz de disponibilização de chaves públicas deve ser organizado. Além disso, o alcance da responsabilidade das partes no caso de divulgação de dados pessoais deve ser formulado e deve ser qualificado em que grau a adoção de mecanismos de segurança servirá de atenuante nesses casos. Tais aspectos relacionam-se, sobretudo, com a legislação própria do comércio eletrônico, ainda que digam respeito à privacidade dos dados na Internet.

3 METODOLOGIA

Os especialistas em pesquisa científica usam diferentes nomes para as metodologias empregadas na realização dos projetos de pesquisa, porém não diferem basicamente em seu conteúdo e se distinguem de acordo com as fontes de dados utilizadas, a amplitude do estudo conforme os objetivos, o tipo de análise que pretendem fazer – quantitativa ou qualitativa – de acordo com o controle das variáveis em estudo (MARCONI, 1990, apud Wollenhaupt, 2004).

3.1 Componentes da Pesquisa Científica

O processo de pesquisa compreende quatro diferentes etapas, cada etapa, diversas fases e cada fase, diversos passos (MATTAR, 1996). A figura 11 mostra as etapas, fases e passos de um processo de pesquisa científica.

As etapas componentes de um processo de pesquisa científica são:

1. **Reconhecimento e formulação de um problema de pesquisa** – consiste na correta identificação do problema de pesquisa que se pretenda resolver e que se possa efetivamente receber contribuições à sua solução;
2. **planejamento da pesquisa** – compreende a definição dos objetivos da pesquisa e de toda sua operacionalização: determinação das fontes de dados, escolha do(s) método(s) de pesquisa, da(s) forma(s) de coleta dos dados, da construção e teste do(s) instrumento(s) de coleta dos dados, da definição do plano de amostragem e do tamanho da amostra, da definição dos procedimentos de campo, da elaboração do plano de processamento e análises, da definição dos recursos necessários (humanos, financeiros, tecnológicos e materiais), da definição de uma estrutura organizacional para a equipe de pesquisa com definição de responsabilidades e do estabelecimento de um cronograma com definição de prazos e datas para o cumprimento de cada etapa e de suas subdivisões;
3. **execução da pesquisa** – a execução da pesquisa compreende duas atividades:

· *coleta de dados* – compreende o efetivo trabalho de recolhimento dos dados no campo junto às fontes de dados. É a etapa geralmente mais cara e crítica da pesquisa, pois é a que mais está sujeita à introdução de erros e atrasos, e por isso exige supervisão muito intensa e um controle rígido para minimizá-los;

· *processamento, análise e interpretação* – compreende a transformação dos dados brutos coletados, que são relevantes para solucionar ou ajudar na solução do problema que deu origem à pesquisa. Esta etapa inclui: verificação do preenchimento dos instrumentos, codificação e digitação das respostas, processamento (geralmente eletrônico) dos dados, realizações de cálculos e testes estatísticos e análises e interpretações.

4. **comunicação dos resultados** – compreende a apresentação escrita e oral das principais descobertas da pesquisa relacionadas ao problema que lhe deu origem, bem como de sugestões e recomendações de ações pertinentes a sua solução.

Diferentes tipos de pesquisa implicam diferentes procedimentos para coleta e análise dos dados, de forma a atender econômica e tecnicamente aos objetivos da pesquisa (MATTAR, 1996).

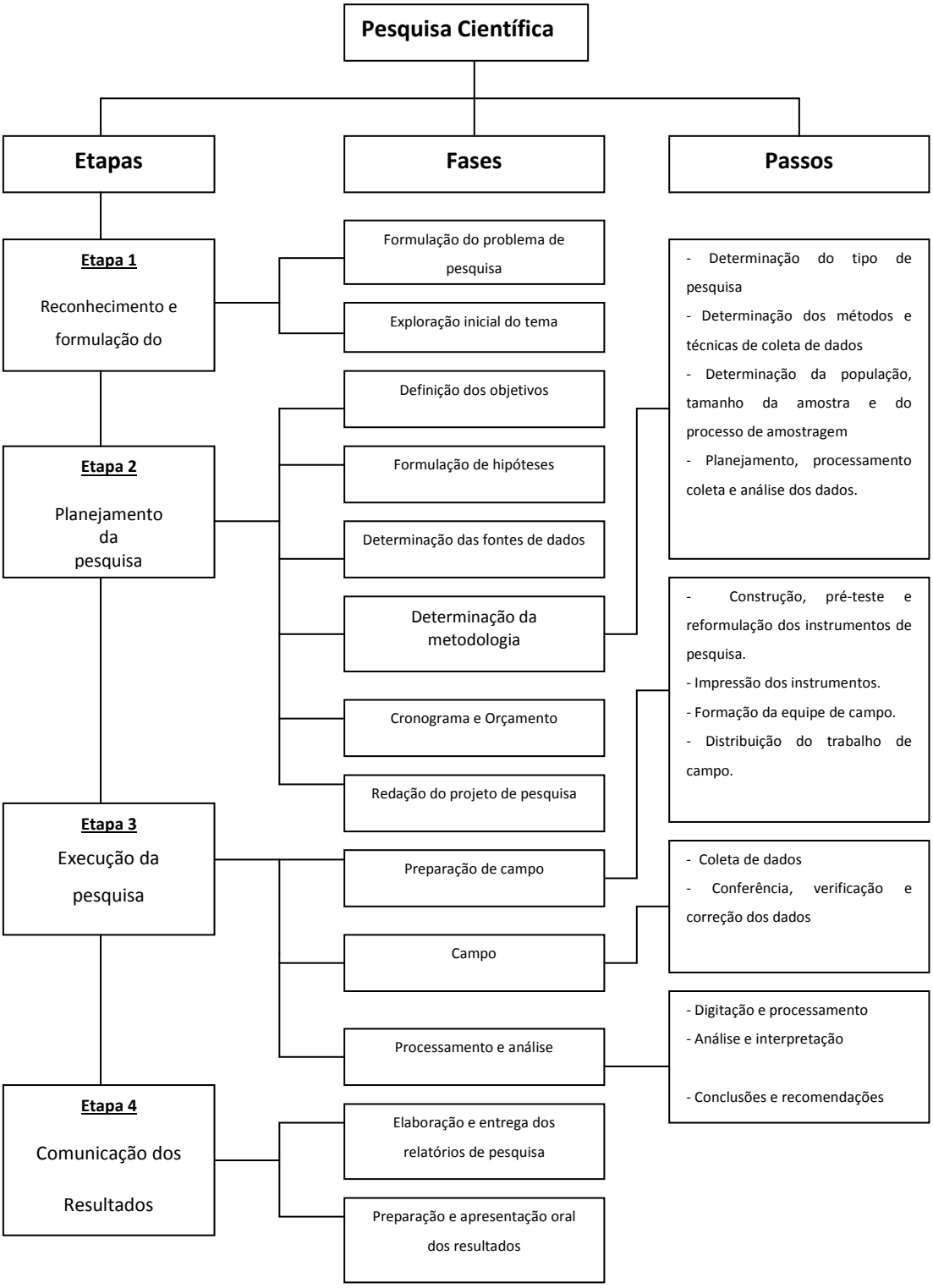

Figura 11: Etapas, fases e passos de um processo de pesquisa científica
Fonte: Mattar, 1996, p. 16.

3.2 Classificação da Pesquisa Científica

Dentro das diversas áreas de conhecimento humano, as pesquisas podem ser classificadas basicamente em quatro tipos: bibliográfica, de campo, experimental e estudo de caso.

3.2.1 Pesquisa Bibliográfica

A pesquisa bibliográfica apresenta uma importância fundamental dentro das atividades acadêmicas. Por ser o tipo mais frequente, representa uma dimensão extremamente importante. Ela procura explicar e responder problemas dentro de uma dimensão teórica.

Na pesquisa bibliográfica, os livros são a ferramenta básica para o pesquisador fundamentar o assunto em questão. Este é o tipo de pesquisa mais usual, por oferecer facilidades na busca do material, mas não podemos esquecer que todos os tipos de pesquisa devem apresentar o seu referencial bibliográfico.

Dentro deste tipo de pesquisa, o pesquisador terá de oferecer ao contexto acadêmico uma bibliografia respeitável e atualizada. Além disso, uma pesquisa não poderá ser feita somente em torno de uma obra. Quanto mais completas forem as fontes consultadas, mais rica e profunda será a pesquisa.

Os trabalhos pedidos durante o semestre, na maioria das vezes, requerem uma pesquisa bibliográfica. Para tal, é fundamental a organização. A ficha de leitura é de grande utilidade, devido à facilidade de se partir daí para a redação do texto.

3.2.2 Pesquisa de Campo

A pesquisa de campo não dispensa a bibliografia. Aliás, esta está presente em todos os tipos. A pesquisa de campo exige que o pesquisador se dirija a um contexto e, através de observação, entrevistas e questionários, encontre uma resposta para ele.

Este tipo de trabalho deveria ser utilizado com mais frequência, pois cria uma integração da universidade com a comunidade. Como toda pesquisa é de interesse social, existe a necessidade desta relação.

A pesquisa de campo é usada, sobretudo, nas ciências humanas e sociais. Tem por fim explicar e interpretar as relações sociais e culturais da sociedade. A grande vantagem desta modalidade de investigação é a possibilidade de apresentar dados novos e atuais. Por se tratar de um trabalho de campo, os resultados só podem ser alcançados mediante uma interpretação dos dados localizados, e a pesquisa favorece o envolvimento da universidade no contexto social.

Cada linha de pesquisa oferece as suas dificuldades. Dentre as mais comuns, destacam-se: contexto da pesquisa e população-alvo, dificuldades no levantamento e precisa interpretação dos dados. Mesmo com essas dificuldades, este tipo de pesquisa dá ao pesquisador um referencial quanto à sociedade pesquisada.

O pesquisador que fizer uso da pesquisa de campo deve ater-se a um planejamento detalhado em relação a: assunto, população-alvo, elaboração do objetivo de levantamento de dados, tempo da coleta de dados, além de uma exploração bibliográfica. Como toda a pesquisa científica, requer precisão, e é indispensável ao investigador um planejamento prévio.

Na pesquisa de campo, é fundamental não haver manipulação de dados. É necessária uma análise precisa dos mesmos.

Na elaboração dos questionários, as questões devem ser bem claras e objetivas. Não devem oferecer ao entrevistado a possibilidade de subjetividade. Quanto mais fiéis forem as respostas, melhores serão os resultados.

A pesquisa de campo procura analisar, classificar, explicar e interpretar os fenômenos observados, o que significa dizer que o pesquisador deverá se ater aos aspectos particulares dentro de um todo. Seja nas respostas que são dadas ou como são dadas, tudo deve ser objeto de interpretação e análise, pois é função do pesquisador objetivar a leitura pessoal do contexto no qual está pesquisando.

3.2.3 Pesquisa Experimental

A pesquisa experimental está ligada às ciências naturais. Necessita de equipamentos e laboratório para a verificação das hipóteses. Mesmo sendo um tipo

de pesquisa na qual os resultados apresentam objetividade, também apresenta subjetividade no observar as coisas.

A pesquisa experimental requer o uso de técnicas e instrumentos que possam oferecer um resultado sólido. Em função dos equipamentos e das técnicas utilizadas, este tipo de pesquisa torna-se bem mais caro. Os equipamentos, por serem de alta resolução, requerem por parte do pesquisador atenção e análise de todos os aspectos observados. A pesquisa experimental se caracteriza por manipular diretamente as variáveis relacionadas com o objeto de estudo. Neste tipo de pesquisa, a manipulação das variáveis proporciona o estudo da relação entre causas e efeitos de um determinado fenômeno. Através da criação de situações de controle, procura-se evitar a interferência de variáveis intervenientes. Interfere-se diretamente na realidade, manipulando-se a variável independente a fim de observar o que acontece com a dependente.

Muitos aspectos de cada tipo de pesquisa não estão desenvolvidos ou não foram levantados. Mas, num primeiro momento, o objetivo deste assunto sobre pesquisa é de tocar em alguns pontos que possam oferecer condições para uma discussão em sala de aula. Não existe o texto, a pesquisa pronta, pois constantemente são oferecidos novos aspectos para a discussão. Estes são alguns exemplos que merecem ser discutidos e analisados a partir de uma reflexão acadêmica.

Sempre que alguém não encontra respostas para algum problema, nasce daí a possibilidade de pesquisa, e isso depende da vontade do pesquisador de encontrar respostas. Estas não surgem graciosamente; ao contrário, exigem muita persistência, pois todo tipo de pesquisa traz grandes dificuldades.

Não se pode fazer uma pesquisa pela simples razão de fazê-la. Há a necessidade de buscar respostas a todo um desenrolar de dúvidas. Para uma pesquisa apresentar um desenvolvimento, ela deve começar pelo interesse do pesquisador. A motivação deve estar presente. Como a pesquisa visa a um fim, ela requer planejamento. É aí que surge a importância do projeto da pesquisa.

3.2.4 Estudo de Caso

É um tipo de pesquisa muito produtivo para estimular a compreensão e sugerir hipóteses e questões para a pesquisa. O estudo de caso pode envolver o

exame de registros existentes, a observação da ocorrência do fato, entrevistas estruturadas e entrevistas não estruturadas. O objeto de estudo pode ser um indivíduo, um grupo de indivíduos, uma organização, um grupo de organizações ou uma situação.

Esse tipo de pesquisa possui três características. A primeira é que os dados podem ser obtidos em tal nível de profundidade que permitem caracterizar e explicar detalhadamente os aspectos singulares do caso em estudo, bem como apontar semelhanças e diferenças quando comparado com outros casos estudados. Dependendo dos objetivos e do objeto em estudo, este método poderá demandar muito tempo. A segunda característica é a atitude receptiva do pesquisador que deve ser caracterizada pela busca de informações e gerações de hipóteses e não por conclusões e verificações. A terceira é a capacidade de integração do pesquisador em reunir, numa interpretação unificada, inúmeros aspectos do objeto pesquisado.

3.3 Encaminhamento Metodológico da Pesquisa

A pesquisa foi conduzida com o objetivo de sintetizar a importância da conduta ética nas relações entre usuários da rede (internet), considerando o tema privacidade de informações, suas implicações nas relações entre usuários e o surgimento de alguns dilemas éticos atuais relacionados ao tema.

Para o alcance do objetivo, optou-se por realizar uma pesquisa do tipo descritiva e, como técnica, utilizou-se a pesquisa documental/bibliográfica.

Desta forma, procurou-se abordar o assunto privacidade na rede com base em leituras de livros, artigos, revistas, jornais, vídeos, enfim, todos os materiais que pudessem contribuir para a construção do presente trabalho. Ressaltam-se as dificuldades de encontrar materiais que contenham relação com o tema proposto, por isso a utilização de diversos meios, alguns pouco usuais, para o embasamento do tema.

4 CONCLUSÃO

Os sistemas de informação (SI) e as tecnologias da informação e comunicação (TICs) fazem parte da realidade cotidiana da vida em sociedade. As interações sociais e as interações de mercado, por exemplo, estão intrinsecamente ligadas à utilização desses aparatos tecnológicos, seja para o lazer, seja para o negócio. Entender o funcionamento, o emprego, o ciclo de vida, as vantagens e desvantagens no uso dessas tecnologias é fundamental para as pessoas entenderem os benefícios e os riscos associados a elas.

A discussão sobre a possibilidade de um indivíduo fazer ou não parte e/ou uso dos meios tecnológicos parece ultrapassada, uma vez que a tecnologia e seus meios estão em toda parte, no lazer, na política, no comércio, no trabalho, no social, e em todos os meios interativos que se possa contar. Isso remete que, se por um lado não temos a possibilidade de autoexclusão desse cenário tecnológico onde cada pessoa é parte dele, por outro lado, compreender seu uso e suas implicações torna-se extremamente importante para a manutenção dos nossos direitos e deveres enquanto usuários do sistema.

As mudanças na sociedade como resultado do aumento do comércio internacional e do intercâmbio entre culturas, frequentemente chamadas globalização, sempre tiveram impacto significativo nas organizações e em seus sistemas de informação. De acordo com Friedman, apud Stair & Reynolds (2011), temos progredido da globalização de países para a globalização de corporações multinacionais e indivíduos. Hoje, pessoas que vivem em áreas remotas podem usar a internet para competir e contribuir com outras pessoas, com grandes corporações e com países inteiros.

O primeiro objetivo da pesquisa foi conceituar e identificar a estrutura de um sistema de informações (SI) e, conforme os diversos autores referidos, os sistemas de informação de hoje conduzem à maior globalização. O acesso de alta velocidade à internet e às redes que podem conectar indivíduos e organizações ao redor do mundo cria oportunidades para todos aqueles que queiram obter vantagens. Os sistemas, por si só, não podem operar isoladamente como foi lembrado ao longo do texto. Os sistemas compõem uma estrutura que considera tecnologia (hardware, software), instalações físicas (layout), pessoas (especializadas, não especializadas), processos (métodos) e procedimentos (normas, políticas) para que possa existir.

Conforme indica o trabalho de pesquisa, nem tudo que é legal é ético e o contrário também é verdadeiro. Conhecer a lei é fundamental, bem como a existência de uma legislação específica para este novo modelo de interação social, política e econômica. Da mesma forma, é fundamental agir de forma correta, honesta, transparente, através de mecanismos específicos que garantam a proteção dos dados privados. Por isso, a importância das políticas de gerenciamento de informações, destacando as relacionadas à segurança e privacidade de dados.

Se o atributo mais valorizado de um administrador é sua ética, conforme Kanitz (2011), este automaticamente será o atributo mais importante da empresa que tenha em sua representação um administrador, uma vez que por trás dos sistemas informatizados há pessoas trabalhando em conjunto com as tecnologias. E considerando que o comércio eletrônico (e-commerce) já se estabelece como uma nova forma de adquirir bens e serviços, novos desafios cercam os diversos usuários desse sistema (empresas, fornecedores, governo, consumidores, etc). Entre tais desafios estão aqueles relacionados à ética em sistemas de informação e questões relativas à segurança e privacidade de dados.

No contexto atual os mais diversos profissionais acreditam que ética é simplesmente cumprir e, conforme Kanitz (2011), a maioria das áreas nem a estuda, considerando-a algo óbvio. Só que ética é coisa séria. Em Stanford e Harvard, por exemplo, ela e a responsabilidade social são áreas bem estruturadas. A primeira coisa que ensinam é que ética é tudo o que decidimos não fazer, apesar de ser correto, legal e permitido. Por isso, ela, para o administrador, está acima da lei, pois deixamos de fazer muitas coisas – apesar de serem absolutamente legais e permitidas.

Nesse sentido, pode-se inferir que a conduta ética é algo pessoal que oriunda do caráter de cada indivíduo, mas que pode perfeitamente ser lapidada à imagem de uma organização, pois uma empresa bem-sucedida tem sua estrutura alicerçada em valores, missão e visão. Este conjunto de normas, regras e princípios regem a direção e o pensamento daqueles que trabalharão para alcançar os resultados daquela organização. Portanto, a ética é tanto individual quanto coletiva.

Drucker, certa vez, disse que o atributo mais importante de um gestor é seu caráter. Isso pode ser estendido para a empresa: o atributo mais importante da empresa é seu caráter expresso pelo conjunto das pessoas que a representam. O caráter pode ser entendido como a conduta ética que a empresa se utiliza para

tomar decisões rotineiras, tratar com clientes e fornecedores, garantir a segurança das informações de seus parceiros e clientes e transmitir informações de ordem pública dentro dos padrões regidos pela transparência, por exemplo. Este conjunto de condutas éticas fortalece a empresa, seus parceiros, seus clientes, seus acionistas, entre outros.

Assim, cumpre-se o segundo objetivo da pesquisa que foi conceituar a ética e identificar a importância dos valores, princípios e condutas éticos que envolvem um sistema de informações (SI).

Quando falamos de sistemas de informação, temos a inocência de relacioná-lo somente à tecnologia que é empregada. Porém, os sistemas de informação são muito mais abrangentes. Os usuários, muito provavelmente, sejam a parte mais importante deste pilar que também envolve estrutura e tecnologia. E quando falamos em usuários, estamos falando de usuário cliente/consumidor e usuário empresa. Ambos devem compreender a utilização das tecnologias relacionadas à informação, os sistemas e a internet, pois o interesse sobre a utilização das informações privadas que percorrem tais sistemas é de ambos.

Para o usuário empresa, conforme Baltzan & Phillips (2012), compreender o impacto direto que a informação tem sobre o resultado final de uma organização é fundamental para gerir um negócio bem-sucedido. Isto indica que a informação é tão importante quanto um bem tangível e deve ser utilizada efetivamente para que resultados positivos sejam alcançados. Isto implica, também, o tratamento adequado de informações privadas, pois em uma sociedade do conhecimento a informação (privada) é um bem precioso e deve ser preservada.

Para o usuário cliente/consumidor o entendimento de como os sistemas de informação e a internet se comportam é um meio de torná-lo mais consciente em relação aos seus direitos e deveres, policiando sua liberdade nos quesitos segurança e privacidade. A internet não pode ser uma “terra sem dono” onde as pessoas (usuários) podem fazer o que bem entenderem, pois isto causaria danos às liberdades individuais. É por isto que existem regras que regem a utilização de muitos sistemas com base na internet, entre eles políticas de segurança e privacidade da informação. Estas regras promovem um ambiente de navegação (interação) mais correto, seguro e ético possível.

Logicamente que, como no meio social tradicional, existem deturpações variadas que podem causar danos a imagem e a honra dos indivíduos, bem como

danos a reputação das empresas, por exemplo. Ambos os lados sofrem revés: o indivíduo pode ter sua vida pessoal invadida por terceiros ou, ainda, verificar que seus dados pessoais estão sendo utilizados por outra empresa a qual nunca teve vínculo; a empresa pode perder credibilidade e confiança por deixar vazar ou, pior ainda, negociar dados de seus clientes com uma empresa parceira sem prévia autorização dos mesmos.

Muitos países adotam medidas rígidas que norteiam a utilização adequada de dados privados, com políticas de banco de dados e políticas anti-spam, por exemplo. As leis contribuem para a manutenção de direitos e deveres que devem ser cumpridos no ambiente virtual. Porém, quando falamos do ambiente internet estamos falando de um ambiente global, além-fronteiras. Neste ponto reside a dificuldade pelo simples fato de haver diferentes culturas e diferentes legislações que podem absorver interesses próprios em detrimento de interesses comuns.

O tema sobre privacidade na rede é bem complexo, pois envolve muitos interesses de ambos os lados: usuário comum e usuário empresa. Podemos citar as tecnologias de monitoramento que já estão presentes em muitos locais de trabalho e lazer, principalmente. Os funcionários podem não saber que estão sendo monitorados remotamente através de seu e-mail e seu telefone particular, o que causa o surgimento de dilemas éticos com relação à liberdade e à privacidade dos indivíduos. Existem softwares aplicativos que realizam a função de monitoramento, bem como dispositivos tecnológicos como câmeras, por exemplo, que monitoram o comportamento de funcionários durante o tempo de serviço. As empresas querem aumentar a sua produtividade, reduzir custos e maximizar o tempo efetivo de trabalho. Os funcionários querem garantir que suas liberdades não sejam feridas.

Ainda, podemos identificar o monitoramento que cada usuário da rede sofre ao visitar um endereço eletrônico na internet. Isso é possível graças ao cruzamento de informações. Cada vez que visitamos uma página na internet nosso número de IP (protocolo de internet – cada computador ou assistente pessoal digital possui um serial que o identifica) está sendo monitorado pelo web site que visitamos através de cookies. Os cookies fazem a troca de dados entre o navegador e o servidor de páginas. Por exemplo, quando nos cadastramos em um site de compras e queremos acessar nossa conta, precisamos fornecer o nome de usuário (login) e a senha respectivos àquela conta. O cookie permite um autopreenchimento destes campos (login e senha), sem a necessidade de digitarmos nosso login e senha. Isso pode

ser muito perigoso, caso o usuário acesse esse web site através de computadores públicos ou de terceiros.

Existem diversos softwares e dispositivos que permitem o monitoramento de acessos, a interceptação de dados através da rede e o controle de computadores remotos. A privacidade está intimamente ligada à segurança da informação, por isso a importância de estarmos atentos às tecnologias, aos processos e as políticas existentes para não termos nossa privacidade invadida.

Assim, percebe-se que os esforços da sociedade para um ambiente virtual mais seguro e privativo é considerado importante para a manutenção deste. O próprio marco civil da internet, um projeto de lei que procura regularizar questões relacionadas ao ambiente virtual e o uso da internet, nasceu da necessidade de garantias para uma navegação mais segura, bem como os direitos e os deveres daqueles que tratam, armazenam e disseminam dados e administram bancos de dados, por exemplo.

O terceiro objetivo da pesquisa cumpre-se ao relacionar a segurança e a privacidade na rede e seus dilemas éticos envolvidos na utilização de tecnologias da informação (TI) no âmbito pessoal e no âmbito do trabalho.

Finalmente, o último objetivo da pesquisa que foi identificar o tratamento de bases de dados, seu armazenamento e sua transmissão segundo a legislação brasileira, demonstrou que não há, ainda, uma regulação específica que trate sobre tais questões.

Nos Estados Unidos e em muitos países da Europa, existem legislações específicas para o tratamento de bases de dados. No Brasil, estamos engatinhando nesse aspecto, embora a inserção e o acesso às tecnologias estejam mais disseminados nesses últimos anos. Escolas, empresas públicas e privadas, usuários comuns, estão aderindo aos novos processos de trabalho, comunicação e comércio que as novas tecnologias oferecem.

Conforme a pesquisa, no Brasil ainda não há uma legislação que regule as relações entre usuários através da rede. Com isso, não é muito difícil entender as preocupações existentes na sociedade sobre a utilização de dados privados por empresas públicas e privadas. Muitas questões, inclusive aquelas relacionadas à segurança, privacidade e liberdade são evidenciadas em movimentos sociais que lutam pela regularização do ambiente virtual. O Marco Civil da Internet no Brasil

surgiu a partir dessas preocupações e está sendo votado, no Congresso nacional, em regime de urgência dentro dos próximos dias enquanto escrevo este texto.

Para finalizar, é importante ressaltar que, embora leis específicas sobre privacidade ofereçam certas garantias, elas não protegem completamente a privacidade individual. Por isso, é fundamental aumentar a proteção de sua própria privacidade. Existem algumas medidas para o usuário proteger-se como a utilização de um firewall em seu computador e a manutenção de seu antivírus que deve ser constantemente atualizado. Ao visitar web sites, verificar se existe um cadeado fechado junto a barra de endereços e se há um “s” junto ao http que significa “seguro”. Verificar certificações, políticas e termos de uso do web site também diminuem os riscos de quebra de segurança e privacidade.

5 LIMITAÇÕES E SUGESTÕES PARA ESTUDOS FUTUROS

O presente trabalho não teve a pretensão de esgotar as questões relacionadas à privacidade na rede, nem de eleger estruturas supostamente mais ou menos adequadas. Ao contrário, este assunto oferece uma gama diversa de possibilidades que podem ser exploradas em muitas áreas de estudo, principalmente àquelas ligadas aos negócios, como a administração, por exemplo. Hoje, qualquer profissional que não esteja familiarizado com as novas tecnologias e suas implicações perecerá no mercado de trabalho.

A privacidade advém da segurança na rede, outro ponto fundamental que gera dilemas éticos que atormentam profissionais de TI, principalmente. Este assunto pode ser explorado sob várias óticas já que a ética, ao contrário das leis, é muito mais reflexiva e conta com o subjetivismo daquele que se utiliza dela. Nesse sentido, muitas outras questões podem ser revistas e aprimoradas conforme a necessidade e a disponibilidade daquele que queira aprofundar o assunto.

Como não poderia ser diferente, esta pesquisa não encerra, em si mesma, a completude do assunto em questão. Por questões de tempo, escassez de materiais publicados, prioridade e até capacidade do pesquisador, alguns pontos não foram investigados com a profundidade necessária, e outros sequer puderam ser mencionados, apesar de estarem correlacionados com o tema pesquisado.

A partir desse trabalho, outros problemas de pesquisa podem ser estudados. Movimentos sociais pela liberdade e privacidade na rede emergem a partir de projetos de lei que ameaçam os direitos dos usuários. SOPA (Stop Online Privacy Act), PIPA (Protect IP Act) e ACTA (Anti-Counterfeiting Trade Agreement) são exemplos que demonstram os problemas enfrentados pela sociedade atual. Espera-se, assim, que o presente trabalho possa contribuir para outras pesquisas que possam surgir e, principalmente, que as conclusões e as recomendações aqui enunciadas possam ser úteis a todos aqueles que desejem manter sua segurança e sua privacidade preservadas na rede.

REFERÊNCIAS BIBLIOGRÁFICAS

ANGELONI, Maria T. **Comunicação nas organizações da era do conhecimento**. São Paulo: Atlas, 2010.

ATHENIENSE, Alexandre. **A venda de banco de dados cadastrais e a legislação brasileira**. Disponível em: <http://www.jusbrail.com.br>. Acesso em: 25/10/2013.

BALTZAN, Paige; PHILLIPS, Amy. **Sistemas de informação**. Porto Alegre: AMGH, 2012.

BERTUCCI, Janete Lara de Oliveira. **Metodologia básica para elaboração de trabalhos de conclusão de cursos (TCC):** *ênfase na elaboração de TCC de pós-graduação Lato Sensu*. 1ª edição. São Paulo: Atlas, 2012.

DONEDA, Danilo. **O vazamento de dados pessoais na iminência de regulação**. Disponível em: <http://culturadigital.br/dadospessoais/>. Acesso em: 28/09/2013.

_____. **Mais um caso de vazamento de dados*:*** *desta vez foi a LG*. Disponível em: <http://observatoriodainternet.br>. Acesso em: 28/09/2013.

DRUCKER, Peter Ferdinand. **Gestão**. Rio de Janeiro: Agir, 2010.

DUBRIN, Andrew J. **Fundamentos do comportamento organizacional**. São Paulo: Thomson, 2003.

FAE. **Manual para a elaboração e apresentação de trabalhos acadêmicos**. Sapucaia do Sul: FAE, 2007.

FERREIRA, Aurélio B. H. **Miniaurélio**: *o dicionário da língua portuguesa*. 6ª edição. Curitiba: Positivo, 2005.

FONSECA, J. J. S. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 1988.

G1 RS notícias. **É má fé, diz secretário de segurança do RS sobre venda de dados pessoais**. Disponível em: <http://www.g1.globo.com/rs>. Acesso em: 25/10/2013.

HAWKINS, Del I; MONTHERSBAUGH, David L; BEST, Roger D. **Comportamento do consumidor**. 10ª edição. Rio de Janeiro: Elsevier, 2007.

JONES, Gareth R.; GEORGE, Jennifer M. **Administração contemporânea**. 4ª edição. São Paulo: McGraw-Hill, 2008.

JORNAL NH. **Cibercrimes:** *danos incluem fraude por roubo de informações bancárias*. Disponível em: <http://www.jornalnh.com.br>. Acesso em: 20/09/2013.

KANITZ, Stephen. **Sua ética**. *Revista administradores.com.br*, João Pessoa, julho de 2011. Ponto final, p. 50.

LINS, Bernardo F. E. **Estudo sobre privacidade e internet**. Consultoria Legislativa. Câmara dos Deputados. Brasília: março, 2000.

MARQUES, Wagner Luiz. **Ética no trabalho**. 1ª edição. Cianorte: Wagner Luiz Marques, 2010.

MASIERO, P. C. BIGONHA, R. S. **Ética e Computação**. Volume 1. Número 1. SBC HORIZONTES: Dez 2008.

O'BRIEN, James A.; MARAKAS, George M. **Administração de sistemas de informação**. 15ª edição. São Paulo: McGraw-Hill, 2012.

REBÊLO, Paulo. **PGP é sistema de segurança avançado para correio eletrônico**. Disponível em: <http://www.uol.com.br/tecnologia/seguranca/>. Acesso em: 12/10/2013.

ROSINI, Alessandro M.; PALMISANO, Angelo. **Administração de sistemas de informação e a gestão do conhecimento**. São Paulo: Thomson, 2003

STAIR, Ralph M.; REYNOLDS, George W. **Princípios de sistemas de informação**. São Paulo: Cengage Learning, 2011.

WOLLENHAUPT, Sandro. **Metodologia científica**. Porto Alegre: Razão, 2004.

O trabalho está licenciado com uma Licença Creative Commons - Atribuição-Não Comercial-Sem Derivações 4.0 Internacional.