Alexander Dias Martins

A ATUAÇÃO DA POLÍCIA MILITAR DE MINAS GERAIS NA PREVENÇÃO E REPRESSÃO AOS CRIMES CIBERNÉTICOS

Belo Horizonte
2010

Alexander Dias Martins

A ATUAÇÃO DA POLÍCIA MILITAR DE MINAS GERAIS NA PREVENÇÃO E REPRESSÃO AOS CRIMES CIBERNÉTICOS

Monografia apresentada à Academia de Polícia Militar de Minas Gerais e à Fundação João Pinheiro, como requisito parcial para obtenção do título de Especialista em Segurança Pública.

Orientador: Cel. PM Divino Pereira de Brito

Belo Horizonte
2010

Alexander Dias Martins

A ATUAÇÃO DA PMMG NA PREVENÇÃO E REPRESSÃO AOS CRIMES CIBERNÉTICOS

Monografia apresentada ao Centro de Pesquisa e Pós Graduação da Polícia Militar de Minas Gerais como requisito parcial para conclusão do Curso de Especialização em Segurança Pública.

BANCA EXAMINADORA

Cel. PM Divino Pereira de Brito
Orientador

Cel. PM Wilson Chagas Cardoso
Avaliador PMMG

Professor Agnez Saraiva
Avaliador da Fundação João Pinheiro

Belo Horizonte, Novembro de 2010

Dedico este trabalho aos meus pais, Walter Martins e Maria José Dias Martins, pelo apoio incondicional e carinho dedicados.....

AGRADECIMENTOS

Agradeço primeiramente a Deus, por ter me dado força e coragem suficientes para a conclusão deste trabalho.

Agradeço imensamente ao meu orientador, Sr. Cel. PM Divino Pereira de Brito, pelo apoio incondicional em todas as etapas de elaboração da pesquisa.

Ao meu irmão, Cel. PM Luis Carlos Dias Martins, pela força e incentivo.

À minha família, mãe, pai e irmãos, pela motivação e torcida, sempre presentes.

À minha estimada esposa, Patrícia, e ao meu filho, João Paulo, pelo incentivo, pela ajuda e por me presentearem com tanta atenção.

Ao Dr Mauro Flávio Ferreira Brandão, Procurador de Justiça, pela compreensão nas horas difíceis.

RESUMO

A presente pesquisa aborda sobre os crimes praticados através da rede mundial de computadores – Internet – e como a Polícia Militar de Minas Gerais (PMMG) deve atuar na prevenção e repressão a esses crimes. Os crimes cibernéticos, de um modo geral, provocam uma grande sensação de insegurança e um sentimento de impotência em suas vítimas, pois são delitos, praticados por pessoas que “nem mesmo existem“, uma vez que, de alguma forma, os seus autores estão fora do alcance de poder do Estado. Os crimes cometidos através da internet, no Brasil, ainda são incontroláveis, devido a sua natureza e complexidade. Um dos aspectos mais danosos decorrentes do uso da internet é que o acesso ao computador tornou-se irrestrito a todas as faixas etárias, sem que haja um controle efetivo sobre esses acessos. Na sociedade moderna, tornou-se comum os pais trabalharem e os filhos menores ficarem em casa a maior parte do dia, tendo como prática mais comum o uso do computador. Daí tem sido comum crianças e adolescentes, à revelia de seus pais ou responsáveis, serem aliciados, ludibriados e atraídos para determinadas práticas, tornando-se vítimas fáceis para os criminosos cibernéticos, através das redes sociais. Diante da realidade em que o mundo moderno se encontra, faz-se necessário conhecer as regras básicas de segurança de navegação através da rede internet, no que se refere aos sites seguros, onde se pode “navegar“ com segurança, com dispositivos de controle pelo próprio usuário, de modo a dificultar ou mesmo impedir a prática dos crimes cibernéticos. Para alcançar bom êxito na prevenção e repressão a essa modalidade criminosa, as forças policiais precisam do apoio da sociedade. É necessário que haja uma coalizão de esforços, com a efetiva participação de técnicos especializados, de cientistas da computação, operadores do Direito, uma polícia tecnicamente preparada e uma sociedade vigilante, além de um esforço legal que considere indispensável a participação do Ministério Público, da Polícia Federal, do Poder Judiciário, de outros órgãos e entidades representativos da sociedade. O Congresso Nacional está se empenhando no propósito de aprovar uma Lei que defina quais são os crimes cibernéticos, o que muito contribuirá para a solução do problema.

Palavras-chaves: Crimes Cibernéticos. Polícia Militar. Atuação. Prevenção. Repressão.

ABSTRACT

This research focuses on crimes committed via the World Wide Web - Internet - and how the Military Police of Minas Gerais (PMMG) should play in the prevention and prosecution of such crimes. The cyber crimes, in general, cause a great sense of insecurity and a feeling of helplessness in their victims because they are vested crimes, committed by people who "do not even exist," because, somehow, their authors are beyond the reach of state power. The crimes committed via the Internet in Brazil are still uncontrollable because of its nature and complexity. One of the most harmful due to the use of the Internet is that access to the computer will become unrestricted access to all age groups, with no effective control over these roads. In modern society it has become common for parents to work and minor children stay at home most of the day, a practice more common to use the computer. It has been common for children and adolescents, in default of their parents or guardians, they are lured, deceived and drawn to certain practices, becoming easy prey for cyber criminals through social networks. Facing the reality that the modern world is, it is necessary to know the basic rules of safe navigation through the internet network, with respect to safe sites where you can "surf" with security, control devices for user himself, so as to hinder or even prevent the commission of cyber crimes. To achieve success in the prevention and repression of this type crime, police forces need the support of society. We need a coalition effort, with the effective participation of technical expertise, computer scientists, law professionals, a police force and engineered a vigilante society, and a nice effort as it deems necessary participation of the public prosecutor of Federal Police, the Judiciary, other agencies and organizations representative of society. The National Congress is working in order to pass a law that defines what the cyber crimes, which will greatly contribute to solving the problem.

Keywords: Cybercrime. Military Police. Performance. Prevention. Repression.

LISTA DE ABREVIATURAS E SIGLAS

ABCID – Associação Brasileira de Centros de Inclusão Digital

ANCED – Associação Nacional dos Centros de Defesa da Criança e do Adolescente

ARPANET – Advanced Research Projects Agency Network

CD-ROM – Compact Disc Ready-Only Memory

CETS – Child Expolitation Tracking System

CPMI – Comissão Parlamentar Mista de Inquérito (Deputados e Senadores)

DES – Data Encryption Standard

DIAO – Diretriz Auxiliar das Operações

ECPAT – End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purpose (Fim da Prostituição Infantil, Pornografia Infantil e Tráfico de crianças para propósitos sexuais)

ESCCA – Exploração Sexual e Comercial de Crianças e Adolescentes

EUA – Estados Unidos da América

FAPESP – Fundação de Amparo à Pesquisa do Estado de São Paulo

GPS – Geografic Position Satelite

IBM – International Business Machines

IP – Internet Protocol

LAN – Local Area Network

MP – Ministério Público

MPF – Ministério Público Federal

MS-DOS – MicroSoft Disc Operation System

OAB – Ordem dos Advogados do Brasil

OAB/SP - Ordem dos Advogados do Brasil – Seção de São Paulo

ONGs – Organizações Não-Governamentais

PC – Personal Computer

PM – Polícia Militar

PMMG – Polícia Militar do Estado de Minas Gerais

PR/GO – Procuradoria da República no Estado de Goiás

PR/SP - Procuradoria da República no Estado de São Paulo

SAFERNET - É uma organização não governamental, sem fins lucrativos, que reúne cientistas da computação, professores, pesquisadores e bacharéis em Direito com a missão de defender e promover os Direitos Humanos na Internet.

SMS – Short Messages System

WWW – World Wide Web

SUMÁRIO

1 INTRODUÇÃO

A presente pesquisa é a atuação da Polícia Militar do Estado de Minas Gerais (PMMG) na prevenção e repreensão aos crimes cibernéticos. O grande avanço tecnológico das últimas décadas permitiu o alcance de extraordinárias mudanças nos sistemas de comunicação, culminando com a criação e expansão da rede mundial de computadores - internet - que possibilita às pessoas se comunicarem de forma interligadas em todos os continentes. A internet permite a transmissão simultânea e em grande escala de diversas informações, trazendo maior comodidade às pessoas em seus relacionamentos.

O estudo terá por escopo principal a análise dos limites e perspectivas encontrados na prevenção e repressão aos crimes cibernéticos, pela Polícia Militar do Estado de Minas Gerais.

A pesquisa tratará de identificar os crimes cibernéticos e suas diferentes modalidades, demonstrando quais desses crimes têm sido mais cometidos no Estado de Minas Gerais, entre os anos de 2007 a 2009.

O Capítulo 1 contém a presente Introdução e uma contextualização a respeito dos crimes cibernéticos no Brasil, com ênfase para as diferentes modalidades desses delitos e os avanços que o computador tem proporcionado, no sentido de facilitar a prática de crimes.

O Capítulo 2 trata sobre o histórico e conceito da internet, como ela surgiu, de que forma surgiu, suas diversas faces, facilidades e crescimento exacerbado e completamente descontrolado de sua utilização no dia a dia das pessoas. Ver-se-á, também, o crescimento da utilização das mídias sociais, dentre elas o Orkut e o Facebook, como algo muito comum tanto entre jovens como em adultos.

O Capítulo 3 traz a abordagem sobre os aspectos jurídicos do uso da internet, enfatizando o domínio e o endereço eletrônico, os direitos autorais na Internet, as redes sociais, os documentos digitais e o comércio eletrônico. Também será observado o que

estabelece a legislação a respeito dos crimes cibernéticos no Brasil e como a PMMG tem se preparado para prevenir e repreender tais crimes.

No Capítulo 4, será abordado a respeito do anonimato nas *lan houses*. Para isso, verificou-se o conceito de *lan house*, destacando-se o seu funcionamento. Abordou-se a questão da utilização dos computadores sem que haja qualquer identificação do usuário e, por oportuno, tratou-se do projeto de lei em trâmite na Câmara Municipal de Belo Horizonte, que estabelece a obrigatoriedade de cadastramento de usuários.

O Capítulo 5 aborda a questão da prevenção e repressão aos cibercrimes pela PMMG. Ver-se-á que a Polícia Militar mineira ainda não se encontra preparada para o enfrentamento de tais crimes, mas, por outro lado, também se verá que existem polícias militares mais avançadas e já qualificadas para lidar com esses delitos, como as de São Paulo e do Paraná, que já possuem sistemas de rastreamento e localização de IP (Internet Protocol), além de manterem intercâmbio com diversos órgãos estatais e da sociedade civil, para o combate aos crimes cibernéticos.

O Capítulo 6 apresenta a análise e interpretação dos dados obtidos através da pesquisa de campo, destacando, através de tabelas e gráficos, como se encontra o nível de informação dos policiais mineiros a respeito dos crimes cibernéticos e como os Batalhões e Companhias Independentes têm atuado para prevenir e repreender tais criminosos.

O Capítulo 7 traz as conclusões da pesquisa e apresenta as propostas para a atuação da PMMG no enfrentamento aos crimes cibernéticos, tanto no aspecto preventivo como repressivo, além de sugerir as possíveis parcerias a serem firmadas com outros órgãos e entidades que lidam com a questão.

Considerando que os crimes virtuais vêm ganhando cada vez mais espaço e os casos têm aumentado em ritmo acelerado no país, com vários desdobramentos e consequências imprevisíveis, entende-se que o tema ora abordado é de extrema relevância e oportunidade para a PMMG, haja vista ser um assunto atual, complexo, pouco explorado e que se apresenta de considerável aplicabilidade na Corporação.

2 HISTÓRICO E CONCEITO DE INTERNET

Tem sido cada vez maior o número de informações transmitidas pelas pessoas e empresas por meio da internet, pela facilidade nessas relações, sejam elas pessoais, comerciais, governamentais, promocionais, religiosas, jurídicas, e outras. Entretanto, por ser uma rede ampla, cujo acesso é individualizado e os instrumentos de controle governamental fragilizados, essa ferramenta se torna vulnerável quanto à confidencialidade das informações transmitidas, ensejando a proliferação de ações criminosas com o uso do computador, os chamados crimes virtuais ou crimes cibernéticos.

No âmbito pessoal, tornou-se comum a prática de crimes de difamação, injúria e calúnia, através das redes sociais (como *Orkut, Facebook* e *Twitter*), tendo em vista a possibilidade de se escrever e postar fotografias, vídeos, matérias ofensivas e difamatórias, valendo-se do anonimato. Tornou-se comum, também, o uso de sites e blogs para ofensas pessoais, com o propósito de atingir a integridade moral de outrem, também com a utilização do anonimato. Até mesmo a privacidade das pessoas fica vulnerável diante de tanta facilidade de acesso por meio da internet.

No âmbito empresarial, cada vez mais as empresas são surpreendidas com a ocorrência de crimes, no ambiente corporativo, que podem assumir proporções devastadoras, comprometendo até mesmo sua integridade financeira. Esses riscos podem manifestar-se sob a forma de atos fraudulentos cometidos pelos próprios empregados e colaboradores da empresa, ou, ainda, por terceiros mal-intencionados.

Desta forma, além da internet se tornar um meio para a prática de crimes, também se tornou um facilitador para a organização dos criminosos e é também utilizada para a atuação do crime organizado, em suas diversas modalidades. Tal organização é realizada através das redes sociais, onde os indivíduos marcam data e local para a prática de determinado delito, como brigas entre torcidas, danos e depredações, disputas de “rachas”, organização de rixas em locais previamente marcados. Seja como meio de prática ou organização, esses delitos são os chamados cibercrimes ou crimes cibernéticos, por serem, todos eles, cometidos com o uso do computador.

Os crimes cibernéticos, de um modo geral, provocam uma grande sensação de insegurança e um sentimento de impotência em suas vítimas, pois são delitos, praticados por pessoas que “nem mesmo existem“, uma vez que, de alguma forma, os seus autores estão fora do alcance de poder do Estado. Os crimes cometidos através da internet, no Brasil, ainda são incontroláveis, devido a sua natureza e complexidade.

Diante da realidade em que o mundo moderno encontra-se, faz-se necessário conhecer as regras básicas de segurança de navegação através da rede internet, no que se refere aos sites seguros, onde se pode “navegar“ com segurança, com dispositivos de controle pelo próprio usuário, de modo a dificultar ou mesmo impedir a prática dos crimes cibernéticos.

Sabe-se que para alcançar bom êxito na prevenção e repressão a essa modalidade criminosa, as forças policiais precisam do apoio da sociedade. É necessário uma coalizão de esforços, com a efetiva participação de técnicos especializados, de cientistas da computação, operadores do Direito, uma polícia tecnicamente preparada e uma sociedade vigilante, além de um esforço legal que considere indispensável a participação do Ministério Público, da Polícia Federal, do Poder Judiciário, de outros órgãos e entidades representativos da sociedade. Sabe-se, também, que o Congresso Nacional está se empenhando no propósito de aprovar uma Lei que defina quais são os crimes cibernéticos, o que muito contribuirá para a solução do problema.

É imperioso que haja um rígido controle em relação às chamadas *Lan Houses* e aos Cyber Cafés, pois esses estabelecimentos são de livre acesso a pessoas de várias faixas etárias, sem que haja a sua identificação e o registro de quem acessou a internet, sobre qual equipamento utilizou e, muito menos, do conteúdo acessado e transmitido.

No Brasil, a Polícia Federal, com a atuação direta da Divisão de Direitos Humanos, em Brasília, tem obtido avanços significativos no enfrentamento aos crimes cibernéticos, sobretudo a exploração sexual infantil pela internet. Visando dar maior agilidade às suas ações, a Polícia Federal adquiriu o Child Exploitation Tracking System (CETS), que é um sistema extremamente moderno de informação e rastreamento de exploração sexual e pornografia infantil pela internet.

Nota-se que o Brasil está de certa forma atrasado no tempo quando se trata de enfrentamento aos crimes cirbernéticos. Considerando que ainda não há uma legislação específica, abrangente e atual sobre essa temática, vê-se, nesta mesma esteira, que os órgãos de segurança pública também não dispõem de estrutura logística e nem pessoal qualificado para fazer frente a essa demanda. Dessa maneira, os criminosos cibernéticos se veem livres para agir, sabedores de que não há punição para os seus atos.

Considerando a proximidade da Copa do Mundo de 2014, no Brasil, e conseqüentemente, a escolha da cidade de Belo Horizonte para ser uma das sedes dos jogos, haverá, certamente, um crescimento natural do turismo nacional e internacional, o que poderá incentivar a prática dos crimes cibernéticos, principalmente o turismo sexual, o tráfico de drogas ilícitas, a pedofilia, o estelionato e as fraudes no sistema bancário, com o uso indiscriminado do computador para a difusão de informações entre os criminosos e agenciadores. Há, também, outra questão preocupante do ponto de vista de segurança pública e segurança nacional, por ocasião dos eventos da Copa do Mundo: os possíveis atos terroristas, com o uso da internet.

Sabe-se que a informação é o elemento primordial para a relação entre as pessoas. Com o crescente desenvolvimento dos mais variados meios de comunicação, o fornecimento e a transmissão de informações se encontram cada vez mais sofisticados na sociedade, o que permite que a comunicação seja realizada em tempo real, através de satélites e uso da internet.

Essa revolução digital ocorrida nos últimos anos contribuiu para a construção da “Sociedade da Informação”, a qual é caracterizada pela prevalência da informação eletrônica, onde as relações econômicas e sociais estão cada vez mais intensas e imediatas.

O número de internautas brasileiros tem crescido em larga escala e em ritmo acelerado, assim como as redes sociais e as relações de consumo no meio eletrônico, o que torna as pessoas cada vez mais dependentes do mundo virtual. Assim, devido a uma série de fatores relacionados ao mercado das telecomunicações, sobretudo a telefonia, os computadores de bordo, a expansão dos serviços da rede mundial de computadores (internet) - o que se chama “*boom tecnológico*” -, aliado aos problemas do cotidiano das

grandes metrópoles, sobretudo as facilidades e as comodidades que a internet oferece, muitas das tarefas do dia a dia têm sido transferidas para a rede mundial de computadores, o que facilita o acesso às informações pessoais.

2.1 Conceito de Internet

Segundo Mendes (2007), o termo Internet é muito utilizado para descrever uma rede onde tudo se consegue, ou seja, qualquer pessoa com um computador conectado a um modem, com uma identificação e uma senha válida, pode lograr êxito em acessar a rede mundial de computadores, uma vez que a Internet trouxe a todas as áreas a possibilidade de compartilhar conhecimento e muito entretenimento.

Redes de computadores estabelecem a forma-padrão de se interligarem para o compartilhamento de recursos físicos ou lógicos. Esses recursos podem ser definidos como unidades de CD-ROM, diretórios do disco rígido, impressoras e outros.

2.2 Histórico

As tarefas repetitivas sempre incomodaram muito ao homem, que sempre buscou formas de aperfeiçoá-las para facilitar o seu trabalho, com menor esforço e melhores resultados. Um dos primeiros instrumentos que se têm conhecimento foi o ábaco, que tinha a função de fazer cálculos e era utilizado inicialmente pelos babilônios, por volta dos anos 2.700 – 2.300 a. C.

Assim, apenas no século XVIII surge a materialização do primeiro projeto de equipamento, um tear automatizado, construído por Joseph Marie Jacquard. Desse ponto em diante, foram surgindo diversos outros equipamentos, cada vez mais avançados, com o intuito de estabelecer uma forma de armazenar e processar informações utilizando relações binárias.

Foi, então, no século XX, que surgiram os primeiros computadores. O primeiro deles, o Mark I, de 1941, media 15m x 2,5m e fazia cálculos complexos sem a necessidade de intermediação humana.

Na década de 70, surgem os primeiros computadores modernos. A Aple foi a primeira empresa a criar o computador pessoal ou PC (Personal Computer), no ano de 1976. Após cinco anos, em 1981, a IBM lança seu modelo e contrata a empresa Microsoft, criada em 1974 por Bill Gates, para desenvolver seu primeiro sistema operacional, o MS-DOS.

A partir de 1983, a IBM começa a lançar vários PC's cada vez mais potentes, tendo sua denominação feita através dos processadores utilizados. A Aple lança no ano seguinte o Macintosh, com um sistema operacional equivalente ao da Microsoft. Desse ponto em diante, os computadores têm evoluído de maneira acelerada, ganhando um vasto mercado de produtos de informática, através de uma competição entre os vários fabricantes, os quais vêm se aprimorando tanto em seus equipamentos como em sistemas operacionais, dando maior comodidade para quem os utiliza.

No final da década de 60, a Agência de Projetos de Pesquisas Avançadas do Departamento de Defesa dos Estados Unidos da América – ARPA começou a consolidar uma rede experimental de computadores de longa distância chamada de ARPANET, que se espalhou rapidamente por todo o país. O objetivo original da ARPANET era permitir aos fornecedores do governo compartilhar caros e também escassos recursos computacionais. Inicialmente, a ARPANET permitia que os laboratórios de pesquisa dos EUA trocassem informações entre si. Desde o início, entretanto, usuários da ARPANET também se utilizavam da rede para a colaboração entre si. Essa colaboração abrangia desde compartilhamento de arquivos e programas e troca de mensagens via correio eletrônico (*e-mail*) até o desenvolvimento conjunto e pesquisas usando computadores remotos compartilhados. (CARVALHO, 2005).

A tecnologia de rede chegou ao estágio da massificação quando os computadores começaram a se espalhar pelo mundo comercial, ao mesmo tempo em que programas complexos multiusuários começaram a ser desenvolvidos (e-mail, banco de dados, internet).

No início da concepção das redes, cada fabricante possuía a sua forma de trabalho e sua própria linha de desenvolvimento de tecnologia. Como exemplo, pode-se citar a placa de rede de determinado fabricante que só poderia estar conectada a uma placa desse mesmo fabricante, por um meio físico (fio) também desenvolvido por ele. Caso houvesse problemas relacionados a preços ou não houvesse um relacionamento cordial ou mesmo um acordo comercial entre as partes, a empresa detentora dos equipamentos não tinha opção naquela época, a não ser a substituição de todo o parque de *hardware* e *software* instalado por equipamentos de outro fabricante. Desta forma, o problema não era resolvido, mas apenas contornado, e os prejuízos eram grandes.

O termo *wireless*, que significa sem fio, possui alguns sinônimos, como a comunicação sem fio, computação móvel e redes de computadores sem fio. Esse tipo de comunicação baseia-se no estabelecimento por meio do ar, ou seja, utiliza o espaço como meio de transporte.

A rede *wireless* possui como objetivo a conexão entre diferentes pontos com alta taxa de transmissão sem a necessidade do uso de cabos metálicos ou cabos de fibras óticas. Redes sem fio transmitem e recebem dados sobre o ar, combinando conectividade dos dados e mobilidade do usuário.

O primeiro sistema de computadores que empregou as técnicas de radiodifusão em vez de cabos ponto-a-ponto foi o sistema de *aloha*, na década de 70. Naquela época, as linhas telefônicas disponíveis eram de péssima qualidade e os preços elevados, não oferecendo confiabilidade na transmissão de dados, entretanto, a necessidade de interligação girava em torno da ligação de sub-redes de universidades (separadas em blocos) aos equipamentos ativos centrais. Assim, a origem e o destino não estavam muito diferentes.

De acordo com Mendes (2007), a rede *wireless* chegou para impulsionar e facilitar a vida do ser humano, onde o homem perdeu completamente a noção de tempo e espaço, pois tudo ficou facilmente ao seu alcance, sem limites ou sem fronteiras.

Apesar do ainda pequeno alcance da população à Internet, sua interatividade e assincronicidade estão promovendo mudanças no comportamento dos telespectadores

em diversos programas interativos, expandindo a limitação típica de se interagirem e poderem participar, e até mesmo opinar sobre determinado assunto. É notória a crescente convergência da televisão com a Internet: filmes, seriados, shows, esportes e noticiários, estão passando a coexistir na tv e na internet.

Os usuários das comunicações virtuais, tais como correios eletrônicos e o chat pressupõem todo um comportamento ético entre si. Essas condutas são denominadas netiquetas ou etiquetas na rede Internet, as quais foram criadas pela própria comunidade virtual, dentro da sua natureza intrínseca da *web* (NET, 2002. p.25).

A privacidade dos usuários e cidadãos no ambiente de novas tecnologias de comunicação e informação fica gradativamente mais comprometida com o aperfeiçoamento e novas facilidades dos sistemas eletrônicos e de telecomunicações. Isso somente acontece devido à capacidade que a Internet possui de abranger mundialmente as comunicações virtuais de maneira prática e eficaz, disseminando dessa forma, uma gama de conhecimentos que podem ser acessados de qualquer lugar e por qualquer pessoa.

Salvo raríssimas exceções, os usuários de serviços gratuitos de rede (provedores gratuitos) têm a sensação de que são anônimos na rede. Contudo, isto é uma falsa impressão, haja vista que se um usuário conecta-se ao provedor Internet a partir de uma linha telefônica, não fornece seus dados pessoais, e faz uso de *login* e senha falsos ou genéricos, ocorre que na conexão, o provedor obtém o número do telefone (consequentemente os seus dados pessoais) e pode monitorar todas as atividades desse usuário, seus usos e costumes de rede, ou seja, é um usuário tão identificado quanto os outros.

2.3 A Tecnologia na Atualidade

Os atuais números de acesso à rede mundial, relativos ou absolutos, não deixam dúvidas quanto ao seu crescimento vertiginoso. Comparados os dados de hoje aos de cinco anos atrás, percebe-se o rápido crescimento das mais diversas formas de

utilização da internet. Em 1994, a Internet suportava cerca de dez mil redes, conectava um milhão de computadores em 40 países e alcançava diariamente cerca de 25 milhões de pessoas. Naquele ano, projetava-se para o ano de 2000 a reunião de um milhão de redes, cem milhões de computadores interconectados e cerca de um bilhão de usuários diretos. (LYNCH, 1994).

Em 1988, a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), por meio de iniciativas, começou a difundir a Internet Brasileira. A disponibilidade para usuários comuns ocorreu no final de 1994, por meio de linhas discadas oferecidas por pequenos provedores e pelas operadoras de telecomunicações (CARVALHO, 2005).

Através da colaboração entre os administradores de redes e provedores (*webmasters* e analistas de segurança) o rastreio de usuários de serviços de *e-mail* gratuitos ou não, como, *Bol, Hotmail*, Yahoo e IG, podem levar à sua identificação. Sob determinadas circunstâncias de fraudes, roubos eletrônicos e invasões, esses administradores e provedores acionam uns aos outros de forma colaborativa nas varreduras e confirmação de informação.

Um importante papel do governo na economia digital é a sua participação na criação e fortalecimento de regras básicas, regulamentações e infraestruturas suficientes para os cidadãos e organizações. Parte dessa função vem sendo suprida de forma crescente através de organismos independentes, sociedades anônimas, de economia mista, organizações não-governamentais nacionais e internacionais. Os governos estão tomando algumas atitudes em benefício dos mercados digitais, cidadãos e empresas, promovendo a cidadania digital, sendo transparentes e desburocratizados. (Osborne, 1992).

Segundo Santos (2009, p. 35), a internet trouxe grande amplitude geográfica, tanto na economia quanto nas ações sociais, o que também proporcionou o aumento da criminalidade em virtude da facilidade de invasão nesta rede.

3 ASPECTOS JURÍDICOS SOBRE O USO CRIMINOSO DA INTERNET

Neste capítulo, faz-se uma abordagem dos aspectos jurídicos dos crimes cibernéticos no Brasil, enfocando-se a interface desses delitos com os crimes comuns e o papel da Polícia Militar, na sua atuação preventiva e repressiva.

Os problemas mais comuns de segurança na rede mundial são aqueles relacionados à privacidade, à autenticação, à autorização, recusa e integridade. Assim, essas mesmas noções também são objeto de cuidados quando se trata de negócios não eletrônicos. Necessário se torna, portanto, descrever o significado desses conceitos.

A ***privacidade*** consiste em manter a informação inacessível a usuários não autorizados. Normalmente, quando se pensa em segurança na Internet, o primeiro raciocínio que aflora à mente é o conceito de privacidade. Atualmente, as maiores empresas presentes na Internet procuram criar e divulgar amplamente suas políticas de privacidade, cujo objetivo é garantir que dados pessoais dos internautas não sejam utilizados sem seu consentimento.

No que concerne à identificação ou ***autenticação***, é importante observar a seguinte questão: como é que se sabe que um determinado usuário é realmente quem ele diz ser? A resposta a essa pergunta é dada pelo processo de autenticação de usuários, responsável por determinar com quem se está comunicando, antes de se revelar dados confidenciais ou se fechar qualquer negócio.

Tradicionalmente, os sistemas validam um usuário através de sua senha, que fica armazenada no arquivo *password*. Como é de se imaginar, a senha gravada no *password* não está em texto claro. Em verdade, ela é cifrada por meio de uma função unidirecional (que não pode ser invertida) variante do DES (Data Encryption Standard). Como não apenas as senhas dos usuários, mas também seus dados básicos (*userid, homedir*[1] etc) estão armazenados no arquivo *password*, e estes são corriqueiramente utilizados pelos aplicativos, o arquivo não possui e não deve possuir nenhum atributo que impeça os usuários de lerem seu conteúdo. Desta forma, também ficam expostas as senhas criptografadas de todos os usuários.

[1] *userid, homedir* são diretórios identificadores de usuários.

Até alguns anos atrás, face à impossibilidade de inverter a função de ciframento das senhas e principalmente devido ao limitado desempenho dos computadores, o que inviabilizava buscas exaustivas de senhas, este mecanismo de criptografia e armazenamento de senhas era seguro.

Atualmente, o grande desempenho dos novos microprocessadores e as redes de computadores permitem que vários deles possam estar interagindo na busca de senhas. Assim, o sistema que apenas se utiliza do mecanismo convencional de senhas tornou-se vulnerável, sendo um sério risco à segurança do sistema.

Os dois mais conhecidos programas de domínio público, que têm por objetivo quebrar senhas, são o "*Crack*" e o "*John the Ripper*". Ambos atuam de forma similar, exaustivamente buscando por palavras de dicionário, ou ainda cadeias de dígitos/letras que, cifrados, coincidam com alguma das senhas armazenadas no arquivo *password*. Quando isso ocorre, significa que a senha de algum usuário foi encontrada. Este tipo de busca normalmente encontra as senhas tidas como triviais (palavras e datas) para, em seguida, após alguns dias de processamento, também encontrar senhas mais complexas.

A ***autorização*** é o processo de permitir ou negar acesso por um usuário a um ou mais recursos existentes numa rede. Nos sistemas de segurança, a autenticação é distinta de autorização, que é o processo de atribuir a indivíduos o tipo de acesso a um sistema baseado na sua identidade. A maioria dos sistemas de segurança é baseada em duas etapas.

A primeira etapa é a autenticação, que assegura que o usuário é quem afirma ser. A segunda etapa é a autorização, que concede a um usuário acesso a recursos de uma rede com base na sua identidade.

Quanto à ***não-repudiação*** ou ***recusa***, esta serve para provar (por meio de assinaturas digitais) que, por exemplo, um consumidor pediu a um fornecedor X artigos a um preço Y de cada. Mesmo que mais tarde o consumidor afirme, no ato da entrega, que encomendou menos artigos que a quantidade X, ou que cada artigo tinha um preço inferior a Y, o fornecedor serve-se dessa prova para que o consumidor não recuse a encomenda.

Convém referir que pedidos falsos, enviados por alguém com intenções maliciosas, são ignorados, uma vez que é preciso a autenticação.

Já as assinaturas digitais são um componente importante na maioria dos mecanismos de autenticação. Consistem em um código digital que pode ser enviado juntamente com uma mensagem eletrônica, que identifica de uma forma única o usuário que enviou essa mesma mensagem. As assinaturas digitais devem ser encriptadas, de forma que ninguém consiga falsificá-las.

Outro ponto a ser abordado é a ***integridade,*** sempre quando se quer que uma mensagem não seja alterada. Refere-se, portanto, à integridade da informação que pode ser comprometida acidentalmente (erros humanos quando os dados são inseridos, erros de transmissão entre um computador e outro, vírus, *bugs*, etc.). Contudo, no comércio eletrônico, as situações a serem evitadas são aquelas em que pessoas mal intencionadas (ex.: *hackers*) comprometam deliberadamente a integridade das mensagens, em benefício próprio, para lesar alguém, ou simplesmente para se auto-promoverem.

O conceito de integridade dos dados não é novo. Há alguns anos, a generalidade dos sistemas de transmissão era analógica, o que implicava uma maior taxa de erros durante a transmissão em relação aos sistemas digitais hoje mais utilizados. Para se detectar esses erros, os protocolos de mais baixo nível começaram a implementar um sistema de detecção. Esse sistema passava por incluir na mensagem um número, o *checksum*, que era obtido a partir de determinadas operações aplicadas à própria mensagem. Esse número era difundido juntamente com a mensagem e, ao chegar ao receptor, as mesmas operações eram efetuadas e o número resultante comparado com o *checksum*[2]. Esse tipo de detecção foi adaptado para protocolos de mais alto nível, de modo a garantir a integridade das mensagens. Obviamente que a complexidade aumentou, uma vez que neste caso o elemento que poderá introduzir erro normalmente poderia alterar também o valor da verificação, de modo a não ser detectado qualquer erro, o que seria muito difícil de acontecer para os erros de transmissão (BERNARDINO, et al, 2004, p. 17).

[2] O *checksum* é um código detector de erros, no qual se utiliza uma sequência numérica para conferir erros específicos no sistema. Fonte: http://pt.wikipedia.org/wiki/Transmission_Control_Protocol

3.1 As Redes Sociais

As redes sociais se tornaram num *boom* deste início de século, onde a privacidade praticamente deixou de existir no mundo virtual e onde todos querem acompanhar a vida alheia. São milhões de usuários de *sites* de redes sociais, como o *Orkut*, o *Facebook* e o *Twitter*, dentre outros.

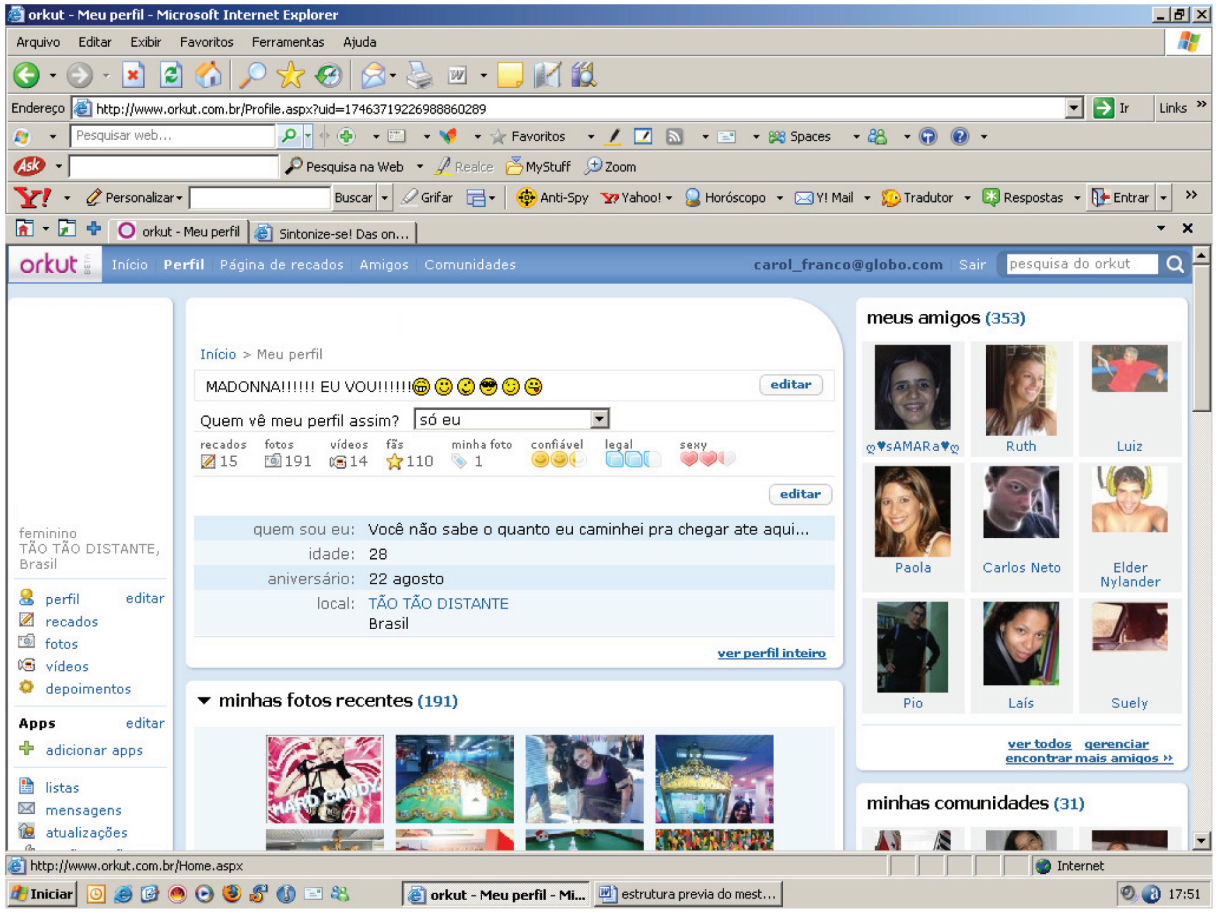
3.1.1 O *Orkut*

O *Orkut*, por exemplo, é um dos *sites* de relacionamento dentre tantos outros existentes na rede. Pertence ao grupo Google e foi criado em 22 de janeiro de 2004, pelo engenheiro de *software* da mesma empresa, o turco Orkut Büyükkökten. Surgiu como um projeto independente enquanto seu criador estudava na Universidade de Stanford nos EUA, sendo aperfeiçoado, posteriormente, durante seu trabalho na Google.

O *Orkut* tem como objetivo maior ajudar seus membros a criarem novas amizades e manter relacionamentos; cada usuário possui uma conta e perfil (*profile*). No perfil encontram-se algumas características pessoais do usuário, como sua descrição física, seu interesse de relacionamento, o país de origem, indicação de outros *sites* pessoais que venha a ter, sua profissão e outros dados. É importante assinalar que tais informações não são de cunho obrigatório nem são, necessariamente, verdadeiras, podendo haver a possibilidade de ser dados falsos ou omissos em alguns tópicos disponíveis para seu preenchimento.

Através da figura 1, podem-se verificar as características gerais de uma página do *Orkut*, cujo formato permite ao usuário conhecer o perfil das pessoas com quem esteja se comunicando. Contudo, pode ser enganado com falsas informações disponibilizadas.

Figura 1 – Foto de um perfil no *Orkut*



Fonte: www.*orkut*.com (2010)

A partir dessa primeira característica, já advêm dois problemas básicos: o primeiro está na exposição demasiada de dados no perfil e que podem ser visualizados por qualquer pessoa, o que atrai a atenção de “criminosos virtuais”, que se caracterizam por aqueles que captam informações através dessas redes, como nome completo, estado civil, profissão e características físicas, e as utilizam conforme seus interesses. Outra questão é a possibilidade de se fazer em perfis com informações falsas, o que facilita o anonimato.

Além desse “cartão de visita”, se é que se pode definir o perfil desta maneira, o *Orkut* ainda disponibiliza aos seus usuários espaço para divulgação de fotos pessoais, vídeos preferidos, depoimento e mensagens, as quais podem ser feitas por amigos que estão interligados à mesma rede de relacionamento. Ademais, possibilita a participação e também a criação de comunidades virtuais sobre vários assuntos, como educação, moda e beleza, religião, música, países e regiões, viagens, dentre outras infinitas categorias disponíveis no ícone específico.

Esta outra característica da rede social abre mais uma margem de possibilidades criminosas na internet: a facilidade de se visualizar fotos do álbum de determinada pessoa, seja por um estranho ou por alguém que possa se passar por um amigo. Nesta particularidade, o *Orkut* permite ao usuário acompanhar o cotidiano da pessoa, averiguar os bens materiais que ela possui (casa, carro, sítio), bem como a localização desses bens. É muito comum se ver atualmente nos noticiários que o autor de determinado crime obteve suas informações através de uma rede social. Outra facilidade que se tornou de uso comum pelos internautas é a localização de qualquer ponto geográfico desejado no país, através do GPS (Geograf Position Satelite), com ampla utilização de mapas urbanos e rodoviários. Também, a possibilidade de se postar mensagens e depoimentos ao perfil de uma pessoa abre precedentes para os chamados crimes contra a honra, como a calúnia, injúria e a difamação.

As comunidades virtuais dão oportunidade ao usuário de poder traçar seu perfil. A partir do momento em que faz a opção de participar de uma determinada comunidade, como por exemplo, “Eu Amo Meus Pais”, “Belém Sampa Connection”, “Mackenzie Mestrado e Doutorado”, “E-Tudo Mais em EAD”, “Apaixonados por Paris”, dentre outras, podem-se identificar alguns traços característicos da pessoa.

As comunidades também têm sido alvo de criminosos, pois através delas pode se descobrir onde o usuário estuda, trabalha ou mora, bem como as suas preferências pessoais.

Note-se, ainda, que o *Orkut* tem sido usado igualmente para manifestar opinião sobre algum acontecimento de grande repercussão, tanto em nível nacional como os internacionais.

Também, as comunidades do *Orkut* têm sido usadas como meio para a prática de crimes em grupo ou para que esses delitos sejam planejados através da internet, como tem sido noticiado com frequência sobre a ocorrência de confrontos entre torcidas organizadas fora dos estádios, por ocasião de grandes clássicos do futebol no Brasil, assim como a organização de pegas em vias públicas e a mobilização para atos de xenofobia.

Cada usuário tem a possibilidade de colocar outros usuários como amigos. Basta fazer o convite e tão logo a pessoa o aceite, ela passa, automaticamente, a fazer parte da mesma rede. Com efeito, o *Orkut* passa a ser uma espécie de banco de dados sobre quem é amigo de quem.

3.1.2 O *Twitter*

Assim como as demais redes sociais, o *Twitter* é um *microbloggin* para trocas de mensagens instantâneas na internet que tomou proporções gigantescas em pouco mais de 4 anos de sua criação, sendo um dos responsáveis pela "debandada" de usuários de outras redes sociais, como o *Orkut* e o *Facebook*, para esta nova tecnologia.

O site Agrega (2009) explica exatamente como surgiu tal tecnologia:

> O *Twitter* nasceu há aproximadamente 3 anos, quando @Jack, @Biz, @Noah, @Crystal, @Jeremy, @Adam, @TonyStubblebine , @Ev, @Dom, @Rabble, @RayReadyRay, @Florian, @TimRoberts e @Blaine trabalhavam em uma empresa chamada Odeo Inc. localizada em South Park, San Francisco. A empresa estava passando por maus bocados pois sofria uma brutal concorrência da Apple e de outros pesos pesados da informática. Em virtude disso, a diretoria adotou a estratégia de "reinventar a empresa".
> "Reinicializar" ou "reinventar" começou com uma divisão de equipes. Cada equipe iria elaborar e explicar suas melhores idéias. O grupo de @Jack descreveu pela primeira vez um serviço que utilizava SMS (mensagens curtas por celular) para pequenos grupos avisando-os sempre sobre "o que você está fazendo". @Jack dizia:
> "Eu quero ter um serviço de envio que nos ligue aos nossos telefones usando texto."
> A idéia era tornar esse serviço tão simples que você não pensasse no que está fazendo, bastava apenas digitar algo, e enviá-lo.
> Posteriormente numa reunião, cada grupo apresentou suas idéias na empresa. Foram selecionadas algumas poucas para prototipagem. Versões demos foram analisadas. A idéia do grupo de @Jack se sobressaiu e subiu ao topo como uma combinação de várias idéias. @Jack, @Biz e @Florian foram incumbidos de construir a versão 0.1, que seria gerenciada pelo @Noah. O resto da empresa ficou focada na manutenção da Odeo.com, para que o grupo de @Jack pudessem se concentrar neste novo projeto sem se preocupar com o dia-a-dia da companhia.

O princípio do *Twitter* é básico: se consiste no envio de uma informação curta e clara a um ou vários usuários, utilizando-se apenas 140 caracteres. Os SMS (sistemas de

mensagens através de celulares) já faziam tal tarefa, o que ocorre de diferente no *Twitter* é que a mensagem fica armazenada publicamente para que todos vejam.

> O *Twitter* pode ser entendido como uma mistura de blog e celular. As mensagens são de 140 toques, como os torpedos dos celulares, mas circulam pela internet como os textos de blogs. Em vez de seguir para apenas uma pessoa, como no celular ou no MSN, a mensagem do *Twitter* vai para todos os "seguidores" – gente que acompanha o emissor. Podem ser 30, 300 ou 409 mil seguidores, como tem Barack Obama. Essa estrutura de troca de mensagens é nova, mas não é o principal.
> A grande novidade do *Twitter* é o ritmo. Por algum motivo inexplicável, as pessoas não param de trocar mensagens. O site do *Twitter* tem uma pergunta básica – "O que você está fazendo?" – e todo mundo responde, várias vezes ao dia: contam que estão almoçando, dizem que o ônibus quebrou, avisam ter visto uma celebridade. Como é possível postar do celular, os twitteiros não descansam na narração do trivial. É um fluxo contínuo de minudências que os americanos chamam de "intimidade ambiental". A comunicação é rápida e contínua, uma pequena e organizada gritaria digital. Visto de fora parece histérico, mas para os envolvidos soa natural. E é um sucesso. (REVISTA ÉPOCA, 13/03/2009)

Através da figura 2, é possível verificar uma página comum do *twitter*, com todas as suas características e as facilidades de acesso.

Figura 2 – Página Inicial do *Twitter*

Fonte: *Twitter* (2010)

O que poucos desconhecem, ou fingem desconhecer, é que o *Twitter* pode ser utilizado para atividades criminosas das mais variadas, uma vez que, assim como no *Orkut*, podem se criar perfis falsos com o intuito de se obterem informações indevidas ou praticar outros crimes.

Em recente reportagem do dia 17/08/2010, cuja matéria encontra-se postada no site Globo.com, foram publicadas fotos do perfil de um jogador de futebol, em que o atleta ofende o árbitro da partida ocorrida no final de semana anterior, praticando assim o crime de calúnia por imputar um crime ao referido árbitro de futebol.

Consta ainda que, ao ser avisado por seus "seguidores"[3], o jogador rapidamente retirou a ofensa do ar, sob a alegação de que houve "invasão" de seu *Twitter* por outrem, não sendo, portanto, ele (o atleta) autor da suposta ofensa.

Figura 3 – Perfil do jogador do Santos Futebol Clube, supostamente ofendendo o árbitro

Fonte: Globo.com (2010)

[3] Seguidor é aquele que adiciona o perfil de uma pessoa para acompanhar suas publicações no *Twitter.*

Ao que tudo indica, as investigações sobre este episódio pararam no campo do Direito Desportivo. É esta impunidade que facilita a ocorrência de tais ocorrências e de outras da mesma natureza, e até mais graves.

Outra descoberta, agora feita pelo *site* I/O Tecnologia (2009), é que o perigo do *Twitter* ainda pode ser maior, pois como as mensagens só têm capacidade para 140 caracteres, quando se enviam *links* para outras pessoas e eles contêm mais caracteres que a regra, tais *links* aparecem de forma simplificada, o que dificulta os meios para se averiguar se a pessoa está sendo direcionada para uma página segura.

Assim, segundo o *site*, se torna fácil a publicação de *links* de downloads de programas maliciosos que possam roubar senhas e dados pessoais das pessoas, pois basta o simples clique no *link* resumido para que estes possam ser executados.

Estes são apenas dois dos exemplos de crimes cometidos pelo *Twitter*, pois, assim como o *Orkut*, existe uma infinidade de práticas delituosas possíveis de serem cometidas, desde a apologia ao tráfico e uso de drogas, o racismo e a pedofilia virtual, além de tantos outros.

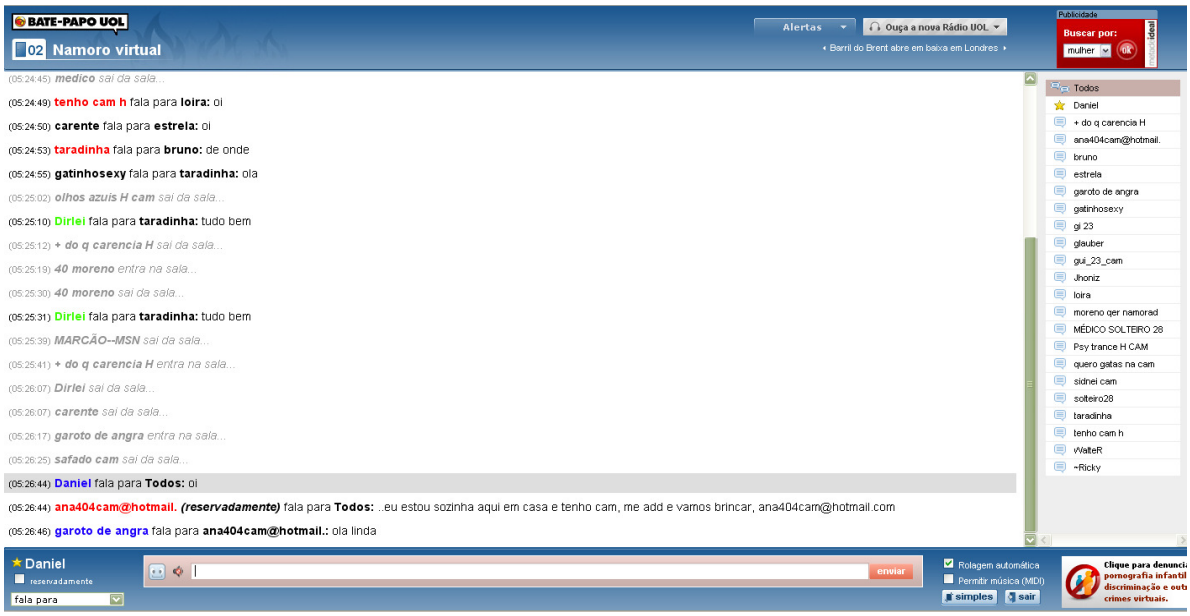
3.1.3 A Salas de Bate-Papo

Ainda mais antigas do que o *Orkut* e o *Twitter*, mas não menos perigosas, são as salas de bate-papo. Estas surgiram com o mesmo intuito dos aplicativos anteriores, ou seja, facilitar a comunicação entre as pessoas e possibilitar o conhecimento de novos indivíduos.

Os *sites* de bate-papo mais conhecidos são o UOL e o TERRA. Através deles, a pessoa escolhe a sala por tema (namoro, sexo, religião, etc.), cidade, idade, entre outros, e pode conversar com inúmeras pessoas ao mesmo tempo, sem saber exatamente quem seja.

A figura 4, a seguir, é exemplo de uma página de bate-papo virtual, em que os assuntos se desdobram em longas conversas, o que facilita aos criminosos obterem informações de seu interesse, para as mais diversas finalidades.

Figura 4 – Exemplo de uma sala de bate papo virtual



Fonte: UOL (2010)

Assim como nas redes sociais, o que ocorre nessas salas de bate-papo é que o usuário mal intencionado pode utilizar nome falso para mentir e/ou omitir informações a seu respeito, com intuito de prejudicar terceiros ou aliciar menores.

Nos crimes de pedofilia com o uso da Internet, na maioria das vezes, o pedófilo se faz passar por alguém mais jovem que sua vítima, a fim de facilitar a conversa e, assim, adquirir a confiança do menor. A partir deste ponto, o indivíduo começa a obter dados da criança ou adolescente, com o intuito de marcar encontros presenciais ou virtuais (pela *webcam*) para a exploração sexual desse menor.

3.1.4 Dados Estatísticos sobre o *Orkut*

Segundo Telles (2005, p. 24):

> O sistema possui atualmente cerca de 13.250.000 usuários cadastrados; o Brasil é o país com maior número de membros, superando inclusive os Estados Unidos; 72,91% dos usuários do sistema são brasileiros; [...] Os Estados Unidos são o segundo país com maior número de membros, possuem uma fatia de aproximadamente 10,59% dos usuários cadastrados.

Diante desses dados, pode-se constatar que a aceitação e utilização do *Orkut*, pelo menos no Brasil, já é expressiva; a maioria de seus usuários inscritos é formada por jovens, em geral estudantes de níveis médio e superior. Sugerem, então, a possibilidade de ser uma ferramenta utilizada para o ensino.

Ainda com relação às redes sociais, o *site* Metamorfose Digital (2010) traz os seguintes dados estatísticos:

Redes sociais

- 126 milhões – O número de blogs na Internet.
- 84% – Percentagem de sites de redes sociais com maior número de mulheres que homens.
- 27,3 milhões – Número de tweets por dia (Novembro, 2009)
- 57% – Percentagem de usuários do *Twitter* que vivem nos Estados Unidos.
- 4,25 milhões – Pessoas que seguem o @aplusk (Ashton Kutcher, o usuário mais seguido do *Twitter*).
- 350 milhões – Pessoas em *Facebook.*
- 500.000 – Número de aplicações para o *Facebook.*

- Imagens
  - 4 bilhões – Fotografias alojadas no Flickr (Outubro 2009).
  - 2 bilhões – Fotografias enviadas cada mês no *Facebook.*

- Vídeos
    - 1 bilhão – O número de vídeos visualizados a cada dia no *YouTube*.
    - 12,2 bilhões – Vídeos visualizados a cada mês no *YouTube* nos Estados Unidos (Novembro 2009).
    - 182 – Número médio de vídeos visto por cada usuário da Internet por mês.
    - 82% – Percentagem de usuários da Internet que vêem vídeos on-line.
    - 39.4% – Quota de mercado de *YouTube.*
    - 81.9% – Percentagem de vídeos compartilhados nos blogs que pertencem ao *YouTube*.

Pode-se observar, pois, que é crescente o número de usuários de redes sociais e sua maioria é composta por mulheres. Ademais, é gigantesco o número de fotos postadas nessas redes, bem como de vídeos, o que demanda um enorme trabalho na busca de fiscalizar os responsáveis pela postagem dessas fotos e vídeos, já que grande parcela desses usuários pode estar envolvida na prática de crimes virtuais, como pedofilia e ofensas à honra de outrem.

A seguir, podem-se observar outras estatísticas relevantes:

- Navegadores *web*
    - 62,7% – Internet Explorer.
    - 24,6% – Firefox.
    - 4,6% – Chrome.
    - 4,5% – Safari.
    - 2,4% – Opera.
    - 1,2% – Outros navegadores.

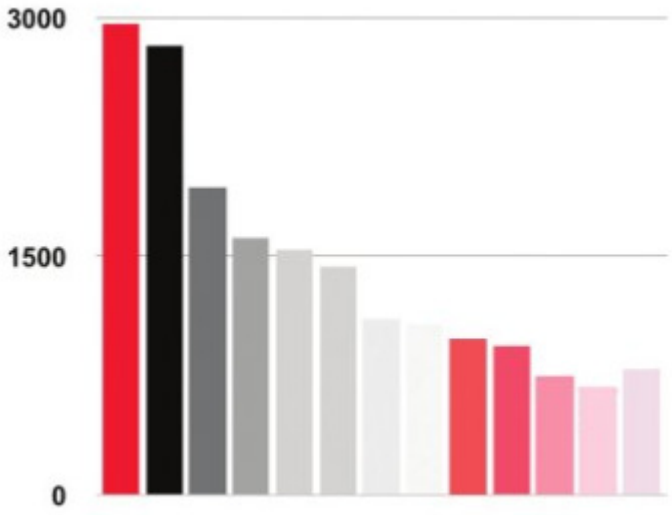
- *Software* malicioso
    - 148.000 – Novos computadores zumbis criadas por dia (utilizadas em redes de botnets para enviar spam, etc.)
    - 2,6 milhões – Número de programas maliciosos no início de 2009 (vírus, trojans, etc.)

Observa-se que a maioria dos usuários opta por utilizar o provedor Internet Explorer, tendo em vista que este já vem com o *Windows*. Outro detalhe é que o número de programas maliciosos cresce assustadoramente, o que dificulta a atualização dos antivírus, que precisam ser cada vez mais rápidos e mais potentes nesses casos.

3.1.5 Dados Estatísticos das Redes Sociais em Geral

A figura 5, a seguir, apresenta os resultados de uma pesquisa realizada pela Revista *Twitter* Brasil, a qual demonstra as ferramentas da *Web* 2.0 mais utilizadas pelos usuários de internet:

Figura 5 – Ferramentas 2.0 que o público usa e utiliza



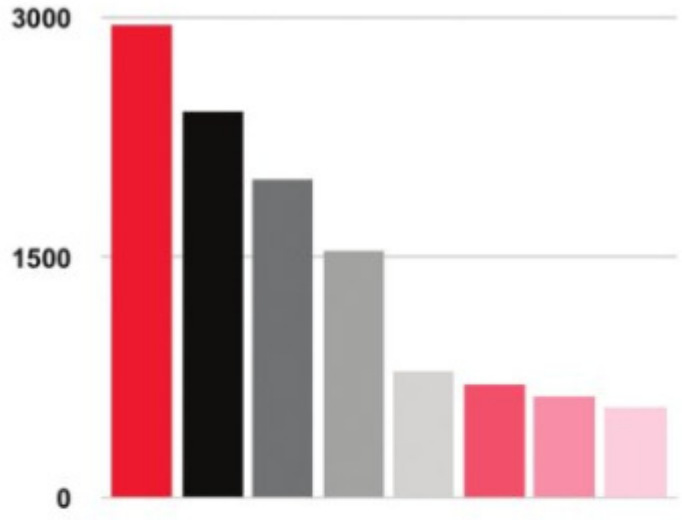
Item	Respostas	%
Orkut	2973	90.97%
Youtube	2831	86.63%
Blog	1937	59.27%
Facebook	1627	49.79%
Flickr	1548	47.37%
Last.fm	1440	44.06%
GoogleReader	1117	34.18%
MySpace	1083	33.14%
Blip.fm	982	30.05%
Delicious	948	29.01%
LinkedIn	755	23.10%
Fotolog	678	20.75%
Outros	791	24.20%

Total de respostas: 3268

Fonte: *Twitter* Brasil (maio/2009)

Através da figura 6, abaixo, pode-se observar que a maioria dos internautas utiliza do *Twitter* para se atualizar.

Figura 6 – Ferramentas que o público utiliza para se atualizar



Item	Respostas	%
Twitter	2961	91.42%
Blogs	2418	74.65%
Portais	1995	61.59%
Indicações de links por amigos	1553	47.95%
Fóruns	795	24.54%
Outros	711	21.95%
E-groups (Lista de e-mails)	640	19.76%
Agregadores de Conteúdo (Sites de Crowdsourcing como Digg, Gafanhoto, Dihitt)	558	17.23%

Total de respostas: 3268

Fonte: *Twitter* Brasil (maio/2009)

3.2 O Comércio Eletrônico e os Documentos Digitais

Outra questão extremamente relevante em termos de crimes cibernéticos está associada às relações comerciais por meio da Internet. Esse sistema de compra e venda por meio eletrônico já atingiu um volume incalculável em todos os continentes e tem

sido utilizado em larga escala, haja vista que oferece uma série de vantagens e facilidades, tanto para as empresas como para os clientes, como comodidade, privacidade, agilidade e redução de custos, dentre outras. Contudo, têm sido cada vez mais frequentes os crimes praticados nessas relações comerciais, sobretudo as fraudes, os golpes e as facilidades de acesso a dados pessoais dos usuários, principalmente informações bancárias e cartões de crédito.

Pode-se definir o *E-commerce* ou comércio eletrônico como todo sistema de realização de compras de bens e serviços, por uma ou mais pessoas, utilizando-se da tecnologia da internet.

Nos dizeres de Albertin (apud MENEZES, 2003, p. 12), pode-se observar que:

> O comércio eletrônico é a realização de toda a cadeia de valor dos processos de negócios num ambiente eletrônico, por meio da aplicação intensa das tecnologias de comunicação e de informação, atendendo aos objetivos de negócio. Os processos podem ser realizados de forma completa ou parcial, numa infra-estrutura predominantemente pública, de fácil e livre acesso, e baixo custo como a Internet.

Assim, esta nova forma de negociar bens e serviços é definida como: processos de negócios feitos pela Internet ou algum sistema não proprietário baseado na *Web*[4]. Na economia tradicional, a forma de negociar bens e serviços é, majoritariamente, presencial, face-a-face, ou ainda por meios eletrônicos como o telefone e o fax. Com a chegada do comércio eletrônico, facilita-se a pesquisa de produtos de diferentes fornecedores, num menor espaço de tempo, e amplia-se, sobremaneira, o mercado de atuação das empresas, que passa a ser global. Os meios de pagamento ampliam-se além dos tradicionais depósitos bancários e cartão de crédito para transações *online* entre vendedor e comprador, aumentando a insegurança das transações.

[4] A World Wide Web -- "a *Web*" ou "WWW" para encurtar -- ("rede do tamanho do mundo", traduzindo literalmente) é uma rede de computadores na Internet que fornece informação em forma de hipermídia, como vídeos, sons, hipertextos e figuras. Para ver a informação, pode-se usar um *software* chamado navegador (*browser*) para descarregar informações (chamadas "documentos" ou "páginas") de servidores de internet (ou "sites") e mostrá-los na tela do usuário.

Segundo Jucá (1998, p. 90), o comércio eletrônico desdobra-se em dois conceitos: “a) *Business-to-Business* (vendas entre empresas); e b) *Business-to-consumer* (vendas para o consumidor de varejo)”.

No que se refere à privacidade, nota-se que têm sido amplamente divulgados os acontecimentos em que as pessoas têm sua privacidade invadida e informações pessoais ou confidenciais disponibilizadas na rede mundial de computadores. Quanto ao crime, a invasão de privacidade está capitulada nos artigos 138, 139 e 140 do Código Penal Brasileiro, os quais são os denominados crimes contra a honra, sendo tais crimes de ação privada, de modo que a Polícia Militar somente pode agir, nesses casos, mediante o acionamento da própria vítima.

3.2.1 Estatísticas Sobre o Comércio Eletrônico

A Tabela 1, abaixo, traz uma estatística mais atualizada referente ao comércio eletrônico em escala mundial, podendo ser observado que o Brasil já ocupa a 6ª colocação nesse *ranking*, com um expressivo crescimento anual.

Tabela 1 - Os 20 países com maior número de usuários da Internet

#	País ou Região	Usuários	Adoção da Internet	% de usuários	População (2008)	Crescimento dos Usuários (2000 - 2008)
1	**China**	**253.000.000**	19,0 %	17,3 %	1.330.044.605	1.024,4 %
2	**Estados Unidos**	**220.141.969**	72,5 %	15,0 %	303.824.646	130,9 %
3	**Japão**	**94.000.000**	73,8 %	6,4 %	127.288.419	99,7 %
4	**Índia**	**60.000.000**	5,2 %	4,1 %	1.147.995.898	1.100,0 %
5	**Alemanha**	**52.533.914**	63,8 %	3,6 %	82.369.548	118,9 %
6	**Brasil**	**50.000.000**	26,1 %	3,4 %	191.908.598	900,0 %
7	**Reino Unido**	**41.817.847**	68,6 %	2,9 %	60.943.912	171,5 %
8	**França**	**36.153.327**	58,1 %	2,5 %	62.177.676	325,3 %
9	**Korea do Sul**	**34.820.000**	70,7 %	2,4 %	49.232.844	82,9 %
10	**Itália**	**34.708.144**	59,7 %	2,4 %	58.145.321	162,9 %
11	**Rússia**	**32.700.000**	23,2 %	2,2 %	140.702.094	954,8 %
12	**Canadá**	**28.000.000**	84,3 %	1,9 %	33.212.696	120,5 %
13	**Turkia**	**26.500.000**	36,9 %	1,8 %	71.892.807	1.225,0 %
14	**Espanha**	**25.623.329**	63,3 %	1,8 %	40.491.051	375,6 %
15	**Indonésia**	**25.000.000**	10,5 %	1,7 %	237.512.355	1.150,0 %
16	**México**	**23.700.000**	21,6 %	1,6 %	109.955.400	773,8 %
17	**Irã**	**23.000.000**	34,9 %	1,6 %	65.875.223	9.100,0 %
18	**Vietnã**	**20.159.615**	23,4 %	1,4 %	86.116.559	9.979,8 %
19	**Paquistão**	**17.500.000**	10,4 %	1,2 %	167.762.040	12.969,5 %
20	**Austrália**	**16.355.388**	79,4 %	1,1 %	20.600.856	147,8 %
Os 20 Mais		**1.115.713.572**	25,4 %	76,2 %	4.388.052.548	284,5 %
Resto do Mundo		**347.918.789**	15,2 %	23,8 %	2.288.067.740	391,2 %
Total - Usuários Mundo		**1.463.632.361**	21,9 %	100,0 %	6.676.120.288	305,5 %

Fonte: www.*e-commerce*.org.br (2010)

De acordo com os dados apresentados em 2008, pode-se observar que o Brasil, apesar do número ainda reduzido de usuários da Internet nas transações comerciais (50 milhões contra os 220 milhões de usuários americanos), registra-se um crescimento da ordem de 900%, anualmente, enquanto que nos Estados Unidos tem-se um crescimento de 130,9%.

3.3 A Pedofilia na Internet

Pode-se assim conceituar pornografia infantil:

> É qualquer representação através de quaisquer meios de uma criança engajada em atividades sexuais explícitas, reais ou simuladas ou qualquer exibição impudica de seus genitais com a finalidade de oferecer gratificação sexual ao usuário, e envolve a produção, distribuição e/ou uso de tal material. (ECPAT apud LIBÓRIO, 2007, p.154)

Os anos finais do século XX e os que inauguram o atual estão sendo marcados por extraordinários avanços na tecnologia da informação e comunicação, e também caracterizados por uma intensa movimentação humana entre territórios, aspectos que produzem fortes e permanentes mudanças geopolíticas. Se a movimentação no meio físico, entre as formas pela qual a ESCCA (Exploração Sexual Comercial de Crianças e Adolescentes) se viabiliza, diz respeito ao tráfico e turismo para este fim, as novas possibilidades de comunicação, no meio virtual, tornaram-se espaço destacado para a pornografia.

Segundo Bauman, a internet, como uma rede mundial e imediata de comunicação, modificou definitivamente o sentido de distância e viagem a ser percorrida pelas informações. Essa nova condição faz da distância não mais um elemento físico, objetivo, mas um produto social. (BAUMAN, 1999)

Tomaz Tadeu da Silva afirma que o termo “discurso” possui diferentes entendimentos de acordo com a perspectiva de análise social em que é empregado. Segundo ele, no contexto da crítica pós-estruturalista, o termo é utilizado para enfatizar o caráter linguístico do processo de construção do mundo social. (SILVA, 2000, p. 43)

Ao serem incorporadas as crianças, adolescentes e/ou seu universo visual simbólico aos discursos pornográficos, esses sujeitos são posicionados como parte da sexualidade que tais imagens propõem (CÂMARA, 2007). Desta forma, ainda que não num movimento consciente, esses mesmos sujeitos passam a integrar o processo de pedofilização, reforçando os significados que suas imagens possuem: o corpo infantil como

naturalmente acessível ao adulto. Assim, a imagem da criança/adolescente utilizada para Exploração Sexual Comercial de Crianças e Adolescentes (ESCCA), através da pornografia, perversamente reforça a pedofilização e o contexto de violência onde ela ocorre.

No documento intitulado Araceli - 31 anos - Impunidade Nunca Mais!, apresentado pelo Comitê Nacional de Enfrentamento à Violência Sexual contra Crianças e Adolescentes e pela ANCED, em 2004, foi destacado o seguinte:

> O Brasil não tem banco de dados unificado sobre crimes cibernéticos e sobre a violência de um modo geral e seus desdobramentos. Quantas violações ocorreram? Quantas foram efetivamente investigadas? Quais os resultados desses procedimentos? Em muitos casos a ausência de informações acoberta culpados e situações de violência continuada. (CPMI, 2004, p.388).

O fato é que a questão da pornografia infantil na internet e, de resto, todos os demais crimes sexuais praticados através da rede mundial ficam, na sua maioria, sem respostas satisfatórias em termos de apuração dos crimes e punição aos criminosos. Como os setores responsáveis, da polícia, estão preparados para lidar com o problema? Onde e como as vítimas podem apresentar suas queixas e terem garantia de resposta aos seus problemas? Como as entidades não governamentais se envolvem na questão? Como os setores do governo se mobilizam para enfrentar o problema? Como os provedores da internet podem colaborar?

A Polícia Militar, como instituição de prestação de serviços públicos de segurança, atua ostensivamente, nos aspectos preventivo e repressivo. A pergunta é sobre como essa Força Pública poderia agir em relação aos crimes de pedofilia na internet. Como o policial militar poderá chegar ao cibercriminoso, prendendo-o em flagrante delito ou mediante mandado? Como os serviços de inteligência poderão contribuir e facilitar o trabalho da polícia nesses casos? Como poderá ser a ação da polícia integrada com outros órgãos de segurança e da Justiça? As respostas a essas perguntas ainda estão por vir, não só da Polícia Militar, mas da parte de todo o aparato policial e dos governos. É sabido que, no Brasil, a primeira força policial a agir na repressão aos crimes cibernéticos deve ser a Polícia Federal, que tem toda a extensão territorial do país como seu campo de atuação, além de agir em parceria com organismos internacionais. Isso deve ser destacado, uma vez que os crimes cibernéticos têm alcance além das fronteiras dos estados e do país, o que dificulta a ação das forças estaduais.

No entanto, o problema não reside exclusivamente na precariedade das políticas públicas, no que se refere à subnotificação identificada nos casos de violência e exploração sexual. A denúncia dos crimes sexuais envolve dimensões complexas, nem sempre enfrentadas pelas campanhas de massa que buscam sensibilizar a sociedade para a proteção infantil, por mais abrangentes que elas sejam.

É na especificidade dos crimes sexuais que reside a dificuldade principal de que ele seja desvelado, impedindo as denúncias. A violência sexual constrói uma aura de segredo em torno de si, marcando a vítima com um tipo de desvalorização e de medo.

3.3.1 Dados Estatísticos da Pedofilia na Internet

De acordo com o *site* do Ministério Público de Santa Catarina, a Associação Italiana Telefono Acrobaleno registrou 42.396 denúncias de *sites* de pedofilia no mundo, o que corresponde a mais do dobro dos casos de denúncia no ano de 2003. Outro fator interessante é que o Brasil é o 4º país com maior número de *sites* hospedados. (MINISTÉRIO PÚBLICO-SC, 2009)

Já outra organização não-governamental situada no Reino Unido, a *Internet Watch Foundation,* registrou 34.000 denúncias no mesmo ano, sendo que 74% dos casos confirmados são de *sites* que realizam a venda de pornografia infantil. Ainda de acordo com o Ministério Público de Santa Catarina (2009), “O mercado de compra e venda de pornografia infantil é suspeito de movimentar cifras milionárias em todo o mundo.”

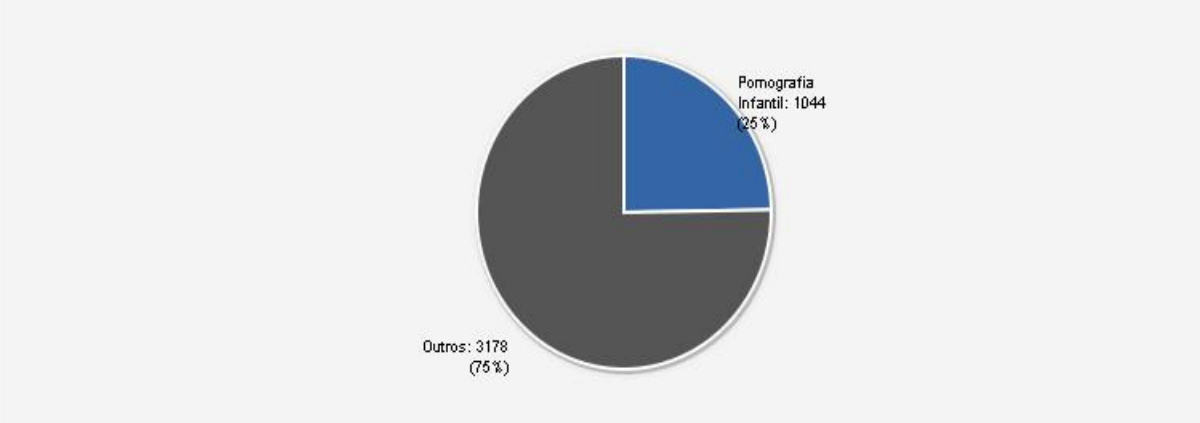
Aqui no Brasil existe o *site* da ONG SaferNet, o qual recebeu 36.584 denúncias sobre casos de pedofilia na internet no período entre janeiro e setembro de 2009, dos quais 72% são relativos aos álbuns de fotos do *Orkut*, de acordo com os dados do Ministério Público de Santa Catarina (2009).

Por oportuno, ao se levantar os dados diretamente no *site* SaferNet, relativos ao ano de 2010, chegou-se aos seguintes números:

Gráfico 5/Tabela 2 – Denúncias de Cibercrimes ao *site* SaferNet em 2010

Denúncias de **1 de Julho de 2010** a **1 de Agosto de 2010**

Tipo de conteúdo	Período de 2010-7-1 a 2010-8-1	
	Únicas	Domínio Orkut
Intolerância Religiosa	99	64
Racismo	455	393
Neo Nazismo	164	137
Tráfico de Pessoas	21	15
Pornografia Infantil	1873	1044
Maus Tratos Contra Animais	277	203
Xenofobia	799	755
Apologia e Incitação a crimes contra a Vida	978	851
Homofobia	795	760
Todos	**5461**	**4222**



Fonte: SaferNet (2010)

3.4 O *Bullyng* e o *Cyberbullyng*

O *bullying* nada mais é do que a brincadeira agressiva e/ou ofensiva que venha a causar danos psicológicos a outrem ou ofensas à sua moral. É considerada, pois, uma violência psicológica.

Albino e Terêncio (2009, p. 1) definem o *Bullying* como:

> {...} todas as atitudes agressivas, intencionais e repetitivas adotadas por uma pessoa ou um grupo contra outro(s), causando dor, angústia e sofrimento. Tal forma de violência ocorre em uma relação desigual de poder, caracterizando uma situação de desvantagem para a vítima, a qual não consegue se defender com eficácia.

De acordo com os autores, apesar de a expressão ser nova (criada na Inglaterra), para os brasileiros, as situações de *bullying* são bastante conhecidas. Elas se configuram pelas ofensas, chacotas e demais violências psicológicas que são muito comuns entre crianças e adolescentes. Normalmente essas ofensas se dão em ambiente escolar e podendo ser observadas também entre professores e alunos. (ALBINO; TERÊNCIO, 2009)

Alguns autores, como Martins (2005, apud ALBINO; TERÊNCIO, 2009, p. 2) classificam o *bullying* em três formas, quais sejam:

> A primeira envolve comportamentos “diretos e físicos”, o que inclui atos como agredir fisicamente, roubar ou estragar objetos alheios, extorquir dinheiro, forçar comportamentos sexuais, obrigar a realização de atividades servis, ou a ameaça desses itens. A segunda forma inclui comportamentos “diretos e verbais”, como insultar, apelidar, “tirar sarro”, fazer comentários racistas, homofóbicos ou que digam respeito a qualquer diferença no outro. Por último, há os comportamentos “indiretos” de *bullying*, como excluir sistematicamente uma pessoa, fazer fofocas ou espalhar boatos, ameaçar excluir alguém de um grupo para obter algum favorecimento ou, de maneira geral, manipular a vida social de outrem.

Definido o *bullying* em sua forma comum e conceitual, pode-se destacar a conceituação de *cyberbullying*, no mundo virtual. O *Ciberbullying* ou *Bullying* através da Internet tomou alguns contornos diferentes do *bullying* comum.

O primeiro deles é que o ambiente em que se realizam as atividades do *cyberbullying* é o meio virtual, ou seja, através das redes sociais, como *Orkut*, *Facebook* e *Twitter*; meios de comunicação como MSN e *Skype*; e através de *sites* e *blogs*.

No concernente às redes sociais, o *bullying* se dá conforme já mencionado anteriormente, ou seja, através de ofensas nessas redes, ameaças, dentre outras formas de constrangimento e ameaças.

O *site* Observatório da Infância publicou, em 18 de janeiro de 2008, uma reportagem a respeito de uma jovem americana de 13 anos que suicidou-se ao sofrer *cyberbullying* através da rede social My Space. Segundo *o site*, a vizinha da adolescente e sua mãe criaram um perfil falso de um homem que supostamente estaria interessado na menina. Com o passar do tempo, começaram as perseguições desse suposto amante, quando a garota recebia diversas ofensas por mensagens, até o dia em que a menina caiu em depressão e se enforcou com um cinto.[5]

O *Cyberbullying* através dos meios de comunicação virtuais, como MSN e *Skype* podem se dar por escrito ou através da voz, quando se tratar de chamadas de voz e/ou vídeo. Nesses casos, normalmente, o agressor já é conhecido da criança e/ou do adolescente e se aproveita da intimidade adquirida através de várias conversas para agredir a vítima.

No concernente aos sites e blogs, não há o contato direto conforme ocorre nos outros meios. Na maioria das vezes, o ofensor é o dono do *site* ou *blog* e se utiliza de um perfil falso para publicar agressões a determinada pessoa. Outra opção encontrada pelo agressor é postar nos comentários de *sites* e *blogs* de terceiros (ou até mesmo da pessoa a ser agredida), contudo, há a desvantagem da moderação de comentários, onde o responsável pelo *blog* tem o poder de aceitar ou não tal comentário.

Por oportuno convém ressaltar que o *Cyberbullying* tem outra particularidade que o diferencia do *bullying* comum, que é o agente ativo do crime. O agente passivo continua sendo a criança ou o adolescente, contudo, o agente passivo pode vir a ser qualquer pessoa que realize a ofensa psicológica, uma vez que o ambiente não é mais apenas o escolar, e sim, um mundo virtual, do qual todos têm acesso na atualidade.

[5] Para maiores detalhes, confira a reportagem na íntegra, através do endereço eletrônico: http://www.observatoriodainfancia.com.br/article.php3?id_article=296.

3.5 Os crimes cibernéticos

Blum e Abrusio (2004, p.86) classificam a prática de crimes cibernéticos como delitos informativos que utilizam ambiente virtual e que possuem certa complexidade por exigirem solução rápida e especializada.

Crimes cibernéticos consistem em qualquer atividade ilegal usando componentes da internet, como *sites* de relacionamento, salas de bate-papo ou *e-mails*. O crime cibernético pode incluir tudo, desde a não-entrega de mercadorias ou serviços até roubo de identidade em uma lista crescente de infrações facilitadas pela internet (LARKIN, 2006, p.20). A lista abaixo mostra alguns tipos de Crimes Cibernéticos (QUINTILIANO, 2007, p.52):

- Fraude cibernética;
- Falsificação;
- *cyberstalkin*;
- Terrorismo cibernético;
- Pornografia envolvendo crianças ou adolescentes;
- Disseminação de programas maliciosos;
- Furto;
- Apropriação Indébita;
- Vandalismo;
- Crime do colarinho branco;
- Sabotagem ou espionagem industrial;
- Divulgação de segredo;
- Ameaça;
- Apologia ao crime ou fato criminoso;
- Crime organizado;
- Estelionato;
- Falsa identidade;
- Lavagem de dinheiro;
- Tráfico de drogas.

Através do Quadro 1 (abaixo), é possível identificar os crimes cibernéticos mais praticados no Brasil e sua tipificação no Código Penal, embora não exista, ainda, uma legislação que trate especificamente desses delitos. O enquadramento aqui verificado é a

lógica que norteia a ação penal, de modo que, mesmo não havendo uma legislação que trate do assunto, é possível a aplicação da lei em todos eles.

Quadro 1 – Ações criminosas cibernéticas e sua tipificação

AÇÃO	TIPO	ARTIGO Código Penal
Falar em um *chat* que alguém cometeu algum crime	Calúnia	Art.138 do C.P.
Dar *forward* para várias pessoas de um boato eletrônico	Difamação	Art.139 do C.P.
Enviar um *e-mail* para pessoa dizendo sobre características (gorda, feia, vaca, etc.)	Injúria	Art.140 do C.P.
Enviar um *e-mail* dizendo que vai pegar a pessoa	Ameaça	Art.147 do C.P.
Enviar um *e-mail* para terceiros com informação considerada confidencial	Divulgação de segredo	Art.153 do C.P.
Enviar um vírus que destrua equipamento ou conteúdos	Dano	Art.163 do C.P.
Copiar um conteúdo e não mencionar a fonte, baixar MP3	Violação ao direito autoral	Art.184 do C.P.
Criar uma comunidade *on-line* que fale sobre pessoas e religiões	Escárnio por motivo de religião	Art.208 do C.P.
Acessar sites pornográficos	Favorecimento da prostituição	Art.228 do C.P.
Criar uma comunidade para ensinar como fazer “um gato”	Apologia ao crime ou criminoso	Art.287 do C.P.
Enviar *e-mail* com remetente falso (caso comum de *spam*)	Falsa identidade	Art.307 do C.P.
Fazer cadastro com nome falso em uma loja virtual	Inserção de dados falsos em sistema	Art.313-A do C.P.
Entrar na rede da organização ou de concorrente e mudar informações (mesmo que com uso de um *software*)	Adulterar dados em sistema de informações	Art.313-B do C.P.
Se você recebeu um *spam* e resolve devolver com um vírus, ou com mais *spam*	Exercício arbitrário das próprias razões	Art.345 do C.P.
Participar de casino *on-line*	Jogo de azar	Art.50 da L.C.P.
Falar em um *Chat* que alguém é isso ou aquilo por sua cor	Preconceito ou discriminação raça, cor, etnia.	Art.20 da Lei 7.716/89
Ver ou enviar fotos de crianças nuas *on-line*	Pedofilia	Art.247 da Lei 8.069/90
Usar logomarca de organização em um *link* na página da *internet*, em uma comunidade, em uma matéria, sem autorização do titular, no todo ou em parte.	Crime contra a propriedade industrial	Art.195 da Lei 9.279/96.
Emprega meio fraudulento, para desviar clientela de outrem, por exemplo, uso da marca do concorrente como palavra-chave ou *link* patrocinado em buscador.	Crime de concorrência desleal	Art.195 da Lei 9.279/96
Usar cópia de *software* sem ter a licença para tanto	Crimes contra *software* “Pirataria”	Art.12 da Lei 9.609/98

Fonte: NG (2007)

Assim, existe um número significativo de crimes cibernéticos que podem configurar invasão de sistemas, pedofilia na internet, calúnia e difamação nas redes sociais, dentre outros. Um dos crimes mais praticados é o acesso não autorizado a dados pessoais, com a finalidade de se obter informações sobre conta bancária, senha e cartão de crédito.

> O acesso não autorizado (unauthorized access) consiste em acessar ilicitamente ou abusar de um sistema de informática para interceptar transmissões e/ou subtrair informação relevante. Já a alteração de dados (data alteration) funda-se em alterar os conteúdos de uma transação durante uma transmissão, tais como "user names", números de cartões de crédito, quantias envolvidas, etc. A monitorização (monitoring) baseia-se em espiar informações confidenciais que são trocadas durante uma transação. O spoofing consiste num site falso passando por servidor de modo a acessar ilicitamente dados de potenciais clientes ou simplesmente tentando sabotar o serviço prestado pelo servidor. A negação de serviço (service denial) consiste na negação de acesso ao serviço, ou até ao encerramento do mesmo. Por fim, a repudiação (repudiation) - ocorre quando uma das partes envolvidas na transação nega que a mesma aconteceu ou foi autorizada. (BERNARDINO, et al, 2004, p. 11)

Já em 1999, Castells (apud SANTOS, 2009, p. 44) já destacava que:

> [...] A novidade não é o maior grau de penetração do crime e seu impacto na política. A novidade é a conexão global do crime organizado, condicionando relações internacionais, tanto econômicas como políticas, à escala e ao dinamismo da economia do crime.

3.6 O conceito de *Hacker* e *Cracker* e sua Identificação

Importante destacar que os criminosos cibernéticos podem ter uma série de objetivos diferentes.

Seguem abaixo os principais objetivos dos criminosos cibernéticos (REIS, 2002):

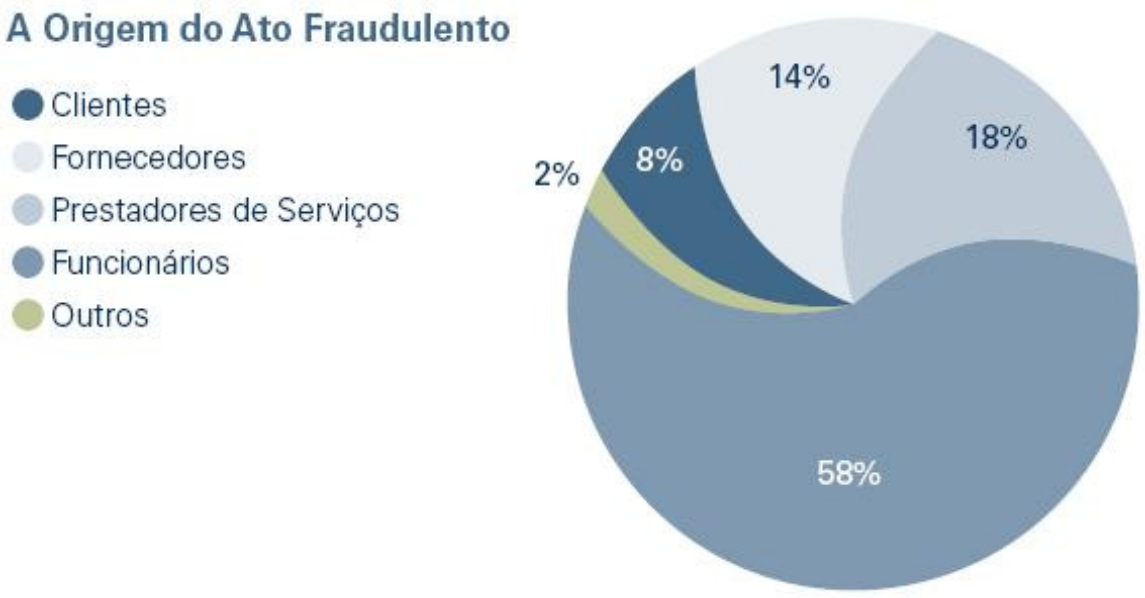
- Diversão;
- Desafio;
- Reconhecimento;
- Espionagem;
- Vingança;
- Causas políticas e sociais;
- Vantagens financeiras ilícitas.

De acordo com Militelli (2008, p.20), um conjunto de fatores psicológicos (conscientes ou não) de ordem intelectual ou afetiva, que agem entre si, determina a conduta de um indivíduo. A engenharia social é o termo mais usado para qualificar fraudadores no ambiente tecnológico e os comportamentos mais comuns são:

- Ataca o lado mais fraco do sistema;
- Torna-se confiável;
- Passa-se por um colega de trabalho que nunca foi visto, ou secretário de um superior;
- Misturam em seu questionário perguntas inofensivas para não levantar suspeita (parte do princípio que para saber, basta perguntar na maioria das vezes);
- Mais do que uma pessoa de tecnologia, é um mestre nas relações interpessoais.

MARTINS (2005, p.12)

Figura 2 – A origem do ato fraudulento – Estatística



Fonte: (BUNCE, 2008, p.28)

Conforme já abordado neste estudo, a Internet se tornou parte do cotidiano das pessoas, num processo irreversível. Com isso, os crimes cibernéticos afetam consideravelmente o estado físico e emocional das vítimas, tendo em vista os transtornos decorrentes dos impactos causados, sobretudo os traumas, os prejuízos financeiros, a

invasão de privacidade e da intimidade das pessoas, os delitos contra crianças e adolescentes. Dependendo do tipo de crime, as pessoas podem ser afetadas psicologicamente (como nos casos de *bullying*, difamação, dentre outros), financeiramente (crimes do comércio eletrônico, estelionato) e até fisicamente (terrorismo, tráfico de mulheres, pedofilia).

3.6.1 O *Hacker*

As empresas vêem o *hacker* apenas como um invasor, que tem o intuito de prejudicar seus ambientes computacionais. Entretanto, convém ressaltar que os profissionais de segurança também precisam conhecer as técnicas de invasão, para que possam proteger, delas, as empresas. Assim, existem 2 tipos de *hackers*: o invasor criminoso e o que cuida da segurança das empresas.

Para Martins (2005, p.55), os profissionais de segurança *hackers* tendem a criar sistemas de proteção mais sólidos, evitando falhas no desenvolvimento que possam possibilitar invasões.

De acordo com o portal G1, em reportagem de Altieres Rohr (2009), o termo "*Hacker*" tanto pode ser entendido como um elogio quanto como um insulto, devido a estas diferenças. De acordo com a reportagem constante desse portal:

> A definição mais conhecida é a de que um *hacker* é um criminoso que usa suas habilidades com computadores para seu próprio proveito. O roubo de senhas, contas bancárias e criação e disseminação de vírus seriam atividades *hacker*, realizadas por pessoas que violam a segurança de sistemas ilegalmente.
>
> [...]
>
> A definição que trata de crimes, no entanto, está marcada como "obsoleta". Para Raymond e outros membros da cultura *hacker*, quem comete crimes é chamado de *cracker*. Os *hackers* verdadeiros -- e o Jargon diz ser o primeiro a usar o termo -- nada têm a ver com eles. (ROHR, 2009)

Assim, o *Hacker* é definido como aquele que trabalha com a segurança dos sistemas e/ou trabalham com *softwares* de código livre ou aberto, com o intuito de melhorá-los. O *Cracker* é que é conhecido como criminoso, conforme se verá a seguir.

3.6.2 O *Cracker*

Já o *cracker* tem a função de invadir e destruir os sistemas, bem como se utilizar dos mesmos procedimentos para aplicar golpes. Ele consegue obter diversas informações do sistema pela própria internet, enquanto planeja seu ataque.

Uma dessas fontes é o site da Febraban - Federação Brasileira dos Bancos - que fornece informações sobre as tecnologias que os bancos utilizam, o número de clientes que acessam o Internet Banking, os serviços que os bancos terceirizam, o volume de transações bancárias através da internet, dentre outros.

3.7 A Presunção de Inocência, Contraditório e Provas Irrepetíveis em Cibercrimes

No que diz respeito aos cibercrimes, o Ministério Público Federal (2006, apud OAB/SP, 2009, p. 80), em seu Manual Prático de Investigação assim destacou:

> De modo geral, podemos dizer que as evidências dos crimes cibernéticos apresentam as seguintes características:
>
> a) possuem formato complexo (arquivos, fotos, dados digitalizados etc);
>
> b) são voláteis, i.e., podem ser apagadas, alteradas ou perdidas facilmente;
>
> c) costumam estar misturadas a uma grande quantidade de dados legítimos, demandando, por isso, uma análise apurada pelos técnicos e peritos que participam da persecução penal.

No caso dos cibercrimes, a dificuldade em se refazer a prova está no fato de se poder apagar, modificar e transferir os dados disponíveis na internet, no computador ou em outros objetos como *pendrives*, CDs e DVDs.

Apesar dessa dificuldade técnica na obtenção de dados, vale destacar que já existem *softwares* capazes de recuperar dados apagados, os quais estão sendo utilizados pela Polícia Federal, conforme destaca a OAB/SP (2009, p. 77):

> Foram desenvolvidas técnicas forenses digitais a exemplo da ferramenta Encase que recupera dados dos discos duplicados e permite que o perito tenha alta produtividade na busca de indícios ou provas contidas na mídia suspeita. Atualmente, a EnCase já está sendo usada por polícias federais, civis e ministérios públicos brasileiros, como também por instituições financeiras e empresas de telecom. Tais ferramentas constituem elementos fundamentais no que tange a identificação de autoria e materialidade do delito, instando destacar que as evidências no meio eletrônico deixam provas complexas e conhecimento especializado para sua coleta.
> Também a Microsoft Brasil e a Polícia Federal que se unem para lançar a versão local do CETS – Child Exploitation Tracking System ("KÉTS") ou Sistema de Rastreamento de Exploração Infantil, um projeto internacional cujo objetivo é o de combater a exploração on-line de crianças. A ferramenta rastreia sites suspeitos e permite intercâmbio de informações entre diferentes países além de permitir que a força policial brasileira se torne ainda mais efetiva em sua luta neste crime abominável e que não respeita fronteiras.

Assim, as provas de crimes cibernéticos são irrepetíveis, devido a esta constante mutação do mundo virtual, o que impossibilita verificar se a prova ainda existe. Também deve-se salientar que os Princípios da Presunção de Inocência e do Contraditório são princípios norteadores de todo o processo penal e, por isso, também devem ser aplicados aos crimes cibernéticos.

3.8 Prisão em Flagrante e Prisão Preventiva em Cibercrimes

A prisão preventiva é uma modalidade de prisão cautelar, cujo nome vem de *cavere*, do latim, ter cuidado, prevenir-se (em alemão, *Shicherung*). Cautela, significa tutela, defesa, proteção. É a prisão preventiva uma garantia, uma proteção da sociedade e que acaba por atingir, isoladamente, um ou vários cidadãos.

A expressão prisão preventiva ou custódia preventiva oferece duas acepções: uma, no sentido lato, e outra restrita. No primeiro sentido é a que se verifica antes do

julgamento irrecorrível. É qualquer detenção ou custódia sofrida pelo imputado, antes ou depois da pronúncia e em qualquer estado da causa, antes do trânsito em julgado definitivamente.

Nessa acepção, ela abrange: a) a prisão em flagrante delito; b) a que resulta da pronúncia; c) a decretada pelo juiz formador da culpa, antes da pronúncia e fora do flagrante delito. A essa última espécie, entretanto, é que comumente se aplica a designação, e é a ela que se refere o artigo.

Em sentido restrito e tendo-se em vista o Código de Processo Penal Brasileiro, ela é a privação da liberdade decretada pelo juiz, no inquérito ou na instrução criminal.

Flagrante deriva do latim *flagran*, *flagrantis*, verbo *flagare*, que significa ardente, crepitando, brilhante. Flagrante delito é o que se vê praticar e que assim suscita, no próprio instante a necessidade de conservar ou restabelecer a ordem jurídica, ameaçada pela violação ou violada pelo acontecimento, ou seja, é a ardência do crime a certeza visual do crime. Será considerado juridicamente como flagrante o delito que está sendo cometido, praticado, é o ilícito patente, irrecusável, insofismável, que permite a prisão do seu autor, sem mandado, por ser considerado a certeza visual do crime.

Hélio Tornaghi, que considera “crime flagrante”, o que está sendo perpetrado. (TORNAGHI, 1963, p. 261)

Fernando da Costa Tourinho Filho expõe o significado da expressão, como “o delito, no instante mesmo de sua perpetuação, o delito que está sendo cometido, que ainda está ardendo (...)”. (TOURINHO FILHO, 1998, p. 371)

Assim, flagrante quer dizer delito em chamas, crime praticado naquele momento. Está ocorrendo ou acabou de acontecer.

Para Magalhães Noronha, ao lembrar os dizeres do Des. Rafael Magalhães, o flagrante seria “a certeza visual do crime”. (NORONHA, 1997, p. 372)

Devido à mutabilidade permanente da Internet, não é em todos os casos de cibercrimes que se consegue a prisão em flagrante. Nos casos de combinação de crimes e tráfico de mulheres, por exemplo, ainda se pode conseguir o flagrante, quando o criminoso combinar qualquer ação com outros criminosos ou com suas vítimas.

A pedofilia por meio da Internet é outro crime em que se consegue a prisão em flagrante, tendo em vista que tal crime pode se dar também de forma permanente, como a manutenção de fotos de crianças nuas nos computadores do criminoso e nas demais mídias digitais. Outras modalidades de crimes também podem ser passíveis de prisão em flagrante, desde que a polícia tenha capacidade técnica para identificar os seus autores e estrutura adequada para efetuar a prisão no momento em que se constatar o ato delituoso, sem descaracterizar o estado de flagrância, como os crimes contra o sistema financeiro, os diversos tipos de golpes, os estelionatos, os crimes do comércio, a xenofobia, o terrorismo, o tráfico de drogas, a extorsão e as várias tentativas de crime.

São notórios na mídia diversos casos em que se conseguiu prender em flagrante delito um pedófilo, a partir da constatação e comprovação da existência de diversos materiais relativos às suas vítimas em seus computadores pessoais. Já nos crimes de comércio eletrônico, há uma dificuldade maior na obtenção do flagrante, uma vez que seu tempo de execução pode ser rápido. Contudo, o flagrante não é impossível. Podem se ter casos em que os criminosos continuem lesando uma pessoa física e/ou jurídica e esta alertar a polícia para que seja feito o flagrante no momento da operação.

3.9 A Busca e Apreensão Domiciliar em Cibercrimes

A Busca e Apreensão domiciliar em Cibercrimes é um importante procedimento para a polícia investigativa na apuração desses delitos, pois é através do acesso aos arquivos disponíveis nos computadores em poder dos criminosos que se poderá fazer a perícia para o rastreamento das informações necessárias.

Os Procuradores da República do Grupo de Combate ao Crime Cibernético, em entrevista ao *site* da Procuradoria da República no Estado de Goiás (PR/GO, 2010), teceram os seguintes esclarecimentos:

> Para comprovar a materialidade do crime cibernético, temos que buscar os elementos de prova no local em que houve a prática e onde os vestígios foram deixados, ou seja, na rede mundial de computadores. Portanto, tanto a materialidade quanto a autoria delitiva são buscadas por meio de sucessivas quebras de sigilo de dados telemáticos. Posteriormente, quando se chega ao local de onde partiu a conexão que deu origem àquele conteúdo ilícito, é expedida ordem de busca e apreensão e enviado o equipamento para perícia. Há casos em que se faz necessária a interceptação telemática, porém, ainda enfrentamos certas dificuldades na sua implementação devido à alegação de algumas empresas de apenas se submeterem, neste caso, à legislação do local de sua matriz, geralmente EUA, mesmo após deferimento de ordem judicial.

Os Representantes do Ministério Público ainda destacam dois métodos de investigação de tais crimes quais sejam:

> Primeiro, a identificação do criminoso a partir dos rastros deixados por ele na rede (quebra judicial de sigilo de dados telemáticos até se chegar ao local de onde partiu a conexão ligada à conduta ilícita, sendo, após uma prévia verificação, requerida a expedição de mandado de busca e apreensão para perícia no equipamento) e, por fim, a interceptação telemática de dados em tempo real. (PR/GO, 2010)

Observa-se, pois, que a busca e apreensão é de grande relevância para solução de tais crimes, tendo em vista que se pode apreender o equipamento utilizado pelo criminoso, quer seja dele ou de terceiros, para que se possa fazer a análise pericial visando à comprovação do delito.

3.10 A Legislação Atual sobre os Crimes Cibernéticos

Preliminarmente, cumpre ressaltar que em 2001 foi realizada a Convenção sobre Cibercriminalidade do Conselho da Europa, a qual teve a participação de representantes de países não integrantes da Comunidade Européia como Japão, Canadá, Estados Unidos e África do Sul.

Um dos resultados concretos da Convenção foi a tipificação de algumas condutas delituosas na esfera virtual, as quais poderiam ser aceitas pelos demais países. Tais condutas são:

> 1. Infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos:
>
>   a) acesso doloso e ilegal a um sistema de informática;
>   b) interceptação ilegal de dados ou comunicações telemáticas;
>   c) atentado à integridade dos dados (conduta própria de um subgrupo *hacker*, conhecido como *cracker*);
>   d) atentado à integridade de um sistema;
>   e) produção, comercialização, obtenção ou posse de aplicativos ou códigos de acesso que permitam a prática dos crimes acima indicados.
>
> 2. "Infrações informáticas":
>
>   a) falsificação de dados;
>   b) estelionatos eletrônicos (v.g., os *phishing scams*).
>
> 3. Infrações relativas ao conteúdo:
>
>   a) pornografia infantil (produção, oferta, procura, transmissão e posse de fotografias ou imagens realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito);
>   b) racismo e xenofobia (difusão de imagens, idéias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica; injúria e xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade).(PR/SP, 2006, p. 10)

De acordo com a Procuradoria da República do Estado de São Paulo (PR/SP, 2006), o Brasil, visando também obter uma legislação a respeito dos cibercrimes, procurou tratar de forma mais sistemática tais condutas, com a criação do Projeto de Lei nº 84/99, na Câmara Federal, de autoria de um parlamentar daquele Estado.

Contudo, em novembro de 2003, um Senador da República propôs um substitutivo para o Projeto de Lei, com o intuito de adequá-lo ainda mais às normas internacionais e se evitar lacunas na legislação. O substitutivo assim delineava:

> a) No capítulo dos crimes contra a administração pública, o art. 313-A do Código Penal sanciona a conduta de "inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano";
> b) O art. 313-B contém a hipótese de "modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente";
> c) A divulgação, sem justa causa, de informações sigilosas ou reservadas contidas ou não nos sistemas de informações ou banco de dados da Administração Pública é sancionada pelo art. 153, § 1o-A;
> d) Ao servidor que viola o sigilo funcional, permitindo ou facilitando, "mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública", ou que se utiliza, indevidamente, do acesso restrito, há a incidência das penas previstas no art. 325 do Código Penal;
> e) A Lei 10.764, de 12 de novembro de 2003, modificou a redação do art. 241 do Estatuto da Criança e do Adolescente para explicitar a possibilidade do crime de pornografia infanto-juvenil ser praticado pela rede mundial de computadores. Além disso, previu a responsabilidade criminal daquele que "assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas" ou "assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens de pedofilia" (cf. item seguinte);
> f) Além dos tipos penais que fazem menção explícita à informática, há outros em relação aos quais é possível haver a subsunção de condutas ilícitas executadas por meio da internet: o *cracker*, por exemplo, pode estar incurso no crime de dano, descrito no art. 163 do Código Penal. A prática ou incitação do racismo é reprimida pelo art. 20, caput e § 2º, da Lei 7.716/89. O *phishing scam* subsume-se perfeitamente ao delito de estelionato.

Como se pode observar, a tramitação dos projetos de lei sobre crimes cibernéticos é extremamente lenta nas casas legislativas, nas três esferas de poder, enquanto que os criminosos avançam de maneira acelerada na busca de novos procedimentos para obterem vantagens e burlar o sistema. Urge que se tomem medidas eficazes e rigorosas, que tenham efeitos práticos com rapidez e oportunidade, pois, do contrário, há o risco de se chegar a uma situação quase que incontrolável em relação aos cibercrimes no Brasil. A falta de uma legislação específica, rigorosa e eficaz dificulta as forças policiais de agirem preventiva e repressivamente no enfrentamento aos crimes virtuais e, de resto, cria embaraços e limitações para todo o sistema de segurança, além de impedirem o Poder Judiciário e o Ministério Público de agirem na esfera de suas competências.

4 AS LAN HOUSES E A QUESTÃO DO ANONIMATO

Importante destacar que muitos criminosos se utilizam das *lan houses* para dificultar a atuação da polícia no rastreamento de informações a seu respeito. Assim, o presente capítulo tratará de conceituar *lan house* e destacar a questão atinente ao anonimato de seus usuários.

4.1 Conceito e Funcionamento de *Lan Houses*

Uma *Lan House* é uma construção social de três camadas. Cada uma delas sendo constituída por uma série de aspectos próprios. Entre a primeira e a terceira camada, ocorre uma transição entre os aspectos objetivos e físicos até os mais subjetivos e simbólicos. A segunda camada mescla diversos aspectos, tanto os relacionados às características físicas do lugar, quanto uma representação estética.

LAN significa *Local Area Network* - rede de área local. Tecnicamente significa uma rede informatizada onde vários terminais e equipamentos estão todos dentro de curta distância uns dos outros (a uma distância máxima de 500 metros no mesmo edifício) e podem ser interconectados por cabos. *Lan House* é um estabelecimento comercial que, possuindo vários computadores interconectados em rede, possibilita que várias pessoas joguem jogos de Realidade Virtual e acessem a Internet. (Feres Neto, 2005).

Para se estabelecer uma avaliação mais consistente a respeito dos avanços das *lan houses* no Brasil, faz-se aqui uma comparação sobre o uso desses estabelecimentos na Coreia do Sul. As *Lan Houses* estão para a Coreia do Sul, assim como os “campinhos de futebol” estão para o Brasil. Lá existem vinte mil *Lans*. Sabe-se que, nesse país, 30% da população está registrada em jogos *on-line*; foi onde surgiram os primeiros “videogames” profissionais e onde surgiram os primeiros campeonatos internacionais de jogos virtuais (Vianna, 2004). A informática está tão desenvolvida nesse país que quase a totalidade da população possui um computador pessoal. Enquanto no

Brasil, entre os anos de 2002 e 2007, a posse de computador entre a população passou de 17% para 34%, na Coreia do Sul ela passou de 86% para 93% (Pew Institute, 2007).

Ambientes como as *Lan Houses* se propagaram muito na última década, com os avanços da informática. Se quiséssemos encontrar um referente no passado, ele estaria nas casas de fliperama. Elas também possuíam equipamentos para jogos eletrônicos. Nas décadas de setenta e oitenta, eram os locais onde os jovens encontravam o divertimento eletrônico proporcionado pelos vídeo games.

4.2 O Anonimato dos Frequentadores de *Lan Houses*

As *Lan Houses* são estabelecimentos frequentados predominantemente por jovens que praticam jogos virtuais, ou que vão até lá para acessarem sua página pessoal do Orkut. O espaço da loja acaba se tornando um ponto de encontro de jovens, para a prática de sociabilidade e reunião de turmas.

No Brasil, nos últimos anos, com a situação econômica estável e a oferta de crédito facilitada, tornou-se comum, e ao alcance da maioria dos brasileiros, a aquisição de computadores e o acesso à internet em casa e quase que em todos os lugares, com os computadores portáteis. Contudo, paralelamente a essa mudança, tornou-se comum, também, o acesso à internet através das *lan houses* espalhadas nos centros urbanos, por ser de fácil acesso e de baixo custo. Um desses motivos está relacionado à privacidade dos seus usuários, tendo em vista que esses indivíduos querem fugir da “fiscalização” existente em suas casas, do trabalho ou da escola. A busca dessa privacidade leva também ao interesse pelo anonimato, pois muitas vezes se quer acessar conteúdos proibidos, praticar atos ilícitos ou realizar determinadas atividades na internet sem que ninguém o saiba.

De um modo geral, o universo das *lan houses* dificulta a identificação de seus usuários, haja vista que não há um controle sistematizado dos indivíduos que lá comparecem e nem uma identificação dessas pessoas, capaz de se chegar a quem utilizou tal equipamento em tal data e horário e, muito menos, qual o conteúdo acessado ou

enviado. Caso eles cometam algum delito pela internet, torna-se difícil para a polícia chegar à autoria, pelas dificuldades técnicas. Não há, pelo poder público municipal, uma legislação rigorosa e nem mesmo uma estrutura de monitoramento das *lan houses*. Não há uma fiscalização permanente e regular nos diversos estabelecimentos e nem nos equipamentos utilizados, o que, em tese, configuraria na quebra de privacidade.

Contudo, com o crescimento dos cibercrimes, passou-se a ter uma preocupação maior com os usuários das *lan houses*, sendo constatado que alguns estados e municípios criaram legislação específica e já exigem dessas casas o cadastro e a identificação dos usuários, para que estes dados possam ser fornecidos à polícia, nos casos de crimes praticados com computadores desses estabelecimentos.

A Associação Brasileira de Centros de Inclusão Digital (ABCID, 2010) destaca que apenas 14% dos crimes cometidos através da internet são advindos das *lan houses*, também conhecidas como Centros de Inclusão Digital. De acordo com o site da associação, a maioria dos crimes virtuais é advinda de computadores pessoais, de casa ou do trabalho.

O que se pode depreender é que, para a maioria dos criminosos, a utilização do computador pessoal estaria protegida pela privacidade dos dados com os provedores de internet. Desta forma, torna-se mais seguro para o criminoso utilizar um computador que só ele tem a posse, a usar um que seja compartilhado com diversas pessoas, em que se pode acessar dados e arquivos alheios, através de programas e vírus facilmente instalados.

Com o propósito de buscar uma solução para os crimes cibernéticos através das *lan houses*, o Ministério da Justiça propôs um anteprojeto de lei denominado de “Marco Civil”, o qual visa criar mecanismos para o monitoramento dos conteúdos não exatamente através das *lan houses*, mas sim, através dos provedores de internet. (ABCID, 2010)

De acordo com o *site* da ABCID (2010), foi apresentada a seguinte exposição de motivos para o encaminhamento do anteprojeto de lei:

> Os provedores de internet é que deverão expor com clareza se guardam ou não as informações cadastrais dos usuários e o destino dessas informações. “Para utilização desses dados, é preciso o consentimento expresso do usuário”, explicou. Já o provedor de acesso deverá guardar os logs (dados do usuário) por seis meses. Todas essas propostas ainda estão em discussão e as maiores polêmicas são em relação à responsabilização por conteúdos gerados por terceiros.

Entende-se, pois, que é importante a fiscalização nos dois setores, ou seja, tanto no que concerne aos provedores de internet, quanto no que diz respeito às *lan houses*, uma vez que, a partir do momento em que houver a efetiva fiscalização dos provedores, os índices de criminalidade com o uso da internet certamente serão reduzidos, já que os criminosos terão maiores restrições na utilização dessas casas para se manterem no anonimato.

4.3 A Legislação de Belo Horizonte sobre o Funcionamento das *Lan Houses*

Conforme já mencionado anteriormente, muitos estados e municípios têm adotado a Lei Antianonimato nas *lan houses* em seus respectivos territórios, com o intuito de reduzir a criminalidade virtual nesses ambientes.

Em Belo Horizonte, não foi diferente. Encontra-se em tramitação na Câmara Municipal o Projeto de Lei nº 907/2006, que prevê o cadastramento de todos os usuários de *lan houses*, *cibercafés* e *cyber offices*. Assim destaca o art. 2º do referido projeto:

> Art 2º. Os estabelecimentos de que trata esta lei ficam obrigados a criar e manter cadastro atualizado de seus usuários, contendo:
> I - nome completo;
> II - data de nascimento;
> III - endereço completo;
> IV - telefone;
> V – número de documento de identidade.

Ainda de acordo com o referido projeto de lei, o documento de identidade não deve ser exigido apenas no cadastramento, mas, sim, em todas as vezes que o usuário utilizar o equipamento, sob pena de não poder utilizá-lo (parágrafos 1º e 3º). Também

caberá ao estabelecimento registrar a hora de início e término de utilização do equipamento (parágrafo 2º).

Ademais, os parágrafos 4º e 5º destacam que o registro deve ser guardado por um período de 60 meses, podendo ser arquivado por meio eletrônico. O projeto de lei ainda veda a utilização destes dados cadastrais, bem como sua divulgação sem o expresso consentimento do usuário ou sem medida judicial que o autorize (parágrafos 6º e 7º).

A Justificativa do poder público municipal para esse projeto de lei está na falta de controle e identificação dos usuários das *lan houses*, o que facilita a prática de delitos com o uso do computador:

> Atualmente há uma absoluta falta de controle quanto à identificação dos usuários desses estabelecimentos, configurando um foco potencial para a prática de infrações, sob o manto do anonimato.
>
> Portanto, necessário se faz que estes estabelecimentos mantenham um cadastro dos usuários, contendo nome, hora, data e permanência nos computadores, propiciando às autoridades uma possível busca nestes estabelecimentos de infratores que venham a utilizá-los para fins ilícitos como pedofilia, golpes no mercado financeiro, venda de drogas, entre outros.

Convém ressaltar que as medidas propostas no referido projeto de lei de Belo Horizonte não chegam a ser tão rigorosas. Há legislações propostas em outros locais, que tratam do mesmo assunto, que podem ser consideradas mais avançadas, a exemplo do Projeto de Lei nº 053/09, do Estado do Paraná, que destaca que, além dos requisitos estabelecidos no projeto mineiro, ainda os estabelecimentos deverão contar com circuito interno de monitoramento eletrônico, para permitir a identificação dos usuários. (CAMPANA, 2009

Segundo Fábio Campana (2009), as autoridades policiais têm aprovado a medida:

> As duas principais autoridades policiais do Paraná que cuidam de crimes na internet afirmam que a nova lei facilitará as investigações. O delegado do Nuciber, Demétrius Gonzaga de Oliveira, explica que a dificuldade maior não é se chegar ao computador em que o crime foi cometido, mas sim na identificação de quem o cometeu quando a máquina está em local público. "Há locais que atendem 100, 200 clientes ou mais por dia. Sem o cadastro é muito difícil identificar quem cometeu crime nesses estabelecimentos."
> Mesma opinião do delegado Flúvio Cardinelle, chefe do Núcleo de Repressão a Cibercrimes da Polícia Federal (PF) no Paraná. "O fato de não termos esses dados hoje não paralisa a investigação, mas atrapalha muito. Com o cadastro, um procedimento de identificação, que atualmente chega a levar meses ou anos, levaria minutos", argumenta.

No caso do Estado de Minas Gerais, que possui 853 municípios, nota-se que as medidas adotadas para se coibir os crimes cibernéticos através das *lan houses* ainda são totalmente insuficientes e não produzem resultados práticos. Não se tem conhecimento da existência de legislação estadual sobre o assunto. É certo que à exceção da capital, nos demais municípios mineiros também não se tem conhecimento de que haja legislação que trata sobre as *lan houses*. Assim, esses estabelecimentos ainda são territórios livres para os criminosos da internet. Não havendo uma legislação específica, rigorosa e de fácil aplicação, a Polícia Militar de Minas Gerais tem muito pouco a fazer no enfrentamento aos cibercrimes praticados nas *lan houses*. Enquanto a situação não ficar claramente definida em termos de legislação, prevalece o entendimento de que não há uma posição institucional a respeito, a não ser no sentido de que se pode atuar na prevenção e repressão, ou em apoio aos municípios na ação fiscalizadora aos estabelecimentos, através de parcerias.

5 ATUAÇÃO DA PMMG NA PREVENÇÃO E REPRESSÃO AOS CRIMES CIBERNÉTICOS

É importante destacar que a Polícia Militar de Minas Gerais pode e deve atuar em todos os casos de crimes cibernéticos, à luz do Código Penal, do Código de Processo Penal e do Estatuto da Criança e do Adolescente, bastando que, para isso, ela seja acionada. De um modo geral, a prática indica que a atuação da PM ao atender uma ocorrência de crime cibernético configura a ação repressiva, ainda que não ocorra a prisão do (s) criminoso (s), mas que a intervenção policial se encerre com o registro do respectivo boletim de ocorrência. Havendo, através da internet, ofensa à integridade física ou psicológica de alguém, danos materiais, financeiros ou morais, violação ou ameaça de violação ao direito de ir e vir e invasão à privacidade da pessoa, a Polícia Militar pode ser acionada e, a partir daí, desencadear as seguintes ações e operações:

- rastreamento e prisão em flagrante dos agentes do delito;
- registro do fato, através do boletim de ocorrência;
- acionamento da perícia técnica, se necessário;
- apreensão de equipamentos (computadores e componentes) utilizados no crime;
- apreensão de materiais e objetos utilizados para a prática delituosa (vídeos, revistas, fotografias e outros, que configurem material pornográfico, nos casos de pedofilia);
- prisão de criminosos mediante mandado judicial;
- busca e apreensão de equipamentos (computadores e componentes), mediante mandado judicial.

A lavratura do boletim de ocorrência, no caso de crime cibernético, ainda que não haja a prisão do criminoso ou a apreensão do material utilizado no crime, é o ponto de partida para que a vítima (pessoa física ou jurídica) ou o seu responsável legal possa impetrar uma ação judicial ou, então, para que a autoridade policial, ao tomar conhecimento do ato delituoso, dê início à investigação, instaurando o devido inquérito policial. O certo é que a Polícia Militar, agindo preventiva ou repressivamente, está aí para atender o cidadão de bem em suas demandas. O que dificulta o trabalho da Polícia Militar, em relação aos crimes cibernéticos, como já mencionado anteriormente, são as limitações impostas pelo próprio sistema de segurança e justiça, além das questões técnicas e outros obstáculos, a saber:

- falta de ação coordenada entre os órgãos de segurança, Ministério Público e Poder Judiciário;
- ausência de banco de dados integrados entre as polícias, sobre os criminosos, os crimes mais praticados e o *modus operandi*;
- ausência de doutrina e normas internas que padronizem as ações;
- falta de delegacias especializadas em crimes cibernéticos;
- falta de estrutura e de capacidade técnica por parte da polícia judiciária, para a devida apuração e comprovação dos crimes.

No entanto, vale ressaltar que a PMMG ainda não se encontra preparada para prevenir e reprimir adequadamente os crimes cibernéticos, pelos motivos já apontados. A

Diretriz Auxiliar das Operações (DIAO), documento que traz todo o arcabouço de infrações e contravenções penais, atos infracionais e condutas antiéticas que ensejam a atuação da Polícia Militar, não menciona os crimes cibernéticos no rol das infrações penais. Percebe-se, então, que a PMMG ainda está lidando com os crimes cibernéticos de maneira muito superficial e pouco eficaz.

Pela sua natureza e peculiaridades, a maioria dos cibercrimes deve ser objeto de ação da polícia investigativa e não da polícia ostensiva. Essa é, certamente, uma das razões pelas quais a Polícia Militar mineira ainda não avançou no enfrentamento a esses crimes, sobretudo porque, não havendo uma legislação específica que tipifique os crimes cibernéticos e não havendo, consequentemente, o devido amparo legal para balizar a ação da polícia judiciária, não faz sentido a PM adotar qualquer medida com vistas a prender os criminosos, sabendo-se que não haverá continuidade nas medidas subsequentes e não haverá aplicação da lei. O fato é que não se tem conhecimento, no Brasil, de que algum cibercriminoso tenha sido condenado.

O que se busca, neste estudo, é verificar exatamente em que circunstâncias a Polícia Militar pode e deve agir em relação aos crimes cibernéticos. Contudo, pode-se perceber que a corporação, em seu nível estratégico, já vem adotando medidas com vistas a uma atuação padronizada em todo o estado, haja vista o crescimento acelerado das ocorrências desses crimes.

No que se refere à atuação preventiva, a PMMG pode agir no sentido de se coibir a prática de crimes cibernéticos através da presença efetiva nos locais abertos ao público, onde as pessoas têm livre acesso ao computador, como *lan houses* e *cibercafés*. Pode também agir preventivamente nas escolas, através de trabalhos educativos, em interação com a comunidade escolar, a pedido do próprio estabelecimento. De igual forma, nos locais públicos onde se disponibiliza o uso coletivo de computadores, a Polícia Militar pode desempenhar importante trabalho na conscientização dos usuários, no sentido de se coibir a prática de crimes.

5.1 O Enfrentamento aos Crimes Cibernéticos em Minas Gerais

Pode-se dizer que o Município de Belo Horizonte está entre os pioneiros no país na iniciativa de se criar normas para disciplinar o funcionamento dos estabelecimentos denominados *lan houses*, o que significa o primeiro passo na busca da prevenção aos cibercrimes, através do projeto de lei que acaba com o anonimato dos usuários de tais estabelecimentos. Entretanto, o assunto ainda está em fase de projeto de lei e cabe à sociedade a tarefa de cobrar do poder legislativo municipal a aprovação desse projeto, para que se tenha resultados práticos.

Outro avanço muito significativo em Minas Gerais veio do Ministério Público, com a criação da Coordenadoria Estadual de Combate a Crimes Cibernéticos, através da Resolução nº 36, de 16 de junho de 2008, da Procuradoria-Geral de Justiça de Minas Gerais.

De acordo com esta Resolução, o Ministério Público Estadual deverá atuar em conjunto com a Diretoria de Inteligência da Polícia Militar, no intuito de reunir esforços no combate aos crimes cibernéticos.

Assim, pressupõe o art. 2º da referida Resolução:

> Art. 2º A Coordenadoria Estadual de Combate aos Crimes Cibernéticos, com o objetivo precípuo de, isoladamente ou em conjunto com as demais Promotorias de Justiça do Estado, articular as medidas judiciais e extrajudiciais necessárias à efetivação do combate aos crimes cibernéticos em Minas Gerais, tem por princípio auxiliar, conjugar esforços e dar suporte técnico, jurídico e administrativo às Promotorias de Justiça do Estado de Minas Gerais.

Vê-se, pois, que esta Coordenadoria servirá como suporte para as demais Promotorias do Estado de Minas Gerais, no intuito de dar todo o apoio necessário no combate aos cibercrimes. Embora a Resolução não faça menção à Polícia Militar, nota-se que isto está implícito no texto, haja vista que a ação do Ministério Público em relação aos crimes cibernéticos, quase que na sua totalidade, está atrelada à PM, principalmente nos casos de prisão dos criminosos mediante mandado, bem como no cumprimento dos mandados de busca e apreensão.

O art. 3º da Resolução nº 36/2008 elenca uma série de atribuições da Coordenadoria Estadual de Combate aos Crimes Cibernéticos, a saber:

> Art. 3º Compete à Coordenadoria Estadual de Combate aos Crimes Cibernéticos:
>
> I - Realizar estudos e pesquisas voltados para a produção, orientação e divulgação de informações quanto à utilização segura das tecnologias de internet, compilando, sistematizando e analisando a legislação e a jurisprudência pertinentes;
>
> II - Propor a celebração de convênios com provedores de serviços na internet ou com outras instituições públicas ou privadas, visando à obtenção de subsídios técnicos aos órgãos de execução, bem como à captação de recursos para o combate aos crimes praticados na rede;
>
> III - Promover, em conjunto com o Centro de Estudos e Aperfeiçoamento Funcional, congressos, seminários e conferências, inclusive em parceria com outras instituições, sobre temas relevantes e pertinentes ao combate aos crimes cibernéticos;
>
> IV - Promover a integração do Ministério Público do Estado de Minas Gerais com outros Ministérios Públicos Estaduais e Federal, instituições afins e a comunidade;
>
> V - Promover campanhas para conscientização da sociedade em relação à utilização adequada da internet, visando à proteção do cidadão-usuário e à efetiva defesa dos Direitos Humanos na sociedade de informação;
>
> VI - Propor a edição e a publicação de revistas, livros, boletins, cartilhas e material de divulgação, além de produzir relatórios e notas técnicas com o objetivo de orientar as políticas públicas de enfrentamento e a atuação dos membros do Ministério Público no combate aos crimes contra o cidadão-usuário perpetrados com o uso das tecnologias de informação e comunicação;
>
> VII - Manter intercâmbio de caráter técnico, cultural e científico com outras associações e entidades, nacionais ou estrangeiras.

Vale ressaltar que essas medidas só serão efetivadas se realizadas em conjunto com as polícias estaduais e com demais órgãos e entidades afins que, com a efetiva participação da sociedade, poderão alcançar êxito na promoção das campanhas preventivas e educativas.

Em relação à Polícia Militar de Minas Gerais, a Corporação já vem atuando no combate aos crimes cibernéticos, contudo, essa atuação é ainda de caráter mais repressivo do que preventivo e ocorre de maneira esporádica, já que há vários fatores que impedem uma atuação completa de todos os órgãos policiais e de Justiça. O fato é que enquanto não há uma legislação que defina, de maneira clara e objetiva, quais são os crimes cibernéticos, qual é o papel institucional de cada órgão e as normas de conduta

operacional, não será possível realizar um trabalho satisfatório, capaz de dar à sociedade uma resposta eficaz em relação aos crimes da Internet.

Ainda assim, tanto o Ministério Público quanto a PMMG, com a criação da Coordenadoria e da atuação da Diretoria de Inteligência, já iniciam sua caminhada na busca da prevenção aos cibercrimes. É um passo importante, mesmo que seja ainda muito embrionário.

Mister se faz destacar que a Polícia Militar de São Paulo é uma das organizações policiais mais avançadas na busca da prevenção e repressão dos cibercrimes, tanto é que a maior parte do material bibliográfico que dá suporte ao presente estudo foi obtida junto àquela corporação co-irmã. Ao se pesquisar nas demais polícias militares do País, constatou-se que quase nada existe sobre o assunto, em termos de legislação, estrutura e capacidade técnica.

A Procuradoria da República, no Estado de São Paulo, lançou em 2006, o "Manual Prático de Investigação", o qual dá suporte para a investigação de crimes cibernéticos, tanto para a Polícia Militar como para o Ministério Público. Dentre essas ações pré-estabelecidas podem-se destacar: a utilização de *softwares* para rastreamento de IP(*Internet Protocol*); a pesquisa de domínio de um determinado site suspeito, bem como sua localização e identificação do proprietário; a interceptação de *e-mails* suspeitos e a identificação de autores de mensagens de chat, de "*instant messengers*" ou de conteúdo criminoso no *Orkut.*

5.2 A Repressão aos Cibercrimes

Como já foi abordado no presente estudo, a participação mais efetiva da polícia no enfrentamento aos crimes cibernéticos concentra-se na investigação. Nesse sentido, os Procuradores da República do Grupo de Combate ao Crime Cibernético, em entrevista ao *site* da Procuradoria da República no Estado de Goiás (PR/GO), destacam os avanços nesse processo:

> Hoje possuímos todos os agentes envolvidos no combate à criminalidade cibernética, peritos e técnicos de informática, agentes policiais, delegados, membros do Ministério Público e até juízes, mais treinados e informados, entre outros fatores, graças aos cursos que buscamos desenvolver, trazendo inclusive profissionais treinados de outros países. Outro fator importante é a colaboração entre os órgãos, que vem se intensificando com o compartilhamento de técnicas e informações para o aperfeiçoamento de todos e com o trabalho em equipe, resultando em operações e forças-tarefas bem-sucedidas na área de combate aos crimes cibernéticos, com destaque para o combate à pornografia infantil pela rede. Nesta área específica, o TAC (Termo de Ajustamento de Conduta) com a Google determinou que houvesse a comunicação ao MPF das páginas do *Orkut* retiradas do ar por indícios de pornografia infantil e que a empresa se obrigasse a comunicar ao National Center of Missing and Exploited Children, o que também contribuiu para o aumento dos casos a serem apurados. (PR/GO, 2010)

Dessa forma, observa-se que a repressão aos cibercrimes só é possível de ser efetivada através de ações conjuntas e interativas entre a polícia, o Ministério Público e os diversos órgãos federais, estaduais e municipais afins, além do necessário engajamento de particulares, como nos casos do Google e dos Provedores de Acesso à Internet.

Além dessas iniciativas, faz-se necessária, também, a participação de outros órgãos e entidades da sociedade civil, principalmente as Organizações Não-Governamentais – ONGs -, como declara Santos (2009, p. 13-14):

> Temos, ainda, outras medidas, algumas de iniciativa privada, tais como: a criação da SaferNet Brasil, organização não governamental, que através da Central Nacional de Denúncias de Crimes Cibernéticos, operada em parceria com o Ministério Público Federal, oferece à sociedade brasileira e à comunidade internacional um serviço anônimo de recebimento, processamento, encaminhamento e acompanhamento on-line de denúncias sobre qualquer crime ou violação aos Direitos Humanos praticado através da Internet. Ademais, temos a Cartilha de Segurança da Internet, que contém recomendações e dicas sobre como o usuário pode aumentar a sua segurança na Internet, disponibilizado pelo centro de estudos, resposta e tratamento de incidentes de segurança no Brasil (http://cartilha.cert.br/). Nesse sentido, o Perito Criminal da Superintendência da Polícia Técnico-Científica de São Paulo, Orlando Ruiz, defende a necessidade de uma maior integração entre governo, usuários e a iniciativa privada para combater os crimes pela internet. Segundo ele, esta medida traria maior eficiência contra os fraudadores do que a criação de leis específicas para crimes on-line.

Portanto, pode-se perceber, pelos esforços até agora levados a efeito, que a maneira mais eficaz de se reprimir os crimes da Internet é através da fiscalização intensiva, aumentando-se as possibilidades de alcançar maior êxito se as ações forem interativas entre a polícia e os demais órgãos afins.

5.3 Variáveis e Indicadores

O rastreamento do IP e a obtenção dos dados do usuário junto aos provedores de Internet são um grande empecilho para a investigação policial. Assim destaca o Manual de Investigação de Cibercrimes da PR/SP:

> Como já dito, uma das mais importantes evidências que podemos coletar é o chamado número IP (Internet Protocol). O número IP é uma identificação que todos os computadores que acessam a Internet possuem; ele aparece no formato A.B.C.D, onde A, B, C e D são números que variam de 0 a 255 (por exemplo, 200.158.4.65). O IP deve estar acompanhado da data, hora exata da conexão ou comunicação e o fuso horário do sistema.
>
> (...)
>
> Como a Internet é uma rede mundial de computadores, os registros indicam a hora, local (05:41:12, no exemplo) e a referência à hora GMT (no caso -08:00). Às vezes, é feita apenas a menção à hora GMT (por exemplo, "Tue, 09 Mar 2004 00:24:28 GMT"). Nos pedidos feitos aos provedores de acesso e às companhias telefônicas, é imprescindível que haja, no mínimo, a menção a esses três indicadores: a) o número IP; b) a data da comunicação; e c) o horário indicando o fuso horário utilizado – GMT ou UTC. Sem eles, não será possível fazer a quebra do sigilo de dados telemáticos. (PR/SP, 2006, p. 15)

Assim, a Procuradoria é enfática ao dizer que apenas com os três indicadores se consegue obter a quebra do sigilo de dados. A dificuldade está, pois, na busca desses indicadores.

Daí advém o problema do anonimato nas *lan houses*, já também mencionado anteriormente, que, mesmo com a identificação do computador e do local de acesso, se não houver o registro do proprietário quanto aos seus usuários, de nada auxiliará nas investigações. Assim, além da legislação que proíbe o anonimato do cliente-usuário das *lan houses*, deve haver uma fiscalização constante dos órgãos policiais e do poder público municipal, visando ao fiel cumprimento da lei.

A falta de controle dos dados publicados na Internet é outro entrave para as investigações policiais. É notório que o conteúdo da Internet tem uma grande mutabilidade e as informações podem ser espalhadas com imensa facilidade. Assim como se pode espalhar, também se pode desaparecer com as informações ou modificá-las de forma extremamente fácil.

Os Procuradores da República do Grupo de Combate ao Crime Cibernético destacam que essa mutabilidade do conteúdo na Internet se dá em progressão geométrica e destacam a importância do “pensar antes de postar”:

> É verdade, perde-se o controle sobre qualquer conteúdo, uma vez que ele seja postado na rede. Por isso dizemos que o conselho que outrora ouvíamos como “pense antes de falar” deve ser adaptado, nos dias de hoje, para “pense antes de postar”. Justamente porque um conteúdo inicialmente colocado na Internet pode ser visto por qualquer pessoa no mundo, reproduzido e até maliciosamente modificado, quantas vezes puder se imaginar. Por considerar que a prevenção é o melhor caminho a seguir na conscientização das pessoas e evitar a disseminação indesejável de material de qualquer natureza na rede, o Grupo promove mensalmente com a Safernet oficinas educativas para o uso seguro e consciente da internet a professores em São Paulo. (PR/GO, 2010)

Os autores, ainda dentro dessa matéria disponibilizada ao site da Procuradoria da República no Estado de Goiás, salientam a falta do Estado dentro da Internet, através de agências reguladoras, que possam controlar melhor o ambiente virtual:

> A Internet foi concebida para funcionar de maneira descentralizada e colaborativa. Atualmente, a sociedade está migrando para este ambiente, exigindo um mínimo de regulamentação para evitar a impunidade e a criminalidade. A internet não possui uma agência reguladora tal como a Anatel (Agência Nacional de Telecomunicações), que regulamenta as concessionárias de serviço de telefonia; no caso dessas empresas que também concedem serviço de acesso à internet, tentamos que houvesse um mínimo de regulamentação ou aplicação analógica destas normas, sem que pudéssemos chegar a um acordo com a Anatel. No Brasil, há uma instituição formada por representantes de várias classes e empresas ligadas ao setor da internet, que disciplina e controla o seu uso no Brasil pelas empresas provedoras de acesso, o CGI – Comitê Gestor da Internet, porém, sem poder regulamentador ou sancionatório. (PR/GO, 2010)

Vê-se, pois, que a Internet ainda se encontra sem uma fiscalização mais rigorosa por parte do poder público, o que se torna um grande entrave na busca da resolução dos crimes cibernéticos.

5.3.1 Informação e Reflexão

A questão da Informação é outro fator que intervém diretamente na atuação da polícia. Há um desconhecimento total por parte dos policiais mineiros sobre os cibercrimes. Nos Batalhões e Companhias, há falta de equipamentos e não há treinamento do pessoal, para que as informações a respeito desses crimes sejam levadas ao conhecimento da corporação, em todos os níveis e em todo o Estado.

Contudo, convém ressaltar que a Coordenadoria Estadual de Cibercrimes teve sua criação recente e, por isso, ainda está em processo de interligação com os demais órgãos, como a Diretoria de Inteligência da Polícia Militar e com as demais polícias militares brasileiras. Na PMMG, pode-se afirmar que ainda falta quase tudo para que a instituição possa efetivamente atuar nos cibercrimes. Desde a capacitação dos policiais, para que tenham conhecimento dos delitos e saibam como agir nessas situações, passando pela criação de doutrina, pela clara definição de procedimentos padronizados, pela estrutura logística, a criação de banco de dados sobre os cibercriminosos e seus *modus operandi*, a atuação interativa com outros órgãos e entidades, a destinação das ocorrências e as ações preventivas.

Destaca-se que em outros estados brasileiros, essa interligação entre os órgãos estatais está em estágio mais avançado, como no caso de São Paulo, que já possui ligação com o Portal de denúncias SaferNet. Ademais, Santos (2009, p. 14) destaca a criação da Comissão do Direito na Sociedade da Informação da OAB/SP, como importante órgão não só para o Estado, como para todo Brasil:

> Não se pode deixar de mencionar a importância para o Brasil da Criação da Comissão do Direito na Sociedade da Informação da OAB/SP. Vive-se hoje o que se convencionou chamar de era informacional, ou a sociedade da informação na União Européia. Neste meio, informação é um ativo de grande valia, movendo mercados e mobilizando consciências e processos legislativos políticos e jurídicos. Aquele que mais rapidamente concentra uma gama de informações qualitativas, diminui seus custos e tempo de transação, ganha vantagem competitiva, evitando gargalos na cadeia logística de empresas públicas e privadas. Na atualidade, vivem-se, relevantes problemas sociais causados pelas assimetrias digitais.

6 PESQUISA DE CAMPO

6.1 Metodologia

Utilizou-se, neste estudo, a pesquisa exploratória, pois foi através dela que se teve um maior aprofundamento acerca do tema. Assim, o conhecimento do tema, qual seja, a atuação da PMMG na prevenção e repressão aos crimes cibernéticos, contribuiu, de forma sistemática, para a compreensão da realidade prática de atuação do órgão.

A pesquisa exploratória, aqui utilizada, também está de pleno acordo quanto aos fins propostos por Vergara (2000), pois consiste no aprofundamento de conceitos preliminares, contemplando maiores informações sobre o assunto a ser investigado, orientação e fixação dos objetivos e sobre a formulação das suas hipóteses.

Optou-se pela pesquisa de natureza quantitativa, por ser mais aplicável a este estudo e aos fins propostos, haja vista que, Segundo Martins (2000), a avaliação quantitativa procura mensurar ou medir variáveis, através de questionários, com questões de múltipla escolha.

Assim, na pesquisa quantitativa, foram utilizados questionários dirigidos aos Oficiais Chefes da Seção de Inteligência dos Batalhões e Companhias Independentes, da Região Metropolitana de Belo Horizonte e do interior do Estado de Minas Gerais. O questionário modelo encontra-se no Anexo I do presente estudo.

O universo de pesquisa é composto por Militares Chefes das Seções de Inteligência de todos os Batalhões e Companhias Independentes da Polícia Militar de Minas Gerais, por serem esses profissionais de segurança pública os que lidam mais frequentemente com os dados estatísticos e banco de dados sobre os crimes e os criminosos.

A PMMG possui, em sua estrutura, um total de 51 Batalhões Operacionais, 07 Batalhões Especializados, 26 Companhias Independentes, 15 Companhias

Independentes de Meio Ambiente e Trânsito e 05 Companhias de Missões Especiais, perfazendo um total de 104 Chefes de Seções de Inteligência a serem pesquisados, os quais constituem a amostra da pesquisa.

Os questionários foram remetidos aos Chefes de Seção de Inteligência por meio eletrônico, através da rede interna da PMMG – Intranet -, sendo essa, atualmente, a ferramenta mais rápida e mais eficaz para essa atividade.

Do total de unidades pesquisadas, 28 chefes de seção deixaram de responder aos questionários em tempo hábil, de modo que retornaram as respostas de 51 Comandantes de Batalhões Operacionais e das 25 Companhias Independentes, perfazendo-se um total de 76 questionários respondidos, conforme se pode verificar da listagem do Anexo II.

As perguntas formuladas na primeira parte do questionário tiveram por finalidade verificar se a PMMG tem atuado preventiva e repressivamente no combate aos crimes cibernéticos. Esses dados permitiram cruzamentos posteriores, permitindo identificar se houve atuação direta da Policia Militar e como ocorreram essas atuações.

As questões fechadas foram tabuladas, as quais são apresentadas através de gráficos e tabelas, e as abertas, depois de lidas e analisadas, possibilitaram estabelecer uma tabela que consolida as respostas mais frequentes.

A seguir, será apresentada a análise e interpretação dos dados da pesquisa, o que já permite, também, a comparação das respostas com o problema levantado e as hipóteses formuladas.

6.2 Análise e Apresentação dos Dados

A primeira pergunta da pesquisa teve por finalidade verificar a quanto tempo os Chefes de Seção de Inteligência estão ocupando seus respectivos cargos, haja vista ser essa pergunta extremamente relevante no sentido de se permitir diagnosticar o nível de envolvimento desses profissionais na prevenção e enfrentamento aos cibercrimes. Por serem os crimes cibernéticos um assunto ainda estranho e de pouco domínio da maioria dos

profissionais de segurança pública, sabe-se que quase a totalidade das polícias militares brasileiras ainda não conta com aparatos e centros de inteligência capazes de solucionar todos esses crimes e, muitas vezes, até os desconhecem, o que resulta na impunidade dos criminosos virtuais. Com a Polícia Militar de Minas Gerais, isso não é diferente e é o que será demonstrado a seguir, de acordo com os resultados da pesquisa.

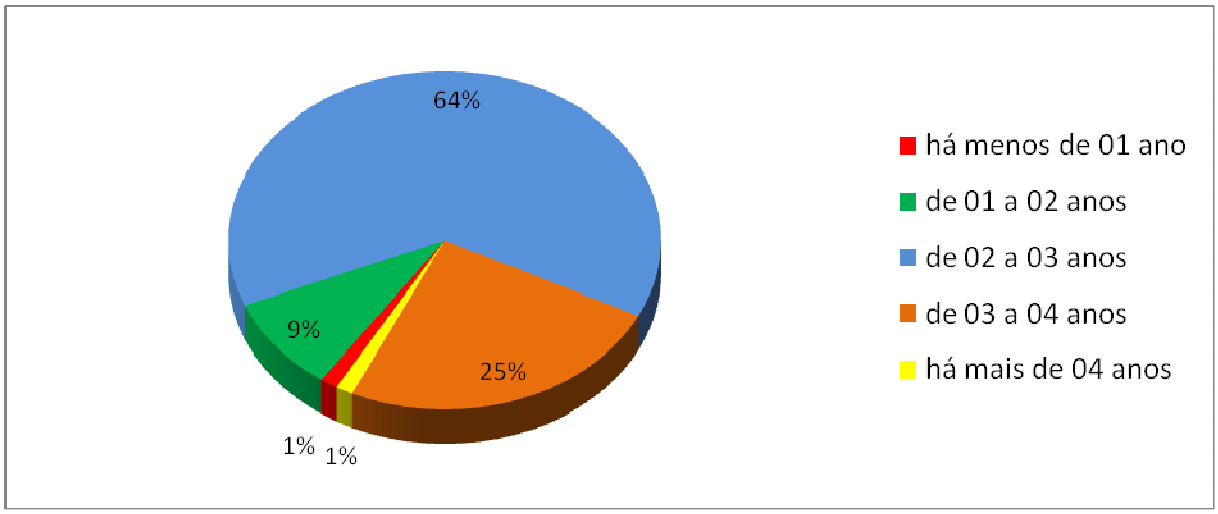
Conforme se pode observar através do gráfico 1 e da tabela 1, a maioria dos Chefes de Seção de Inteligência – 90% - estão há mais de 2 anos no exercício da função, o que demonstra que já estão acostumados ao cotidiano e ao funcionamento da seção em que se encontram.

Tabela1 – Tempo de Chefia na 2ª Seção

Há quanto tempo é Chefe da 2ª Seção?	**Quant.**	**Percentual**
Há menos de 01 ano	1	**1%**
De 01 a 02 anos	7	**9%**
De 02 a 03 anos	49	**64%**
De 03 a 04 anos	19	**25%**
Há mais de 04 anos	1	**1%**
Respostas	**77**	**100%**

Fonte: Dados da pesquisa

Gráfico 1 – Tempo de Chefia na 2ª Seção



Fonte: Dados da pesquisa

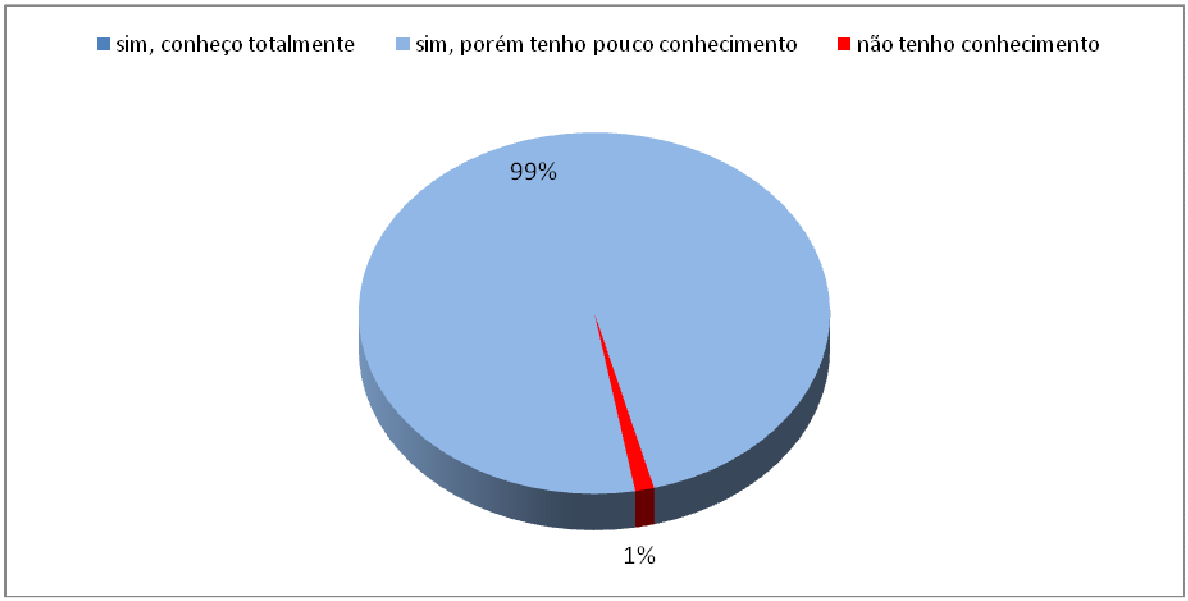
Foi perguntado aos chefes de 2ª Seção dos Batalhões e Companhias Independentes se eles possuem conhecimento a respeito dos cibercrimes. Pelas respostas apresentadas, através da tabela e gráfico 2, percebe-se que 100% dos pesquisados desconhecem totalmente ou têm pouco conhecimento a respeito desses crimes. Nota-se, assim, que, no âmbito da Polícia Militar de Minas Gerais, os crimes praticados através da internet ainda são totalmente fora de domínio da corporação, sendo certo que falta muito para que essa modalidade delituosa seja tratada com o seu devido rigor, tanto na prevenção como a repressão. Num primeiro momento, pode-se concluir que a falta de conhecimento e domínio sobre o assunto já é, por si só, uma barreira para que haja uma atuação sistêmica, continuada e eficaz no enfrentamento aos cibercrimes. Pode-se concluir que, enquanto não houver o domínio, o conhecimento amplo sobre o assunto e as ferramentas adequadas para permitir a ação eficaz da polícia, certamente não haverá iniciativas no sentido de se combater essa modalidade criminosa.

Tabela 2 - Conhecimento sobre os crimes cibernéticos

Você tem conhecimento sobre crimes cibernéticos?	**Quant.**	**Percentual**
Sim, conheço totalmente	0	**0%**
Sim, porém tenho pouco conhecimento	76	**99%**
Não tenho conhecimento	1	**1%**
Respostas	**77**	**100%**

Fonte: Dados da pesquisa

Gráfico 2 - Conhecimento sobre os crimes cibernéticos



Fonte: Dados da pesquisa

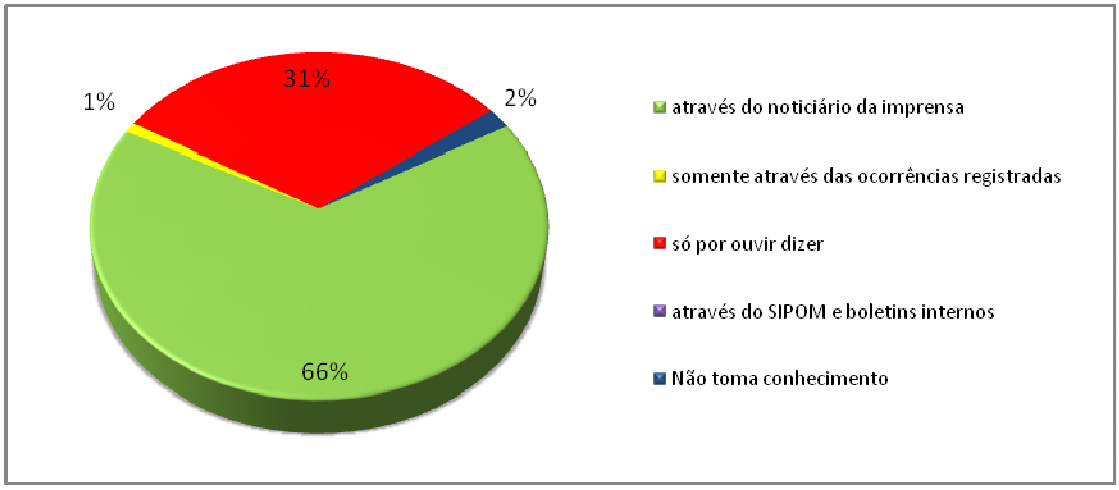
A Tabela 3 e seu respectivo gráfico trazem a pergunta sobre como os Chefes de 2ª Seção têm tomado conhecimento a respeito dos crimes cibernéticos em suas respectivas áreas de atuação. Novamente, se observa que esses profissionais de segurança pública ainda têm pouquíssimo envolvimento no sentido de lidarem com o assunto e somente ficam sabendo sobre crimes cibernéticos de uma maneira muito superficial. A maioria (66%) toma conhecimento através do noticiário da imprensa, enquanto que outros 31% ficam sabendo sobre cibercrimes apenas por ouvir dizer.

Tabela 3 – Atualização do conhecimento à respeito dos crimes cibernéticos na unidade

Indique como você normalmente toma conhecimento sobre os crimes cibernéticos na área de sua unidade (pode marcar mais de uma opção)	**Quant.**	**Percentual**
Através do noticiário da imprensa	70	**66%**
Somente através das ocorrências registradas	1	**1%**
Só por ouvir dizer	33	**31%**
Através do SIPOM e boletins internos	0	**0%**
Não toma conhecimento	2	**2%**
Respostas	**106**	**100%**

Fonte: Dados da pesquisa

Gráfico 3 - Atualização do conhecimento à respeito dos crimes cibernéticos na unidade



Fonte: Dados da pesquisa

Observa-se que nenhum dos pesquisados tomou conhecimento dos cibercrimes através do Sistema de Informações da Polícia Militar (SIPOM) ou dos boletins internos, o que demonstra a falta de preparo da polícia mineira e a falta de investimentos na capacitação dos policiais para atuarem nesses crimes. É relevante observar, também, nas respostas a esta questão, que 31% dos policiais pesquisados tomam conhecimento dos

cibercrimes por ouvir dizer, o que destaca que, além da falta de aparato da própria polícia para proporcionar os meios necessários ao desempenho dos policiais na atuação frente a tais crimes, esses policiais militares, aparentemente, não têm demonstrado empenho em tratar da questão. É possível afirmar, também, com base nas respostas a este questionário, que não têm havido registros de ocorrência sobre cibercrimes na maioria das unidades da PMMG.

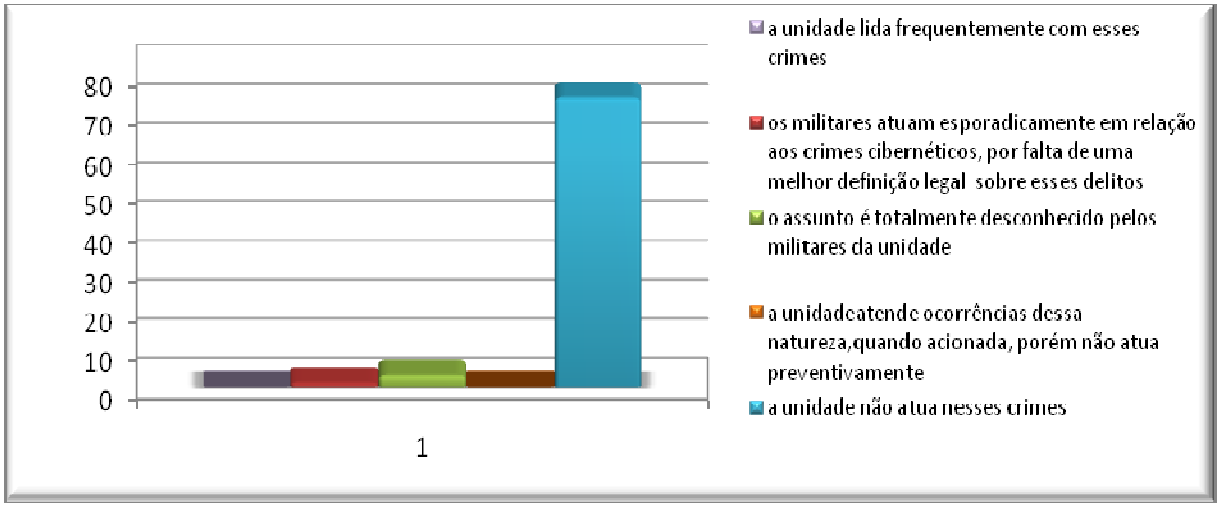
Através do Gráfico e da Tabela 4, buscou-se diagnosticar junto aos policiais militares pesquisados sobre como têm atuado preventiva e/ou repressivamente em relação aos crimes cibernéticos. Como esta pergunta tem certa relação com as anteriores, as respostas vêm confirmar não só o total desconhecimento sobre os crimes cibernéticos como também a ausência de ações preventivas e repressivas frente a esses crimes. Nota-se, pelas respostas, que, rotineiramente, a Polícia Militar de Minas Gerais não tem atuação nos crimes cibernéticos, seja pela falta de conhecimento sobre o assunto, seja por falta de uma definição legal ou até mesmo pelo fato de a sociedade não acionar a PM para atuar.

Tabela 4 – Atuação preventiva e/ou repressiva nos crimes cibernéticos

Indique como sua unidade tem atuado preventiva e/ou repressivamente em relação aos crimes cibernéticos (pode marcar mais de uma opção)	**Quant.**	**Percentual**
A unidade lida frequentemente com esses crimes	0	**0%**
Os militares atuam esporadicamente em relação aos crimes cibernéticos, por falta de uma melhor definição legal sobre esses delitos	1	**1%**
O assunto é totalmente desconhecido pelos militares da unidade	3	**4%**
A unidadeatende ocorrências dessa natureza,quando acionada, porém não atua preventivamente	0	**0%**
A unidade não atua nesses crimes	74	**95%**
Respostas	**78**	**100%**

Fonte: Dados da pesquisa

Gráfico 4 - Atuação preventiva e/ou repressiva nos crimes cibernéticos



Fonte: Dados da pesquisa

Através da Tabela e do Gráfico 5, buscou-se o diagnóstico a respeito dos registros de ocorrências de crimes cibernéticos nas unidades pesquisadas, entre janeiro de 2007 a dezembro de 2009. Os números confirmam a total ausência de registros sobre esses crimes. Pode-se concluir, a princípio, que a principal motivação para essa ausência de registros se deve ao fato de que as pessoas não têm recorrido à Polícia Militar para atuação nesses crimes.

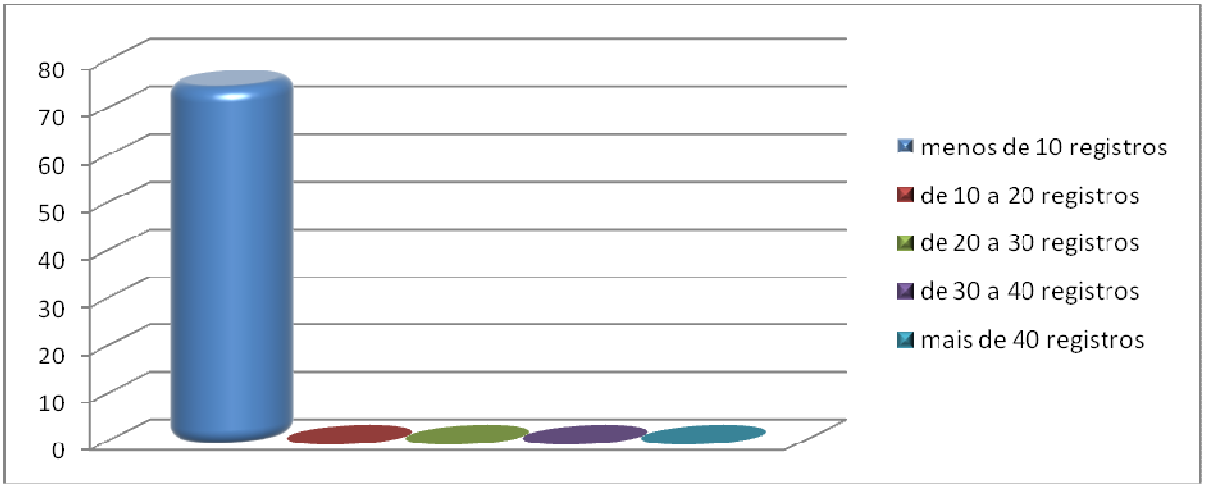
Apesar do expressivo número de denúncias de crimes cibernéticos em todo o país aos *sites* especializados, seja de comércio eletrônico, pedofilia, dentre outros, pode-se destacar pelas respostas às perguntas da Tabela 5, a seguir, que as ocorrências registradas nos Batalhões da PM mineira não chegaram a 10 (dez), no período de 3 anos.

Tabela 5 – Número de ocorrências de cibercrimes, registrados entre jan/2007 a dez/2009

Quantas ocorrências sobre crimes cibernéticos foram registradas nesse Batalhão/Companhia Independente no período de janeiro de 2007 a dezembro de 2009? Considere para resposta o total de ocorrências no período mencionado	**Quant.**	**Percentual**
Menos de 10 registros	75	**100%**
De 10 a 20 registros	0	**0%**
De 20 a 30 registros	0	**0%**
De 30 a 40 registros	0	**0%**
Mais de 40 registros	0	**0%**
Respostas	**75**	**100%**

Fonte: Dados da pesquisa

Gráfico 5 – Número de ocorrências de cibercrimes, registrados entre jan/2007 a dez/2009



Fonte: Dados da pesquisa

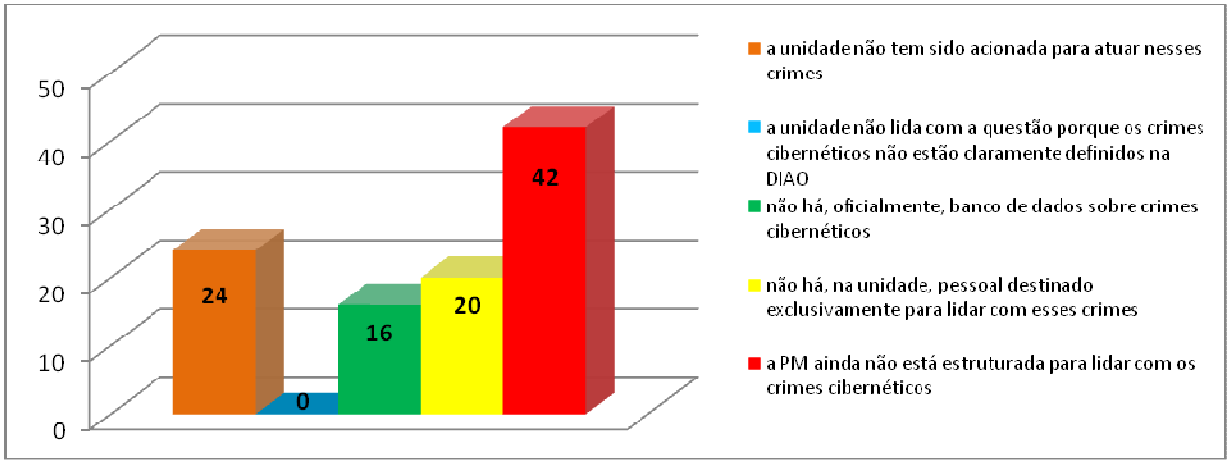
No intuito de identificar como os policiais militares lidam com os crimes cibernéticos em Minas Gerais, formularam-se as perguntas constantes da Tabela e Gráfico 6, cujas respostas permitem verificar em que níveis a PMMG tem voltado as suas atenções para os cibercrimes. O fato comprovado pelas respostas é que por vários fatores os policiais não dão atenção a esses crimes, apontando para a necessidade de se iniciar todo um processo voltado para inserir a Polícia Militar nesse contexto. A necessidade de uma norma legal que tipifique os crimes cibernéticos na legislação brasileira e, consequentemente, a formulação de doutrinas e normas de procedimentos por parte da polícia, a formatação de banco de dados sobre crimes cibernéticos, a capacitação de pessoal e a estruturação das unidades operacionais e setores de inteligência da PM para lhes permitir atuar técnica e sistematicamente no enfrentamento a esses crimes são demandas que a própria pesquisa indica.

Tabela 6 – Tratamento dos casos de crimes cibernéticos

Na sua unidade, como têm sido tratados os casos de crimes cibernéticos? (pode marcar mais de uma opção)	**Quant.**	**Percentual**
A unidade não tem sido acionada para atuar nesses crimes	24	**24%**
A unidade não lida com a questão porque os crimes cibernéticos. Não estão claramente definidos na DIAO	0	**0%**
Não há, oficialmente, banco de dados sobre crimes cibernéticos	16	**16%**
Não há, na unidade, pessoal destinado exclusivamente para lidar com esses crimes	20	**20%**
A PM ainda não está estruturada para lidar com os crimes cibernéticos	42	**41%**
Respostas	**102**	**100%**

Fonte: Dados da pesquisa

Gráfico 6 – Tratamento dos casos de crimes cibernéticos



Fonte: Dados da pesquisa

Outra questão relevante para este estudo, diagnosticada através das perguntas formuladas na Tabela e Gráfico 7, trata da estrutura logística necessária para que os policiais militares possam atuar satisfatoriamente frente aos crimes cibernéticos. Buscou-se o foco nas questões de pessoal qualificado, nas ferramentas adequadas, a destinação dos boletins de ocorrência, a questão doutrinária e as dificuldades na definição de quais são os crimes cibernéticos. Nota-se, pelas respostas, que são várias as dificuldades encontradas, sendo certo que tanto a falta de logística, falta de pessoal qualificado e ausência de doutrina são os principais fatores dificultadores nesta questão e que impossibilitam a PM de atuar. Para 35% dos pesquisados, a dificuldade é determinada pela falta de ferramentas adequadas, como computadores, mobiliário e espaço adequado. Para 38%, as dificuldades residem na falta de pessoal qualificado e para 25% a falta de doutrina é a principal causadora dessas dificuldades. Com fundamento nas respostas a esta pergunta, corroborando com as respostas dos questionários anteriores, tem-se a comprovação da hipótese básica da pesquisa, qual seja:

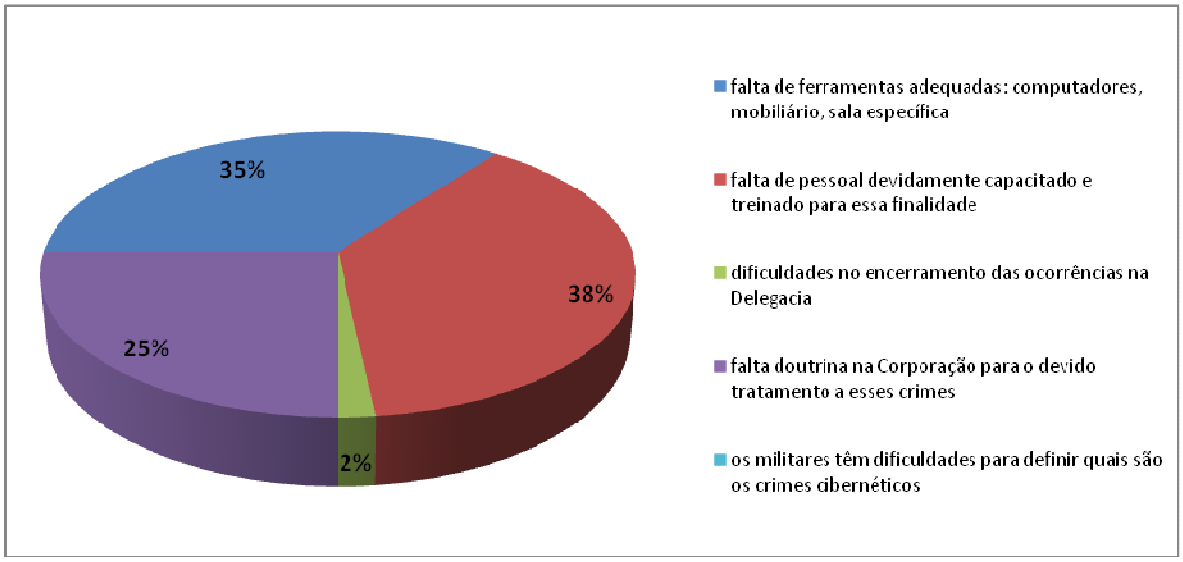
> *"A Polícia Militar de Minas Gerais não conhece a extensão dos crimes cibernéticos praticados no Estado; não possui, em suas unidades operacionais, pessoal qualificado e nem ferramentas adequadas para agir na prevenção e repressão aos crimes virtuais e não possui doutrina específica para atuação frente a essa modalidade criminosa."*

Tabela 7 – Dificuldades da estrutura logística e de pessoal Unidade

Em termos de estrutura logística e de pessoal, na sua Unidade, quais são as dificuldades encontradas no atendimento a ocorrências envolvendo crimes virtuais? (pode marcar mais de uma)	**Quant.**	**Percentual**
Falta de ferramentas adequadas: computadores, mobiliário, sala específica	41	**35%**
Falta de pessoal devidamente capacitado e treinado para essa finalidade	44	**38%**
Dificuldades no encerramento das ocorrências na Delegacia	2	**2%**
Falta doutrina na Corporação para o devido tratamento a esses crimes	29	**25%**
Os militares têm dificuldades para definir quais são os crimes cibernéticos	0	**0%**
Respostas	**116**	**100%**

Fonte: Dados da pesquisa

Gráfico 7 – Dificuldades da estrutura logística e de pessoal Unidade



Fonte: Dados da pesquisa

Vê-se, pois, que a dificuldade dos policiais para definirem os cibercrimes é apenas parte do problema, como pode ser verificado pelas respostas dos pesquisados, haja vista que, mesmo que superficialmente, os policiais têm certo conhecimento sobre esses crimes. Percebe-se que o que falta é aprofundar mais acerca destes crimes e de como deve ser seu tratamento.

Outro questionamento relevante inserido neste estudo foi no sentido de se levantar junto aos pesquisados como deve ser a atuação da PMMG no enfrentamento aos crimes cibernéticos. Pelas respostas apresentadas, permite-se constatar que, para 43% dos policiais militares, a PM somente deve atuar nesses crimes quando for acionada; para 27%

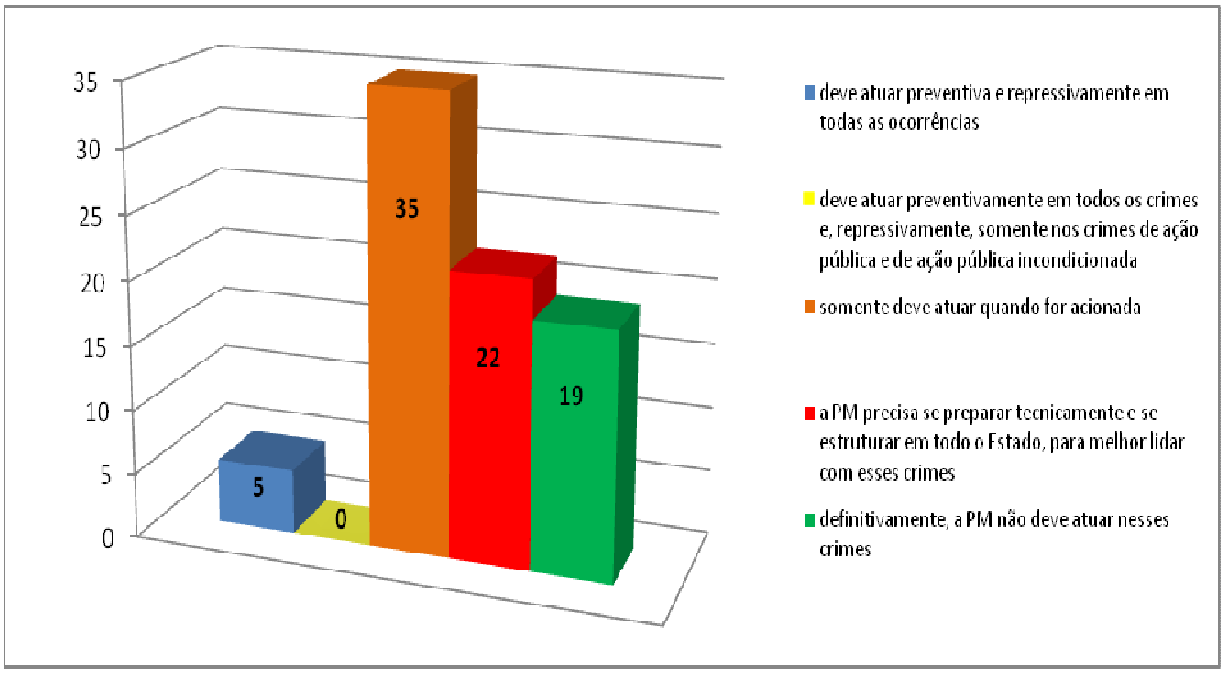
dos pesquisados a PM precisa se preparar tecnicamente e se estruturar em todo o Estado, para melhor lidar com a questão; e para 23%, definitivamente, a PM não deve atuar nos cibercrimes. Esse posicionamento dos pesquisados infere que o assunto – crimes cibernéticos – ainda demandará um tempo considerável até ser tratado como uma questão de segurança pública, ou seja, aparentemente, esses delitos ainda não estão inseridos no rol de prioridades para a ação da polícia.

Tabela 8 - Atuação da PMMG em relação aos crimes cibernéticos

Na sua opinião como deve ser a atuação da PMMG em relação aos crimes cibernéticos? (pode marcar mais de uma opção)	**Quant.**	**Percentual**
Deve atuar preventiva e repressivamente em todas as ocorrências	5	**6%**
Deve atuar preventivamente em todos os crimes e, repressivamente, somente nos crimes de ação pública e de ação pública incondicionada	0	**0%**
Somente deve atuar quando for acionada	35	**43%**
A PM precisa se preparar tecnicamente e se estruturar em todo o Estado, para melhor lidar com esses crimes	22	**27%**
Definitivamente, a PM não deve atuar nesses crimes	19	**23%**
Respostas	**81**	**100%**

Fonte: Dados da pesquisa

Gráfico 8 - Atuação da PMMG em relação aos crimes cibernéticos



Fonte: Dados da pesquisa

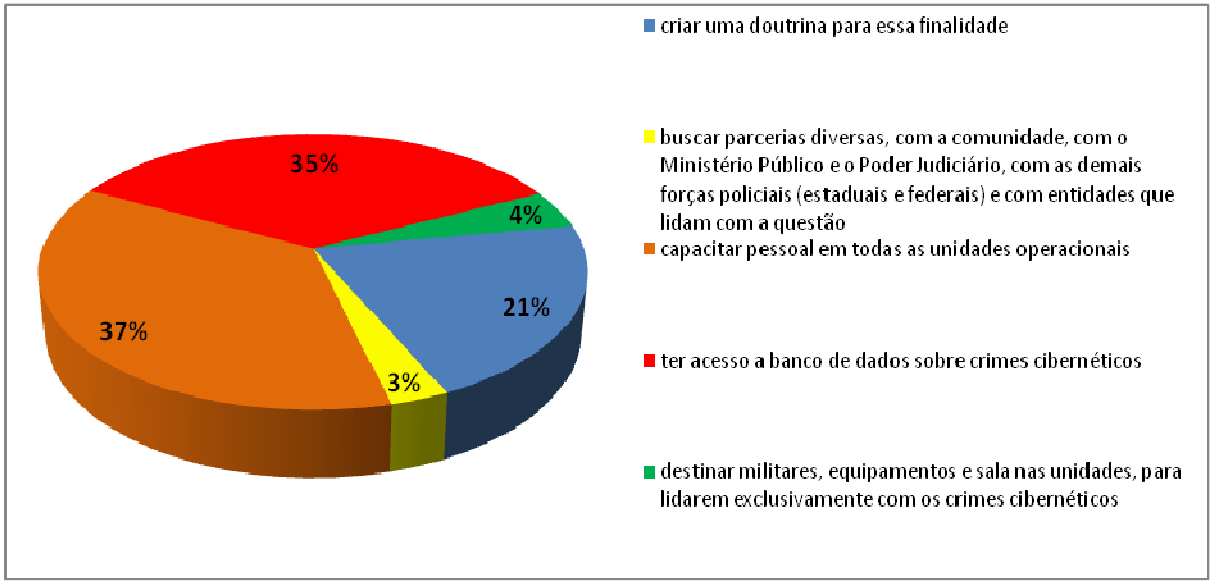
Através da Tabela e do Gráfico 8, buscou-se a opinião dos pesquisados sobre quais as medidas devem ser adotadas para que a PMMG fique adequadamente estruturada e em condições de atuar nos crimes cibernéticos. Para 37% dos pesquisados, a PM precisa, primeiro, capacitar o seu pessoal para que, em todas as unidades operacionais, haja policiais militares aptos a lidarem com os crimes cibernéticos. A pergunta foi formulada de modo que os pesquisados pudessem responder mais de uma opção. Para 35% dos pesquisados, é importante ter acesso a banco de dados sobre crimes cibernéticos e para 21% é fundamental que se crie doutrina a respeito dos cibercrimes. Tais respostas indicam a necessidade de se priorizar as providências que deverão anteceder às iniciativas da PMMG em sua missão institucional, deixando-a apta a agir preventiva e repressivamente.

Tabela 9 – Estrutura necessária à PMMG no combate aos crimes cibernéticos

Na sua opinião, para que a PMMG seja adequadamente estruturada, a fim de lidar com os crimes cibernéticos ela precisa: (pode marcar mais de uma opção)	**Quant.**	**Percentual**
Criar uma doutrina para essa finalidade	28	**21%**
Buscar parcerias diversas, com a comunidade, com o Ministério Público e o Poder Judiciário, com as demais forças policiais (estaduais e federais) e com entidades que lidam com a questão	4	**3%**
Capacitar pessoal em todas as unidades operacionais	49	**37%**
Ter acesso a banco de dados sobre crimes cibernéticos	47	**35%**
Destinar militares, equipamentos e sala nas unidades, para lidarem exclusivamente com os crimes cibernéticos	6	**4%**
Respostas	**134**	**100%**

Fonte: Dados da pesquisa

Gráfico 9 – Estrutura necessária à PMMG no combate aos crimes cibernéticos



Fonte: Dados da pesquisa

Às perguntas da Tabela 10, os Chefes de Seção pesquisados, os quais afirmaram conhecer os cibercrimes, foram instados a citar alguns desses crimes com os quais já lidou, contudo, apenas um dos entrevistados soube responder, destacando o crime de estelionato na internet. Considerando que o Estado de Minas Gerais possui 853 municípios e sendo certo que em todos eles a rede mundial de computadores – internet – já é uma realidade, percebe-se que a atuação da PM nos crimes cibernéticos ainda é totalmente embrionária, insignificante, baseados nos dados da pesquisa. Faz-se necessário iniciar todo um trabalho voltado para a atuação dos policiais militares nesses crimes, até porque, a avaliar pelo ritmo acelerado dos avanços da internet, em escala mundial, em breve haverá clamor público para que as forças de segurança deem respostas à sociedade sobre a atuação dos criminosos virtuais.

Tabela 10 - Principais crimes cibernéticos com os quais já lidou ou tem conhecimento

Caso tenha respondido <u>SIM</u> em relação à 2ª pergunta, cite os principais crimes cibernéticos com os quais já lidou ou tem conhecimento.
1) 171 (estelionato pela Internet) - 15º BPM - Patos de Minas

Fonte: Dados da pesquisa

7 CONCLUSÃO E PROPOSTAS

7.1 Conclusão

O presente estudo objetivou destacar a atuação preventiva e repressiva da Polícia Militar de Minas Gerais no combate aos crimes cibernéticos.

A PMMG está presente em todos os 853 municípios mineiros e em vários distritos, sendo, portanto, a instituição do Estado que mais se faz presente junto aos cidadãos. A corporação está estruturada em rede interna de computadores – rede intranet – o que lhe permite comunicação rápida e instantânea em todas as suas unidades e em todos os níveis de direção. Desse modo, para o enfrentamento aos crimes cibernéticos a Polícia Militar não teria maiores dificuldades em se estruturar técnica e logisticamente, haja vista que em seu organograma já existe um setor de inteligência, em nível de Diretoria, que abrangeria toda a gama de informações e a formulação de doutrinas a respeito dos crimes virtuais, além de direcionar, de forma padronizada e articulada com a Diretoria de Atividades Operacionais toda a conduta operacional dos policiais militares. Vale ressaltar, também, que, em Minas Gerais, a segurança pública é tratada a partir de uma nova concepção em termos de gestão, de modo que foi criado um sistema de defesa social, do qual fazem parte todos os órgãos de segurança, cuja atuação se dá de forma integrada, em todos os níveis de execução.

Conforme se observou neste estudo, o Brasil é o país que tem o maior crescimento de internautas no mundo e já possui a 5ª colocação dentre os países com maior número de usuários da Internet, daí a crescente preocupação com a segurança virtual.

Observou-se, também, que os crimes virtuais são os mais variados possíveis, configurando-se desde uma simples invasão de computadores a ações de terrorismo, racismo, tráfico de mulheres e pedofilia.

Para combater essa criminalidade, em alguns municípios brasileiros já foram criadas delegacias especializadas e núcleos de inteligência interligados com diversos órgãos estatais e da sociedade civil, com o intuito de centralizar as informações e melhor capacitar os policiais que atuam nesse campo. No entanto, por falta de uma legislação adequada e que dê melhor suporte às ações da polícia, muito pouco se fez, até o momento, no enfrentamento a esses crimes.

No Estado de Minas Gerais não foi diferente. A criação recente da Coordenadoria Estadual de Combate aos Cibercrimes tem o intuito de integrar as ações do Ministério Público com as realizadas pela Diretoria de Inteligência da PMMG. Entretanto, esta integração está apenas no início e há muito que se fazer ainda.

Ao se pesquisar 76 Batalhões e Companhias Independentes, geograficamente distribuídos em todo o território mineiro, constatou-se que a quase totalidade dos policiais nem sequer tem conhecimento a respeito dos cibercrimes e aqueles que possuem algum conhecimento o adquiriram através dos meios de comunicação.

Também se observou a falta de pessoal qualificado para a transferência do conhecimento, falta de materiais e equipamentos para o treinamento de policiais nesta área, bem como a falta de comunicação e troca de informações entre os batalhões e companhias.

7.2 Propostas

Pelas conclusões chegadas através da presente pesquisa, é possível afirmar que os crimes praticados através da Internet vêm aumentando consideravelmente no Brasil, em todos os estados, nas pequenas, médias e grandes cidades. Concluiu-se também que, para que haja uma atuação efetiva e com melhores êxitos da PMMG, tanto em seus aspectos preventivos como repressivos, faz-se necessário que a Corporação se prepare adequadamente para essa importante missão, e que haja uma legislação específica sobre os crimes cibernéticos, de modo que as condutas delituosas sejam

tipificadas, permitindo que o ciclo de polícia seja completo e que os criminosos sejam punidos na exata medida de suas condutas. Assim, são apresentadas as seguintes propostas:

1) Criar, na estrutura da Diretoria de Inteligência, um setor para cuidar especificamente dos crimes cibernéticos, com a missão de elaborar doutrina e normas de conduta operacional, padronizar as ações da PMMG em todo o Estado, centralizar e gerenciar o banco de dados sobre os criminosos da Internet e ser referência da PM no trato desta questão junto a todos os órgãos afins.

2) Criar, na estrutura da Polícia Militar, junto às Agências de Inteligência, núcleos regionais, descentralizados e qualificados, que sejam interligados entre si e à Diretoria de Inteligência, com a missão de atuarem exclusivamente nos crimes cibernéticos.

3) Criar programas e cursos de capacitação e treinamento de pessoal, para que os policiais possam atuar de forma concreta na prevenção e repressão aos crimes cibernéticos.

4) Disponibilizar, nos setores de inteligência que cuidarão dos cibercrimes, equipamentos e mobiliário, como computadores, impressoras, mesas, cadeiras, salas separadas e outros materiais de apoio, como cartilhas e manuais, para à efetiva atuação dos policiais militares.

5) Promover campanhas educativas junto à comunidade, com o envolvimento da mídia e em parceria com outros órgãos e entidades, visando a conscientização da população e para que os cidadãos atuem como agentes fiscalizadores no combate aos cibercrimes.

6) Adquirir *softwares* específicos para o rastreamento e localização de IPs, visando facilitar a busca de informações e a identificação dos criminosos da Internet.

7) Através da Diretoria de Inteligência, integrar-se com os demais órgãos do sistema de defesa social, com as forças policiais de outros estados da Federação, com o Serviço de Inteligência das Forças Armadas, com o Ministério Público Estadual e Federal, com a Polícia Federal, com o Poder Judiciário, a Polícia Rodoviária Federal, com os demais órgãos governamentais e da sociedade civil, para a permanente troca de informações quanto aos cibercrimes, objetivando as seguintes ações:

a) troca de informações disponíveis em banco de dados sobre criminosos e arquivos informatizados sobre crimes planejados através da Internet;

b) atuação em apoio aos municípios na ação fiscalizadora junto a estabelecimentos comerciais que disponibilizam computadores para lazer e pesquisa, principalmente as *lan houses*;

c) atuação preventiva e repressiva no combate à pedofilia através da Internet;

d) atuação preventiva e repressiva nos atos de vandalismo, nos crimes de dano e brigas entre torcidas organizadas, planejados e divulgados por meio da Internet;

e) atuação preventiva no combate aos crimes bancários, fraudes, estelionatos, crimes do comércio e os diversos golpes praticados com o uso da Internet;

f) atuação preventiva, com ênfase para a Copa do Mundo de 2014, principalmente no que tange às ações terroristas, em suas diversas modalidades.

8) Nos municípios onde houver legislação específica, firmar parceria visando à participação da PMMG no apoio e na fiscalização dos estabelecimentos denominados *lan houses* e outros similares, como forma de atuar preventivamente em relação aos crimes cibernéticos.

9) Inserir na grade curricular dos cursos de formação da Academia da Polícia Militar, na disciplina de Direito, ensinamentos sobre crimes cibernéticos, incluindo visitas a órgãos e entidades afins.

REFERÊNCIAS BIBLIOGRÁFICAS

ABCID – ASSOCIAÇÃO BRASILEIRA DE CENTROS DE INCLUSÃO DIGITAL. **Só 14% dos delitos virtuais ocorrem em lan house.** Disponível em: http://www.abcid.org.br/so-14-dos-delitos-virtuais-ocorrem-em-lan-house; Acesso em: 04/08/2010.

AGREGA. Hephesto. **Como nasceu o Twitter.** 2009. Disponível em: http://www.hephesto.com/agrega/; Acesso em 23/05/2010.

ALBINO, Priscilla Linhares; TERÊNCIO, Marlos Gonçalves. Considerações Críticas Sobre o Fenômeno do Bullying: Do Conceito ao Combate e à Prevenção. **Revista Jurídica do Ministério Público Catarinense**, n. 15, jul./dez. 2009, p.169-195. Disponível em: http://www.mp.sc.gov.br/portal/site/conteudo/cao/cij/bullying/artigo%20bullying%20final.pdf; Acesso em 26/07/2010.

BAUMAN, Zygmunt. **Modernidade e ambivalência.** Rio de Janeiro: Jorge Zahar, 1999.

BERNARDINO, Anabela Moreira, et al. **Autenticação**. Universidade do Minho. Escola de Engenharia. Departamento de Sistemas de Informação. 2004. Disponível em: <http://papadocs.dsi.uminho.pt:8080/retrieve/79/ce_autentica%C3%A7%C3%A3o.pdf>; acessado em 06/09/2006.

BLUM Renato O.; ABRUSIO, Juliana C. Crimes Eletrônicos: os crimes eletrônicos exigem uma solução rápida e especializada. **Revista Evidência Digital**, cidade. n1, p.6, jan./mar.2004. Disponível em: <http://www.guiatecnico.com.br/EvidenciaDigital/Download.asp?id=01 >. Acesso em 10 fev 2010.

Brasil Escola. **Cuidados que os alunos devem ter nas salas de bate-papo.** Disponível em: http://www.brasilescola.com/educacao/cuidados-com-bate-papo.htm; Acesso em: 03/07/2010.

BRITO, José Augusto Pereira. **Uma Reflexão sobre a Revolução da Informação e da Comunicação.** 2. ed. São Paulo: Atlas, 2002.

BUNCE, David; SCHARRER, Werner. **A fraude no Brasil – Relatório da Pesquisa 2004.** Disponível em: < http:// www. kpmg. com. br/ publicacoes/ forensic/ Fraudes 2004 site. pdf >. Acesso em: 20 jan 2010.

CÂMARA, Adriane. **Gênero e sexualidade na revista Sexy: um roteiro para a masculinidade heterossexual.** 2007. Dissertação (Mestrado em Educação) Universidade Federal do Rio Grande do Sul, Porto Alegre, 2007.

CAMPANA, Fábio. **Nova lei acaba com o anonimato dos usuários de lan houses.** Disponível em: http://www.fabiocampana.com.br/2009/06/nova-lei-acaba-com-o-anonimato-dos-usuarios-de-lan-houses/.; Acesso em 05/08/2010.

CARVALHO, Gustavo de; LOTITO, Alberto. **Tecnologias de Acesso à Internet.** São Paulo, Novatec, 2005.

CASTELLS, Manuel. **A era da informação: Economia, sociedade e cultura.** Vol. II. O poder da identidade. São Paulo: Paz e Terra, 1999.
ECommerceOrg. **Evolução da Internet e do e-commerce.** Disponível em: http://www.ecommerceorg.com.br/stats.php; Acesso em 03/05/2010.

CPMI. **Relatório final da Comissão Parlamentar Mista de Inquérito**. Brasília, DF: Senado Federal, 2004.

FERES NETO, Alfredo. 2005. **Videogame e educação física/ciências do esporte: uma abordagem à luz das teorias do virtual.** Disponível em http://www.efdeportes.com/Revista Digital – Buenos Aires – Año 10 -- nº 88 – Setiembre de 2005, Acesso em 30/07/2010.

FERREIRA, Alex. **O perigo que cresce com o Twitter. Olhar Digital. I/O Tecnologia.** Disponível em: http://www.iotecnologia.com.br/perigo-twitter-url/.; Acesso em 14/06/2010.

FREE LEGAL ADVICE HELP. **Estatísticas Lawsuit On violação de direitos autorais.** Disponível em: http://www.freelegaladvicehelp.com/Portuguese/copyrights/copyright-infringement/Lawsuit-Statistics-On-Copyright-Infringement.html; Acesso em 13/04/2010.

GLOBO.COM. **STJD divulga quarta se denuncia Neymar. Jogador já foi intimado.** 17/08/2010 12h00 - Atualizado em 17/08/2010 12h37. Disponível em: http://globoesporte.globo.com/futebol/times/santos/noticia/2010/08/stjd-divulga-quarta-se-denuncia-neymar-que-pode-pegar-quatro-jogos.html; Acesso em 18/08/2010.

I/O Tecnologia. O perigo que cresce com o Twitter. Disponível em: http://www.iotecnologia.com.br/perigo-twitter-url/; Acesso em 23/06/2010.

JUCÁ, K. R. L. **Uma Abordagem de Detecção de Intrusão Baseada no Sistema Imunológico Humano**. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, Florianópolis, SC, Dezembro 1998.

LAKATOS, Eva Maria; MARCONI, Maria de Andrade. **Metodologia Científica.** 6. ed. São Paulo: Atlas, 2001.

LARKIN, Daniel. Combate ao crime on-line. **Revista e-Journal USA - Questões Globais.** mar. 2006. Disponível em: < http: // www. america. gov/ media/ pdf/ ejs/ 0306ejpo.pdf > Acesso em 08 mar 2010.

LGF - LUIZ FLÀVIO GOMES. SANTOS, Andrea Alves dos. **Da produção de provas pelo magistrado no processo penal.** Disponível em: http://www.lfg.com.br/public_html/article.php?story=20081007105909522&mode=print.; Acesso em: 28/07/2010.

LIBÓRIO, Luís Alencar; MOTA, A.R.S; MOREIRA, J.G.. Midia e valores familiares numa abordagem psicossocial. In: **V Semana de Integração Universidade Católica e Sociedade e XIX Jornada de Iniciação Científica**, 2007, RECIFE-PE. Anais eletrônicos - UNICAP. RECIFE-PE: UNICAP, 2007, v. 1. p. 552-557.

LYNCH, R. P. **Alianças de negócios, a arma secreta competitiva:** como planejar, negociar e gerenciar alianças estratégicas competitivas. São Paulo: Ed. Makron Books, 1994.

MARTINS, Fabrício. **A impunidade na Internet está com os dias contados.** 07 mar 2005. Disponível em: < http: // www1. folha. uol. com. br/ folha/ informatica/ ult124u18101. shtml >. Acesso em 20 jan. 2010.

MENDES, Douglas Rocha. **Rede de Computadores Teoria e Prática.** Primeira impressão: julho, 2007.

MENEZES, H. **Comércio eletrônico para pequenas empresas.** Florianópolis: Visual Books, 2003.

Metamorfose Digital. **As estatísticas da Internet em 2009.** Disponível em: http://www.mdig.com.br/index.php?itemid=10066; Acesso em 14/04/2010.

MILITELLI, Leonardo Cavallari. **Ameaças em ambientes interconectados:** Os desafios atuais de Auditoria. Disponível em: <http://nsrav.lsi.usp.br/>. Acesso em 27 jan. 2010.

Ministério Público de Santa Catarina. **Navegação Segura na Internet e Combate à Pedofilia - informe-se.** Disponível em: http://www.mp.sc.gov.br/portal/site/portal/portal_detalhe.asp?campo=8105; Acesso em 16/05/2010.

MINISTÉRIO PÚBLICO FEDERAL 2006, apud SANTOS, 2009, p.80

MOTTA, Sylvio; DOUGLAS, William. **Direito Constitucional - Teoria, Jurisprudência e 1000 questões.** Unidades 1 a 3. Disponível em: http://www.scribd.com/doc/20536855/Direito-Constitucional-Teoria-Jurisprudencia-e-1000-questoes-Unidades-1-a-3-2004-SYLVIO-MOTTA-WILLIAM-DOUGLAS; Acesso em 27/07/2010.

NET Usuability. International Standards for HCI and usability, 2002. Disponível em: http://www.hostserver150.com/usabilit/tools/r_international.htm; Acesso em: 11/07/2010.

NG, Reynaldo. **Forense Computacional Corporativa.** Rio de Janeiro: Brasport, 2007.

NORONHA, E. Magalhães. **Curso de Direito Processual Penal**. 25 ed. São Paulo: Saraiva, 1997.

Observatório da Infância. **Bullying na Internet leva adolescente ao suicídio.** Rio de Janeiro 18 janeiro 2008. Disponível em: http://www.observatoriodainfancia.com.br/article.php3?id_article=296; Acesso em 15/07/2010.

ORKUT. Disponível em: www.orkut.com; Acesso em: 06/07/2010.

OSBORNE, D. & GAEBLER, T. **Reinventando o Governo: Como o Espírito Empreendedor está Transformando o Setor Público.** Editora MH Comunicação, Brasília, DF, 1992.

PEW INSTITUTE. 2007. **47-Nation Pew Global Attitudes Survey.** Disponível em: http://www.pewglobal.org; Acesso em 4/05/2010.

PROCURADORIA DA REPÚBLICA NO ESTADO DE GOIÁS. **Entrevista**. Procuradores da República do Grupo de Combate ao Crime Cibernético. Disponível em: http://www.prgo.mpf.gov.br/fato_tipico/pagina_edicoes002-entrevista.html; Acesso em 28/07/2010.

PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO. MINISTÉRIO PÚBLICO FEDERAL. Crimes Cibernéticos: Manual Prático De Investigação. São Paulo: abril de 2006.

QUINTILIANO, Paulo. **The International Journal of Forensic Computer Science (IJoFCS)**. Disponível em: <http://cnasi.com.br>. Tradução livre. Acesso em 20 jan. 2010.

REIS, Marcelo; GEUS, P. **Modelagem de Um Sistema Automatizado de Análise Forense:** Arquitetura Extensível e Protótipo Inicial, 2002.

Revista Âmbito Jurídico. **A Internet e os direitos Autorais.** Disponível em: http://www.ambito-juridico.com.br/pdfsGerados/artigos/173.pdf; Acesso em 15/04/2010.

REVISTA ÉPOCA. **O Twitter vê e mostra tudo.** 13/03/2009. Disponível em: http://revistaepoca.globo.com/Revista/Epoca/0,,EMI64069-15228,00-O+TWITTER+VE+E+MOSTRA+TUDO.html; Acesso em 22/06/2010.

ROHR, Altieres. **Entenda o que faz um hacker e a polêmica em torno desta palavra.** Portal G1, 05/01/09 - 08h51 - Atualizado em 05/01/09 - 08h52. Disponível em: http://g1.globo.com/Noticias/Tecnologia/0,,MUL943271-6174,00-ENTENDA+O+QUE+FAZ+UM+HACKER+E+A+POLEMICA+EM+TORNO+DESTA+PALAVRA.html; Acesso em 13/09/2010.

SaferNet Brasil. **Indicadores: Central Nacional de Denúncias.** Disponível em: http://www.safernet.org.br/site/indicadores; Acesso em 12/05/2010.

SANTOS, Ana Carolina Oliveira dos. **Ser ou não ser Internauta?** Os significados da internet a partir do seu uso para jovens graduandos em redes de computadores na cidade de Salvador. Dissertação de Mestrado apresentada à Universidade Católica do Salvador. Salvador, 2009.

SANTOS, Coriolano Aurélio Almeida Camargo. **As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico.** São Paulo: OAB/SP, 2009.

SANTOS, Coriolano Aurélio Almeida Camargo. **Atual Cenário dos Crimes Cibernéticos no Brasil.** 2009. Disponível em: http://www2.oabsp.org.br/asp/comissoes/sociedade_informacao/artigos/crimes_ciberneticos.pdf; Acesso em 13/04/2010.

SENADO FEDERAL. Portal de Notícias. **Azeredo: lei dos cibercrimes nos alinha com o primeiro mundo.** Disponível em: http://www.senado.gov.br/noticias/verNoticia.aspx?codNoticia=76866&codAplicativo=2; Acessso em 03/08/2010.

SILVA, Tomaz Tadeu da (org.). **Quem precisa da identidade?** Petrópolis (RJ): Vozes, 2000.

Twitter Brasil. Maio de 2009. In: **Estatística do Twitter no Brasil.** Mestre Seo. Disponível em: http://www.mestreseo.com.br/twitter-seo/estatisticas-twitter-brasil; Acesso em 25/06/2010.

TELLES, A. **Orkut.com: como você e sua empresa podem tirar proveito do maior site de relacionamento do Brasil.** São Paulo: Landscape, 2005.

TORNAGHI, Hélio. **Instituições de processo penal.** São Paulo: 1963, vol. II.

TOURINHO FILHO, Fernando da Costa. **Processo Penal**. 3 v. 20 ed. São Paulo: Saraiva, 1998.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração.** São Paulo: Atlas, 2000.

VIANNA, Túlio Lima. **Dos crimes por computador.** Revista dos tribunais, São Paulo, v.91, n.801, p.405-421, jul. 2004

ANEXOS

Anexo 1 – Glossário

- **Ameaça**: Crime (de ação privada) que consiste em ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de modo a causar-lhe mal injusto e grave. O crime vem descrito no art. 147 do Código Penal Brasileiro.

- **Apologia ao Crime ou Fato Criminoso**: é a publicação de um fato criminoso ou de um autos de um crime.

- **Apple Inc**.: é uma empresa multinacional norte-americana que atua no ramo de aparelhos eletrônicos e informática famosa principalmente pela fabricação do computador de marca registrada, Macintosh, com seu próprio sistema operacional, Mac OS, entre outros produtos.

- **Apropriação Indébita**: É a posse legítima de coisa alheia móvel, porém vindo o agente a se comportar como dono da coisa, é o crime previsto no artigo 168 do Código Penal brasileiro.

- **Bullying**: é um termo inglês utilizado para descrever atos de violência física ou psicológica, intencionais e repetidos, praticados por um indivíduo (bully - «tiranete» ou «valentão») ou grupo de indivíduos com o objetivo de intimidar ou agredir outro indivíduo (ou grupo de indivíduos) incapaz(es) de se defender.

- **CD-ROM**: Os CD-ROM podem armazenar qualquer tipo de conteúdo, desde dados genéricos, vídeo e áudio, ou mesmo conteúdo misto. Os leitores de áudio normais só podem interpretar um CD-ROM, caso este contenha áudio.

- **Cibercrimes**: é a palavra dada a uma prática que consiste em fraudar a segurança de computadores ou redes empresariais.

- **Cyberbullying**: é um conjunto de comportamentos agressivos, intencionais e repetitivos que são adotados por um ou mais alunos contra outros colegas via *blogs, Orkut, YouTube*, entre outros tipos de sites, além de mensageiros instantâneos e mensagens de texto escritas no telefone celular.onde podem modificar as suas fotos e coloca-las na internet.

- **Cracker**: indivíduo que invade sistemas com o objetivo de destruir redes ou promover golpes burlando sistemas.

- **Crime do Colarinho Branco**: é uma modalidade de crime cometido por uma pessoa respeitável, de alta posição social, no exercício de suas ocupações.

- **Crime Organizado**: é toda organização cujas atividades são destinadas a obter poder e lucro, transgredindo as leis formais das sociedades.

- **Crimes Cibernéticos**: crimes que são cometidos na internet ou que se utilizam da mesma para sua consecução.

- **Cyber Café**: é um local que, podendo funcionar também como bar ou lanchonete, oferece a seus clientes acesso à internet, mediante o pagamento de uma taxa, usualmente cobrada por hora.

- **Cyberstalking**: é o constrangimento cibernético quando se estar navegando.

- **Disseminação de Programas Maliciosos**: são programas instalados através da internet (*Web*) com a finalidade de instalar vários tipos de vírus que deterioram a memória do computador.

- **Espionagem Econômica**: atividade que visa o recolhimento de notícias ou informações por métodos clandestinos ou legais.

- **Estelionato**: é obter para si ou para outrem vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento, captulado no artigo 171 do Código Penal Brasileiro.

- **Facebook**: é uma rede social lançada em 4 de fevereiro de 2004. Foi fundado por Mark Zuckerberg, um ex-estudante de Harvard. Inicialmente, a adesão ao *Facebook* era restrita apenas aos estudantes da Universidade Harvard.

- **Falsificação**: é copia ou reprodução de um produto ou um serviço, de forma a adotar uma marca pertencente a outro.

- **Fraude Cibernética**: é a falsificação ou acesso sem autorização a sistemas de computador, cópia ilegal de programas de computador.

- **Furto**: é uma figura de crime prevista nos artigos 155 do Código Penal Brasileiro, e 203º do Código Penal Português, que consiste na subtração de coisa alheia.

- **Hacker**: pessoas com alta capacidade mental que utilizam sua inteligência para prejudicar de alguma forma o ambiente computacional das empresas.

- **IBM**: International Business Machines é uma empresa estadunidense voltada para a área de informática.

- **Internet**: é um conglomerado de redes em escala mundial de milhões de computadores interligados pelo TCP/IP que permite o acesso a informações e todo tipo de transferência de dados.

- **Lan House**: é um estabelecimento comercial onde, à semelhança de um cybercafé, as pessoas podem pagar para utilizar um computador com acesso à internet e a uma rede local, com o principal fim de acesso à informação rápida pela rede e entretenimento através dos jogos em rede ou online.

- **Lavagem de Dinheiro**: é uma expressão que se refere a práticas econômico-financeiras que têm por finalidade dissimular ou esconder a origem ilícita de determinados ativos financeiros ou bens patrimoniais, de forma a que tais ativos aparentem uma origem lícita ou a que, pelo menos, a origem ilícita seja difícil de demonstrar ou provar.

- **Login**: é um conjunto de caracteres solicitado para os usuários que por algum motivo necessitam acessar algum sistema computacional. Geralmente os sistemas computacionais solicitam um login e uma senha para a liberação do acesso.

- **MySpace**: é um serviço de rede social que utiliza a Internet para comunicação *online* através de uma rede interativa de fotos, *blogs* e perfis de usuário. Foi criada em 2003.

- **MSN Messenger**: é um programa da mensagens instantâneas criado pela Microsoft Corporation. O serviço nasceu a 22 de Julho de 1999, anunciando-se como um serviço que permitia falar com uma pessoa através de conversas instantâneas pela Internet.

- **Orkut**: é uma rede social filiada ao Google, criada em 24 de Janeiro de 2004 com o objetivo de ajudar seus membros a conhecer pessoas e manter relacionamentos. Seu nome é originado no projetista chefe, Orkut Büyükkokten, engenheiro turco do Google.

- **Password**: é uma palavra ou uma ação secreta previamente convencionada entre duas partes como forma de reconhecimento. Em sistemas de computação, senhas são amplamente utilizadas para autenticar usuários e conceder-lhes privilégios — para agir como administradores de um sistema, por exemplo — ou permitir-lhes o acesso a informações personalizadas armazenadas no sistema.

- **Pornografia Infantil**: é uma forma ilegal de pornografia que utiliza crianças pré-púberes, ou, num sentido mais amplo, de crianças e adolescentes menores de idade.

- **Sabotagem ou Espionagem Industrial**: é o seqüestro de informações e a manipulação de dados e alterações estatísticas.

- **Skype**: é um software que permite comunicação pela Internet através de conexões de voz sobre IP (*VoIP*).

- **Terrorismo Cibernético**: é a utilização de técnicas de destruição e/ou incapacitação de redes de computadores, por terroristas.

- **Tráfico de Drogas**: é o tráfico de substâncias ilícitas, entorpecentes.

- **Twitter**: é uma rede social e servidor para *microblogging* que permite aos usuários enviar e receber atualizações pessoais de outros contatos (em textos de até 140 caracteres, conhecidos como "*tweets*"), por meio do *website* do serviço, por SMS e por *softwares* específicos de gerenciamento.

- **Vandalismo**: é uma ação motivada pela hostilidade contra a arte de uma cultura, ou destruição intencional de bens e propriedades alheios.

- **Wireless**: refere-se a uma rede de computadores sem a necessidade do uso de cabos – sejam eles telefônicos, coaxiais ou ópticos – por meio de equipamentos que usam radiofrequência (comunicação via ondas de rádio) ou comunicação via infravermelho, como em dispositivos compatíveis com IrDA.

Anexo 2 – Modelo de Questionário enviado aos Batalhões e Companhias Independentes

POLÍCIA MILITAR
DE MINAS GERAIS

ACADEMIA DE POLÍCIA MILITAR
CENTRO DE PESQUISA E PÓS GRADUAÇÃO

Belo Horizonte, abril de 2010.

Prezado Companheiro!

Estou cursando, atualmente, o Curso de Especialização em Segurança Pública (CESP-2010), na Academia da Polícia Militar, e estou desenvolvendo uma pesquisa cujo Tema é "***A Atuação da PMMG na prevenção e repressão aos crimes cibernéticos"***. Assim, gostaria de merecer a sua gentileza em responder, sincera e atenciosamente, o questionário abaixo, para subsidiar o presente estudo. A sua resposta será de grande importância para a consolidação dos dados da pesquisa e contribuirá significativamente para a formulação de propostas para futuras medidas a serem implementadas pela Polícia Militar. Não é necessário se identificar.

Atenciosamente,

Alexander Dias Martins, Cap PM
Aluno do CESP

1) Há quanto tempo é Chefe da 2ª Seção?

a) ( ) há menos de 01 ano;

b) ( ) de 01 a 02 anos;

c) ( ) de 02 a 03 anos;

d) ( ) de 03 a 04 anos;

e) ( ) há mais de 04 anos.

2) Você tem conhecimento sobre crimes cibernéticos?

a) ( ) sim; conheço totalmente;

b) ( ) sim, porém tenho pouco conhecimento;

c) ( ) não tenho conhecimento.

3) Indique como você normalmente toma conhecimento sobre os crimes cibernéticos na área de sua unidade **(pode marcar mais de uma opção).**

a) ( ) através do noticiário da imprensa;

b) ( ) somente através das ocorrências registradas;

c) ( ) só por ouvir dizer;

d) ( ) através do SIPOM e boletins internos;

e) ( ) não toma conhecimento.

4) Indique como a sua unidade tem atuado preventiva e/ou repressivamente em relação aos crimes cibernéticos **(pode marcar mais de uma opção).**

a) ( ) a unidade lida freqüentemente com esses crimes;

b) ( ) os militares atuam esporadicamente em relação aos crimes cibernéticos, por falta de uma melhor definição legal sobre esses delitos;

c) ( ) o assunto é totalmente desconhecido pelos militares da unidade;

d) ( ) a unidade atende ocorrências dessa natureza, quando acionada, porém não atua preventivamente.

e) ( ) a unidade não atua nesses crimes;

5) Caso tenha respondido SIM em relação à 2ª pergunta, cite os principais crimes cibernéticos com os quais já lidou ou tem conhecimento:

_____

_____

---

6) Quantas ocorrências sobre crimes cibernéticos foram registradas nesse Batalhão/Companhia Independente, no período de janeiro de 2007 a dezembro de 2009? **Considere para resposta o total de ocorrências no período mencionado.**

a) ( ) menos de 10 registros (quantas?_____);

b) ( ) De 10 a 20 registros;

c) ( ) De 20 a 30 registros;

d) ( ) De 30 a 40 registros;

e) ( ) Mais de 40 registros.

7) Na sua Unidade, como têm sido tratados os casos de crimes cibernéticos? **(pode marcar mais de uma opção)**.

a) ( ) a unidade não tem sido acionada para atuar nesses crimes;

b) ( ) a unidade não lida com a questão porque os crimes cibernéticos não estão claramente definidos na DIAO;

c) ( ) não há, oficialmente, banco de dados sobre crimes cibernéticos;

d) ( ) não há, na unidade, pessoal destinado exclusivamente para lidar com esses crimes;

e) ( ) a PM ainda não está estruturada para lidar com os crimes cibernéticos;

8) Em termos de estrutura logística e de pessoal, na sua Unidade, quais são as dificuldades encontradas no atendimento a ocorrências envolvendo crimes virtuais? **(pode marcar mais de uma opção)**

a) ( ) falta de ferramentas adequadas: computadores, mobiliário, sala específica;

b) ( ) falta de pessoal devidamente capacitado e treinado para essa finalidade;

c) ( ) dificuldades no encerramento das ocorrências na Delegacia;

d) ( ) falta doutrina na Corporação para o devido tratamento a esses crimes;

e) ( ) os militares têm dificuldades para definir quais são os crimes cibernéticos;

9) Na sua opinião, como deve ser a atuação da PMMG em relação aos crimes cibernéticos? **(pode marcar mais de uma opção).**

a) ( ) deve atuar preventiva e repressivamente em todas as ocorrências;

b) ( ) deve atuar preventivamente em todos os crimes e, repressivamente, somente nos crimes de ação pública e de ação pública incondicionada;

c) ( ) somente deve atuar quando for acionada;

d) ( ) a PM precisa se preparar tecnicamente e se estruturar em todo o Estado, para melhor lidar com esses crimes;

e) ( ) definitivamente, a PM não deve atuar nesses crimes.

10) Na sua opinião, para que a PMMG seja adequadamente estruturada, a fim de lidar com os crimes cibernéticos, ela precisa: **(pode marcar mais de uma opção)**

a) ( ) criar uma doutrina para essa finalidade;

b) ( ) buscar parcerias diversas, com a comunidade, com o Ministério Público e o Poder Judiciário, com as demais forças policiais (estaduais e federais) e com entidades que lidam com a questão;

c) ( ) capacitar pessoal em todas as unidades operacionais;

d) ( ) ter acesso a banco de dados sobre crimes cibernéticos;

e) ( ) destinar militares, equipamentos e sala nas unidades, para lidarem exclusivamente com os crimes cibernéticos;

Anexo 3 – Relação de Batalhões e Companhias Independentes pesquisados

1	1º BPM (Batalhão)	Belo Horizonte
2	2º BPM	Juiz de Fora
3	3º BPM	Diamantina
4	4º BPM	Uberaba
5	5º BPM	Belo Horizonte
6	6º BPM	Valadares
7	7º BPM	Bom Despacho
8	8º BPM	Lavras
9	9º BPM	Barbacena
10	10º BPM	Montes Claros
11	11º BPM	Manhuaçu
12	12º BPM	Passos
13	13º BPM	Belo Horizonte
14	14º BPM	Ipatinga
15	15º BPM	Patos de Minas
16	16º BPM	Belo Horizonte
17	17º BPM	Uberlândia
18	18º BPM	Contagem
19	19º BPM	Teófilo Otoni
20	20º BPM	Pouso Alegre
21	21º BPM	Ubá
22	22º BPM	Belo Horizonte
23	23º BPM	Divinópolis
24	24º BPM	Varginha
25	25º BPM	Sete Lagoas
26	26º BPM	Itabira
27	27º BPM	Juiz de Fora
28	28º BPM	Unaí
29	29º BPM	Poços de Caldas
30	30º BPM	Januária
31	31º BPM	Conselheiro Lafaiete
32	32º BPM	Uberlândia
33	33º BPM	Betim
34	34º BPM	Belo Horizonte
35	35º BPM	Santa Lucia
36	36º BPM	Vespasiano
37	37º BPM	Araxá
38	38º BPM	São João Del Rei
39	39º BPM	Contagem
40	40º BPM	Ribeir]ao das Neves
41	41º BPM	Belo Horizonte
42	42º BPM	Curvelo
43	43º BPM	Valadares
44	44º BPM	Araruama
45	45º BPM	Paracatu
46	46º BPM	Patrocínio
47	47º BPM	Muriaé
48	48º BPM	Ibirité
49	49º BPM	Belo Horizonte
50	50º BPM	Montes Claros

51	51º BPM	Janaúba
52	1ª Companhia Independente	Nova Lima
53	2ª Companhia Independente	Taiobeiras
54	3ª Companhia Independente	Itaurama
55	4ª Companhia Independente	Frutal
56	5ª Companhia Independente	Itajubá
57	6ª Companhia Independente	Leopoldina
58	7ª Companhia Independente	Igaparé
59	8ª Companhia Independente	Ouro Preto
60	9ª Companhia Independente	Araguarí
61	10ª Companhia Independente	Ituitaba
62	11ª Companhia Independente	Pirapora
63	13ª Companhia Independente	Formiga
64	14ª Companhia Independente	São Lourenço
65	15ª Companhia Independente	Sabará
66	16ª Companhia Independente	Três Corações
67	17ª Companhia Independente	João Moulevade
68	18ª Companhia Independente	Alfenas
69	19ª Companhia Independente	Pará de Minas
70	20ª Companhia Independente	São Sebastião do Paraíso
71	21ª Companhia Independente	Ponte Nova
72	22ª Companhia Independente	Caratinga
73	23ª Companhia Independente	Capelinha
74	24ª Companhia Independente	Nanuque
75	25ª Companhia Independente	Guanhães
76	26ª Companhia Independente	Itaobim

Anexo 4 – Projeto de Lei Nº 907/2006

Dispõe sobre as atividades de "Lan Houses", "Cybercafés", "Cyber Offices" e estabelecimentos congêneres no município de Belo Horizonte.

A Câmara Municipal de Belo Horizonte decreta:

Art. 1º - São regidos por esta lei os estabelecimentos comerciais instalados no Município de Belo Horizonte que ofertam a locação de computadores e máquinas para acesso à internet, utilização de programas e de jogos eletrônicos, abrangendo os designados como "lan houses", cibercafés e "cyber offices", entre outros.

Art. 2º - Os estabelecimentos de que trata esta lei ficam obrigados a criar e manter cadastro atualizado de seus usuários, contendo:

I - nome completo;

II - data de nascimento;

III - endereço completo;

IV - telefone;

V - número de documento de identidade.

§ 1º - O responsável pelo estabelecimento deverá exigir dos interessados a exibição de documento de identidade, no ato de seu cadastramento e sempre que forem fazer uso de computador ou máquina.

§ 2º - O estabelecimento deverá registrar a hora inicial e final de cada acesso, com a identificação do usuário e do equipamento por ele utilizado.

§ 3º - Os estabelecimentos não permitirão o uso dos computadores ou máquinas:

I - a pessoas que não fornecerem os dados previstos neste artigo, ou o fizerem de forma incompleta;

II - a pessoas que não portarem documento de identidade, ou se negarem a exibi-lo.

§ 4º - As informações e o registro previstos neste artigo deverão ser mantidos por, no mínimo, 60 (sessenta) meses.

§ 5º - Os dados poderão ser armazenados em meio eletrônico.

PL 907/2006

DIRLEG | FL. 02

CÂMARA MUNICIPAL DE BELO HORIZONTE

§ 6º - O fornecimento dos dados cadastrais e demais informações de que trata este artigo só poderá ser feito mediante ordem ou autorização judicial.

§ 7º - Excetuada a hipótese prevista no § 6º, é vedada a divulgação dos dados cadastrais e demais informações de que trata este artigo, salvo se houver expressa autorização do usuário.

Artigo 3º. É vedado aos estabelecimentos de que trata esta lei:

I - permitir o ingresso de pessoas menores de 12 (doze) anos sem o acompanhamento de, pelo menos, um de seus pais ou de responsável legal devidamente identificado;

II - permitir a entrada de adolescentes de 12 (doze) a 16 (dezesseis) anos sem autorização por escrito de, pelo menos, um de seus pais ou de responsável legal;

III - permitir a permanência de menores de 18 anos após a meia-noite, salvo se com autorização por escrito de, pelo menos, um de seus pais ou de responsável legal;

IV - permitir a permanência de menores de 18 anos trajando uniformes escolares.

Parágrafo único - Além dos dados previstos nos incisos I a V do artigo 2º, o usuário menor de 18 (dezoito) anos deverá informar os seguintes:

I - filiação;

II - nome da escola em que estuda e horário (turno) das aulas.

Artigo 4º. Os estabelecimentos de que trata esta lei deverão:

I - expor em local visível lista de todos os serviços e jogos disponíveis, com um breve resumo sobre os mesmos e a respectiva classificação etária, observada a disciplina do Ministério da Justiça sobre a matéria;

II - ter ambiente saudável e iluminação adequada;

III - ser dotados de móveis e equipamentos ergonômicos e adaptáveis a todos os tipos físicos;

IV - ser adaptados para possibilitar acesso a portadores de deficiência física;

V - tomar as medidas necessárias a fim de impedir que menores de idade utilizem contínua e ininterruptamente os equipamentos por período superior a 3 (três) horas, devendo haver um intervalo mínimo de 30 (trinta) minutos entre os períodos de uso;

VI - regular o volume dos equipamentos de forma a se adequar às características peculiares e em desenvolvimento dos menores de idade.

Artigo 5º. São proibidos nos locais a que se refere esta lei a utilização de jogos ou a promoção de campeonatos que envolvam prêmios em dinheiro.

DIRLEG FL. 03

PL 907/2006

CÂMARA MUNICIPAL DE BELO HORIZONTE

Artigo 6º. O Poder Executivo regulamentará esta lei no prazo de 60 (sessenta) dias, especialmente quanto à atribuição para fiscalizar seu cumprimento e impor as penalidades a que se refere o artigo 6º.

Artigo 7º. Esta lei entra em vigor após decorridos 30 (trinta) dias de sua publicação oficial.

Belo Horizonte, 27 de março de 2006.

Totó Teixeira
Vereador – PMDB

PL 907/2006

DIRLEG | FL. 04

CÂMARA MUNICIPAL DE BELO HORIZONTE

JUSTIFICAÇÃO

Apresenta-se esta proposição com o intuito de disciplinar alguns aspectos relativos ao funcionamento de "lan houses", cybercafés, "cyber offices", e estabelecimentos congêneres, que colocam à disposição dos consumidores computadores e outros equipamentos, para acesso à internet, utilização de programas e jogos eletrônicos.

Trata-se de um segmento em franca expansão, o que é altamente positivo, mas que reclama a intervenção do Poder Público, a fim de preservar o bem comum e os interesses dos usuários desses serviços, especialmente os menores de idade.

Atualmente há uma absoluta falta de controle quanto à identificação dos usuários desses estabelecimentos, configurando um foco potencial para a prática de infrações, sob o manto do anonimato.

Portanto, necessário se faz que estes estabelecimentos mantenham um cadastro dos usuários, contendo nome, hora, data e permanência nos computadores, propiciando às autoridades uma possível busca nestes estabelecimentos de infratores que venham a utilizá-los para fins ilícitos como pedofilia, golpes no mercado financeiro, venda de drogas, entre outros.

Outro ponto diz respeito ao ingresso e permanência de menores nesses estabelecimentos. Evidentemente, o que se busca não é a proibição, mas a imposição de limites, em benefício dos próprios menores.

Ainda, proibindo a permanência de menores trajando uniforme escolar aumenta a garantia dos pais destes menores de que seus filhos estão na escola, contribuindo para a diminuição da evasão escolar.

Pretende-se, enfim, contribuir para a saúde, educação, e segurança da sociedade.

DIRLEG | FL. 09

CÂMARA MUNICIPAL DE BELO HORIZONTE

PROJETO DE LEI Nº 907 / 06

Nos termos do art. 87, § 1º, II, "b" da Lei Orgânica, esta proposição sujeita-se ao *quorum* de:

- ☐ Maioria dos presentes;
- ☒ Maioria dos membros da Câmara;
- ☐ 2/3 dos membros da Câmara.

Distribuir em avulsos e encaminhar às seguintes comissões, conforme art. 52 do Regimento Interno:

- **Legislação e Justiça, I, "a";**
- **Direitos Humanos e Defesa do Consumidor, VIII, "d", "g", e "h";**
- **Meio Ambiente e Política Urbana, IV, "h".**

Em 04 / 04 / 2006.

Presidente – CMBH

Avulsos distribuídos em 05/04/06

SECTEC

Anexo 5 – Resolução PGJ Nº 36, de 16 de Junho de 2008

Cria a Coordenadoria Estadual de Combate aos Crimes Cibernéticos.

O Procurador-Geral de Justiça do Estado de Minas Gerais, no exercício das atribuições que lhe confere o art.75 da Lei Complementar nº 34, de 12 de setembro de 1994;

Considerando ser função institucional do Ministério Público, na forma do artigo 129, inciso III, da Constituição Federal, a proteção dos direitos constitucionalmente garantidos e a propositura, em caráter privativo, da ação penal pública, inclusive em se tratando de crimes praticados por meio da rede mundial de computadores;

Considerando que, sendo certa a importância do combate aos crimes cibernéticos, não existe ainda, no âmbito administrativo-organizacional do Ministério Público do Estado de Minas Gerais, unidade especializada que coordene as ações referentes ao desempenho adequado e eficiente das atribuições ministeriais relativas à matéria;

Considerando, por fim, que a criação de uma Coordenadoria Estadual de Combate aos Crimes Cibernéticos constitui iniciativa no sentido de gerar mecanismos de apoio às atividades dos órgãos de execução presentes nas comarcas do Estado, propiciando uma ação conjunta, organizada e eficaz para a efetividade dos direitos garantidos pelo ordenamento jurídico; resolve

Art. 1º Criar, na estrutura do Centro de Apoio Operacional das Promotorias Criminais, de Execução Penal, do Tribunal do Júri e da Auditoria Militar do Ministério Público do Estado de Minas Gerais, a Coordenadoria Estadual de Combate aos Crimes Cibernéticos, denominada Promotoria Estadual de Combate aos Crimes Cibernéticos.

Art. 2º A Coordenadoria Estadual de Combate aos Crimes Cibernéticos, com o objetivo precípuo de, isoladamente ou em conjunto com as demais Promotorias de Justiça do Estado, articular as medidas judiciais e extrajudiciais necessárias à efetivação do combate aos crimes cibernéticos em Minas Gerais, tem por princípio auxiliar, conjugar esforços e dar suporte técnico, jurídico e administrativo às Promotorias de Justiça do Estado de Minas Gerais.

Art. 3º Compete à Coordenadoria Estadual de Combate aos Crimes Cibernéticos:

I - Realizar estudos e pesquisas voltados para a produção, orientação e divulgação de informações quanto à utilização segura das tecnologias de internet, compilando, sistematizando e analisando a legislação e a jurisprudência pertinentes;

II - Propor a celebração de convênios com provedores de serviços na internet ou com outras instituições públicas ou privadas, visando à obtenção de subsídios técnicos aos órgãos de execução, bem como à captação de recursos para o combate aos crimes praticados na rede;

III - Promover, em conjunto com o Centro de Estudos e Aperfeiçoamento Funcional, congressos, seminários e conferências, inclusive em parceria com outras instituições,

sobre temas relevantes e pertinentes ao combate aos crimes cibernéticos;

IV - Promover a integração do Ministério Público do Estado de Minas Gerais com outros Ministérios Públicos Estaduais e Federal, instituições afins e a comunidade;

V - Promover campanhas para conscientização da sociedade em relação à utilização adequada da internet, visando à proteção do cidadão-usuário e à efetiva defesa dos Direitos Humanos na sociedade de informação;

VI - Propor a edição e a publicação de revistas, livros, boletins, cartilhas e material de divulgação, além de produzir relatórios e notas técnicas com o objetivo de orientar as políticas públicas de enfrentamento e a atuação dos membros do Ministério Público no combate aos crimes contra o cidadão-usuário perpetrados com o uso das tecnologias de informação e comunicação;

VII - Manter intercâmbio de caráter técnico, cultural e científico com outras associações e entidades, nacionais ou estrangeiras.

Art. 4º O Procurador-Geral de Justiça designará membro do Ministério Público para dirigir a Coordenadoria Estadual de Combate aos Crimes Cibernéticos e eventualmente outros membros para auxiliá-lo.

Art. 6º Esta Resolução entra em vigor na data de sua publicação.

Art. 7º Revogam-se as disposições em contrário.

Belo Horizonte, 16 de junho de 2008.
JARBAS SOARES JÚNIOR
Procurador-Geral de Justiça