

PROJETO DE REDES
www.projetoderedes.com.br

GERALDO MAJELA VILELA

O USO DO TERMO HACKER NAS NOTÍCIAS
VEICULADAS PELA INTERNET BRASILEIRA

LAVRAS
MINAS GERAIS — BRASIL
2006

GERALDO MAJELA VILELA

O USO DO TERMO HACKER NAS NOTÍCIAS
VEICULADAS PELA INTERNET BRASILEIRA

Monografia de Pós-Graduação “Lato Sensu”
apresentada ao Departamento de Ciência da
computação para obtenção do título de Espe-
cialista em “Administração em Redes Linux”

Orientadora:
Professora Msc. Kátia Cilene Amaral Uchôa

Co-Orientador:
Professor Msc. Joaquim Quinteiro Uchôa

LAVRAS
MINAS GERAIS — BRASIL
2006

GERALDO MAJELA VILELA

O USO DO TERMO HACKER NAS NOTÍCIAS
VEICULADAS PELA INTERNET BRASILEIRA

Monografia de Pós-Graduação “Lato Sensu”
apresentada ao Departamento de Ciência da
computação para obtenção do título de Espe-
cialista em “Administração em Redes Linux”

Aprovada em 29 de Setembro de 2006.

Professor Dsc. Heitor Augustus Xavier Costa

Professor Msc. Joaquim Quinteiro Uchôa

Professora Msc. Kátia Cilene Amaral Uchôa
(Orientadora)

LAVRAS
MINAS GERAIS — BRASIL
2006

Agradecimentos

Agradeço primeiramente à Deus, pois sem Ele eu não existiria, em seguida à meus pais João Vilela e Maria Araújo e irmãos Ronaldo, Fátima, Elizabeth, Gilmar e Elaine, que são alicerces que sempre posso me apoiar. Agradeço também a minha noiva Rosamaria Maia, pelas várias horas de apoio e compreensão durante a elaboração deste trabalho e para finalizar agradeço a todos os meus Mestres do passado e presente pela cooperação, colaboração e socialização dos seus conhecimentos. Um agradecimento especial para minha orientadora Kátia, pela paciência e apoio constante.

Dedicatória

Dedico este trabalho especialmente à minha mãe que me criou e educou nos mais elevados princípios éticos, morais e religiosos, mesmo diante de enormes dificuldades sociais e financeiras.

SUMÁRIO

LISTA DE SIGLAS.....	7
RESUMO.....	8
1 INTRODUÇÃO.....	9
2 CONTEXTUALIZANDO OS “HACKERS”.....	13
2.1 Conceitos básicos	13
2.2 A Evolução histórica e tecnológica dos “hackers”	22
2.2.1 As gerações de “hackers”	24
2.3 A Ética dos “hackers”	28
3 SOCIEDADE DA INFORMAÇÃO.....	36
3.1 Formação da opinião pública e a influência da mídia...	36
3.2 A Utilização indevida do termo “hacker”	39
4 AS REPORTAGENS SOBRE OS “HACKERS”	44
4.1 As matérias selecionadas	45
5 CONSIDERAÇÕES FINAIS.....	60
REFERÊNCIAS BIBLIOGRÁFICAS.....	62

LISTA DE SIGLAS

BBS – Bulletin Board System

FIP – Faculdade de Informática de Passos

UEMG – Universidade Estadual de Minas Gerais

MIT – Massachusetts Institute of Technology

SL – Software livre

IBM – International Business Machines

RESUMO

Este trabalho apresenta de forma concisa como é a utilização do termo “*hacker*” na internet. Busca primeiramente mostrar os diversos conceitos atribuídos ao tema, na ótica de vários autores que discutem o assunto. Assim, esbarra-se no confronto conceitual dos termos, que na sua maioria, denigre a imagem dos “*hackers*”. Mostra-se que os “*hackers*” não são piratas digitais como citado nas variadas reportagens da internet que foram analisadas. Para tanto, mostrou-se também a história dos “*hackers*” e o processo de evolução tecnológica que teve muita contribuição positiva dos mesmos. “*crackers*” quem são os piratas digitais. É necessário um melhor entendimento do tema e o respeito à ética dos “*hackers*” para que essa imagem negativa vá desaparecendo. A internet tem o poder de influenciar a formação de opiniões e por isso suas mensagens, ou seja, as informações repassadas através dela, devem ter em sua base o fator da veracidade e de conceituação real. Mas é necessário que a mídia, principal responsável por esta imagem, deixa de repassar apenas o lado negativo e informe também o lado de contribuição desta comunidade.

1 INTRODUÇÃO

A evolução da informática e, conseqüentemente, o desenvolvimento da internet representa hoje para a sociedade um caminho progressivo na busca de informações e no coroamento de um processo de informatização que facilitou o acesso às diversas pesquisas de todos os níveis da sociedade. Na atualidade, o desenvolvimento nas várias áreas de conhecimento está atrelado ao mundo digital, de forma que fica difícil pensar em desenvolvimento sem pensar em informática. É possível afirmar que, de certa forma, a internet facilita a vida das pessoas, possibilitando acessos rápidos a diferentes dados informacionais.

Diante desta disseminação da informação para saber da evolução de uma lei, um cidadão não precisa contatar um profissional em Direito, basta ligar o computador e acessar a internet. Também não é mais preciso esperar meses para ter em mãos uma Legislação que acabou de ser promulgada, uma vez que pode ser obtida em *sites* oficiais antes mesmo de sua publicação. Ainda é possível encontrar, em muitas *homepages*, artigos de autores respeitados sobre temas atualíssimos, muito antes de serem publicados em revistas, ou outros veículos de comunicação.

Testemunha-se o avanço da internet que está fornecendo, a qualquer pessoa que esteja conectada a ela, acesso a informações provindas de várias partes do mundo, podendo acessar ofertas de emprego, divulgação de serviços a domicílio, curiosidades sobre seu ídolo, reportagens de jornal sobre o assunto de sua preferência e novas descobertas da ciência e tecnologia.

Nesta época de crescente desenvolvimento e de tantas esperanças na cibernética¹, inclusive quando posta a serviço da sociedade, questiona-se a utilização do termo “*hacker*” veiculada na internet. Atualmente, não é difícil encontrar esse termo sendo utilizado na mídia como sinônimo de vandalismo. Por isto, essa reflexão põe-se de modo concreto pelo interesse ao tema e como relator colocam-se apenas os resultados das próprias investigações. É importante dizer que refletir sobre os resultados da própria investigação é sempre tarefa primordial, sempre refletindo e não somente descrevendo, consegue-se agrupar uma modesta teoria sobre o tema ora proposto.

O caminho percorrido ao longo deste trabalho, o contato com diferentes conceitos e idéias, a preocupação com o alcance do objetivo proposto e o desejo de fazer desta pesquisa um apoio para um futuro estudo mais aprofundado, foram alguns dos motivos que contribuíram para que eu persistisse nesse tema de pesquisa. Espera-se que esse trabalho possa resgatar e trazer à tona a discussão do verdadeiro significado do termo “*hacker*”, tanto para as pessoas técnicas quanto para as não técnicas e que fomente também, uma discriminação desse termo, a qual mais aproxime de seu real significado.

Assim, o objetivo geral desta pesquisa consiste em analisar e verificar a utilização do termo “*hacker*” pela internet, verificando a adequação dos vários conceitos atribuídos, e se estes estão de acordo com a definição tida como adequada pelos teóricos que discutem o assunto.

Os objetivos específicos buscam descrever a evolução histórica e tecnológica dos “*hackers*”; relatar a ética destes; descrever como a internet

¹ Em uma visão geral, Cibernética é uma teoria dos sistemas de controle da comunicação interna e externa do sistema e da sua função no ambiente. Conforme Ferreira (2002), é a ciência que estuda as comunicações e o sistema de controle nos organismos vivos e também nas máquinas.

interfere na formação da opinião pública; e realizar uma análise crítica sobre o uso conceitual do termo “*hacker*” nas reportagens lançadas pela internet.

Para atender os interesses desde estudo, realizou-se uma pesquisa bibliográfica e exploratória, tendo como fonte de coleta de dados: livros de autores da área, artigos científicos, teses de mestrado, monografias e *sites* da internet que foram pesquisados na biblioteca da Faculdade de Informática de Passos (FIP) no campus da Universidade Estadual de Minas Gerais (UEMG). Dentre os principais autores que discutem sobre os “*hackers*”, podem ser citados: Levy (1994), Cebrian (1998), Raymond (1999), Hell (2000), Himanen (2001) e Medeiros (2002). Foram selecionadas várias reportagens da internet que abordam a atuação dos “*hackers*” no ciberespaço¹, verificando como esse termo é por ela empregada, em suas redações, buscando relacionar os conceitos e as publicações sobre os “*hackers*” e entender a veiculação das notícias na internet, a fim de chegar ao entendimento necessário sobre o tema.

Para tanto, a primeira parte deste trabalho traz uma explanação sobre os conceitos do termo e apresenta-se um pouco da história dos “*hackers*”, uma vez que é necessário conhecer o passado para entender o presente e gerar perspectivas para o futuro. Ainda nesta parte, apresenta-se a ética dos “*hackers*” e seus princípios básicos, além de mostrar as diferenças existentes entre os “*hackers*” e os criminosos virtuais.

Na segunda parte, aborda-se a sociedade da informação e a influência na formação da opinião pública, em uma análise parcial sob o recorte de um dos meios de comunicação atualmente onipresente na sociedade no conhecimento: a

¹ O termo *cyberspace* foi inventado pelo escritor de ficção científica William Gibson no seu monumental *Neuromancer* de 1984. Para Gibson, o ciberespaço é um espaço não físico ou territorial, que se compõe de um conjunto de redes de computadores através das quais as informações (sob suas mais diversas formas) circulam. (MEDEIROS, 2002, p. 17)

internet. Busca analisar como tem sido a formação destas opiniões e as conseqüências da utilização do ciberespaço como veículo de divulgação da informação.

A terceira parte traz uma análise crítica a partir do que foi encontrado nas reportagens pesquisadas, selecionadas e retiradas da internet verificando como a internet aborda o termo “*hacker*”, ora criminosos, ora especialistas na informática.

Por fim, são apresentadas as Considerações Finais desta pesquisa, bem como são apontadas às perspectivas de trabalho futuros.

2 CONTEXTUALIZANDO OS “*HACKERS*”

2.1 Conceitos básicos

A teoria sobre o tema mostra que “*hacker*” é o termo originário do inglês usado para designar pessoas que criam e modificam software e hardware de computadores. Entre programadores, o termo “*hacker*” refere-se a pessoas habilidosas em programação, administração e segurança. Por vezes, a palavra é usada em sua amplitude maior não somente referindo-se a pessoas com habilidade em programação, mas que destacam-se em outras áreas como na eletrônica.

Comumente na mídia e em algumas populações, usa-se o termo “*hacker*” para designar “*crackers*”, ou seja, pessoas que praticam atos ilegais ou sem ética. Conforme Hell (2000), a origem do termo é anterior à era da informática, quando existiam artesãos que usavam como principal ferramenta de trabalho, o machado. De acordo com a história, estes foram os primeiros “*hackers*” e originalmente o termo indicava um especialista em qualquer área. Ao longo do tempo, com a informatização, o termo começou a ser utilizado mais frequentemente para a área de informática, designando especialistas em computação.

A controvérsia sobre o significado do termo encontra-se largamente associado à “*crackers*” que, conforme Couto (2001), em uma primeira análise de conceito, praticam atividades criminosas usando várias técnicas e tecnologias como: invasão de computadores, furto de informações e depredação de *sites*, etc. Porém, essa associação direta é criticada por vários segmentos, mais notavelmente pela comunidade de *software* livre que utiliza o termo para designar seus

principais programadores, bem como os próprios especialistas que não se identificam com a vertente obscura e criminosa.

De acordo com Cebrian (1998), em 1985, o termo “*cracker*” foi utilizado com uma nítida intenção em demonstrar que “*hackers*” e “*crackers*” eram seres diferentes e, assim, deveriam ser reconhecidos. Mas, essa tentativa mostrou-se frustrante diante da dificuldade em diferenciar um do outro.

Segundo Masieiro (2000), a conotação atual da palavra “*hacker*” tem um sentido mais pejorativo. Mas, há outra conotação um pouco mais antiga que também é usada para designar o “*hacker*” como um profissional extremamente talentoso e dedicado, que procura vencer desafios relacionados aos computadores, desenvolver projetos altamente complexos e conhecer os detalhes internos dos computadores e de seu *software* básico.

Conforme Raymond (2001), Medeiros (2002) e Cebrian (1998), os termos “*hackers*” e “*crackers*” surgiram em momentos histórico-sociais diferentes. Na década de 50, estudantes e professores do *Massachusetts Institute of Technology* (MIT) começaram a empregar o termo “*hacker*” para alguém que tinha grande conhecimento na área de informática, tanto para *software* quanto para *hardware*.

Torvalds (2001), descrevendo sobre a importância dos “*hackers*”, mostra que os programadores que trabalham com o *Linux* e outros projetos de código fonte aberto, deixam de lado o sono, a ginástica, os jogos dos filhos e, de vez em quando, o sexo, porque adoram a programação. Eles adoram fazer parte de um esforço colaborativo global.

Para Medeiros (2002), em 1985, o termo “*cracker*” começa a ser usado pelos próprios “*hackers*”, para definir uma nova tribo que começava a tomar conta do ciberespaço. O autor relata que, desde meados da década de 80, tenta-se fazer uma separação entre os termos “*hacker*” e “*cracker*”, mas a dificuldade

imposta pela mídia instaurou barreiras e criou no imaginário do senso comum uma aura de criminalidade sobre os “*hackers*”.

Para Medeiros (2002), a diferença é que no caso dos “*crackers*”, além da existência explícita da intenção de ganho monetário, os “*crackers*” podem buscar um objetivo político-ideológico. Eles também produzem e disseminam programas que podem ser usados em varreduras de rede com o intuito de quebrar sistemas.

Muitos termos foram criados para conceituar estes novos personagens do ciberespaço. Segundo o dicionário *JARGON FILE* (2001), esses personagens (*lammer, wannabe, phreaker, cracker*) se diferenciam dos “*hackers*” pelas formas de atuação de cada um deles. Medeiros (2002) relata que estes termos são quase inexistentes nas manchetes da grande imprensa, mas muito conhecidos pelos habitantes do submundo.

De acordo com Medeiros (2002), os “*crackers*” partem do princípio de que o acesso aos sistemas deve ser ilimitado e total, porém sem danificar os sistemas, uma outra característica da famosa ética “*hacker*”. Medeiros (2002) relata que, neste ponto, os “*crackers*” diferenciam-se dos “*hackers*”, ou seja, entram, observam e não danificam nada.

Isto significa que o acesso deve ser ilimitado e total, se tiver como objetivo final o (auto) conhecimento, com discrição. Mas, não é isso que os “*crackers*” fazem, eles usam o argumento do acesso ilimitado para roubar ou destruir dados. Para os “*hackers*”, este tipo de atitude só é válido por ideologia e não por ganho monetário. Mesmo praticada por ideologia, esta atitude pode ser considerada como criminosa perante o Estado.

Masieiro (2000) considera como os crimes mais comuns dos “*crackers*” os casos em que envolvem bancos e instituições financeiras. Também é típico o roubo e o uso de cartões magnéticos para acessar caixas

automáticos, clonagem de cartões de crédito para compra em nome de outra pessoa, além da clonagem de telefones celulares.

Ainda, conforme Medeiros (2002), alguns usuários da internet, que também intitulam-se “*hackers*”, promovem invasões de sistemas computacionais, disseminação de vírus por computador e gostam de divulgar seus codinomes, observa-se que esses codinomes em si são poucos divulgados nos noticiários *online*, os quais enfatizam os termos “*hackers*” ou “*crackers*”.

Para Dom (2003), “*hacker*” é uma palavra inglesa que não possui uma tradução exata para a língua portuguesa. A tradução mais próxima seria “fuçador” ou aquele que aprende “fuçando”. Com certeza, um sentido bem próximo da palavra autodidata, mas não é exatamente isso, pois é bem mais longe do que o autodidata, uma vez que ele tem por curiosidade descobrir como mexer em tudo, buscando primeiramente o conhecimento das falhas de sistemas, depois como usar estas falhas para burlar proteções e, depois, como concertar estas falhas.

No mundo real, qualquer um pode ser considerado “*hackers*” em alguma coisa: como aqueles que resolvem problemas por conta própria, através da compreensão de sua origem, após a leitura de literaturas, após várias tentativas e erros. Tentativa e erro é uma forma demorada para se resolver problemas, mas com certeza é um dos caminhos que pode levar alguém a compreender processos ocultos que seriam desconhecidos ou não seriam ensinados em livros, nem por outras pessoas.

Partindo dessa definição, percebe-se que os “*hackers*”, não são os bandidos. Para Dom (2003), a maioria das ações dos “*hackers*” é moralmente errada e, às vezes, ilegal. Mas, para este autor, moral e justiça são coisas relativas, ainda mais que a coisa justa e a coisa legal nem sempre são compatíveis. Se não fossem os “*hackers*”, hoje as pessoas não estariam fazendo

compras seguras pela internet, pois, as empresas de comércio eletrônico não teriam o grau de automação tecnológica que possuem hoje, devido as contribuições diretas ou indiretas dos “*hackers*”, para segurança da grande rede.

Conforme Dom (2003), a pessoa que utiliza as falhas de sistemas para provocar prejuízos e ganhar dinheiro é conhecida por “*cracker*”. O “*cracker*” é realmente um criminoso no sentido mais puro da palavra. Algumas literaturas os classificam como terroristas digitais, pois ele usa o conhecimento adquirido para prejudicar pessoas ou empresas e ainda se sair bem na história. São as ações dessas pessoas que distorceram o conceito do “*hacker*”. Isto vem provocando uma verdadeira guerra digital que esta acontecendo neste exato momento no lugar denominado submundo eletrônico.

“*Hacker*” são contratados por empresas para proteger seus sistemas contra o ataque de “*crackers*”. Esta talvez seja a melhor forma de diferenciar os dois tipos. Conforme Dom (2003), os “*crackers*” são classificados de acordo com suas especialidades podendo ser destacados:

- *WAREZ*: São piratas, “*crackers*” que quebram a proteção de programas, como os que rodam somente com o CD original, os distribuídos com tempo de avaliação, e também distribuem pequenos programas, chamados “*crackers*”, que quando executados geram senhas de programas ou modificam arquivos do sistema para fazer com que um determinado *software* instalado como demonstração, passe a funcionar por completo;
- *PHREAKER*: Estes possuem ótimos conhecimentos de telefonia. Eles conseguem invadir centrais telefônicas, o que lhes permite, entre outras coisas, efetuar ligações internacionais sem pagar, fazendo ataques a partir de servidores situados em outros países. Geralmente, um *phreaker* é um ex-

funcionário de companhias, que usa exclusivamente seus conhecimentos para prejudicar as empresas de telefonia.

Dom (2003) explica que para se tornar um “*cracker*” é necessário ter sido um “*hacker*”. A linha que separa ambos termos é muito tênue, além disso o “*cracker*” contribui para a má fama dos “*hackers*”, pois um “*cracker*”, conhecido por ser um ótimo “*hacker*”, pode ser preso por causar algum dano a alguém. Dessa forma, a imprensa publicará que o “*hacker*” é criminoso.

A partir dessa linha tênue que separa um “*hacker*” de um “*cracker*” e vice-versa, aliada a falta de informação e o marketing feito pela imprensa, formam elementos que contribuem para a perpétua disseminação desse termo.

Dom (2003) afirma que “*crackers*” causam danos, têm-se também os *lamers*, que, conforme este autor, causa muito pânico e quase nenhum dano e quem geralmente fica com a fama de mal são os “*hackers*”.

Quase todos os novatos em computação precisaram da ajuda de um “*hacker*”. Aquele disquete que um amigo recuperou e que você dava como perdido; um amigo que instalou e configurou aquele programinha para proteção contra ataques mal intencionados pela internet e o ensinou a usar; aquele amigo que burlou o seu computador para que ele rodasse aquele jogo que só funcionaria com mais memória RAM do que seu computador realmente possuía e etc. Pode-se dizer que mesmo essas ações mais simples de um “*hackers*”, estão relacionadas a atitudes amigáveis dispostas a ajudar e ensinar, sem se gabar do que fazem.

Summitt (2005), ao explicar o termo “*hacker*” utiliza várias definições. De acordo com esse autor, os “*crackers*” que constituem aqueles que invadem computadores, através da quebra de códigos. Os que fazem alterações em *sites* são os *Defacers* e quem cria vírus são os *Virii-Makers*. Para ele, os “*hackers*”

sabem que conhecimento é poder e afirma: "Quem rouba informações ou dinheiro não é *“hacker”*, é ladrão".

Para Paschoal (2004), a imagem produzida no senso-comum para a figura do *“hacker”* é construída nos caminhos das conexões via internet. Apesar dessa visão se encontrar distante da realidade, a definição mais forte do termo surge do efeito que essas atividades podem gerar. O conhecimento das ferramentas que acionam e regem sistemas e programas podem ser usados para democratizar informações, o que é feito pelos *“hackers”* ou para atos criminosos, o que é feito pelos *“crackers”*.

Permanecem as constantes tentativas de classificar os *“hackers”* como pessoas que promovem a liberdade de expressão e de informações e esclarecer que os *“crackers”* é que são causadores de prejuízo. Mas, essa classificação também gera uma confusão de sentidos. A palavra *“cracker”* vem do verbo em inglês *to crack*, que significa quebrar códigos de segurança. Nesse sentido, para promover a livre informação, é preciso *“crackear”*, o que pode levar a entender que o legítimo *“hacker”* é também um *“cracker”*.

É importante entender que os *“hackers”*, em geral, partem do princípio de que os sistemas de segurança têm alguma falha e a função deles é encontrar essa porta, verificar os problemas e as possíveis soluções.

De acordo com Stallman (1999), a história mostra que os primeiros *“hackers”* passaram a utilizar o verbo *hack* para definir não somente as pessoas ligadas a informática, mas os especialistas em diversas áreas. É importante lembrar que existe uma cultura por trás desse sentido da palavra *“hacker”*. A Cultura *“hacker”* define diversos pontos para estilo e atitude e, por mais que pareça estranho, muitas das pessoas que se tornam os chamados programadores extraordinários possuem esse estilo e atitude naturalmente. Estas características serão tratadas no item 2.3 (A ética *“hacker”*)

A título de conhecimento, é importante mostrar que outros termos são utilizados para diferenciar os tipos de “*hacker*” e “*cracker*”. Conforme Dom (2003), assim estão expostos:

- ✓ *White hat* – (aka “*hacker*” ético) “*hacker*” em segurança, utiliza os seus conhecimentos na exploração e detecção de erros de concepção, dentro da lei. A atitude típica de um *White hat* é, ao encontrar falhas de segurança, entrar em contato com os responsáveis pelo sistema, comunicando o fato. Geralmente, “*hackers*” de chapéu branco violam seus próprios sistemas ou sistemas de um cliente que o empregou especificamente para auditar a segurança. Pesquisadores acadêmicos e consultores profissionais de segurança são dois exemplos de “*hackers*” de chapéu branco;
- ✓ *Gray hat* – Tem as habilidades e as intenções de um “*hacker*” de chapéu branco na maioria dos casos, mas por vezes utiliza seu conhecimento para propósitos menos nobres. Um “*hacker*” de chapéu cinza pode ser descrito como um “*hacker*” de chapéu branco que às vezes veste um chapéu preto para cumprir sua própria agenda. “*hackers*” de chapéu cinza tipicamente enquadram-se em outro tipo de ética, que diz ser aceitável penetrar em sistemas desde que o “*hacker*” não cometa roubo, vandalismo ou infrinja a confidencialidade. Porém, algumas pessoas argumentam que o ato de penetrar em um sistema por si é antiético;
- ✓ *Black hat* – (aka *cracker* ou *dark-side hacker*) criminoso ou malicioso “*hacker*”, um “*cracker*”. Em geral, “*crackers*” são menos focados em programação e no lado acadêmico de violar sistemas. Eles comumente confiam em programas de “*cracking*” e exploram vulnerabilidades

conhecidas em sistemas para descobrir informações importantes para ganho pessoal ou para danificar a rede ou sistema alvo;

- ✓ *Script kiddie* – Indivíduo que não tem domínio dos conhecimentos de programação, pouco experiente, com poucas noções de informática. Porém, tenta fazer-se passar por um “*cracker*” a fim de obter fama, o que acaba gerando antipatia por parte dos “*hackers*” verdadeiros, cerca de 95% dos ataques virtuais são praticados por *script kiddies*;
- ✓ *Lamer* – Uma pessoa inepta ou ineficaz. Também é empregado para designar uma pessoa que não possui conhecimentos técnicos sobre computadores, porém, faz-se passar por um especialista;
- ✓ *Newbie* – É aquele jovem aprendiz de “*hacker*” que possui uma sede de conhecimento incrível, pergunta muito e é ignorado e ridicularizado na maioria das vezes. Ao contrário do *Lamer*, não tenta se por acima dos outros, geralmente é muito simples e possui uma personalidade ainda fraca;
- ✓ *Phreaker* – “*hacker*” especialista em telefonia móvel ou fixa.

Uma coisa é certa: os “*hackers*” e “*crackers*” são indivíduos da sociedade moderna e possuem conhecimentos avançados na área tecnológica e de informática. Porém, a diferença básica entre ambos é que os “*hackers*” geralmente constroem coisas para seu aprendizado e bem comum e os “*crackers*” visam alcançar objetivos financeiros e pessoais, muitas vezes destruindo sistemas para alcançar tais objetivos. A defesa de que os “*hackers*” são voltados para o bem se faz a partir da análise da ética destes, exposta mais adiante, no item 2.3.

2.2 A Evolução histórica e tecnológica dos “hackers”

A atualidade tem sido marcada por grandes transformações. No plano tecnológico, a partir da década de 70, observou-se o surgimento de novas tecnologias com base na micro-eletrônica resultantes da convergência das telecomunicações e a informática. Conforme Lemos (2003), a internet, uma das principais tecnologias resultantes dessa convergência, através de seus diversos serviços (correio eletrônico, bate-papo *online*, *web*, listas de discussão, *newsgroup* etc.), possibilitou à sociedade uma conexão generalizada em âmbito global e uma nova configuração comunicacional.

Para Souza (2004), o desenvolvimento gradativo destas novas tecnologias e sua constante impregnação nos diversos setores da sociedade resultou no que se chama hoje de Sociedade da Informação ou Informacional. Concomitante a estas inovações tecnológicas presencia-se a transição de um mundo moderno, marcado pela racionalização, individualismo e pragmatismo, para uma outra realidade, a pós-modernidade, com novas formas de sociabilidade.

Da relação simbiótica entre esta sociedade informacional e pós-moderna, emerge uma cultura subjacente às TICs (Tecnologias de Informação e Comunicação) com sua nova forma sócio-cultural denominada: Cibercultura (Lemos (2003); Uchôa (2003), Levy (1999); Piscitelli (1995)).

Neste sentido, da mesma forma que o desenvolvimento técnico tornou possível o surgimento de novas formas de sociabilidade, a cultura construída a partir do uso destas mesmas tecnologias começa a influenciar a forma como o próprio desenvolvimento tecnológico tem acontecido. Inseridos neste contexto de evolução encontram-se os “hackers”.

Conforme Medeiros (2002), nos anos 60, o termo “*hacker*” era usado para designar as pessoas que se interessavam em programar computadores. A utilização relacionada com a informática surgiu nesta época entre os estudantes do MIT (*Massachusetts Institute of Technology*), que a usavam para designar sucessos em determinadas áreas, fosse com uma solução não particularmente elegante para um problema, uma partida inteligente pregada a alguém, ou ligar os sistemas informáticos e telefônicos para fazer chamadas grátis.

Segundo Lemos (2001), os “*hackers*” cumpriram papel fundamental nas principais transformações tecnológicas e sociais da sociedade contemporânea. Eventualmente, o termo passou a ser utilizado exclusivamente nas áreas de programação ou eletrônica, em que passou a ser usado para designar indivíduos que demonstravam capacidades excepcionais nestes campos, efetivamente expandindo-os com atividades práticas.

No entanto, na década de 80, o termo “*hacker*” foi popularizado através dos meios de comunicação de massa para denominar os “piratas das redes de computadores”. Isto levou a uma percepção social dos “*hackers*” como intrusos maliciosos e perversos, ao invés de exploradores do ciberespaço (Lemos, 2002). Em virtude deste fato, atualmente, “*hacker*” é um termo repleto de controvérsias, sendo utilizado para se referir tanto aos criminosos digitais, na verdade, “*crackers*”, quanto aos ciberativistas da liberdade da informação e desenvolvedores de *Software Livre* (SL).

Fora do contexto especializado, o termo encontra-se geralmente associado à prática de atividades maliciosas e criminosas, como invasão de computadores, furto de informações e depredação de *sites*, entre outros. Essa associação é frequentemente criticada por várias comunidades (notavelmente pelos grupos produtores de SL), que usam o termo para distinguir os seus principais programadores, não estando estes ligados a atividades ilícitas.

Diante dos autores estudados, é possível verificar que não há apenas um entendimento histórico do termo “*hacker*”. Medeiros (2002) apresenta em sua obra o entendimento do termo “*hacker*”, a partir das três gerações expostas por Levy (1994A). Levy descreve o que ele chama de três gerações de “*hackers*” utilizando uma separação temporal (décadas de 50, 70 e 80) e objetivos apresentados pelos “*hackers*”, em cada uma delas. Enquanto Medeiros (2002) relata o surgimento da quarta geração de “*hackers*”, na década de 90, caracterizando-os também quanto aos seus objetivos.

2.2.1 As gerações de “*hackers*”

A primeira geração nasceu no MIT e foi responsável pelo aprimoramento dos programas de computadores. Foi neste momento que nasceu a ética “*hacker*”, formada por seis princípios, que são detalhados na seção 2.3 - A ética “*hacker*”.

De acordo com Levy (1994), exposta por Medeiros (2002), a segunda geração de “*hackers*” apareceu na década de 70, influenciada pela geração da contracultura e lutando pela democratização da informática, enquanto criticavam a *International Business Machines* (IBM).

Os “*hackers*” da segunda geração lançaram idéias sociais e deram início a um movimento pela popularização dos computadores. É nesse momento que a defesa do acesso irrestrito aos sistemas informatizados ganha força.

A luta desses guerreiros era pelo acesso massificado à informática. Eles chegaram a criar um projeto chamado *Memória Comunitária*, planejada para ser uma rede de pequenos terminais de computadores distribuídos pela área da baía

de São Francisco em USA. Um outro projeto, criado antes do *Memória Comunitária*, se chamava *Recurso Um*, que tinha como objetivo oferecer o acesso ao computador sem custo para o usuário, e contou com a contribuição de várias corporações e fundações. Medeiros (2002) afirma que este foi o início da luta dos “*hackers*” nos anos 70.

“A linhagem dos “*Hackers*”, que se reuniram em lugares como Homebrew, tinha andado às margens do mundo *hight tech* por alguns anos. Muitos deles eram pessoas que abandonaram a universidade e veteranos de uma política recente de contracultura da baía de São Francisco. Segundo um participante observador, o estilo ‘tinha o código genético dos anos 60, com atitudes contra-institucionais, contra-guerra, pro-liberdade e antidisciplina’.” (Roszak, p. 215, in: Medeiros, 2002, p. 32).

Para Roszak (2001), os “*hackers*” da segunda geração eram envolvidos por um forte espírito comunitário. Estes “*hackers*” criaram o computador pessoal e a possibilidade para a democratização do acesso à informação. Na década de 70, um fato relevante que impulsionou a criação do *Homebrew* foi o lançamento de um *kit* para a montagem de um microcomputador.

A terceira geração de “*hackers*”, segundo Levy (1994), é formada pelos responsáveis pelo desenvolvimento dos jogos de computador. Os primeiros games nasceram com a famosa primeira geração do MIT (o jogo de xadrez e o famoso *spacewar*, o primeiro jogo desenvolvido para o computador PDP – 1, da IBM). Mas, foi na década de 80 que os jogos começaram a ganhar um novo impulso com interfaces mais arrojadas e com estratégias mais inteligentes.

Além disso, os jogos passaram a ser *on-line* e eram jogados por várias pessoas através dos famosos *Bulletin Board System* (BBS). Outra característica interessante, verificada por Medeiros (2002), nesta época, era a tentativa de quebrar o sistema fechado de *videogames*, como o Atari 800.

Medeiros (2002) relata que os “*hackers*” da década de 80 levaram aos BBS e às redes abertas a radicalização da proposta inicial desenvolvida pelos “*hackers*” da primeira geração. Os princípios do acesso irrestrito a dados, liberdade da informação e desburocratização uniram-se, agora, em um ambiente de rede e não estavam mais restrito ao *Homebrew* ou ao laboratório do MIT.

Medeiros (2002) ainda esclarece que esta terceira geração também caracteriza-se pela explosão dos BBS, que foi uma nova forma de comunicação entre os “*hackers*”, que viria impulsionar, por exemplo, a criação das primeiras publicações *on-line* do gênero, como a revista *2600: The “hacker” Quarterly*, editada por Emmanuel Goldstein desde 1984. Até hoje essa revista é uma referência no submundo da informática.

Para Rheingold (1996), a década de 80 trouxe também, em larga escala, a profissionalização da indústria de *software* e *hardware*. A informação não era mais vista de uma forma ingênua como na década de 60. Ela começava a fazer parte do cotidiano das sociedades e, sob a ótica capitalista, era uma mercadoria com valor monetário de troca.

Os princípios da ética “*hacker*” não poderiam, nem iriam, ser entendidos como ingênuos diante da nova visão que se tinha da informação binária. As redes, que antes eram restritas, começaram a ganhar *status* econômico e passaram a ser vistas como uma nova forma de estabelecimento da comunicação.

De acordo com Rheingold (1996), o *software*, que antes era uma arma manipulada de forma peculiar e criativa pelas mãos dos clássicos “*hackers*”, transformou-se em um produto protegido por *copyright*, ganhando as prateleiras das lojas.

Esta década de 80 é o ponto chave para o entendimento de como os “*hackers*” (e sua ética clássica) vão transformar-se em vilões e é a partir desta

década, que começa a se configurar o submundo do ciberespaço. Na apresentação e explicação das três gerações expostas por Levy (1999), Medeiros (2002) vai mais além e delinea também a quarta geração. O autor considera que foi diante do surgimento e da explosão das redes telemáticas de forma massiva e comercial, a partir que meados da década de 90, de vários grupos de adolescentes que se inicia esta geração negativa. Estes adolescentes possuíam um pouco de conhecimento de programação ou às vezes nem isso e usavam estes conhecimentos para fazer um tipo de ataque muito conhecido hoje como *defacement*, que consiste em descaracterizar, substituir ou alterar a página de rosto (*home page*) de um *site*. As alterações mais comuns são deixá-la em branco, inserir desenhos e mensagens.

Este autor ainda considera que a unificação dos sistemas informatizados (desenvolvimento da microinformática, da capacidade de transmissão de dados via fibra ótica, do desenvolvimento dos satélites e dos *software*) com os de telecomunicações, faz do computador um meio de comunicação capaz de criar, inclusive, novos papéis sociais e culturais dentro do mundo virtual.

O autor relata que, desde meados da década de 80, tenta-se fazer uma separação entre os termos “*hacker*” e “*cracker*”, mas a dificuldade imposta pela mídia instaurou barreiras e criou no imaginário do senso comum uma aura de criminalidade sobre os “*hackers*”.

2.3 A ética “*hacker*”

Conforme Medeiros (2002), quando o termo "*hacker*" é utilizado hoje em dia, logo liga-se aos cibercriminosos que possuem alto conhecimento sobre os computadores e as redes de comunicações para praticarem delitos, causando danos a terceiros e/ou enriquecendo-se com essa prática. Mas, como foi falado no decorrer deste trabalho, este termo está sendo usado incorretamente. Esta confusão poderia ser evitada se esses cibercriminosos não fossem denominados "*hackers*", mas "*crackers*".

Diversos trabalhos foram desenvolvidos no intuito de compreender, sob vários aspectos, os "*hackers*" e sua ética. Levy (2001A) apresenta de forma sistemática os princípios fundamentais compartilhados pelos primeiros "*hackers*" da década de 60 e 70. Entre tais princípios destacam-se: liberdade da informação, a aversão a hierarquias, o uso da meritocracia e um olhar lúdico sobre o seu ofício (Levy, 2001A).

Desses, a relação lúdica dos "*hackers*" com o seu ofício é abordada de maneira mais ampla pelo filósofo finlandês Pekka Himanen (2001). Segundo o autor, os "*hackers*" compartilham significâncias sobre o trabalho, tempo e dinheiro que definem o que ele denomina de ética "*hacker*". Esta ética dos "*hackers*" no trabalho, contrapõem a ética Protestante.

Para Himanen (2001), a sociedade contemporânea ainda sofre forte influência da ética Protestante. Se na ética Protestante a realização pessoal, o entretenimento e o trabalho estão dissociados, na ética "*hacker*" estas experiências unem-se novamente.

Buscando a separação dos termos, Himanen (2001) explica o que entende por “*hacker*”:

“É uma pessoa que programa entusiasticamente e que acredita que compartilhar informação é um poderoso bem concreto e que seja um dever moral compartilhar a sua perícia escrevendo software livre e facilitando o acesso à informação e a recursos computacionais onde for possível, é alguém que acha programar interessante, empolgante e divertido.”

Ele lembra importantes nomes do “*hackerismo*”, como: *Vinton Cerf*, *Tim Berners-Lee*, *Steve Wozniak* e *Linus Torvalds* destacando-os como responsáveis pela criação dos fundamentos da Sociedade da Informação nos últimos 30 anos. É esse compromisso que os “*hackers*” têm com a informação, é essa paixão pela criatividade que se transformou na ética “*hacker*” e isso tem tudo a ver com a inclusão digital da sociedade.

De acordo com Himanen (2001), a ética “*hacker*” é diferente da antiga ética de trabalho que ainda predomina na sociedade, que Max Weber chamou de “ética de Trabalho Protestante”, durante a Era Industrial. Neste tipo de pensamento, o trabalho é a coisa mais importante para o homem, é o que há de mais essencial em sua vida. Explica Himanen que é daí que vem à ascensão do capitalismo.

Diferentemente, a ética “*hacker*” propaga a idéia de paixão e prazer pelo trabalho. O dinheiro, para ele, não é visto como algo essencial, mas Himanen (2001) afirma: “a ética “*hacker*” começa a ser apelativa para o mundo dos negócios. É uma vantagem competitiva, pois fomenta a criatividade, a inovação e perspectiva de longo prazo.”

A análise de Himanen (2001) vai ao encontro das idéias que defende Medeiros (2002), pois afirma que os “*hackers*” possuem uma forma

diferenciada de encarar o trabalho e o dinheiro. Diante do trabalho, posicionam-se com “paixão e liberdade”. Sobre o dinheiro, ele escreve:

“Eles não vêem o dinheiro com um valor em si mesmo, mas como motivação para que possam estabelecer metas de valor social e franqueza” (Himanen, 2001, p.140). Isso significa dizer que os “*hackers*” procuram desenvolver trabalhos que visam o bem comum da sociedade. No caso específico da atual sociedade da informação, eles seriam uma espécie de herói, que lutam contra o monopólio da indústria do *software* e a perda da privacidade.

De acordo com Himanen (2001), a ética “*hacker*”, que deve ser entendida abrangendo as áreas de atividade humana e não apenas a Computação, é uma nova ética de trabalho que questiona a ética protestante e propõe um espírito alternativo para a sociedade em rede. Embora seja mais próxima da ética de trabalho pré-protestante, ela não concebe este como sendo um castigo e não descreve o paraíso como sendo um lugar onde não se faz coisa alguma. Na visão do “*hacker*”, o sentido da vida está em dedicar-se a uma paixão. Esta paixão é, na realidade, uma atividade significativa, inspiradora e prazerosa para o indivíduo, seja ela rotulada como “trabalho” ou como “diversão”.

No entanto, a sua realização nem sempre é apenas prazer e alegria, podendo envolver aspectos menos interessantes e apaixonantes e muito trabalho duro e tedioso. Ainda assim, o “*hacker*” está disposto a realizar este esforço em prol de algo que considera maior. A significação do todo faz valer a pena qualquer esforço despendido na execução de suas partes menos atraentes. Além disso, é bem diferente ter de fazer partes menos prazerosas ao realizar uma paixão do que ter de se sujeitar permanentemente a um trabalho desagradável.

Um outro aspecto da ética “*hacker*” é uma visão fortemente diferente do dinheiro com relação à vigente na sociedade capitalista, na qual este é o maior e mais valorizado bem. Para o “*hacker*”, o dinheiro é uma questão secundária.

Não é um objetivo de vida nem a razão do seu trabalho. Por fim, não é o propósito de uma ação.

A motivação social é um fator importante nesta nova ética. Como foi dito, a realização da paixão “*hacker*” está intimamente ligada com alguma espécie de colaboração na construção de um bem maior para a sociedade.

“Talvez esteja no “*hacker*” o melhor exemplo do lado positivo da globalização, entendendo-se “*hackerismo*” como um grupo de indivíduos realizando suas paixões juntos e fora das estruturas de corporações ou governos. Não importa a nacionalidade, cor, raça das outras pessoas. O que importa é que elas estão juntas, provavelmente por meio da internet, para fazer coisas que acham interessantes e construtivas.” HIMANEN (2001)

Todo “*hacker*” tem um código de ética, são regras que seguem quando está invadindo um *site*. As ações de um verdadeiro “*hacker*” são muito diferentes das ações de criminosos. Estas pessoas sujam o nome dos verdadeiros “*hackers*”. Elas são pura e simplesmente criminosas.

Para a ética “*hacker*”, piratear software é roubo. Qualquer pessoa pode piratear um software comercial e igualmente poderia conseguir alguns vírus e rodar no seu próprio computador. Isso não requer nenhuma habilidade ou inteligência. O verdadeiro “*hacker*” preza pelo seu código ético, respeitando os computadores que ele invade.

Além disso, o verdadeiro “*hacker*” não se envolve em brigas insignificantes e estúpidas que se vê na rede do tipo "você destruiu minha página da *web* então eu vou destruir a sua". Aqui, estão algumas regras do código de ética:

“Nunca apague intencionalmente ou danifique um arquivo em um computador que você tenha invadido. Trate os sistemas que você invade como você trataria seu próprio computador. Notifique os administradores de sistemas sobre qualquer brecha de segurança que você encontrar. Não invada para roubar dinheiro. Não invada para roubar informações. Não distribua ou coleccione software pirateado. Nunca corra riscos estúpidos - tenha consciência da sua habilidade. Sempre esteja disposto a compartilhar e repassar seu conhecimento e os métodos que utiliza. Respeite quem está aprendendo (seja humilde)”. ANASTACIO (2002)

Pode-se também falar sobre uma ética “*hacker*” a partir dos seus princípios clássicos propostos ainda pela primeira geração que ficou conhecida pela criação e aprimoramento dos primeiros *software*. De acordo com Levy (1994, p. 39-49), foram os primeiros “*hackers*”, vindos dos laboratórios do MIT, os criadores de um código de ética que define seis princípios:

- ✓ O acesso a computadores – ou a qualquer coisa que possa lhe ensinar algo sobre o funcionamento do mundo – deve ser ilimitado e total;
- ✓ Toda informação deve ser livre;
- ✓ Desconfie de toda autoridade. Promova a descentralização;
- ✓ “*hackers*” devem ser julgados pela qualidade de suas realizações, e não por critérios falsos como escolaridade, idade, raça ou posição social;
- ✓ É possível criar arte e beleza em um computador;
- ✓ Computadores podem mudar a sua vida para melhor.

Estes princípios, como relatam Levy (1994), surgiram inspirados na convivência dos estudantes com o que pode ser chamado de ‘o primeiro computador pessoal do mundo’, o TX-O (ou simplesmente Tixo), como ficou mais conhecido entre eles. Tixo transformou-se em um ícone de liberdade para aqueles estudantes do MIT.

Conforme Masieiro (2000), além dos princípios estabelecidos na ética “*hacker*”, estes também se inspiram através de motivações, como:

- ✓ Proeza: jovens fascinados por computação que procuram emoções fortes no exercício de suas habilidades em computação. Esta parece ser a motivação mais comum, como o de: Robert T. Morris;
- ✓ Proteção: em alguns casos a motivação parece ter sido a de descobrir falhas nos sistemas, procurando melhor entendê-los e melhorá-los posteriormente. Muitos desses “*hackers*” habilidosos têm sido contratados nas áreas de segurança de grandes empresas;
- ✓ Punição: vírus são escondidos em programas com o propósito de punir os compradores de *software* piratas;
- ✓ Espreita: muitos ataques parecem estar relacionados com um certo tipo de “voyerismo” eletrônico, isto é, pessoas que apenas querem entrar em um computador para descobrir quais informações existem, sem intenções de usar a informação ou de causar danos;
- ✓ Filosofia/Ideologia: muitos dos “*hackers*” acreditam que a informação é um bem público ao qual o acesso não deve ser proibido, isto é, os sistemas devem ser abertos para acesso e seu conteúdo deve ser compartilhado.

Para Levy (1994), o desejo dos “*hackers*” em usar o computador está relacionado a melhorar a vida das pessoas e, ao mesmo tempo, promover a descentralização da autoridade. Acredita este autor que este princípio ético impulsionou o desenvolvimento da microinformática e, conseqüentemente, do computador pessoal.

“Seguramente, a sociedade poderia se beneficiar se o mundo fosse baseado na ética “*hacker*”. Esta era uma convicção explícita dos “*hackers*”, e eles acabaram por estender o ponto de vista convencional que se tinha dos computadores, do que eles deveriam ou poderiam fazer – conduzindo o mundo a uma nova forma de ver e interagir com os computadores”. (LEVY, 1994, P.46)

Estes princípios éticos desenvolvidos pelos primeiros “*hackers*” da história da informática, como Dutsch, Peter Samson e Alan Kotok vão tornar-se, com o tempo, contrários à proposta econômica imposta pelo capitalismo. É a partir dessa análise que pode-se afirmar, de antemão, que a ética “*hacker*” busca um caminho alternativo para a utilização das tecnologias telemáticas.

Para Raymond (2001), entendida do ponto de vista histórico, essa ética “*hacker*” não chegava a ser uma proposta revolucionária, anti-capitalista. Principalmente, porque na década de 60 os computadores ainda estavam restritos às universidades e alguns órgãos do governo. Mas, a partir do momento que os computadores começam a fazer parte da vida cotidiana, a ética “*hacker*” passa a ser entendida como uma ameaça ao *status quo*. É importante dizer que foram os “*hackers*” que possibilitaram a criação da maioria das tecnologias telemáticas atualmente usadas.

“ “*Hackers*” construíram a internet. “*Hackers*” fizeram do sistema operacional Unix o que ele é hoje. “*Hackers*” mantêm a Usinet. “*Hackers*” fazem a *World Wide Web* funcionar”. (RAYMOND, 2001)

A avaliação de Medeiros (2002), no que se refere a esta ética, não é totalmente favorável a avaliação feita por Raymond (2001). Medeiros afirma que os princípios éticos defendidos pelos primeiros “*hackers*” constituem, hoje, uma forma de resistência ao mundo globalizado. Este mundo inspirado na clássica ética do dinheiro e do trabalho, criado pelo capitalismo monopolista, é cristalizado pelo chamado capitalismo Pós-Industrial.

Os princípios expostos levam a entender que existe certa resistência ao capitalismo globalizado, uma vez que o produto final não é o dinheiro, mas esta

resistência, ou seja, a ética exposta, agora concordando com Raymond (2001), não deixa claro o anti-capitalismo.

A partir do que foi exposto sobre a ética “*hacker*”, é com tranquilidade que se afirma que ser um “*hacker*” é muito mais do que ser invasor de sistemas, é dominar verdadeiramente vários sistemas operacionais e suas técnicas de administração. Não basta apenas saber um pouco de *Windows*, faz-se necessário dominar o maior número possível de métodos de proteção de sistemas, protocolos entre várias outras ferramentas. A ética e os seus princípios mostram que o “*hacker*” vai preservar os dados do sistema invadido e não irá corromper, deletar ou alterar esses dados.

Um “*hacker*” de verdade invade, olha, aprende o máximo possível e deixa tudo intocado, isso significa uma busca de conhecimentos e tentará sempre conseguir ampliar seus conhecimentos. Mas, o que deve ficar claro é o conhecimento adquirido ser utilizado apenas para o benefício da aquisição de mais conhecimento. É a confirmação do princípio de quem usa o trabalho para o bem comum da sociedade.

A próxima parte traz um pouco sobre a sociedade da informação e a influência da mídia para a formação da opinião pública. Busca-se mostrar como a força da mídia vem influenciando no entendimento do que realmente representa os “*hackers*” para a sociedade.

3 SOCIEDADE DA INFORMAÇÃO

3.1 Formação da opinião pública e a influência da mídia

Falar de opinião pública é assunto muito interessante, uma vez que envolve a sociedade como um todo e também os meios de comunicação. Pela profundidade do assunto, tem-se consciência de que não será esgotado, mas indica-se alguns parâmetros para a sua discussão.

Na verdade, o conceito de opinião pública vem transformando-se através dos tempos. Conforme Souza (2004), no século XIX, ocorreu a primeira revolução industrial, surgiu a imprensa e as reivindicações deixaram de representar apenas os interesses de um grupo dominante, abrangendo caráter não só político, mas social e econômico.

O senso comum utiliza o termo opinião pública com naturalidade, mas ao investigador interessa saber o que é opinião pública. A reflexão leva, automaticamente, a lembrar de grupo, de público, de atitude de maioria, de opinião, do indivíduo no grupo, no público.

Conforme Downing (2003), a opinião é um fenômeno social. Ela existe apenas em relação a um grupo, é um dos modos de expressão desse grupo e difunde-se utilizando as redes de comunicação do grupo. Atualmente, um dos meios de comunicação mais utilizados para os grupos difundirem suas idéias tem sido a internet. Para Souza (2004), a opinião tem sua origem nos grupos, mas só assim não se caracteriza a opinião pública, porque esses grupos transformam-se em públicos quando se organizam em torno das controvérsias,

com ou sem contiguidade espacial, discutem, informam-se, refletem, criticam e procuram uma atitude comum.

Conforme Souza (2004), além da classificação dos grupos, os fatores sociais, os psicológicos, a persuasão e os veículos de comunicação massiva interferem na formação e desenvolvimento da opinião pública. O tipo de sociedade ao qual se pertence, a classe social e as várias relações estabelecidas interferem na formação da opinião pública.

“Os fatores psicológicos são os que melhor explicam a formação da opinião pública, pois opinião relaciona-se com o conjunto de crença e ideologia de um indivíduo que tem disposição para expressar-se (caso não se expresse trata-se de uma atitude latente) e a opinião seria um dos modos de expressão dessa disposição, surgindo a propósito de um acontecimento determinado. Sendo essencialmente a expressão e a opinião de natureza comunicativa e interpessoal.” (SOUZA, 2004, p. 28)

No dia a dia, a sociedade é constantemente bombardeada pelos veículos de comunicação massiva que agem sobre nossas opiniões, nossas atitudes, nossas ações. Bombardeiam os lares e influenciam na formação das crenças.

Os veículos de comunicação massiva usam e abusam da propaganda. São veículos onerosos e somente grupos poderosos podem mantê-los e manejá-los. Mas, é importante lembrar que a opinião pública existe, não pode continuar a ser manipulada de maneira abusiva e deseja-se chegar mais próxima da verdade.

Nesse sentido, a internet tem importante papel na formação da opinião pública e, mais uma vez, lembra-se que os grupos de interesse colocam a controvérsia e esforçam-se para obter aliados entre os desinteressados.

Desta forma, o desinteresse e a não informação contribuem para a ação dos grupos de interesse. Esses grupos de interesse, no seu esforço para moldar

opiniões, podem provocar, pela conceituação indevida, o estabelecimento de atitudes e sentimentos. Pode-se dizer que esta é uma explicação para o conceito negativo do termo “*hacker*”. Os receptores de informações, lêem, escutam, mas pelo desinteresse, não questionam e reproduzem a informação da forma como recebeu, sem ponderações.

Acredita-se que a opinião pública deve funcionar como fiscal necessário e, para que isto ocorra, os seres racionais devem tornar-se cada vez mais racionais. Em uma sociedade de massas o interesse privado geralmente sobrepõe-se ao interesse público.

É importante ressaltar a característica de unilateralidade que existe nas relações que envolvem produtores da cultura e informação (meios de comunicação de massa) e o público receptor. Há uma relação de verticalidade. O receptor não tem como escolher o que deseja ver, ouvir ou ler.

Nesse sentido, entende-se o receptor com sendo, apenas, uma vítima, exposto, portanto, a uma situação de imposição de conceitos e ideologia. Quando se pensa desta maneira, percebe-se também o que vem acontecendo com os “*hackers*”. Os meios de comunicação divulgam as informações e os receptores recebem estas sem questionar a sua fonte ou veracidade. Algumas vezes, acreditam que, se estão sendo divulgadas, é porque são confiáveis. Assim, vai se formando as opiniões públicas, a partir de informações, que muitas vezes podem não serem totalmente confiáveis.

Atualmente, se discute a diminuição do poder massificante dos meios de comunicação. Gonçalves (2002) mostra que retrata a criação e consolidação das chamadas redes telemáticas, incluída aí, a internet.

Sabe-se que na internet não há limites para a informação. Milhões de computadores em todo o mundo estão interligados em sintonia propiciando o nascimento de uma sociedade da informação. Neste universo, também há lugar

para o comércio. Uma vez que a internet saiu dos circuitos universitários e hoje atinge um grande público consumidor.

Para Virilio, citado por Medeiros (2002), a consolidação da sociedade da informação traz consigo, não só a possibilidade de melhora do mundo, mas, a institucionalização de um problema. A visão desenvolvida por este autor parte de uma crítica ao uso exagerado da razão instrumental para a possível criação de um monstro, ou como ele mesmo diz, de uma “bomba informática” pronta para explodir conceitos e comportamentos institucionalizados na maioria dos países.

Para a teoria da comunicação, a emergência das redes telemáticas nas décadas de 70 e 80 e a consolidação da internet comercial, na década de 90, é considerada um marco. Foi ainda em meados da década de 80 que a grande imprensa começou a dar espaço de destaque para os “*hackers*”. Neste sentido, diz-se que a mídia de massa como um todo (TV, rádio, jornais e revistas) é uma das principais responsáveis pela deturpação do termo clássico “*hacker*”. Foram os jornalistas que começaram a usar o termo “*hacker*” para designar alguém que usa seus conhecimentos com o intuito criminoso.

3.2 A utilização indevida do termo “*hacker*”

Há aproximadamente vinte anos, o número de usuários de microcomputadores no mundo era pequeno. Os custos elevados à aquisição das máquinas, as complexas formas de ensinamento da tecnologia apropriada, entre outros elementos, tornavam os benefícios inerentes à informática acessíveis a um número bastante limitado de pessoas ao redor do mundo.

Com o passar dos anos, em uma progressão geométrica, de razão elevadíssima, milhares de pessoas passaram a ter acesso aos microcomputadores, que trouxeram muitos benefícios à sociedade, sobretudo com o surgimento e aprimoramento da internet.

Conforme Anastácio (2002), com o crescimento da internet e a consolidação da chamada Sociedade da Informação, muito tem sido dito sobre os "*hackers*". "Piratas da Rede", "meliantes digitais" e outras denominações que variam do ridículo ao romantismo cibernético e contribuem para a criação de uma atmosfera mítica coberta de mistério e, certamente, equívocos em torno destes personagens.

É comum deparar-se na mídia com este termo sendo usado em um sentido bastante pejorativo, conotando indissociável relação com o crime e a ilegalidade. Seja nos filmes de Hollywood ou no jornal cotidiano, os "*hacker*" usam seu profundo conhecimento do funcionamento dos computadores e das redes de comunicações para perpetrarem sofisticados delitos, causando danos a terceiros e/ou enriquecendo em um digitar de teclas.

Colocando o sensacionalismo e a extravagância de lado, isto tudo poderia estar correto exceto pelo fato de que os agentes de atividades desta estirpe não são "*hackers*", mas "*crackers*". A parte anterior mostrou com clareza a evolução dos termos e a diferença de atuação entre estes.

É importante dizer que esta confusão não é apenas um erro de tradução. A origem deste equívoco, como citado, remonta a meados dos anos 80, quando surgiram os primeiros crimes computacionais, e a mídia, não sabendo como designar tais criminosos, aplica o termo de forma um tanto infeliz.

Injustiça esta que se torna ainda mais evidente diante da elucidação das contribuições fundamentais dadas pelos "*hackers*" para o embasamento tecnológico da sociedade emergente. Como destacado por Himanen (2001),

alguns dos símbolos mais conhecidos dos tempos atuais - a internet, o computador pessoal e *software* como o sistema operacional Linux. É de suma importância destacar que esses foram criados primordialmente por alguns entusiásticos indivíduos que começaram a concretizar suas idéias com outros de pensamento semelhante, trabalhando em um ritmo livre.

Rezende (2000) destaca que, por vezes, para amenizar o erro de designação, tais indivíduos são chamados de "*hackers* éticos". No entanto, isto só piora a confusão, pois reforça a idéia de que o "*hacker*" por natureza não é ético. Tal suposição não poderia ser mais difamatória, pois não apenas o "*hacker*" é ético em sua natureza original, mas, como exposto no item 2.3, pode-se falar de toda uma ética "*Hacker*".

Para amenizar os efeitos da confusão feita pela mídia com relação ao termo "*hacker*", Rezende (2000) sugere a cunhagem de uma nova palavra para designar esta comunidade, pois não se tem muito controle sobre a evolução de uma língua (como ele diz, "o uso faz o idioma"). Porém, até o momento, não se percebe a rotulação de outro termo que seja favorável.

A preocupação permanece a mesma, ou seja, amenizar a contaminação que foi infringida ao termo original nas últimas décadas. Na verdade, a melhor solução para esta confusão seria a fortificação da ideologia "*hacker*", tornando-a clara e conhecida por todos, o que a deixaria menos vulnerável a falácias nominais.

É possível que, conforme a sociedade da informação vá seguindo o seu caminho e vão amadurecendo, as próprias necessidades naturais, que inevitavelmente aparecem, encarreguem-se de implantar esta nova ética de trabalho, a qual, espera-se, possa ser ao menos um pouco melhor do que a atual.

É preciso entender que hoje, os mercenários digitais são classificados como “*crackers*”, que utilizam o conhecimento adquirido para a invasão ilícita de sistemas e o roubo de informações confidenciais.

O mais terrível é a sua inevitável comparação com os “*hackers*”, ou pior a triste ilusão de que os ditos “*crackers*” ajudam administradores de sistemas a taparem seus furos na segurança em suas redes. É um engano pois esses fazem justamente o contrário, quando invadem um sistema estão invadindo com o propósito de roubar e destruir informações vitais em um sistema.

Conforme Medeiros (2002), quando o termo “*cracker*” foi usado pela primeira vez, em 1985, havia uma nítida intenção em demonstrar que “*crackers*” eram seres diferentes e, assim, deveriam ser reconhecidos. Mas, essa tentativa mostrou-se frustrante diante da dificuldade em diferenciar um do outro e, também, da decisiva atuação da grande imprensa. Hoje, o termo está relacionado somente a atitudes negativas, se esquece da importância dos “*hackers*” para o desenvolvimento da sociedade.

É importante ressaltar que, mesmo com o desenvolvimento das redes abertas e do novo conceito de ciberespaço, a grande imprensa (ou a mídia de massa) continua a ter um grande poder de influência sobre a formação da opinião pública. Principalmente, porque essa grande imprensa ainda é a maior responsável pela instauração de comportamentos éticos e morais dentro das principais sociedades capitalistas.

Para o analista de segurança, Tiago Zaninoti, a mídia tem culpa pelo uso abusivo do termo “*hacker*”. Em entrevista apresentada na obra de Medeiros (2002), Zaninoti afirma que houve uma falta de cultura. A mídia percebeu que havia um nicho a ser divulgado, que era a internet e sua segurança.. Foi o caso do *Kevin Mitnick*, que chamou a atenção da imprensa. A imprensa se preocupou em seguir as classificações da época que diziam o seguinte: “o Mitinick é um

hacker". Porque ele era um "*hacker*" no sentido do conhecimento, mas ele era um "*cracker*" no sentido de usar seus conhecimentos para praticar atos ilícitos.

Pode-se afirmar que, na verdade, os chamados Meios de comunicação de Massa continuam a ser, ainda, mais influentes diante da sociedade do que o ciberespaço. O sistema de mídia brasileiro, incluindo a internet, apresentam um conjunto de características que permitem classificá-lo como um sistema formador de opiniões.

Na próxima parte, apresenta-se um relatório das reportagens selecionadas na internet, todas relacionadas à imagem que é transmitida a comunidade virtual, no que se refere aos "*hackers*".

4 AS REPORTAGENS SOBRE OS “*HACKERS*”

A intenção nesta parte da pesquisa é mostrar a partir das reportagens analisadas como o termo vem sendo explorado pela mídia, enfatizando as matérias acessadas na internet. A título de informação é preciso esclarecer que foram realizadas várias pesquisas, em variadas páginas da internet, buscando subsídios consistentes para afirmar como vem sendo a utilização do termo nas matérias de acesso virtual.

É pertinente esclarecer que as matérias foram adquiridas através de uma pesquisa eletrônica, utilizando os termos “*hacker*” e “*cracker*”. A primeira impressão, quando se iniciou a pesquisa e avaliando o conteúdo das matérias, foi que existe um exagero da mídia ao tratar do assunto. No início da seleção das reportagens, ainda acontecia uma revisão bibliográfica sobre a história dos “*hackers*”. Acreditava-se que com o passar do tempo e o aprofundamento da teoria se chegaria à outra visão, mas isso não aconteceu.

Esta pesquisa é, em um primeiro momento, descritiva, pois se pretendeu expor as idéias de autores que discutem o assunto afim de possibilitar uma maior compreensão sob a utilização dos termos pela internet. Buscou-se a partir da análise teórica verificar como a mídia divulga suas notícias. Foram selecionadas 34 reportagens que apresentavam a utilização do termo “*hacker*”. Nas escolhas privilegiou-se, as reportagens que já no título apontava o termo “*hacker*”.

4.1 As matérias selecionadas

Apresenta-se aqui, o título e parte do conteúdo das matérias que apontam o termo, a fim de realizar os comentários pertinentes e constatar a utilização do termo na internet.

1. *“Hackers” éticos x “crackers”* - Jornal do Brasil 17/02/2000. *“O 'cracker' é o invasor que quer quebrar a segurança de um sistema e provocar estragos, pelo simples prazer de conseguir ou por ganhos financeiros. Normalmente, é um 'hacker' de nível avançado, sabe tudo sobre sistemas operacionais e linguagens de baixo nível.”*
2. Os *“hackers”* brasileiros não querem mais ter a fama de criminosos - Jornal Hoje - Globo 20/04/2005. *“Mesmo sem usar o usuário e senha, consegue-se ver todos os arquivos, tudo que tem no servidor invadido.”*
3. *“Hackers”* tiram o sono de 43% dos usuários de TI - *Computer World* 28/09/2005. *“Hackers', acessos indevidos, quebras de firewall e prevenção contra intrusos vêm tirando o sono de muitos profissionais de tecnologia”.*
4. Bancos da Flórida sofrem novo tipo de ataque *online* - *IDG Now* 31/03/2006. *“Três bancos no estado norte-americano da Flórida tiveram suas páginas comprometidas por 'hackers' em um ataque que os especialistas de segurança estão chamando de primeiro do seu tipo.”*
5. Entrevista: *“Hackers”* ditam o futuro da segurança - *Infosecurity* 30/12/2005. *“O futuro é conduzido pelo 'hacker'. Isso não é simplesmente um mercado em que nós antecipamos as tecnologias para atender as necessidades dos clientes.*

O usuário malicioso determina para onde vai a próxima ameaça e quando você vê a comunidade 'hacker', a grande mudança nos últimos dois anos tem sido os grupos organizados motivados pelo dinheiro.”

6. “Hacker” é a principal ameaça em TI, dizem gestores - *Computer World* 18/10/2005. “Os 'hackers' representam a principal ameaça aos sistemas de tecnologia da informação, segundo executivos pesquisados pela consultoria.”

7. “Hackers” publicam na web código que explora falha grave do Sistema Windows - *IDG Now* 27/03/2006. “Esse é o primeiro passo para que 'hackers' criem um vírus ou worm que explore a falha não corrigida do Internet Explorer. Um código que explora uma falha ainda não corrigida, foi publicado em diversos sites.

8. Publicado código que explora falha do Firefox 1.5 - *IDG Now* 09/02/2006. “Pesquisas indicam ainda que os ataques por 'hackers' nem sempre são externos.”

9. “Hackers” roubam dados do Orkut - *Monitor das Fraudes* 13/2/2006. “É bom tomar cuidados com o Orkut, pois os 'hackers', com facilidade captam todos os dados disponíveis.”

10. “Hackers”: entre a ideologia libertária e o crime - [comciencia](#) 10/04/2002. “Mas, muitas vezes para promover a livre informação é preciso 'crackear', fazendo do legítimo 'hacker', também um 'cracker'.”

11. Empresas de segurança apoiarão ferramentas “anti-hackers” - *Infoguerra* 01/02/2006. “Querem padronizar as ações de combate a programas que roubam informações ou transformam em zumbis os computadores invadidos.”

12. Guerra civil online – O perigo “hackeano” - *Folha online* 27/01/2006. “Criminosos que usam o conhecimento de forma destrutiva.”

13. *"Hackers": a ética por trás do folclore - Universidade de Brasília 29/09/2002. "Com o crescimento da internet e a consolidação da chamada Sociedade da Informação, muito tem sido dito sobre os tais dos 'hackers'. "Piratas da Rede", "meliantes digitais" e outras denominações que variam do ridículo ao romantismo cibernético."*
14. *"Hackers" buscaram dinheiro e não só a fama em 2005 - IDG Now. 27/12/2005. "Pragas que buscam dinheiro e dados após infecção crescem quatro vezes mais que os vírus no período e ilustram novo perfil nos ataques."*
15. *"Hackers": criminosos ou libertários? - SecurityFocus 05/08/2005. "Fraudadores on line fazem parte de grupos especializados. O golpe envolve e-mails, cartas ou faxes a vítimas em potencial, atraindo-as para um negócio falso."*
16. *"Hackers", "crackers" & "phreakers" - Guia do "hacker" brasileiro 25/11/2003. "São os 'crackers', que invadem contas bancárias, destroem sites e praticam pirataria pela internet."*
17. *Especialistas identificam novas ameaças à segurança da informação – Security Focus 30/11/2005. "Quais cuidados tomar na implantação da segurança contra os 'hackers'."*
18. *Guia do "Hacker" Brasileiro - Folha online 20/04/2004. "Hackers 'ensinam como invadir e roubar sistemas."*
19. *PF prende 21 "hackers" brasileiros - Grupo desviou R\$ 100 milhões - Correio Web. "A polícia federal acredita que em cada dez quadrilhas de 'hackers' no mundo, oito são brasileiras."*
20. *Quem são os hackers", os chamados piratas eletrônicos? (um pouco de etimologia) – Advogado.com 15/11/200. "A grande verdade é que os 'hackers'*

são muito bons e sabem escrever códigos que realmente funcionam. São pessoas que detêm um conhecimento acima da média, em níveis informáticos.”

21. *“Hackers” – Brasileiros são a maioria - Correio Web 11/09/2004. “Eles compram com nossos cartões, destroem informações sigilosas de grandes empresas, divulgam imagens de crianças nuas, violam nossa correspondência, falsificam dinheiro e ameaçam vidas.”*

22. *Afinal, será que ser “hacker”, realmente, é o que a mídia divulga? - Comciencia 20/02/2005. “O termo vem sendo amplamente divulgado como pirata digital.”*

23. *Uma breve descrição do termo “hacker” - Avocati Locus 2001. “Abreviando, sob pena de nos tornarmos cansativo, temos que os piratas inequivocamente foram os primeiros cidadãos do mundo, os pais do comércio internacional, homens de inteligência invejável e conhecimentos ímpares. Entendido o que é pirata, vejamos o que é 'hacker'.”*

24. *Sobre o uso do termo “hacker” - Segurança computacional 04/2004. “O termo 'hacker' tem sido utilizado na mídia como sinônimo de pirata digital, vândalo, etc.”*

25. *“Hacker” invade sistema e limpa tudo - forum.tibiabr 20/03/2005. “As últimas ações dos 'hackers' tem causado grandes danos às corporações brasileiras.”*

26. Qual o verdadeiro significado do termo “*hacker*”? - Jornal Hoje - Globo 05/01/2005. “*Os 'hackers' brasileiros não querem mais ter a fama de criminosos.*”
27. “*Hackers*” publicam na web código que explora falha grave do IE - IDG Now 24/03/2006. “*Como se não bastasse a invasão no sistema, os 'hackers' ainda divulgam as falhas na internet.*”
28. “*Hacker*” X “*Cracker*” - Sisnema.com 18/03/2004.. “*Palestra vai ajudar na luta contra os ataques dos 'hackers'.*”
29. “*Hackers*” - quem são eles? - Jornal Hoje – Globo 23/11/2003. “*Suas atividades contraventoras são hoje exploradas pelas mídias de massa, gerando assim, um efeito dominó nas empresas, que passam a olhar com mais atenção para os ambientes corporativos e a identificar vulnerabilidades que antes passavam despercebidas.*”
30. “*Hackers*” e “*crackers*”, você sabe qual é a diferença? - Estadão 04/07/2005. “*A cultura 'hacker' nos ofereceu uma visão colaborativa do universo tecnológico, e dos benefícios da livre circulação da informação.*”
31. Verdadeiro significado do termo “*hacker*”? Infoguerra 01/2006. “*Se a expressão está correta, não discutiremos. O Importante é que você tenha certeza de não estar aplicando este termo a um aliado apenas da tecnologia, cujo passado é desconhecido o futuro arriscado.*”
32. “*Hackers*” são bandidos ou mocinhos? - Coluna Firewall - IDG Now 07/08/2001. “*São mais de 320 milhões de usuários online, números mundiais que representam um banquete para os chamados 'hackers' e variações.*”
33. Roubo de dados na Web tem crescimento - Vírus e Cia 25/07/2006. “*Os clientes e as operadoras de cartões de crédito envolvidos no episódio já foram*

notificados. O roubo de dados realizado por uma 'hacker', aconteceu durante o último final de semana.”

34. “Hacker” invade loja da AT & T e rouba dados de 19 mil. Virus e cia 02/02/2006. “Hacker ' invade loja de AT & T e rouba dados financeiros e pessoais de clientes da companhia.”

Da amostra de 34 reportagens, constatou-se o seguinte: 21 reportagens abordam negativamente o termo “hacker”, representando 62% do total. Apenas, 15% apresenta o “hacker” como detentores de conhecimentos avançados de informática, ou seja 5 reportagens. O restante, que são 23%, abordam a divergência do termo, ou a ausência de conhecimento entre o que significa “hacker” e “cracker”. O quadro abaixo ilustra estas informações.

Quadro 1 – Reportagens conforme a visão sobre o termo “hacker”

Tipos de Visão	A - Visão Negativa do termo	B - Visão Positiva do termo	C - Visão sobre a divergência nos termos
Matérias selecionadas	3, 4, 5, 6, 9,10, 11, 12, 14, 15, 17, 18, 19, 21, 25, 27, 28, 29, 32, 33, 34	1, 2, 16, 20, 30	7, 8, 13, 22, 23, 24, 26, 31,
Total	21	5	8

Fazendo uma análise das reportagens selecionadas pode-se dizer estamos num momento de contradições e incertezas. A teoria estudada mostrou a

história dos “*hackers*” e foi possível verificar a contribuição importante que representaram para o desenvolvimento dos principais dispositivos tecnológicos que são utilizados hoje. Porém ainda permanece a falta de entendimento sobre o termo.

Na visão A, que representa reportagens que falam negativamente, verifica-se a utilização generalizada do termo, ou seja, todas as ações que se referem à pirataria digital, roubos, invasões, são relacionadas diretamente aos “*hackers*”. A matéria 3 ao apontar que os “*hackers*” vem tirando sono de muitos profissionais de tecnologia, deixa entender que à prática de acesso indevidos não se refere à profissionais. A matéria 4, também utiliza o termo negativamente; ao falarem de “especialistas de segurança” falam de profissionais que não são os “*hackers*”, atribuindo o caráter negativo ao termo.

Ainda nesta visão negativa pode-se atribuir parte da responsabilidade da divulgação negativa, às empresas de segurança. As matérias 5, 6, 11, 17 e 28 estão relacionadas à segurança para as empresas. As informações mostram que os gestores desta área utilizam o termo “*hacker*” para realizarem propagandas de vendas de seus sistemas. Em outros casos, divulgam ferramentas “anti-*hackers*”, oferecendo às empresas ações de combate à programas que roubam informações.

Estas informações mostram que nem os profissionais de segurança tem consciência do real significado do termo “*hacker*”. Em pouquíssimos casos o termo “*cracker*” é apresentado em primeira instância, para designar os invasores. Conforme as reportagens, são os “*hackers*” os maiores responsáveis pela pirataria digital. Observou-se também que quando se une o “*hacker*” ao “*cracker*” no título da matéria, no decorrer texto, concentra-se apenas o termo “*hacker*”. Um exemplo é a matéria de número 28, que divulga palestra que vai ajudar na luta contra o ataque dos “*hackers*”.

Com relação aos dados disponíveis no *orkut*, na matéria 9, novamente os “*hackers*” são apontados como os responsáveis pela captação de dados, mostrando que o termo é utilizado em todas as matérias relacionadas com a invasão de dados. Em todos os sentidos, quando não se tem o conhecimento de quem é o invasor, o termo “*hacker*” é apontado.

Nas matérias 10, 12, 14, 15, 21, 25, 27, 29, 33 e 34, o termo é utilizado sem poupar comentários. Os “*hackers*” são apresentados como criminosos perigosos que usam o conhecimento de forma destrutiva. A matéria 14 exagera em dizer que “*pragas crescem quatro vezes mais que vírus..*”, nestas matérias são apresentados termos como criminosos, fraudulentos, contraventores, comparando o “*hacker*” a um vírus.

O autor da matéria 10, num primeiro momento aborda a tentativa de classificar os “*hackers*” como pessoas que promovem a liberdade de expressão e de informações, e os “*crackers*” como causadores de prejuízos, mas na sua análise aponta também que para promover a livre informação é preciso “*crackear*”, fazendo do “*hacker*”, também um “*cracker*”. Percebe-se aqui o duplo sentido, do termo, levando a entender, que “*hacker*” e “*cracker*” é a mesma coisa.

Infelizmente, as fontes de divulgação em que circulam estas reportagens são meios conceituados que possuem um público leitor constante, como o Jornal Hoje. Mas verifica-se que neste mesmo veículo, expõe-se também matérias que questionam a utilização do termo, conforme matéria 26. Nesta matéria, o autor aponta a magia que existe ao redor do termo “*hacker*”, tentando desmistificar o caráter negativo do termo. Às vezes, muitas pessoas que se julgam “*hacker*” não têm o conhecimento necessário para tanto.

Vale lembrar aqui, que o conhecimento em computação se adquire com estudo, se conquista com tempo, com trabalho e pesquisa. A pessoa que se

dedicar terá um grande conhecimento, tornando-se um excelente profissional, mas o perfil de uma pessoa é complicado de modificar, pois foi construído ao longo da vida, dependendo de vários fatores. Então, as pessoas que usam a computação para cometer seus crimes, devem ser tratados como criminosos quaisquer.

Outro ponto negativo divulgado pela mídia na internet pode ser observado na matéria 19, que afirma que a maioria das quadrilhas de “*hackers*”, são de brasileiros. Esta informação é divulgada pela Polícia Federal ao Correio *Web*, sem uma estatística precisa e também utilizam o termo “*hacker*” sem o real conhecimento do seu significado.

Na matéria 32, percebe-se que diante de uma indefinição do termo a ser utilizado para os que invadem sistemas, a mídia atribui a responsabilidade aos “*hackers*”, mas deixa claro que o termo possui outras variações, porém não são identificadas.

Numa avaliação da visão B, que fala positivamente sobre o termo “*hacker*” percebe-se um entendimento sobre quem são os piratas digitais. As matérias deste grupo deixam claro que o “*cracker*” é o invasor que quer quebrar a segurança de um sistema e provocar estragos. Estas matérias, como exemplo a nº 2, mostram que ainda há uma esperança para o entendimento do termo, pois apresentam que os “*hackers*” protegem os computadores e por isso devem conhecer bem as técnicas digitais, entendendo que criminosos são os que usam o conhecimento de forma destrutiva. Ainda afirma que são os “*crackers*”, que invadem contas bancárias, bancos e grandes empresas. E os “*hackers*” são utilizados para combater os “*crackers*”.

A matéria 16, seguindo a mesma linha de interpretação, vai mais além e mostra as várias denominações utilizadas, mas especificam também que os que invadem as contas bancárias e praticam a pirataria pela internet, são os

“*crackers*”. Do mesmo modo, na matéria 20, é apresentado que os “*hackers*” são muito bons e sabem escrever códigos que realmente funcionam, visto que detêm conhecimentos acima da média, em níveis informáticos. Isto reforça a colocação durante todo o trabalho de que os “*hackers*” possuem uma ética que vai de encontro a um desenvolvimento tecnológico.

Considera-se importante atribuir um destaque a matéria 30, onde o autor mostra a diferença entre “*hacker*” e “*cracker*” e explica que os “*hackers*” são *experts* em tecnologia e os que valem do seu conhecimento para invadir sites são os “*crackers*”.

As reportagens que apresentam a visão C, mostra, por um lado a importância das atividades dos “*hackers*” e por outro lado, a forma indefinida da divulgação do significado do termo “*hacker*”. A matéria 7 apresenta que os “*hackers*” descobriram falhas graves no Sistema *Windows*. Do mesmo modo na matéria 8, é exposta outra falha do Sistema. Estas matérias foram apresentadas por *IDG Now* e mostram que os “*hackers*” emitem avisos de identificação das falhas encontradas, mas em alguns casos, não é atribuído um caráter crítico pelas empresas.

Em outra linha de interpretação, mas ainda relacionado à divergência dos termos, as matérias 13, 22, 23, 24 e 31, deixam visível a falta de entendimento sobre o real significado do termo “*hacker*”. As matérias apresentam a necessidade de um conhecimento mais afinado sobre as ações dos “*hackers*”, questionando as divulgações da mídia. Considera-se este percentual de 23% positivo para o momento crítico que a história dos “*hackers*” vem passando. Pode-se dizer que há um interesse, de parte da mídia, em esclarecer o significado dos termos.

É possível perceber que a confusão vem sendo mantida pela mídia. A teoria mostrou que a cultura “*hacker*” oferece uma visão colaborativa do

universo tecnológico, e dos benefícios da livre circulação da informação. Se os “*hackers*” compartilham conhecimento e produzem de forma descentralizada, e são os responsáveis pela criação do *software* livre e do *Linux*, então, são um benefício para a sociedade.

Assim, ao finalizar a pesquisa, a impressão permanece a mesma. Existe um exagero na conceituação do termo, mas, acima de tudo, uma distorção no significado real do que representa os “*hackers*” para a sociedade. O que se percebe é um total desconhecimento do significado do termo e também da história da evolução da informática e do que os “*hackers*” representaram neste processo de transformação tecnológica.

Poulsen (1999) bem esclareceu que a mídia começou a abordar o tema “*hacking*” desde 1985, quando o governo começou a plantar a idéia de um perigo eminente sobre o poder de controlar redes telefônicas por satélite. Desde então, o “*hacker*” passou a ser tratado de forma alarmista pela mídia com o intuito de criar a idéia de uma possível guerra cibernética.

Na obra de Medeiros (2002, p.93), encontra-se a seguinte reportagem:

“Um déspota armado com um computador, juntamente com pequeno grupo de “*hackers*” especialistas, pode ser tão perigoso e perturbador quanto qualquer adversário que nós já enfrentamos desde a segunda guerra mundial”

Esclarecendo como o termo passou a ser divulgado pela mídia, Medeiros (2002) explica que foi a partir de reportagens redigidas com redação deste tipo que iniciou a confusão gerada na década de 90. A forma dos “*hackers*” como criminosos tomou conta das manchetes de jornal.

Como diz Medeiros (2002): Havia um novo inimigo a ser combatido e a mídia cumpriu e ainda cumpre muito bem seu papel de algoz com o assunto: “*hacker*.”

É imprescindível dizer que os “*hackers*” não devem ser citados como os principais responsáveis pela insegurança da internet, pois verifica-se que a imprensa, não questiona a estrutura vulnerável da internet e a falta de qualidade dos softwares. A porção redentora e ética dos “*hackers*”, pode ser bem entendida nas citações de Pekka Himanen, o que precisa ser divulgado com maior eficiência é a história dos “*hackers*” e o que representam a sua ética.

Diante da análise das matérias constata-se o exagero com que a mídia trata do assunto. Lembra-se que cita-se apenas a internet, mas sabe-se que nos jornais impressos, televisão, etc, o assunto é tratado na mesma dimensão.

A imprensa esquece de dizer que muitos dos ataques são concluídos, muitas vezes, em função da incompetência das empresas de tecnologias e do próprio desleixo dos órgãos públicos com relação a segurança dos seus *sites*. O que os “*hackers*” têm feito é demonstrar o alto grau de vulnerabilidade que existe na grande rede. Quem ameaça o comércio eletrônico não são os “*hackers*”, mas a própria constituição da internet, que não foi construída para dar total segurança a este tipo de uso, pelo menos por enquanto.

A imprensa, mais do que culpar os “*hackers*” por esses crimes, deveria questionar as vulnerabilidades da grande rede. Este sim é um assunto pouco encontrado nas páginas dos jornais. Sem esquecer de que muitas dessas manchetes se referem a tipos de invasões que não se pode dizer categoricamente que foram feitas por “*hackers*”.

A avaliação das matérias mostra ainda que para a imprensa não se pode ser “*hacker*” sem ser criminoso. Mas, basta se passar para o lado da indústria e, como em um passe de mágica, transforma-se em protetor e agente de segurança das mesmas empresas que ameaçava.

Fica difícil saber, pela grande imprensa, como entender o termo “*hacker*”. Pela forma como se tem feito essa divulgação, os “*hackers*” podem

ser criminosos de primeira linha, pichadores cibernéticos ou se forem bem comportados, se transformarem em consultores de segurança ou defensores nacionalistas.

Para os jornais, daria muito trabalho e demandaria muito espaço para tentar explicar as minúcias que envolvem a questão. É muito mais simples e objetivo incluir os tecno-rebeldes na categoria “*hacker*” do que tentar fazer uma suposta separação.

Infelizmente, esta é uma das características da grande imprensa, a de não possuir envolvimento aprofundado com o assunto, que fez com que se criasse uma visão forjada do termo “*hacker*”. Porém, a mídia não cria esse equívoco de forma solitária, mas com a cumplicidade das grandes corporações, que necessitam do controle, do poder sobre a grande rede para continuar seu reinado.

Percebe-se também que o jornalismo age, muitas vezes, com essa intenção mercadológica. É uma característica que põe a imprensa lado a lado com os interesses de um determinado sistema, seja este capitalista ou não.

Resende (2000) explica que a insistência nesse erro, aqui e ali, contribui não apenas para confundir habilidade com má intenção no mundo virtual, refletindo e amplificando a tendência humana ao medo ante o desconhecido, como também para encobrir a complexidade do problema da segurança nele.

Os “*hackers*” não podem ser coletivamente classificados como criminosos indesejáveis, pois muitos deles desempenham para o software um papel semelhante ao da seleção natural na evolução das espécies, descobrindo falhas de segurança nos *software* em uso pelo mundo e reportando suas descobertas aos desenvolvedores, às vezes sugerindo estratégias de reparo. São também os grandes responsáveis pelo enorme patrimônio intelectual em

software livre que circula pelo mundo hoje e do qual engajados na revolução digital estão se beneficiando.

Himanen, em uma reportagem para o Jornal “Valor Econômico” de 22/02/2006, faz uma referência a importância dos “*hackers*” e afirma que no ano 2020 a internet será uma mídia universal. Isso requer trabalho consciente e a formação de novos heróis. Ele afirma ainda que a rede não pode existir sem a ação individual e, por vezes, anônima, dos bons “*hackers*”, nomes como os de programadores voluntários, considerados por ele, verdadeiros heróis da generosidade.

Himanen defende a tese de que “enquanto a moral protestante foi a ética do trabalho da Era Industrial, a moral “*hacker*” é a filosofia de trabalho “natural” da Era da Informação e do Conhecimento.

Ele mostra que a ética “protestante” ensinou que qualquer que fosse o trabalho exercido, devia ser encarado como um dever - o seu dever mais importante em vida, ou seja, a mentalidade hoje convencional de que “isto tem de ser feito”. Nesta moral, o sofrimento no trabalho é considerado nobre.

Em contrapartida, os “*hackers*” devotam as suas vidas a fazer coisas com paixão - algo que acham intrinsecamente interessante, excitante e alegre. Os “*hackers*” trabalham naquilo em que podem ser criativos, realizam-se pessoalmente. O que é totalmente diferente da ética protestante.

“A ética protestante era indispensável para a sociedade industrial. O que exigia uma moral que visse o trabalho como um fim em si. A moral “*hacker*” não é protestante - a condenação ao trabalho em que não nos realizamos -, nem cristã - esta última fazia uma separação entre a semana de trabalho e o domingo. A filosofia “*hacker*” é fazer aquilo em que se sente inspiração e prazer. Ponto final. Seja o que se clarifica de trabalho ou de lazer - essas etiquetas foram abolidas.” (HIMANEN)

Enfim, as pesquisas mostraram que não existe um real entendimento sobre o termo “*hacker*” e nesse sentido, o que a internet vai repassando aos seus usuários é: os “*hackers*” são aqueles que invadem sistemas. Poucas reportagens abordam a diferença entre “*hackers*” e “*crackers*”. Percebe-se também, ao realizar as pesquisas que algumas reportagens têm no seu título o termo “*cracker*” e quando se realiza a leitura, é o termo “*hacker*” que está divulgado como pirata digital. Assim, o significado do termo “*hacker*”, utilizado pela internet, não está adequado aos conceitos verificados no decorrer deste trabalho.

Então, resta a insistência em afirmar que os “*hackers*” são os responsáveis por grandes contribuições para a evolução da informática e que os que praticam atos ilícitos não fazem parte do grupo que estão voltados para o desenvolvimento da era da informação.

Assim, a internet, como uma das fortes influenciadoras na formação da opinião pública, deveria constar de reportagens incentivadoras para a apuração da verdade e definição dos conceitos, mostrando realmente o entendimento sobre o que está divulgando e contribuindo para a formação de opiniões mais centradas na história e na real apuração dos conceitos.

5 CONSIDERAÇÕES FINAIS

Acredita-se que chegou o final desta pesquisa. Infelizmente, não restam dúvidas da veiculação do termo “*hacker*” na internet de forma negativa, que vem denegrindo a imagem destes atores da evolução tecnológica. Sabe-se que o progresso da sociedade está intimamente relacionado com o desenvolvimento da informática e que esta tem um grande potencial de formação de opinião pública, por isso, deve ser tratada com zelo e muito cuidado.

Lamentavelmente, como o desenvolvimento costuma surgir de problemas carecedores de soluções, continua a luta em favor da real definição conceitual do que representa os “*hackers*” e, não sendo isto possível, busca-se a defesa de que os repórteres, através dos seus veículos de comunicação, devem possuir a preocupação de transmitir/informar sobre assuntos que conheçam sobre a sua história.

Ficou claro que a grande imprensa teve um papel crucial na divulgação da criminalização do “*hacking*”, foi a partir dela que se construiu um equívoco que se espalhou pelo mundo e se perpetua até hoje, pois o lado obscuro da internet é bastante heterogêneo. Há criminosos assumidos, aqueles que tentam desviar dinheiro de banco, por exemplo, e sabotadores com algum motivo pessoal. É o caso do funcionário demitido que resolve agredir o ex-patrão ou do cliente mal atendido que derruba um *site* de comércio eletrônico por vingança. Isto não significa que seja um “*hacker*”.

Foi possível concluir também que falar sobre “*hackers*” é algo rentável, existem dezenas de livros que vendem técnicas milagrosas para invadir redes. Existem *sites* que esbanjam o nome “*hacker*” em atividades criminosas em

busca de obter retorno de investimento, vendendo programas de defesa contra os piratas da internet.

Há também pessoas da comunidade de segurança dando cursos e mais cursos visando nada mais nada menos do que fórmulas de como se livrar dos “*hackers*”. Jornalistas atrás de fama que fazem qualquer coisa para uma ascensão.

O “*hacker*” é maior do que tudo isto, a beleza do “*hacking*” não pode ser comercializada, pois pouca gente conseguiria visualizar a leveza e grandiosidade que envolve a ética “*hacker*”. A ética “*hacker*” é capaz de nos ensinar valores morais que a sociedade se alegraria em ver. Ela está além de uma única pessoa, está além de uma comunidade ou de único pensamento. A essência do “*hacker*” é a liberdade. É preciso que se respeite isso, pois há muitos outros criminosos que precisam ser perseguidos.

Enfim, o que importa entender é que há muitas controvérsias sobre o tema, mas que existe uma ética dos “*hackers*” que merece ser considerada por trazer embutida em suas linhas o desejo constante de conhecimento e de contribuição para o pleno desenvolvimento do fascinante mundo dos sistemas informatizados.

REFERÊNCIAS BIBLIOGRÁFICAS

ANASTACIO, Teixeira. *O que é Indústria Cultural*. 12.Ed. São Paulo: Brasiliense, 2002, 66p.

COUTO, Sérgio P. *O que pensar dos hackers?* In: Revista Geek, Ano III, Número 14. Digerati Editorial. Agosto, 2001.

CEBRÍAN, Juan Luis. *La Red: Como Cambiarán Nuestras Vidas Los Nuevos Médios DE Comunicación*. Bueno Aires: Taurus, 1998, 197p.

GONÇALVES, Elias Machado. *A Dialética do Discurso Jornalístico*. Rio de Janeiro, Escola de Comunicação e Artes da Universidade Federal do Rio de Janeiro, 1992. (Dissertação de mestrado), 186p.

DOM, Rodnei. 2003. *Hackers – Quem são eles?* Disponível em www.consciencia.br/resenhas.html.

DOWNING, John. *Mídia radical: rebeldia nas comunicações e movimentos sociais*. São Paulo: Senac, 2003.

FERREIRA. Aurelio B. H. Mini Diconário da língua portuguesa. Ed. Nova Fronteira. 4 ed. RJ, 2002.

HELL. B.L. *A consciência Hacker – Uma visão objetiva*. São Paulo: Book Express, 2000.

HIMANEN, P. *A ética dos hackers e o espírito da sociedade da informação*. Rio de Janeiro: Campus, 2001.

JARGON FILE. Eric Steven Raymond (editor). Documento disponível em 30 de Maio de 2001: www.ccil.org/jargon.

JORNAL Valor Econômico. 22/02/2006. Disponível em www.imprensa.com.br. Acesso em 30 jul 2006.

LEMOS, A. L.; SEARA, S.; P □ RSIO, W. *Hackers no Brasil*, 2001. Disponível em

[http://www.facom.ufba.br/ciberpesquisa/andrelemos/Hackers%20no%20Bra-si.htm](http://www.facom.ufba.br/ciberpesquisa/andrelemos/Hackers%20no%20Brasil.htm). Acessado em setembro de 2004.

_____. *Cibercultura: tecnologia e vida social na cultura contemporânea*. Porto Alegre: Sulina, 2003.

_____. *Cibercultura. Alguns Pontos para compreender a nossa época*, 2003. Disponível em <http://www.facom.ufba.br/ciberpesquisa/andrelemos/cibercultura.pdf>. Acessado em setembro de 2004.

_____. *Cibercultura e Identidade Cultural*. Em direção a uma cultura copyleft?, 2004. Disponível em <http://www.facom.ufba.br/ciberpesquisa/andrelemos/copy-left.pdf>. Acessado em setembro de 2004.

LEVI, Pierre. *A inteligência coletiva: por uma antropologia do ciberespaço*. 1 ed. São Paulo: Ed. 34, 1994A.

LEVY, P. *Cibercultura*. São Paulo: Editora 34, 1999B.

LEVY, S. *Hackers: heroes of computer revolution*. Penguin Putnam, 2001A.

LEVI, Pierre. *A inteligência coletiva: por uma antropologia do ciberespaço*. 1 ed. São Paulo: Ed. 34, 1994C.

LEVY, P. *Cibercultura*. São Paulo: Editora 34, 1999D.

LEVY, Steven. *Hackers: Heroes of de Computer Revolution*. New York: Penguin Books, 1994B, 455p.

MASIEIRO, Paulo César. *Ética em Computação*/São Paulo: Editora da Universidade de São Paulo, 2000 – (Academia, 32), 213p.

MEDEIROS, Assis. *Hackers: Entre a ética e a Criminalização*/Florianópolis: Editora Visual Books, Junho de 2002 – 182p.

PASCHOAL, S.S. (2004). *Roubo de informações pela internet: entenda as diferenças entre hacker, cracker e lammers*. Disponível em

www.mulher.com.br/template.asp?canal=trabalho&id-mater=2257. Acesso em 25 maio 2006.

PISCITELLI, M. A Sociedade em Rede. 2 ed. São Paulo: Paz e Terra, 1995, vol. 1, 617p. Disponível em www.unicamp.com.br/teses. Acesso em 20 jul 2006.

POULSEN, Kevin. *Hacking the Hacks*. Publicado em 19 de Fevereiro de 1999 na página da TechTV. Documento disponível em 30 de Maio de 2001: <http://www.techtv.com/cybercrime/chaostheory/story/0,23008,2210323,00.html>.

RAYMOND, Eric Steven. (1999). A história dos *hackers*. Documento disponível : <http://comciencia.vom.br/>. Acesso em 20 jun 2006.

RAYMOND, Eric Steven. *Como se Tornar um Hacker*. Documento disponível em 30 de Maio de 2001: <http://nagoo.vila.bol.com.br/>.

REZENDE, Pedro A. D. Sobre o uso do termo "hacker". In: <http://www.cic.unb.br/docentes/pedro/trabs/hackers.htm>. Abril, 2000.

RHEINGOLD, Howard. *A Comunidade Virtual*. Lisboa: Gradiva, 1996, 367p. RHEINGOLD (1996) RHEINGOLD (1996) RHEINGOLD (1996)

ROSZAK, Theodore. *O Culto da Informação: o Folclore dos Computadores e a Verdadeira Arte de Pensar*. São Paulo: Brasiliense, 1988, 335p.

STALLMAN, R. *O Projeto GNU – a primeira comunidade a compartilhar software*. In: GASS, Elvino. *Software Livre*. Porto Alegre: Assembléia Legislativa/RS, 1999.

SOUZA, Stuart. *A identidade cultural na pós-modernidade*. 9 ed. Rio de Janeiro: DP&A, 2004.

STRACK, Jair. *Sistemas de Processamento Distribuído*. Rio de Janeiro: Livros Técnicos e Científicos Editora, 1984.

SUMMITT & PAUL M., MARY J. *Hackers: Piratas ou Patriotas?* In: HARRIS, Stuart Et al. *Cyberlife*. São Paulo: Berkeley, 1995, p. 359-377.

SUMMITT, MARY J. *Hackers: Quem são eles?*. São Paulo: Berkeley, 2005, p. 359-377.

TORVALDS, Linus; DIAMOND, David. *Só por Prazer Linux - Os bastidores da sua criação* - Editora Campus LTDA, RJ, 2001, p. 149 de p. 297.

UCHÔA, Kátia Cilene Amaral et al. *Introdução a Cibercultura. 3.ed.* Lavras: UFLA/FAEPE, 2003.

RAYMOND, E. Homesteading the Noosphere, 1999. Disponível em <http://www.catb.org/~esr/writings/homesteading/homesteading/>. Acessado em outubro de 2004.

_____. The Cathedral and the Bazaar, 2000. Disponível em <http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/>. Acessado em outubro de 2004.

BIBLIOGRAFIA COMPLEMENTAR

BELTRÃO, Luiz. *Jornalismo Interpretativo: Filosofia e Técnica. 2. ed.* Porto Alegre: Sulina, 1980.

BRETON, P. *História da Informática.* São Paulo: Editora da Unesp, 1991.

DUPAS, Gilberto. □ *tica e poder na sociedade da informação*
Gilberto Dupas, Ed. Unesp, São Paulo, 2000.

LADEIRA, J.D.M. Troca de Arquivos par-a-par: Napster, Gnutella e o Desenvolvimento de Tecnologias de Comunicação na internet. Programa de Pós-Graduação em Comunicação. PPGCOM/UF. Niterói, 2003. Dissertação.

LEMOS, A. L. Cultura Cyberpunk, 1993. Disponível em <http://www.facom.ufba.br/ciberpesquisa/lemos/culcyber.html>. Acessado em setembro de 2004.

_____. O Imaginário da Cibercultura, 1998. Disponível em <http://www.facom.ufba.br/ciberpesquisa/andrelemos/imaginario.htm>. Acessado em setembro de 2004.

<http://www.facom.ufba.br/ciberpesquisa/andrelemos/Hackers%20no%20Brasil.htm>. Acessado em setembro de 2004.

___. Ciberultura: tecnologia e vida social na cultura contemporânea. Porto Alegre: Sulina, 2002.

___. Ciberultura. Alguns Pontos para compreender a nossa época, 2003. Disponível em <http://www.facom.ufba.br/ciberpesquisa/andrelemos/ciberultura.pdf>. Acessado em setembro de 2004.

___. Cibercidades: um modelo de inteligência coletiva. In: LEMOS, A. L. (Org.). Cibercidade: as cidades na ciberultura. Rio de Janeiro: E-papers, 2004. p. 19-26.

___. Ciberultura e Identidade Cultural. Em direção a uma cultura copyleft?, 2004. Disponível em <http://www.facom.ufba.br/ciberpesquisa/andrelemos/copy-left.pdf>. Acessado em setembro de 2004.

LEMOS, A. L.; SEARA, S.; PEREIRA, W. *Hackers no Brasil*, 2001.

MACONDES FILHO, Ciro. *Sociedade Tecnológica*. São Paulo: Scipione, 1994. *O Capital da Notícia*. São Paulo: Ática, 1986.

MELO, José Marques de. *A Opinião no Jornalismo Brasileiro*. Petrobrás: Vozes, 1985, 207p.

SCHWINGEL, C. *Comunicação e criação na internet: análise das equipes de desenvolvimento web e dos grupos de desenvolvimento de softwares*. Programa de Pós-Graduação em Comunicação e Cultura Contemporâneas. FACOM/UFBA, Salvador, 2002. Dissertação.

SILVA, Agostinho Rosa. *A imprensa e os "hackers"*. Acesso em 17/07/2006. Disponível em <http://www.agostinhorosa.com.br>.