_POLÍTICA DE INTEGRAÇÃO DE SEGURANÇA E ÉTICA NA INTERNET: PERSPECTIVAS DE UMA MELHOR PROTEÇÃO PARA AS INFORMAÇÕES

Inalmir Bruno Andrade da Silva
Universidade Estadual da Paraíba (UEPB)
bruno_sjs@hotmail.com

Maria Givaneide Araújo da Silva
Universidade Estadual da Paraíba (UEPB)
givaneideadm2010@hotmail.com

Resumo_Como tudo na vida apresenta vantagens e desvantagens, na internet existe um lado bom e outro ruim. Este artigo aborda a questão da integração da segurança e da ética na internet, como perspectiva de manter a integridade das informações. O objetivo consiste em demonstrar os benefícios e os riscos relativos ao uso da internet. A metodologia resulta da revisão da literatura dos itens pertinentes ao tema e uma pesquisa informal realizada com clientes da empresa ValeOline Internet, localizada em Santa Luzia\PB, visando obter respostas mais precisas sobre o tema em questão. Portanto, conclui-se o estudo evidenciando a relevância dos serviços oferecidos pela internet, bem como os danos que tais serviços podem causar para as pessoas e as organizações em geral.

Palavras-chave_internet; política de segurança; princípios éticos na internet.

1 Introdução

A Constituição Federal em seu artigo 5º, inciso X, assegura a todos os cidadãos o direito à preservação da privacidade, da intimidade, da honra e da imagem das pessoas. Sendo, portanto, indenizado pelo dano material ou moral o cidadão que vier a sofrer esse tipo de violação. Mesmo sendo menor de idade, há lei específica para punir o ofensor.

A carta Magna também garante o direito à liberdade de pensamento, sendo vedado o anonimato. Além de assegurar a liberdade de atividade intelectual, artística, científica e de comunicação, independente de censura ou licença. Porém, essa liberdade não é absoluta; existem, portanto, as restrições. Os li-

mites da liberdade que se tem para expressar o que se pensa implica a não ofensa aos outros.

O inevitável desenvolvimento tecnológico aliado à necessidade de manter comunicação, tanto para as necessidades das empresas como para as atividades domésticas, permitiu a conectividade entre diferentes plataformas, gerando a internet. As vantagens trazidas por esse avanço têm proporcionado o incremento dos crimes comuns, como o furto, estelionato, pornografia infantil, o que possibilita que esses delitos cresçam na mesma proporção dos avanços das tecnologias.

Desse modo, a internet constitui uma rede que proporciona experiências positivas, como as pesquisas, as trocas de mensagens, as compras, o pagamento, enfim, permite a realização de uma infinidade de tarefas com maior facilidade. Por outro lado, propicia abertura para a prática de diversos crimes. Por isso requer uma série de medidas para que o usuário não seja mais uma vítima dos mal-intencionados.

Nessa ótica, atenta-se para a reflexão sobre as questões éticas. Entendendo-se o termo "ética" como uma palavra simples, mas que tem diferentes interpretações. A conduta de uma pessoa pode não ser igual à de outra, uma vez que a individualidade, os princípios e os costumes fazem parte da personalidade de cada um e são influenciados pela sociedade na qual o indivíduo está inserido. O estudo da ética consiste ainda em uma ramificação da filosofia que enfoca o comportamento moral do ser humano, classificando-o como bom, ruim, certo, errado. Tal conceito existe desde as civilizações antigas, porém é pouco usado na internet em virtude do fato de essa tecnologia ser relativamente nova.

Portanto, o projeto de segurança de uma rede deve contemplar questões operacionais indispensáveis para manter a integridade das informações registradas no ambiente virtual. Então, a pergunta problema que serviu de aporte à realização do estudo resume-se em: Como usufruir das potencialidades oferecidas pela internet sem pôr em risco a si próprio ou outras pessoas?

Desse modo, o objetivo geral consiste em demonstrar os benefícios e os riscos que a internet oferece. Desse objetivo, desdobram-se os seguintes objetivos específicos: expor noções básicas sobre a internet e segurança na internet, apontando os aspectos que favorecem e dificultam a navegação na web. Bem como, identificar as estratégias e as dicas para a garantia de uma informação segura.

Sendo assim, o tema foi escolhido por sua relevância nos dias atuais, pela facilidade no desenvolvimento das atividades comuns do cotidiano, tanto das pessoas como um todo como pelas organizações corporativas, bem como por

sua importância no processo de transformação e integração das pessoas no meio social. Desse modo, o estudo propiciou, para os autores do artigo em questão, um aprendizado que é imprescindível ao crescimento pessoal e profissional.

2 A internet e suas funcionalidades

A internet é uma ferramenta que se tornou um fenômeno em escala mundial. Cresce mais rapidamente do que qualquer outro meio de comunicação já inventado. Constitui uma rede mundial que interliga diversos computadores de todos os tipos e capacidades, por meio de linhas de comunicação, utilizando um conjunto de regras (protocolos) para viabilizar o envio e o recebimento de mensagens (CUNHA, 2010).

O desenvolvimento da internet superou quaisquer previsões e\ou expectativas, constituindo uma verdadeira revolução na sociedade moderna. Uma vez que se tornou num pilar das comunicações, do entretenimento e do comércio em qualquer lugar do planeta. Baseia-se no uso do protocolo TCP\IP e suas diversas camadas de protocolos dependentes. Tal protocolo permite o acesso a informações e todo tipo de transferência de dados.

Para Menezes (2013), a internet possui quatro funções principais. A primeira refere-se ao ensino-aprendizagem, na qual é usada para os que procuram conhecer coisas e pessoas, bem como adquirir cultura e conhecimento. A segunda diz respeito ao entretenimento, direcionado para jogos virtuais e *sites* de bate-papo. A terceira faz alusão à comunicação para os que buscam explorar recursos de *e-mail* e MSN. Já a quarta função refere-se ao trabalho para os que usam essa tecnologia visando obter recursos financeiros.

Mesmo sendo a internet considerada como ícone facilitador do cotidiano, tanto das pessoas como das organizações em geral, como toda tecnologia, conforme Ribeiro (2012, p. 1), precisa "ser dosada de forma a proporcionar os seus usuários um ambiente produtivo, seja qual for a finalidade dela e com isto contribui para o crescimento das pessoas em todo os segmentos da vida".

Falando sobre modelos dos dispositivos de comunicação, com base nas relações entre emissores e receptores, para melhor compreender as mudanças ocorridas na internet, Galli (2010) classifica tais dispositivos em três modelos. O primeiro do tipo "Um e Todos" é representado pelos modernos meios de comunicação em massa, possuindo um centro emissor e vários receptores, em que a mensagem é divulgada em um único sentido, inexistindo interatividade entre as partes.

O segundo dispositivo, conforme a mesma autora, é o tipo "Um e Um", que proporciona uma interação perfeita entre as partes, porém não possui a emer-

gência do coletivo na transmissão da informação. Enquanto o terceiro dispositivo, "Todos e Todos", não permite distinção entre emissores e receptores, visto que todas as partes em contato podem ocupar as duas posições, estabelecendo um novo tipo de interação. A internet se enquadra nesse último modelo.

Desse modo, embora a internet seja uma poderosa e importante ferramenta que permite o envio e o recebimento de informações em tempo real, sem medir distâncias, e que certamente tende a melhorar a vida das pessoas, por outro lado pode trazer malefícios. Portanto, deve-se ter cuidado com essa nova onda que invadiu o mundo, avaliando o uso e tendo consciência nas escolhas as quais são postadas na tela de um computador.

Nesse mesmo entendimento, os crimes cibernéticos estão cada vez mais frequentes, visto que a web é um poderoso meio de troca de informações instantâneas. Milhares de negócios jurídicos são realizados em questão de segundos. Mas, por outro lado, têm sido alvo constante de piratas cibernéticos, que se aproveitam dos conhecimentos e das falhas de todo o sistema para obter diversas vantagens, da mesma forma e com o mesmo dinamismo das atividades virtuais (GALLI, 2010).

3 Noções básicas sobre segurança na internet

A segurança na internet está estritamente relacionada à proteção de um conjunto de informações. Significa preservar o valor que a informação possui para um indivíduo ou organização. "Do ponto de vista dos usuários, a segurança está associada aos riscos de insucesso, falhas e fraudes no Comercio Eletrônico, especialmente nas transações eletrônicas" (LEITE; ADRIAN apud ALBERTINI, 2013, p. 4).

A segurança da informação é formada pelos seguintes pilares básicos que podem ser definidos da seguinte forma: a Disponibilidade – que garante o acesso permanente e/ou sempre que necessário de recursos e informação; a Confiabilidade – que assegura que uma informação somente seja acessada por alguém de direito; a Integridade – garante que a informação não seja corrompida; e a Autenticidade – assevera a veracidade e certeza de exatidão da informação.

Para Morais (2013), o termo segurança na internet implica utilizar de forma responsável, segura e com princípios éticos as tecnologias de informação e comunicação. Pois não há segurança em sentido absoluto na internet nem segurança absoluta em nada. Visto que haverá sempre alguém que usa a informação de forma antiética, irresponsável, insegura e/ou talvez pela falta de informação/conhecimento.

> Um problema de segurança em seu computador pode torná-lo indisponível colocar em risco a confidencialidade e a integridade dos dados nele armazenados. Além disto, ao ser comprometido, seu computador pode ser usado para a prática de atividades maliciosas como, por exemplo, servir de repositório para dados fraudulentos, lançar ataques contra outros computadores (e assim esconder a real identidade e localização do atacante), propagar códigos maliciosos e disseminar spam (CERT, 2013, p. 3).

Assim, para sentir-se protegido no ambiente virtual é necessário adotar certos padrões de segurança. Segundo Charles (2013), deve-se, *a priori*, ter conhecimentos básicos sobre tipos de *softwares* que podem atacar o computador, bem como saber como evitar ser lesado por outros tipos de ataques, que tentam induzir os usuários a liberar informações particulares para o invasor.

Charles (2013) lembra, ainda, da existência de duas categorias de ataques baseados na internet, a saber: os ataques técnicos e os sociais. Sendo que, estes tentam convencer o usuário a fornecer senhas e outras informações de conta para a pessoa errada. Aqueles destinam-se ao computador, normalmente sem o conhecimento do usuário.

4 Estratégias de segurança para uma informação segura

A internet é uma ferramenta responsável pela facilitação da realização de atividades diversas, permitindo a socialização entre as pessoas, o que tende a cultivar novos valores, a melhoria da cultura e, sobretudo, a aquisição de novos conhecimentos. É possível navegar de forma segura, fazer compras e movimentações em bancos, sem correr o risco de ser enganado por terceiros, desde que se adote mecanismos de segurança.

Os ataques na internet costumam ocorrer por conta de diversos objetivos, com vistas a diferentes alvos e por meio da utilização de diversas técnicas. Assim, qualquer serviço, computador ou rede que esteja com acesso à internet pode ser alvo de um ataque. Da mesma forma, qualquer computador acessível à internet também pode participar de um ataque (CERT, 2013).

Os motivos que levam os atacantes a disseminar ataques na internet são os mais diversos, variando desde a simples diversão até a realização de ações criminosas. Tais motivos são os seguintes:

> Demonstração de poder: mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente. Prestígio: vangloriar-se, perante outros atacantes,

> por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar *sites* considerados visados ou difíceis de serem atacados... Motivações financeiras: coletar e utilizar informações confidenciais de usuários para aplicar golpes. Motivações ideológicas: tornar inacessível ou invadir *sites* que divulguem conteúdo contrário à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia (CERT, 2013, p. 17).

Para alcançar tais objetivos os atacantes costumam utilizar as seguintes técnicas: exploração de vulnerabilidades, em que os intrusos tentam executar ações maliciosas, como invadir sistemas; varredura em rede ou *scan* que consiste em efetuar buscas minuciosas em redes a fim de identificar computadores ativos e coletar informações sobre eles; falsificação de *e-mail*, em que visam alterar campos de cabeçalho, na tentativa de confundir a origem do *e-mail* enviado.

Ademais, existe a técnica da força bruta que permite descobrir, por tentativa ou erro, nome de usuários e senhas para praticar ações nocivas. Já a desfiguração da página ocorre quando é alterado o conteúdo da página da web de um site. A navegação de serviços configura um computador ou uma rede conectada à internet. Diante desse cenário, a possibilidade de um ataque na internet ser ou não bem-sucedido dependerá de um conjunto de medidas preventivas que os usuários devem adotar.

Para se proteger dessas ações maliciosas, Charles (2013) aponta o *software* de segurança como a salvaguarda para os programas nocivos alojados no computador, tal como o *malware* que tenta tomar o controle do computador, disseminando os programas nocivos. Para evitá-lo, têm-se os *firewalls* de rede que bloqueiam determinados tipos de atividades da rede, restringindo o fluxo de informações entre duas redes. Outra maneira de evitar ataques é manter um sistema operacional e aplicativos atualizados para suas últimas versões.

> Existem diversas tecnologias para impedir acessos não autorizados. Uma das técnicas mais comuns de segurança é a implementação de um servidor de Proxy. Essa técnica consiste em conectar uma máquina à internet que agirá como agente de comunicação. Tal máquina terá uma interface de comunicação com a internet, bem como uma outra interface de comunicação com a rede local (GUILHERME, 2013, p. 1).

Sob esse aspecto, o mesmo autor menciona ainda que, o servidor Proxy tem utilização limitada. Assim, para determinadas situações, há o *software firewall* cuja função é analisar cada pacote de dados que passa da internet

para a rede local e vice-versa. Desse modo, existe a possibilidade de filtrar dados e pacotes indesejáveis, da mesma forma como pacotes provenientes de locais não desejáveis.

Na visão de Villa (2013), não adianta utilizar as ferramentas de segurança como *firewalls*, antivírus, se os usuários não adotarem medidas de segurança na internet. Assim, para não correr o risco de ser enganado ao navegar na internet é importante seguir as seguintes estratégias: evitar abrir mensagens com remetentes reconhecidos; desconfiar de tudo o que vem por *e-mail*, evitar fornecer informações pessoais ou financeiras por *e-mail*, bem como nunca clicar em *links* recebidos por *e-mail*.

Ademais, o mesmo autor aconselha a configurar o certificado de segurança para que a troca de informações sigilosas seja de forma criptografada; deve-se ter cuidado ao abrir arquivos anexados aos *e-mails*, independente de quem enviou; evitar baixar arquivos executáveis, visto que estes tendem a ocultar tentativas de ataques. Deve-se sempre desconfiar das propostas tentadoras; mantendo-se informado sobre os golpes e ataques praticados na internet e, por fim, usar o bom senso.

Destarte, o *software firewall* não previne totalmente dos riscos derivados das ações maliciosas da internet, uma vez que nos próprios sistemas operacionais existem falhas que são aproveitadas por mal-intencionados. No entanto, um *firewall* corre dentro do sistema operativo e, sendo assim, também está sujeito a falhas de segurança do próprio sistema operativo. Tal *software* restringe algumas das atividades *on-line* (GUILHERME, 2013).

5 Reflexões sobre ética na internet

De acordo com Villares (2013), o mundo está passando por uma quarta onda de transformações, assim como a que ocorre hoje a era da revolução da informação, conduzida pela tecnologia disponível, que é responsável pela eliminação das barreiras no que se refere à língua e à cultura, favorecendo a aquisição de novos processos de produção, de novas formas de diversão, e conduzindo a um novo modo de viver, pensar, agir e interagir.

Segundo Edmundo (2013), desde os tempos mais remotos, o homem vem se comunicando e interagindo com as pessoas. A comunicação constitui uma das principais ferramentas que permitem o desenvolvimento e o aperfeiçoamento da humanidade. A estrutura da internet favorece a interação entre as pessoas em tempo real, independentemente de espaço.

As principais mudanças mundiais resultam das formas de comunicação, principalmente por causa do avanço da informática e dos meios eletrônicos.

Em tempos anteriores, os diálogos ocorriam pessoalmente. No final do século XX, a comunicação passou a ocorrer por meio do telefone e hoje se dá pelo computador (VILLARES, 2013).

A noção do que é certo e do que é errado sempre acompanhou a humanidade e foi evoluindo na mesma proporção do desenvolvimento da civilização. É previsível um futuro certo e feliz para toda a humanidade, porém os caminhos são imprevisíveis. A questão da criminalidade está ligada à questão social. O direito penal vem contribuindo, com suas teorias, na construção e elaboração de alternativas para combater a criminalidade (OLIVEIRA JR, 2001).

Além de beneficiar a globalização, a internet cria interferência de informações entre culturas distintas que, certamente, modifica a forma de pensar das pessoas. Assim, o desenvolvimento moral e social das pessoas pode ser influenciado na medida em que elas, com ideias e culturas diferentes, recebem um grande número de informações (SOUZA, 2013). Assim, "quanto mais veloz e voraz é o avanço tecnológico, maior é o abismo que separa o mundo tecnologicamente 'in' do mundo tecnologicamente 'out'" (VILLARES, 2013, p. 1).

O mesmo autor menciona que, as conversas hoje são registradas e que as comunicações virtuais não garantem o anonimato aos usuários. Lembra ainda que, não se pode ofender as pessoas impunemente nem imputar conduta imoral ou desonrosa a alguém. Mesmo que o ofensor seja menor de idade, ele será responsabilizado pelo ato praticado, segundo o Estatuto da Criança e do Adolescente (ECA), uma vez que essa lei oferece direitos às crianças e aos adolescentes, mas também os pune.

Diante desse cenário, atenta-se para as reflexões sobre a ética que, para Ribeiro (2012), é uma palavra de origem grega derivada de ethos que lida com a compreensão das noções e dos princípios que sustentam as bases da moralidade social e da vida individual. Para Leão (2013) é a ciência que estuda a moral, procurando avaliá-la criticamente, tendo em vista o alcance de valores sustentáveis e universais.

> [...] a boa convivência na Internet depende de uma série de regras conhecidas como netiqueta ou etiqueta na rede. As regras incluídas na netiqueta não foram definidas por uma autoridade no assunto, mas criadas pelos próprios usuários ao longo do tempo. Também não existe um texto único e definitivo sobre o tema, mas várias interpretações espalhadas pela rede (VILLARES, 2013, p. 2).

O comportamento das pessoas no mundo real tende a ser reproduzido no ambiente virtual. Para Silva (2013, p. 1), "a sensação de anonimato e de invisibilidade no uso da internet é falsa, pois por meio do IP (Protocolo de Internet) é possível se descobrir de que máquina uma determinada ofensa foi publica-

da". Do ponto de vista ético, o autor mencionado recomenda que as pessoas não façam com as outras o que não gostariam que fizessem com elas próprias.

6 Resultados encontrados

A internet está presente na vida da maioria da população mundial e, provavelmente, essas pessoas não conseguiriam imaginar suas atividades sem usufruir das diversas facilidades e oportunidades proporcionadas por essa tecnologia. Aproveitar os benefícios trazidos por essa mídia requer uma série de cuidados para que as informações registradas na web não venham a afetar negativamente sua vida social e/ou profissional. Dessa forma, além de adotar as medidas preventivas, deve-se considerar a ética como principal passo para evitar os acessos não autorizados.

Neste item serão demonstrados relatos de entrevistas de caráter informal realizadas com clientes da empresa ValeOnline Internet, que distribui internet de banda larga, via cabo e via rádio a seus clientes. A pesquisa trata dos riscos, o bom senso proveniente da utilização da internet, bem como os mecanismos de prevenção necessários para tornar a navegação na web sustentável. Tal empresa localiza-se em Santa Luzia/PB, mas oferece suporte a várias cidades circunvizinhas. O acesso à internet dos entrevistados resulta de computadores, *notebooks*, *tablets*/ou telefones celulares.

Sobre a questão dos cuidados que se deve ter ao liberar os filhos para navegar no ambiente web, verificou-se que os entrevistados afirmaram que são a favor de que seus filhos conversem com amigos/conhecidos, acessem *sites* compatíveis com a idade de cada um e, principalmente, dentro de um tempo de acesso estipulado para que a internet colabore com seu desenvolvimento. Relataram ainda que os *sites* e pessoas desconhecidos são proibidos para os menores e, caso ocorra acesso, eles não devem fornecer dados pessoais, senhas, uma vez que os *sites* desconhecidos representam um risco para quem os acessa.

Quanto à reação dos usuários diante do problema do *cyberbullying,* que significa a prática do *bullying* por meio das tecnologias de informação, os entrevistados relataram que deve-se tomar cuidado com as ameaças, não dando importância para as humilhações e tomar as providências cabíveis. Foi constatado também que muitos usuários acreditam que somente o antivírus instalado no seu computador é suficiente para bloquear a maioria das ameaças a que o computador está sujeito.

Em relação às pesquisas que são realizadas e os *sites* acessados, verificou-se que a maioria dos usuários prefere a internet para obter as respostas

rápidas, sem questionar quanto à veracidade das informações, tampouco confrontar as várias fontes para terem mais garantia de que a informação procurada é confiável e de qualidade. Os usuários afirmaram também que a internet cria uma relação de dependência, em virtude da facilidade e a rapidez oferecida. Assim, os livros estão ficando em segundo plano para as pesquisas, desvalorizando a cultura e o hábito da leitura.

Quanto às atitudes que se deve adotar ao publicar informações na internet foi constatado que alguns colaboradores têm pouca preocupação em relação às informações publicadas. Outros relataram ter mais cuidado, visto que nem todas as informações podem ser removidas da internet. Ao deixar uma pegada digital seus dados podem ser utilizados no futuro. Assim, deve-se evitar a publicação de informações no ambiente virtual, tendo em vista a exposição desnecessária.

Em relação aos padrões éticos na internet, os colaboradores da pesquisa definiram tal conceito como a prática de algo tendo a consciência das consequências que ocorrerão. Falaram ainda que é preciso determinar o que é bom para o próprio indivíduo tanto para a sociedade como um todo. Pois o homem vive em sociedade com outros homens e, sendo assim, deve pensar e repensar antes de agir perante os outros.

Sobre as indagações feitas aos entrevistados a respeito de como se comportar para cultuar a ética com o outro, eles relataram que não se deve usar o computador para roubar senhas bancárias, interferir no trabalho de outra pessoa, prestar falso testemunho, copiar ou roubar *software* pelo qual não pagou, utilizar os trabalhos intelectuais de outra pessoa, enfim, é preciso pensar nas consequências sociais daquilo que se escreve, bem como usar o computador respeitando e considerando os terceiros.

7 Considerações finais

Nos últimos anos, o número de buscas na internet tem crescido em uma velocidade sem precedentes. Afinal de contas, a internet é considerada como uma rede classificada como WAN, que conecta várias redes em todo o mundo por meio de *backbones* (rede de transportes que designa o esquema de ligações centrais de um sistema mais amplo, geralmente de elevado desempenho).

A internet é uma poderosa ferramenta que facilita a vida das pessoas. Cresce mais rapidamente que qualquer outro meio de comunicação já inventado e está presente no cotidiano da maior parte da população que, provavelmente, não conseguiria imaginar sua vida sem usufruir dos benefícios proporcionados por essa tecnologia. Assim sendo, deve-se utilizá-la para promover o bem das pessoas e das comunidades. Partindo desse princípio, precisa-se

pensar criticamente sobre o que está sendo exposto nas redes sociais, uma vez que existe legislação para punir a maioria dos crimes praticados pela internet, mesmo que os ofensores sejam menores de idade.

Como tudo na vida apresenta um lado bom e outro ruim, na internet ocorre da mesma forma e/ou de modo semelhante. O que é bom para algumas pessoas pode não ser para outras. Essa tecnologia pode ser usada tanto para divulgar informações, como para explorar, manipular, dominar e corromper sistemas. A segurança na internet relaciona-se com a proteção de um conjunto de informações. Significa preservar o valor que a informação possui para um indivíduo ou uma organização.

A segurança no ambiente web vai além dos recursos tecnológicos. Para garantir que um conjunto de informações mantenha sua integridade, é necessário adotar medidas preventivas necessárias para que os benefícios ofertados pela internet sejam usufruídos de forma segura. Visto que os crimes podem ser evitados por meio da combinação entre tecnologia e legislação, esta possibilita a reparação dos danos, seja moral ou material, às vítimas dos ataques provocados por meio dos recursos tecnológicos.

A informação, hoje em dia, tem se tornado objeto de grande valor e consumo em todos os segmentos da sociedade. Isso ocorre em razão da importância e do uso que a ela tem para cada um dos usuários. Para se proteger das ações maliciosas e garantir a integridade das informações, é preciso adotar estratégias de segurança como *softwares*, antivírus e *firewalls*, bem como sistemas operacionais e aplicativos atualizados. Além dessas medidas, deve-se ficar atento para não abrir *links* dos quais se desconhece a origem.

Nessa ótica para manter a integridade de dados e das informações, é preciso que as pessoas adotem atitudes de segurança, desconfiando sempre das propostas tentadoras, informando-se sobre os golpes e os ataques praticados na internet e, principalmente, usem o bom censo e os princípios que sustentam as bases da moralidade social e da vida individual, pensando e repensando criticamente sobre o que é postado na tela do computador.

Sobre a pesquisa informal, verificou-se que os clientes da empresa ValeOnline Internet, alvo da pesquisa, possuem certo conhecimento sobre os riscos provenientes da internet. Porém, do ponto de vista da segurança na internet tais clientes possuem poucas informações, acreditando até que somente o antivírus instalado em seus computadores é suficiente para proteger todas as informações ali registradas.

Por outro lado, constatou-se que os colaboradores da pesquisa possuem comportamento compatível para com os princípios éticos, ou seja, procuram

cultuar a ética com o outro, tendo consciência das consequências sociais daquilo que se escreve na tela do computador, respeitando e considerando os terceiros.

Portanto, reiterando mais uma vez, a legislação vigente pode ser aplicada para a maioria dos crimes praticados por meios eletrônicos, assim é possível descobrir a autoria dos delitos praticados por tais meios. Destarte, ilude-se aquele que escondido atrás da tela do computador, praticando ações nocivas, ficará na impunidade. Para tanto, deve-se tomar cuidado quando ofender alguém pelas redes sociais, pois se estará sujeito a indenizá-lo.

Politics of integration of safety and ethics in the internet: perspectives of a better protection for the information

abstract_As everything in the life has advantages and disadvantages, in the internet a good and other side bad exists. This article approaches the subject of the safety's integration and ethics in the internet as perspective of maintaining the integrity of the information. The objective consists of demonstrating the benefits and the relative risks to the use of the internet. The methodology results of the revision of the literature of the pertinent items to the theme and an informal research accomplished with customers of the company ValeOline Internet, located in Santa Luzia/PB, seeking to obtain more necessary answers on the theme in subject. Therefore, the study is concluded evidencing the relevance of the services offered by the internet, as well as the damages that such services can cause for the people and the organizations in general.

Keywords_internet; politics of safety; ethical principles in the internet.

8 Referências

COMITÊ GESTOR DA INTERNET NO BRASIL. *Cartilha de Segurança para Internet* (CERT.br), versão 4.0. São Paulo, 2012. Disponível em: <http://://pt.slideshare.net/morresi_emerson/cartilha-de-segurana-para-internet-14085883>. Acesso em: 10 de fev. 2013.

CUNHA, J. C. *O que é internet, conceitos de internet, internet e suas funcionalidades, como usar a internet, introdução a internet, funções para internet*, 2010. Disponível em: <http://www.jeancarloscunha.wordpress.com>. Acesso em: 24 mar. 2010.

CHARLES, C. *A importância da segurança na internet*. Disponível em: <http://www.liberdadyorganizacion.org>. Acesso em: 20 fev. 2013.

EDMUNDO, C. *Comunicação Virtual*. Disponível em: <http://www.portaldoprofessor.mec.gov.br>. Acesso em: 27 mar. 2013.

GALLI, F. C. S. *Linguagem da internet*: um meio de comunicação global, 2010. Disponível em: <http://www.hotelsolardaslajes.com.br/upload/arquivos/2012-03-15-bf0c-941feb.pdf>. Acesso em: 27 mar. 2013.

GUILHERME, L. M. B. *A segurança na internet*: noções básicas. Disponível em: <http://www.student.dei.uc.pt/~lmborges/cp/artigo.pdf>. Acesso em: 19 mar. 2013.

LEÃO, C. *Ética, o que é e como se aplica*. Disponível em: <http://www.http://planetasustentavel.abril.com.br/noticia/desenvolvimento/etica-profissional-imagem-retidao--artigo-514891.shtml>. Acesso em: 24 mar. 2013.

LEITE, J. C.; ADRIAN, K. C. *Segurança na internet*: a percepção dos usuários como fator de restrição ao comércio eletrônico no Brasil. Disponível em: <http://www.anpad.org.br/diversos/trabalhos/EnANPAD/enanp ad_2005/ADI/2005_ADIB2784.pdf>. Acesso em: 25 mar. 2013.

MENEZES, V. M. *Funções da internet*. Disponível em: <http://www.comunicaçãoblibica.blogspot.com>. Acesso em: 24 mar. 2013.

MORAIS, T. *Segurança na internet*. Disponível em: <http://www.edecacaotecnologia.org.br>. Acesso em: 25 mar. 2013.

OLIVEIRA JR, J. B. C. de O. A internet e os "novos" crimes virtuais. A fronteira cibernética. *Jus Navigandi*, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/revista/texto/2097>. Acesso em: 24 mar. 2013.

RIBEIRO, L. *As funções e finalidades da internet*, 2012. Disponível em: <http://www.murall.com.br/as-funcoes-e-finalidades-da-internet/>. Acesso em: 3 mar. 2013.

SILVA, J. G. da. *Ética no uso da internet*. Disponível em: <http://www.eticaegestao.ifsc.edu.br/ideias-e-reflexoes/etica-no-uso-da-inter net/>. Acesso em: 15 mar. 2013.

SOUZA, R. M. de. *Segurança da informação*. Disponível em: <http://www.segurança-informação-ranieri.blogspot.com>. Acesso em: 20 mar. 2013.

VILLA, A. *Dez dicas de segurança na internet*. Disponível em: <http://www.contasemrevista.com.br/samba/10-dicas-de-seguranca-na-internet.html>. Acesso em: 20 mar. 2013.

VILLARES, G. D. *Ética na internet ou internet com ética?* Disponível em: <http://www.agricultura.gov.br/arq_editorEtica/etica_na_Intern-et.pdf>. Acesso em: 15 mar. 2013.