1 INTRODUÇÃO

1.1 DEFINIÇÃO DO PROBLEMA E MOTIVAÇÃO

Vivemos a chamada “era da informação”[1], que tem como característica a crescente facilidade do acesso à informação e ao conhecimento pela propagação de conteúdo via rede mundial de computadores, onde, cada vez mais, as pessoas estão conectadas, e por onde transita um vasto fluxo de dados. É indiscutível que este é um caminho sem volta. Cada vez mais, a internet e os dispositivos conectados são o meio para o desenvolvimento de todo o tipo de atividades – estudo, trabalho, lazer, comunicação, comércio, etc.

Progressivamente, aumentam também os riscos e as ameaças. Tarefas comuns do dia a dia, antes realizadas somente no ambiente “real”, como ir ao banco, fazer compras, etc, são cercadas de riscos; da mesma forma, quando se realiza tais tarefas na internet, deve-se ter o mesmo cuidado, pois os riscos também se transferiram para o ambiente virtual. Cuidado que nem sempre está presente por parte dos usuários, que, especialmente pelo seu comportamento inadequado, ficam expostos aos mais variados perigos na rede.

É neste contexto que se situa o problema que este trabalho se propõe a examinar: os chamados crimes cibernéticos, também conhecidos como crimes de internet, crimes digitais, crimes de informática, ou ainda, cibercrimes; de que forma os usuários de internet são atingidos; como agir para tentar evitá-los; e como o Estado brasileiro empreende o combate e repressão a este mal crescente; quais os principais problemas verificados, e alternativas para a busca de melhores resultados. Ao termino do trabalho, se buscará responder a pergunta-problema:

“Quais os crimes cibernéticos mais incidentes e como se dá a investigação desses delitos no Brasil?”.

A motivação para a escolha do tema foi apresentar um estudo que demonstre a importância de se conhecer os crimes de informática e buscar a prevenção a partir

[1] Segundo Crespo (2011, p.25), comumente se conhece a Era da Informação como o período que vem após a Era Industrial, alicerçado nas invenções do microprocessador, das redes de computadores, da fibra ótica e do computador pessoal.

do conhecimento dos principais problemas relacionados à segurança no uso de computadores e internet, servindo como fonte de pesquisa em caráter não exaustivo mas com o fim de despertar o interesse pelo tema.

1.2 OBJETIVO GERAL

Identificar os crimes cibernéticos e verificar como é feita a investigação policial deste tipo de delito no Brasil.

1.3 OBJETIVOS ESPECÍFICOS

Identificar as ameaças à navegação na rede mundial de computadores; conhecer os crimes cibernéticos, a legislação vigente sobre o tema, a atuação dos órgãos de segurança pública na repressão e os resultados obtidos.

1.4 METODOLOGIA

Foi efetuada uma pesquisa exploratória. A coleta de dados se deu por meio de pesquisa nas obras literárias referenciadas; em sites oficiais de entidades públicas; em sites de organizações não governamentais reconhecidas pelo seu comprometimento com as causas relacionadas ao presente trabalho; e no material disponibilizado na internet por operadores da segurança pública especialistas em crimes cibernéticos.

1.5 ESTRUTURA DO TRABALHO

Inicialmente será apresentada uma contextualização, para melhor compreensão do problema, conceituando-se o meio e atores envolvidos. Assim, serão apresentados conceitos de redes de computadores, internet, crime, usuários, informação e segurança da informação. Também neste capítulo serão apresentadas as principais vulnerabilidades e ameaças presentes na rede de computadores, além

dosprocedimentos de segurança, que se constituem nos meios de prevenção existentes acessíveis aos usuários.

Em seguida será apresentada a definição de crime informático e os tipos penais previstos na legislação, além das diversas condutas on-line que se constituem em crimes e principais formas de atuação dos criminosos.

No capítulo seguinte, serão abordados os aspectos relativos à investigação deste tipo de crime no Brasil; como os órgãos de segurança pública estão estruturados e como procedem na investigação dos principais tipos de crimes de informática.

Por fim, serão apresentadas as conclusões, o que foi apurado relativo ao contexto atual do cibercrime no Brasil, que resultados são obtidos na repressão, quais as principais dificuldades encontradas, chegando-se ao objetivo principal do trabalho, que é o conhecimento desta realidade, buscando nortear uma conduta preventiva.

2 CONTEXTUALIZAÇÃO

Como já dito, o objetivo principal deste trabalho é aprofundar o conhecimento acerca dos chamados crimes cibernéticos e os meios de prevenção e repressão. Introdutoriamente se faz necessário apresentar alguns conceitos acerca do ambiente onde gravitam.

2.1 REDES DE COMPUTADORES

Aurélio Buarque de Holanda em seu Novo dicionário da língua portuguesa, conceitua computador como:

> Máquina capaz de receber, armazenar e enviar dados, e de efetuar, sobre estes, seqüências previamente programadas de operações aritméticas (como cálculos) e lógicas (como comparações), com o objetivo de resolver problemas.

"Redes de computadores" é um termo genérico para denominar uma rede que permite a comunicação entre pontos distintos, ou seja, um sistema que permite a troca de informações e o compartilhamento de recursos entre os dispositivos

conectados (OLIVEIRA e REHDER, 2006). Neste sentido, ante a crescente proliferação de dispositivos que se conectam, devido aos avanços tecnológicos, o termo “redes de computadores” soa quase desatualizado, pois é possível afirmar que computadores, hoje em dia, respondem por apenas uma parcela dos dispositivos conectados. Constantemente surgem novos dispositivos com acesso à rede, para se juntar aos computadores, telefones celulares, televisores, *tablets*, *smartphones*, entre outros, além de incontáveis novos dispositivos que são desenvolvidos e lançados no mercado.

As redes possibilitam que várias pessoas compartilhem dados, programas, periféricos e outros recursos disponíveis, sem se considerar a localização física dos recursos e dos usuários. Uma rede fornece um meio de comunicação eficiente entre pessoas que estão distantes umas das outras.

Oliveira e Rehder (2006, p. 13) assim definem os três componentes mínimos de uma rede: o emissor; o meio através do qual a informação trafega; e o receptor. Descrevem ainda os componentes básicos da rede, que são os seguintes:

a) Servidor: é um computador que oferece algum recurso à rede;

b) Cliente: qualquer micro ou dispositivo que acesse os recursos oferecidos pela rede;

c) Recurso: qualquer item que possa ser oferecido e utilizado pelos clientes de uma rede, tais como arquivos, impressoras, modens, etc;

d) Protocolo: é uma linguagem genérica, que permite que todos os dispositivos de uma rede possam se entender independentemente do programa usado ou fabricante dos componentes;

e) Placa de rede: permite a conexão dos dispositivos à rede. Cada placa de rede possui uma identidade única, um endereço que a individualiza na rede;

f) Hardware de rede: periféricos que podem ser utilizados para efetuar ou melhorar a comunicação de uma rede, como os hubs e roteadores;

g) Cabeamento: cabos através dos quais são transmitidas as informações que são trocadas em uma rede.

As redes recebem ainda classificação quanto à sua área de cobertura, ou escala, sendo assim descritas por Tanenbaum e Wetherall (2011):

a) PAN (Personal Area Network): rede pessoal, que permite a comunicação de dispositivos pelo alcance de uma pessoa; por exemplo, uma rede sem fio que conecta um computador com seus periféricos;

b) LAN (Local Area Network): rede local, composta por dispositivos conectados fisicamente perto um do outro, geralmente no mesmo prédio ou recinto. Enquadram-se nesta definição as redes domésticas e pequenas redes corporativas. Normalmente é uma rede privada. LANS são muito usadas para conectar computadores pessoais e aparelhos eletrônicos, para permitir que compartilhem recursos (como impressoras), e troquem informações. Quando usadas por empresas, são chamadas de redes empresariais;

c) MAN (Metropolitan Area Network): cobre uma área geográfica de média dimensão, como o campus de uma universidade ou uma cidade, ou ainda, podendo ser uma interligação de várias redes LAN. Pode ser uma rede privada ou pública;

d) WAN (Wide Area Network): rede que está dispersa por uma grande área geográfica, como um país ou um continente. São exemplos de WAN: redes públicas controladas por operadoras de telecomunicações; redes conectadas via rádio, via satélite ou por conexões telefônicas. Muitas WANs são redes compostas, criadas a partir da interligação de mais de uma rede.

Para Tanenbaum e Wetherall (2011), a Internet é um conglomerado interligado em nível mundial, composta, portanto, de várias redes de menor escala.

2.2 A REDE MUNDIAL DE COMPUTADORES

A internet é definida uma rede mundial que conecta milhares de dispositivos computacionais ao redor do mundo (KUROSE e KEITH, 2010). A utilização da internet tem sofrido um aumento exponencial a cada ano que passa, muito em virtude do barateamento dos computadores e dispositivos móveis, e de sua evolução

tecnológica. A internet não possui um “dono”; grosso modo, não existe, em escala mundial, uma entidade mantenedora ou reguladora da internet, sendo que cada empresa é responsável pela manutenção de seus servidores, disponibilizando conteúdo e/ou mantendo páginas *web*, proporcionando um fluxo de dados imensurável e ininterrupto, através das estruturas físicas de transmissão mantidas pelas empresas de telecomunicações.

Ferreira, já destacava que a própria evolução tecnológica trazia consigo o ônus da criminalidade e neste sentido;

> A evolução das técnicas nessa área e a sua expansão foram acompanhadas por aumento e diversificação das ações criminosas, que passaram a incidir, a partir dos anos 80, em manipulações de caixas bancários, pirataria de programas de computados, abusos nas telecomunicações, etc., revelando uma vulnerabilidade que os criadores desses processos não haviam previsto e que carecia de uma proteção imediata, não somente através de novas estratégias de segurança no seu emprego, mas também de novas formas de controle e incriminação das condutas lesivas. (FERREIRA, 2005)

A internet é usada para as mais variadas finalidades, que incluem negociações comerciais, buscar conhecimento, manter relacionamentos, expandir redes de contatos, lazer, trabalho, marketing pessoal, entre outras, sendo que atualmente tornou-se muito comum o uso dos sites classificados como redes sociais, onde o usuário cria uma conta e expõe todo o tipo de conteúdo e informações, inclusive pessoais; além de serviços que se tornaram úteis e relevantes, como e-mail e sites de bate-papo, por proporcionarem a comunicação com pouco ou nenhum custo financeiro.

A imagem a seguir demonstra a expansão do uso da internet no Brasil nos últimos anos, apresentando o percentual de domicílios com acesso à internet sobre o total de domicílios brasileiros, segundo o Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (CETIC.br) do Comitê Gestor de internet no Brasil (CGI.br):

Segundo a pesquisa divulgada pelo CGI.br, em 2012 o Brasil possuía 28,1 milhões de domicílios com computador, e 24,3 milhões de domicílios com acesso à internet, que corresponde a quarenta por cento do total de domicílios brasileiros.

2.3 A SEGURANÇA DA INFORMAÇÃO: PRINCÍPIOS BÁSICOS

Não é o objetivo deste trabalho detalhar aspectos de segurança da informação, entretanto, é relevante conhecê-los ainda que superficialmente, pois o problema estudado é reflexo de questões relacionadas à segurança.

Informação, segundo o dicionário Michaelis on-line, é o ato ou efeito de informar; transmissão de notícias; ação de informar-se; transmissão de conhecimentos[2]. Já no dicionário Aurélio on-line, encontramos a seguinte definição de informação: fator qualitativo que designa a posição de um sistema, e eventualmente transmitido a outro[3].

Em suma, informação compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servido a determinado propósito e sendo de utilidade ao ser humano. Trata-se de tudo aquilo que permite a aquisição de conhecimento[4].

O Diário Oficial da União do dia 14 de Junho de 2000, define segurança da Informação como;

> Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaça a seu desenvolvimento. (D.O.U 14/06/2000)

Lyra (2008) relata que segurança da informação está relacionada com proteção de um conjunto de dados específicos, de maneira a preservar o real valor que possuem tanto para um indivíduo quanto para uma organização, ou seja, envolve uma junção de medidas que tendem resguardar e conservar dados e sistemas de informações, sendo constituída por três princípios básicos que norteiam a sua implementação: confidencialidade, integridade e disponibilidade. Vejamos uma breve definição de cada um deles:

a) CONFIDENCIALIDADE: capacidade de um sistema em permitir que informações sejam acessadas somente por pessoas a quem são destinadas ou possuam a devida autorização para isso, impedindo que usuários não

[2] Disponível em: http://michaelis.uol.com.br/moderno/portugues/definicao/informacao%20_983588.

autorizados tenham acesso. A aplicação deste princípio normalmente está relacionada ao cadastramento de usuários com diferentes níveis de acesso.

b) INTEGRIDADE: previne a modificação não autorizada de informações; a informação deve estar correta, ser verdadeira e não estar corrompida, ou seja, precisa ser mantida nas mesmas condições de quando foi disponibilizada por seu proprietário.

c) DISPONIBILIDADE: provê suporte a um acesso seguro e imediatamente disponível às informações; a informação deve estar disponível para todos que dela necessitem.

Além destes três principais princípios, outros aspectos também são considerados, dentre eles: o princípio da autenticidade, ou autenticação do usuário, que garante que um usuário é realmente quem descreve ser; o princípio do não repúdio é a capacidade do sistema de provar quem fez a ação, impedindo o usuário de negar esta participação; o princípio da legalidade assegura que o sistema esteja de acordo com a legislação pertinente; e ainda, cabe ressaltar que todo sistema precisa ser auditável, assegurar que mantenha armazenadas todas as ações dos usuários, detectando, em uma eventual auditoria, fraudes e tentativas de ataques.

2.4 AS AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

O objeto da tutela da segurança da informação é o ativo de informação. (É considerado “ativo” qualquer coisa que tenha valor para uma organização). Ativo de informação é qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos do negócio de uma unidade ou área de negócio (LYRA, 2008). Assim, ativo de informação é composto pela informação e tudo aquilo que dá suporte ou se utiliza dela, como a tecnologia, o meio que a suporta e mantém (redes, servidores), as pessoas, e o ambiente onde a informação está inserida.

O ponto fraco de um ativo ou falha na segurança de um sistema é chamado de vulnerabilidade, que pode vir a ser explorada ou não. Exemplos de vulnerabilidades são erros na execução do projeto, na implementação ou na programação, assistência ou nos próprios equipamentos eletrônicos e de rede.

Ameaça é um agente externo que, aproveitando-se da vulnerabilidade, poderá quebrar um ou mais dos aspectos básicos da segurança da informação. É o

ataque ao ativo de informação propriamente dito. As ações danosas geradas pelo ataque a um sistema são proporcionadas basicamente por dois recursos: códigos maliciosos e engenharia social, ou as duas técnicas aliadas.

O CERT.br é o Grupo de Respostas a Incidentes de Segurança para a internet brasileira, mantido pelo Comitê Gestor de Internet do Brasil. Tem a responsabilidade de tratar de incidentes em geral que tratem de segurança em computadores que abarquem redes ligadas à internet brasileira, atuando como ponto central para as notificações de incidentes de segurança no Brasil, atuando também no trabalho de conscientização sobre os problemas de segurança, com o intuito de elevar as condições de segurança e dehabilidade de resolução de incidentes das redes conectadas à internet no Brasil .

Uma acepção muito ampla de possibilidades de ações criminosas é dada por Ferreira;

> As várias possibilidades de ação criminosa na área de informática, assim entendida no seu sentido lato, abrangendo todas as tecnologias de informação, dos processamentos e transmissão de dados, originaram uma forma de criminalidade que, apesar da diversidade de suas classificações, pode ser identificada pelo seu objeto ou pelos meios de atuação, os quais lhe fornecem um dominador comum, embora com diferentes denominações nos vários países ou nos diferentes autores. (FERREIRA, 2005)

Observa-se atualmente através dos mais variados meios de comunicação um considerável aumento do número de ocorrências de incidentes computacionais nos últimos anos e geralmente estão relacionadas principalmente a tentativas de fraude, ataques a servidores web, varredura e propagação de códigos maliciosos.

Rosa tem uma definição mais específica para Cibercrimes,

> 1. É a conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar. 2. O ”Crime de Informática” é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc. (ROSA, 2002)

Os *malwares* são softwares criados para agir de forma prejudicial entre variados tipos de dispositivos informáticos.Os principais motivos pelos quais tais códigos são desenvolvidos e propagados pelos atacantes, são para obter vantagens financeiras ilícitas, vandalismo,autopromoção, e obtenção de dados confidenciais. Há várias maneiras de um programa malicioso infectar um computador. Ele pode ser enviado como anexo em um e-mail, oculto ou disfarçado, recebido e executado pela vítima em sua máquina. Também é comum os atacantes explorarem vulnerabilidades de sistemas operacionais e programas desatualizados, encontrando brechas para instalarem e executarem seus códigos. Outra maneira é a disseminação através de mídias removíveis (*pen drive*). Normalmente o sistema operacional dos computadores é por padrão configurado para auto executar qualquer dispositivo que venha a ser conectado via USB, e desta forma, pen drives infectados ao serem conectados ao computador, automaticamente executam o programa malicioso.

As ameaças são, portanto, as ações ou procedimentos que podem vir a causar danos de maior ou menor potencial lesivo, podendo constituir-se em crimes, por isso merecem uma descrição mais detalhada, apresentada a seguir.

2.4.1 Vírus

Vírus podem ser definidos de forma simples como softwares maliciosos que se auto reproduzem integrando-se a outros arquivos ou softwares. Os principais meios de propagação dos vírus, atualmente, são as mídias removíveis (CDS, DVDS, *pen drives*), e-mails, e até mesmo acessando páginas web é possível ser infectado.

A primeira modalidade de vírus conhecida a causar danos consideráveis a um grande número de usuários de computador foi o vírus de *boot*, que se instala na parte de inicialização do sistema operacional do computador, surgido na final da década de 80 (WENDT e JORGE, 2012), mas que ainda hoje continua a fazer estragos.

O vírus *time bomb* se caracteriza por ser programado para executar em uma determinada data. Ele permanece escondido no dispositivo infectado, até a data programada, quando então executa propagando seus efeitos maliciosos. Por este motivo este tipo de vírus é conhecido também como bomba-relógio.

Os vírus para telefone celular se propagam mediante a transmissão de dados via *bluetooth,* ou troca de mensagens. O usuário recebe o arquivo infectado e oexecuta. Estes softwares tem o poder de conduzir, alterar ou apagar arquivos e agenda telefônica, efetuar ligações, drenar a carga da bateria, além de se propagarem para outros celulares.

2.4.2 Worms

Os *worms* (que significa vermes em português) são programas capazes de se replicar automaticamente pelas redes, enviando suas réplicas idênticas de uma máquina para outra. Devido à capacidade de se reproduzir automaticamente, geralmente consome muitos recursos afetando o desempenho do computador infectado. Diferente dos vírus, eles se replicam e se disseminam pela rede sem que seja necessária qualquer ação por parte do usuário. .

O *worm* tem a capacidade de fazer uma varredura na rede para identificar computadores alvos, e tentam se propagar de diversas maneiras, como por exemplo: enviados como anexo em e-mails; em conteúdo compartilhado nas redes sociais; em programas de mensagens instantâneas; em pastas compartilhadas em redes locais ou em redes ponto a ponto.

O principal objetivo dos *worms* são roubar vários tipos de senhas ou mesmo dados sigilosos e podem até mesmo encher um HD por conta da grande quantidade de cópias que eles criam.

2.4.3 Spyware

Spyware pode ser definido como um programa fabricado e preparado para vigiar as ações de um sistema como um todo e enviar as informações angariadas para seu criador ou terceiro por ele determinado.

Pode ser usado de forma legítima ou maliciosa, dependendo do uso que é feito. Será de uso legítimo quando, por exemplo, o próprio dono do computador empreende a instalação, para atender seus interesses particulares e de segurança. É considerado de uso malicioso quando sua instalação não é autorizada, e seu uso compromete a privacidade do usuário e segurança do computador. Com ele o

invasor pode monitorar e capturar informações referentes à navegação do usuário, ou dados inseridos em outros programas, como por exemplos, contas de usuário e senhas, dados bancários e de cartão de crédito.

Um tipo específico e o mais conhecido de programa *spyware* é o *keylogger,* capaz de capturar e registrar todas as teclas que são digitadas pelo usuário no teclado do computador. Permite portanto, capturar dados de cartões de crédito e contas bancárias em acesso aos *internet banking*. Estes programas poder ser capazes também de monitorar a utilização do mouse, salvando seus cliques diretamente na tela do computador, sendo assim possível de capturar dados inseridos em teclados virtuais dos sites bancários. A captura da tela se dá por sucessivas fotos ou gravando em vídeo toda a operação, depois enviando os arquivos para um e-mail cadastrado pelo invasor. Existem ainda programas que tem o poder de capturar os cliques do mouse no monitor e são conhecidos como *screenlogers.*

2.4.4 Cavalo de Tróia

Cavalo de Tróia é um software que o usuário deseja ter em sua máquina, mas não tem conhecimento do quão malicioso ele pode ser. Geralmente vêm disfarçados ou incluídos em outros programas, como jogos, protetores de tela, álbuns de fotos, etc. Eles não têm a capacidade de se replicar, e normalmente são convidados pela vítima a se instalarem no seu computador. É comum se apresentarem em anexos de *e-mails*, que, quando abertos, são executados. Possuem a capacidade de causar a destruição ou subtração de dados; de criar uma “porta dos fundos” no computador, mediante a instalação de um programa que permita ao invasor retornar ao computador em qualquer momento que desejar; também possibilitam a instalação de *keyloggers* e *screenlogers*, furtos de senhas e outras informações sensíveis.

2.4.5 Engenharia social

É o emprego de um conjunto de métodos que tem a finalidade de enganar a vítima, para que ela acredite e queira as informações anunciadas e tenha convicção para que possa entregar de boa fé seus dados pessoais que o delinquente tenha

interesse ou para executar alguma ação específica. Geralmente ocorre utilizando-se da ingenuidade da vítima, de forma parecida com o crime de estelionato.

Um exemplo deste tipo de ataque é o recebimento de ligação do atacante, que se passa por funcionário da operadora de cartão de crédito, solicitando à vítima dados pessoais, inclusive a confirmação do número do cartão e até mesmo do código de segurança, para atualização de cadastro ou prometendo incluir a vítima em alguma promoção. De posse desses dados o atacante poderá fazer compras no comércio eletrônico utilizando dados do cartão de crédito da vítima.

Através da engenharia social pode também o atacante convencer a vítima a adotar procedimentos que venham a instalar no seu computador programas maliciosos; o sucesso do ataque depende única e exclusivamente da ação do usuário induzido a realizar alguma tarefa.

Segundo Crespo (2011, p. 82), a engenharia social, por si só, na maioria das vezes, leva à configuração de um estelionato. Entretanto, quando somada à invasão do computador alheio e prejuízo à máquina, pode configurar os mais diversos crimes, desde dano até violação de direitos autorais.

2.4.6 Phishing scam

Phishing scam pode ser definido como um tipo de fraude onde um criminoso tenta alcançar dados exclusivos ou financeiros através de uma mistura de tecnologia com engenharia social.

Caracteriza-se pelo envio de mensagens, geralmente por *e-mail*, onde o atacante faz-se passar por uma instituição conhecida, oferecendo serviços à vítima, mediante o preenchimento de um cadastro com dados pessoais, seja para participar de ofertas, seja para atualização de dados, ou outras situações, sendo que a vítima é direcionada para um site falso controlado pelo atacante. Um exemplo comum é o envio de *e-mail* identificando-se como de instituição bancária, solicitando atualização de cadastro, direcionando para uma página falsa, onde a vítima vai inserir os seus dados pessoais e bancários, enviando diretamente para o criminoso.

2.4.7 Procedimentos de segurança

Ainda que seja praticamente impossível tornar um sistema cem por cento seguro, alguns procedimentos são indispensáveis para prover a segurança dos computadores, no sentido de evitar ataques e infecções por programas maliciosos.

Primeiramente, é recomendado manter todos os *softwares* instalados atualizados, principalmente o sistema operacional, mas também os outros programas, pois programas desatualizados oferecem vulnerabilidades que podem ser exploradas por atacantes (WENDT e JORGE, 2012). Neste sentido, é prudente também desinstalar todos os programas que não sejam mais usados, pois programas sem uso tendem a ser esquecidos e desta forma não serão atualizados, vindo a se constituir em risco. Para minimizar problemas com mídias removíveis infectadas, uma providência importante é desabilitar a função de auto execução dos dispositivos pelo sistema operacional, e submeter qualquer mídia de armazenamento externo a uma varredura por programas antivírus, antes de abrir os arquivos.

Os programas antivírus e anti-*spywares* protegem o computador contra programas maliciosos. Alguns programas cumprem as duas funções. A principal função dos programas antivírus é não permitir que arquivos sejam infectados por vírus, ou que arquivos já infectados e com danos irreversíveis sejam removidos do sistema (OLIVEIRA e REHDER, 2006). O antivírus oferece proteção em tempo real e também por varredura no sistema efetuada de tempos em tempos, oferecendo também varredura em dispositivos de armazenamento externos. Eles localizam e eliminam os vírus com base em dois métodos: definição (o sistema antivírus mantém em seu banco de dados, partes de códigos dos vírus conhecidos, e através de comparação deste código com os programas instalados no computador, identificam os vírus e os eliminam) e heurística (técnica capaz de identificar comportamentos característicos de vírus).

Os anti-*spywares* tem funcionamento parecido com os dos antivírus. Cuidam da detecção e eliminação de programas espiões que são instalados sem que o usuário perceba, com o objetivo de espionarem tudo o que é feito no computador e convertem em dados as ações e enviam para uma determinada localização externa (OLIVEIRA e REHDER, 2006).

Um *firewall* (traduzido do inglês: “parede de fogo”) é um esquema de segurança que pode ser implementado via *software* ou *hardware*. A sua principal função é proteger uma rede de computadores de ataques e tentativas de invasões externas. Cria uma barreira de proteção que isola a rede dos perigos provenientes dos ambientes externos. O *firewall* monitora os pacotes de dados que trafegam pela rede, e caso ele detecte algum pacote de dado não autorizado tentando acessar algum serviço ele imediatamente bloqueia esta comunicação (OLIVEIRA e REHDER, 2006). Os sistemas operacionais modernos possuem programa firewall instalado.

A criptografia que tem uma grande importância na segurança da informação, pode ser entendida como a forma de escrever mensagens em código para aumentar a proteção contra ataques de criminosos ao usuário de internet.Por meio do uso da criptografia, é possível proteger os dados sigilosos armazenados no computador e também as comunicações realizadas pela internet, como o envio de e-mails e as transações bancárias e comerciais. Existem programas que efetuam a criptografia de arquivos, e até mesmo o próprio sistema operacional do computador possui ferramentas para este fim.

3 O CIBERCRIME

3.1 CARACTERÍSTICAS E PREVISÃO LEGAL

A constituição da República Federativa do Brasil, em seu artigo 5º, inciso XXXIX, determina: “Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”[3]. Assim, toda ação lesiva praticada por meios eletrônicos contra algo ou alguém, só será considerada criminosa se encontrar amparo na legislação penal existente. Toda conduta, ainda que nociva, será considerada atípica se não for prevista em lei. Com o passar do tempo e o surgimento de novas tecnologias, também a legislação vem sendo atualizada para abranger novas condutas criminosas.

> O aparecimento da Informática no meio social ocorreu de forma tão rápida e passou a exigir, com a mesma rapidez, soluções que o Direito não estava preparado para resolver. Com isso, a necessidade social aparenta estar desprovida da tutela do Direito e a busca ansiosa por regular a matéria pode provocar a criação de leis excessivas e desnecessárias (SILVA, 2003)

O exemplo mais recente é a Lei 12.737/2012 (ver item 3.1.2) que criminalizou, dentre outras, a conduta de invadir e infectar computadores alheios com *malwares*, conduta esta que, embora nociva, até então não era considerada crime.

Não foi encontrado um texto legal que defina “delito informático”, tendo sido trazidas definições dadas pelos autores pesquisados, entendendo-se como sinônimos: crimes de informática, cibercrime, crime cibernético, ou ainda, crime digital.

Crespo (2011, p. 63) define “crimes informáticos” como sendo “qualquer ilícito praticado com o uso da tecnologia, seja ela o instrumento da conduta, seja o objeto do ilícito”.

3.1.1 Crimes cibernéticos abertos

O quadro a seguir apresenta exemplos de crimes não exclusivamente cibernéticos, ou “crimes cibernéticos abertos”, segundo Wendt e Jorge (2012). O que

[3] O mesmo texto consta no artigo 1º do Decreto-Lei 2848 de 7 dez. 1940, (Código Penal), constituindo-se no princípio da anterioridade da lei.

os torna classificáveis como crimes cibernéticos é o uso de computador e outros recursos telemáticos para a sua execução. De acordo com Wendt (2011, p. 69), “pode-se reconhecer que a evolução da tecnologia ocasionou um upgrade e/ou impulsionou alguns tipos de crimes antes restritos tão somente ao “mundo real”. Na coluna à esquerda é apresentado um exemplo de conduta que configura o crime tipificado na coluna da direita:

Quadro 1 : Crimes cibernéticos abertos

Conduta	**Tipificação**
Acusar alguém em rede social ou blog, de ter cometido um crime (que não cometeu)	Calúnia – Artigo 138 do C.P.
Disseminar um boato difamatório contra uma pessoa, para vários destinatários, via rede social, e-mail, blog, etc.	Difamação – Artigo 139 do C.P.
Enviar uma mensagem direta para uma pessoa, ofendendo-lhe a dignidade ou o decoro	Injúria – Artigo 140 do C.P.
Enviar uma mensagem para uma pessoa, ameaçando lhe agredir ou causar qualquer mal grave	Ameaça – Artigo 147 do C.P.
Publicar em página web, em rede social, ou enviar e-mail para terceiros, sem justa causa, acerca de informação considerada confidencial, e cuja divulgação possa produzir dano a outrem	Divulgação de segredo – Artigo 153 do C.P.
Efetuar operação bancária, via *internet banking*, que venha a subtrair dinheiro da conta de terceiro, usando indevidamente os dados bancários deste	Furto qualificado mediante fraude – Artigo 155, parágrafo 4º, inciso II do C.P.
Publicar conteúdo de terceiro sem mencionar a fonte e/ou sem autorização, compartilhar ou fazer download ilegalmente de conteúdo protegido por direitos autorais	Violação de direito autoral – Artigo 184 do C.P.
Publicar tutoriais que ensinam a violar	Apologia de crime ou criminoso –

segurança de computadores para invadir, a quebrar senhas ou furtar dados sensíveis	Artigo 287 do C. P.
Enviar e-mail com remetente falso (exemplo: envio de *spam* utilizando um *bot*)	Falsa identidade – Artigo 137 do C.P.
Efetuar uma publicação que incite ou induza a discriminação ou preconceito de raça, cor, etnia ou religião (exemplo: desqualificar toda a raça negra)	Racismo – Artigo 20 da Lei 7.716/89.
Enviar mensagem ofendendo alguém em razão de sua raça, cor, etnia ou religião (exemplo: chamar alguém de “preto safado”, “macaco”)	Injúria qualificada – Artigo 140, parágrafo 3º do Código Penal
Usar em página web logomarca de empresa sem autorização, ou imitá-la de modo que possa induzir à confusão	Crime contra a propriedade industrial – Artigo 195 da Lei 9.279/96
Criar sites falsos de *e-commerce*, oferecer produtos à venda, receber o pagamento e não entregar o produto	Estelionato – Artigo 171 do C.P.

O quadro apresentado não tem a intenção de esgotar o assunto, mas de apresentar os exemplos mais comuns. Há outros crimes que podem integrar esta lista, tais como: importunação ofensiva ao pudor, falsificação de documentos, espionagem industrial, tráfico de drogas e armas. Enfim, qualquer crime que possa ser praticado com ou por intermédio de computadores, mas não exclusivamente desta forma.

Acrescenta-se ainda a esta lista o previsto na Lei nº 11.829/08, que modificou o Estatuto da Criança e Adolescente (Lei 8.069/90), para inserir tipos penais visando o combate à pornografia infantil e à pedofilia na internet:

> Art. 241-A: Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar **por qualquer meio**, **inclusive por meio de sistema de informática ou telemático**, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e
> multa. § 1º Nas mesmas penas incorre quem:
> I – assegura meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;

> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.
> Art. 241-B Adquirir, possuir ou armazenar, **por qualquer meio**, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

Como se vê, os crimes definidos nos artigos anteriores podem ser praticados com ou sem recursos informáticos.

3.1.2 Crimes exclusivamente cibernéticos

Existe uma série de crimes que só podem ser praticados utilizando-se recursos de informática e internet, que, segundo a classificação dada por Wendt e Jorge (2012), são apresentados como crimes exclusivamente cibernéticos. Enquadram-se nesta descrição os delitos apresentados no quadro a seguir:

Quadro 2: Crimes exclusivamente cibernéticos

Conduta	Tipificação
Induzir ou convencer menor de 18 anos a praticar algum crime, utilizando-se de salas de bate-papo da internet	Corrupção de menores em salas de bate-papo da internet – Artigo 244-B, parágrafo 1º da Lei 8.069/90
Reproduzir ou comercializar programa de computador sem autorização expressa do autor; violar direitos do autor; vender, expor à venda, introduzir no país, adquirir, para fins de comércio, original ou cópia de programa de computador produzido com violação de direito autoral	Violação dos direitos de autor de programa de computador – Artigo 12 da Lei 9.609/98
Crime praticado por funcionário público que, em função do cargo, insere ou facilita a inserção de dados falsos ou modifica dados corretos nos bancos de dados da	Inserção de dados falsos em sistemas de informações – Artigo 313-A do C.P.

Administração Pública para obter vantagem ou causar danos	
Obter acesso a sistema de tratamento automático de dados, a fim de alterar a apuração ou a contagem de votos; provocar danos no referido sistema, ou provocar qualquer outro resultado diverso do esperado, mediante o uso de instrução, comando ou programa de computador	Crimes contra equipamentos usados pelo serviço de votação eleitoral (Artigo 72 da Lei 9.504/97)

Fonte: Elaboração própria (2015)

Além dos crimes acima apresentados, há os tipos penais criados com a Lei 12.737/12, de 30 de novembro de 2012, que serão examinados com mais detalhes.

Embora já houvesse discussões e projetos de lei tramitando no Congresso Nacional acerca do tema, um fato amplamente divulgado na imprensa impulsionou a aprovação da Lei 12.737: em maio de 2012, a atriz Carolina Dieckmann teve furtadas de seus arquivos pessoais digitais, mediante acesso não autorizado, cerca de trinta e seis fotografias íntimas, que foram divulgadas na internet. A lei foi apelidada pela imprensa de “Lei Carolina Dieckmann”, tendo entrado em vigor em 02 de abril de 2013.

A referida lei alterou o Código Penal, trazendo a tipificação criminal do que ela chama de “delitos informáticos”. As alterações criaram dois novos tipos penais que vem a se juntar ao rol dos delitos considerados crimes cibernéticos; contemplam condutas nocivas muito freqüentes na internet. São eles: invasão de dispositivo informático e interrupção de serviço informático, telemático ou de informação de utilidade pública.

O crime de invasão de dispositivo informático foi criado com a inclusão do artigo 154-A no Código Penal. Vamos examinar o *caput* do artigo:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

Portanto, fica enquadrada neste tipo de crime, entre outras condutas, a instalação de *malwares,* por exemplo: um vírus que cause a destruição de dados; um *spyware* que proporcione ao invasor obter dados sigilosos da vítima; um cavalo de tróia que depois de instalado, libera uma porta permitindo a invasão da máquina. O texto da lei exige que haja violação indevida de mecanismo de segurança, que pode ser um sistema antivírus.

Os parágrafos do artigo 154-A, não reproduzidos aqui, estendem o rol de condutas criminosas abarcadas pelo artigo, criminalizando a conduta de quem produz, oferece, distribui, difunde ou vende programas nocivos; e ainda, prevê aumentos de pena em diferentes formas de agravamento dos prejuízos impostos à vítima.

Outro delito tipificado pela supracitada lei é o crime de interrupção de serviço informático, telemático ou de informação de utilidade pública. Primeiramente vamos examinar o caput do artigo 266 do Código Penal, que antes da alteração, tratava do crime de interrupção ou perturbação de serviço telegráfico, radiotelegráfico ou telefônico:

> Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena: detenção, de 1 (um) a 3 (três) anos, e multa.

Este texto não foi alterado, mesmo com a evidente obsolescência dos serviços telegráficos e radiotelegráficos. Nesta linha, certamente devido aos avanços da informática e dos serviços telemáticos, com presença cada vez maior de informações de utilidade pública disponíveis na rede mundial de computadores, a alteração introduzida pela Lei 12.737/12 deu a seguinte redação ao parágrafo primeiro do supramencionado artigo:

> § 1º Incorre na mesma pena quem interrompe o serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

Um típico exemplo são os conhecidos como ataque de negação de serviço, que, como já visto, consistem em uma enxurrada de acessos usando computadores zumbis, para tirar do ar determinado site. Será considerado crime, quando a permanência do site no ar for considerada de utilidade pública. Exemplo: um ataque que tornar indisponível o site da Polícia Federal, estaria indisponibilizando o serviço de emissão de guias de transporte de armas de fogo, ou solicitação de passaportes,

serviços que, de outro modo, não estariam acessíveis de forma viável a boa parte da população, constituindo-se, assim, em serviços de utilidade pública.

3.2 SUJEITOS DOS CRIMES DE INFORMÁTICA

3.2.1 Sujeito passivo

Sujeito passivo é o ente sobre o qual recaia a ação ou omissão realizada pelo sujeito ativo; pessoa ou entidade titular do bem jurídico protegido por lei e sobre a qual recai a conduta do sujeito ativo. Nos crimes praticados através da internet, pode ser pessoa física ou jurídica, tanto de natureza privada quanto de natureza pública.

3.2.2 Sujeito ativo

Os *hackers*, definindo de forma bastante objetiva são pessoas que se valem das suas noções para invadir dispositivos de informática, sem interesse em causar prejuízo às vítimas, mas como um desafio pessoal as suas técnicas, inteligência e habilidades.

Eles não têm intenção de prejudicar, mas apenas de demonstrar que conhecimento é poder; em geral são exímios programadores, e conhecedores dos segredos que envolvem as redes e os computadores, e geralmente não gostam de ser confundidos com *crackers*. É comum empresas contratarem *hackers* para testar seus sistemas de segurança.

Os *crackers* são indivíduos que invadem sistemas para roubar informações e causar danos às vítimas (NAKAMURA e GEUS, 2007). O termo *crackers* também é uma denominação utilizada para aqueles que decifram códigos e destroem proteção de softwares. Portanto, o cibercriminoso é o *cracker*, embora seja muito comum aparecer definido equivocadamente como *hacker*.

Conforme Crespo (2011), a prática dos crimes digitais impróprios não requer conhecimentos técnicos específicos; já para os crimes próprios, depende de conhecimentos específicos de computação, nos quais se verifica, então, a ação dos *crackers*.

4 A INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS NO BRASIL

Os principais crimes virtuais praticados no Brasil são: a pornografia infantil; as roubo de senhas bancárias; os crimes contra que atingem a honra, a apologia e incitação aos crimes contra a vida, e o tráfico de drogas.

O combate ao cibercrime no Brasil se dá em nível federal, pela atuação da Polícia Federal e do Ministério Público Federal, e em nível estadual, pelas Polícias Civis dos estados, no exercício de suas atribuições constitucionais.

Wendt (2011) ressalta a atuação nesse campo da organização não-governamental SaferNet Brasil, que surgiu em 2005, inicialmente com iniciativas para combater a pornografia infantil na internet, e se tornou referência no combate aos crimes e abusos que atentem contra os Direitos Humanos utilizando-se da internet ou suas ferramentas. O site “SaferNet” mantém um serviço de recebimento de denúncias, anônimas ou não, através de seu sítio, acerca dos seguintes crimes: pornografia infantil (pedofilia on-line); racismo, xenofobia e intolerância religiosa; neonazismo; incitação a crimes contra a vida; homofobia; e apologia a práticas cruéis contra animais[4]. Após submeter a denúncia a uma verificação, análise de conteúdo e comprovação de materialidade, através do rastreamento de informações disponíveis publicamente na internet, a equipe do site elabora um relatório e o envia ao Ministério Público Federal e à Polícia Federal, para os procedimentos de investigação policial. No caso de denúncias contra sites estrangeiros, os responsáveis pelo site encaminha para locais próprios para apuração de caráter internacionais.

4.1 ESTRUTURA DOS ÓRGÃOS POLICIAIS

Os órgãos responsáveis pela segurança pública no Brasil estão definidos no artigo 144 da Constituição Federal:

> Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos:
> I - polícia federal;
> II - polícia rodoviária federal;

[4] Disponível em: http://www.safernet.org.br. Acesso em: 01 nov. 2015.

> III - polícia ferroviária federal;
> IV - polícias civis;
> V - polícias militares e corpos de bombeiros militares.

Em relação ao combate aos crimes cibernéticos, a responsabilidade recai sobre as polícias judiciárias, responsáveis pela apuração das infrações penais: a Polícia Federal e as Polícias Civis dos estados.

4.1.1 A Polícia Federal

A Polícia Federal é um órgão do poder executivo da União, subordinada ao Ministério da Justiça, e tem suas atribuições descritas no parágrafo primeiro do artigo 144 da Constituição Federal:

> Art. 144 (...)
> § 1º A polícia federal, instituída por lei como órgão permanente, organizado e mantido pela União e estruturado em carreira, destina-se a:
> I - apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei;
> II - prevenir e reprimir o tráfico ilícito de entorpecentes e drogas afins, o contrabando e o descaminho, sem prejuízo da ação fazendária e de outros órgãos públicos nas respectivas áreas de competência;
> III - exercer as funções de polícia marítima, aeroportuária e de fronteiras; IV
> - exercer, com exclusividade, as funções de polícia judiciária da União.

Portanto, verifica-se que a Polícia Federal atuará sempre que o sujeito passivo da infração penal for a União, suas autarquias e entidades públicas, e ainda quando a prática delituosa tenha repercussão interestadual ou internacional, e exija repressão uniforme.

A Polícia Federal conta com o Centro de Monitoramento do Serviço de Repressão a Crimes Cibernéticos, localizado em Brasília, tratando-se de um instrumento de prevenção e investigação a ataques cibernéticos contra sistemas de informação e infraestruturas críticas do Governo Federal[5]. O Serviço de Repressão a Crimes Cibernéticos possui vários grupos operacionais especializados espalhados pelas unidades da Federação. Segundo Wendt (2011, p. 70), “a atuação da Polícia Federal frente à problemática dos cibercrimes envolveu, em princípio, duas ações

[5] Disponível em: <http://www.dpf.gov.br/>. Acesso em: 01 nov. 2015.

básicas essenciais: central de recebimento de denúncias de pornografia infantil (pedofilia) e análise, processamento e investigação de fraudes eletrônicas".

4.1.1.1 Fraudes eletrônicas bancárias

A partir do ano de 2009, a Polícia Federal alterou a metodologia de investigação de fraudes eletrônicas, com a elaboração do "Projeto Tentáculos". Até então, a investigação era feita isoladamente em toda e qualquer denuncia de fraude eletrônica, resultando em pouca eficiência e muitos casos de duplicidade de inquéritos policiais instaurados em diferentes estados, acerca da mesma quadrilha. A partir do Projeto Tentáculos, a PF organizou um banco de dados nacional, com comunicação de ocorrências centralizada e eletrônica, e através do cruzamento de informações passou a atuar diretamente na fonte do problema, que é a organização criminosa envolvida na fraude, ao invés de investigações pulverizadas em fatos isolados e específicos. O projeto, além de maior produtividade, proporcionou a otimização de recursos humanos e materiais (WENDT, 2011).

Em matéria publicada no site do Tribunal Regional Federal da 4ª Região, em 12 de março de 2013, o Delegado de Polícia Federal João Vianey Xavier Filho, então chefe-substituto do Serviço de Repressão a Crimes Cibernéticos do Distrito Federal relatou que a implantação do Projeto Tentáculos foi fundamental para o combate ao crime organizado, e que antes da instalação do projeto, 99% dos inquéritos policiais eram meramente formais, sem efetividade. Conforme as declarações do Delegado, o volume de inquéritos de fraudes bancárias tramitando na PF é imenso, contando com 463 mil inquéritos instaurados em andamento, em março de 2013, de violação dos sistemas de *internet banking* e clonagem de cartões, e que são priorizados os casos mais importantes e que atingem um volume maior de pessoas[6].

4.1.1.2 Pornografia infantil

A Polícia Federal intensificou o combate à pornografia infantil a partir do ano de 2009, após um convênio firmado com o Safernet, o Comitê Gestor de Internet do

[6] Disponível em: <http://www2.trf4.jus.br/trf4/controlador.php?acao=noticia_visualizar&id_noticia=8942>. Acesso em: 01 nov. 2015.

Brasil (CGI.Br) e a Secretaria Especial de Direitos Humanos, com o objetivo de centralizar as denúncias de pornografia infantil, crimes de ódio e genocídio, com a finalidade de agilizar o fluxo do processamento e encaminhamento das denúncias e a investigação por parte dos agentes federais, buscando a apuração da autoria responsabilização dos criminosos que usam a internet para praticar atos ilícitos (Wendt, 2011).

Atualmente a Polícia Federal mantém em seu portal na internet um serviço de recebimento de denúncias, acessível através do endereço“http://denuncia.pf.gov.br/”, onde recebe denúncias acerca de crimes cometidos via internet dos tipos pornografia infantil, crimes de ódio, genocídio e tráfico de pessoas. No combate à pedofilia na internet, a PF, no trabalho de inteligência policial, atua coletando evidências da participação dos envolvidos e suas relações com outros criminosos, deflagrando operações em nível nacional, com obtenção de mandados de busca e de prisão de vários criminosos ao mesmo tempo.

Assim foi, por exemplo, na “Operação Glasnot”, divulgada no site da Polícia Federal em 19 de novembro de 2013, sendo noticiado que a investigação foi realizada ao longo de dois anos, identificando quase uma centena de brasileiros envolvidos com a produção e o compartilhamento de imagens relacionadas à exploração sexual de crianças e adolescentes na internet[7]. O balanço da operação divulgado no site apontava a prisão de 20 pessoas, até o dia 20 de novembro de 2013.

4.1.2 As polícias civis

As polícias civis são órgãos subordinados ao poder executivo dos estados, e têm sua competência definida no parágrafo quarto do artigo 144 da Constituição Federal

> Art. 144 (...)
> § 4º - às polícias civis, dirigidas por delegados de polícia de carreira, incumbem, ressalvada a competência da União, as funções de polícia judiciária e a apuração de infrações penais, exceto as militares.

Portanto, é responsabilidade das polícias civis a apuração de um rol extenso de infrações penais, pois se excetuam apenas as infrações penais militares e às de competência da Polícia Federal.

[7] Disponível em: <http://www.dpf.gov.br/agencia/noticias/2013/11/operacao-glasnost-combate-a-pedofilia-em-11-estados-brasileiros>. Acesso em: 01 nov. 2015.

As polícias civis de alguns estados da federação mantêm departamentos especializados na investigação dos crimes cibernéticos, uma unidade localizada na capital do estado. O SaferNet mantém em seu sítio na internet a relação dos órgãos especializados, com endereço e contatos[8]. De acordo com a referida entidade, atualmente os seguintes estados mantém estas unidades especializadas: Espírito Santo, Goiás, Mato Grosso do Sul, Minas Gerais, Pará, Paraná, Pernambuco, Rio de Janeiro e Rio Grande do Sul. Mas mesmo nestes estados, também outras delegacias de polícia, não especializadas, recebem a notícia-crime e promovem a investigação. Já no Distrito Federal, há uma unidade de apoio denominada DICAT – Divisão de Repressão aos Crimes de Alta Tecnologia - que não registra boletins de ocorrências e nem instaura inquéritos, mas presta apoio às delegacias de polícia do DF nas investigações de crimes que envolvam alta tecnologia, com computadores e internet.

Quanto à atuação das polícias civis no combate ao cibercrime, ainda são tímidas as iniciativas neste terreno, conforme as palavras do especialista em inteligência policial e repressão aos crimes de informática, Delegado de Polícia Emerson Wendt, da Polícia Civil do Rio Grande do Sul:

> As atuações das polícias civis do Brasil em relação aos cibercrimes ainda são insipientes, face à inexistência de uma política conjunta de todos. No entanto, alguns esforços estão sendo feitos a esse respeito e merecem ser destacados. O principal aspecto é em relação à inexistência de delegacias de polícia específicas para a investigação dos crimes cometidos pela internet na maioria dos estados brasileiros (WENDT, 2011. p. 73).

4.2 A INVESTIGAÇÃO POLICIAL

O trabalho da polícia judiciária na investigação dos crimes de informática obedece o mesmo rito de qualquer outro crime, previsto no código de processo penal (Decreto-Lei 3.689, de 3 out. 1941), sendo precedido do registro de um boletim de ocorrência e instauração do inquérito policial. A respeito do inquérito policial, tratam o artigo quarto e seguintes do referido dispositivo legal, prevendo, entre outros detalhes, que a autoridade policial (Delegado de Polícia) procederá a instauração do inquérito policial, logo que tomar conhecimento do fato delituoso, e

[8] Disponível em: <http://www.safernet.org.br/site/prevencao/orientacao/delegacias>. Acesso em: 03 nov. 2015.

promoverá todas as ações para buscar a apuração dos fatos e sua autoria, inclusive requisitando perícias técnicas se for o caso.

É justamente na produção das provas que começam as diferenças entre a investigação dos crimes de informática e os outros crimes. Nos crimes praticados por intermédio da internet, a investigação inicial procura preservar o material comprobatório do delito. Toda ação criminosa via internet deixa vestígios, e a preservação destes é fundamental para se iniciar um caminho, geralmente longo, em busca da descoberta do autor.

O que se busca, geralmente, seja em sites fraudulentos, *e-mails*, redes sociais, comunicadores instantâneos, ou qualquer página de internet, é identificar o endereço IP utilizado pelo criminoso durante a ação. O endereço IP, também conhecido como endereço lógico, é um sistema de identificação universal onde cada computador possa ser identificado exclusivamente, independente da rede em que esteja operando (FORUZAN e FEGAN, 2010).

O endereço IP é o meio pelo qual se identificará o titular da conexão de internet usada no momento da ação. Isso porque, apesar de o endereço IP ser um número atribuído dinamicamente pelos provedores de internet, cada vez que se efetua uma conexão, nunca um mesmo endereço será utilizado em dois computadores ao mesmo tempo, possibilitando assim, com base no dia e horário utilizado, a identificação do responsável.

Segundo Cassanti (2014), descobrir o IP utilizado pela máquina que gerou o crime é a única maneira de identificar quem é o culpado. Este procedimento é efetuado após uma solicitação de quebra de sigilo telemático feita pela polícia. Quando o número do endereço IP for descoberto, basta solicitar, junto ao provedor da conexão, os dados cadastrais do utilizador daquele endereço IP na data/hora do fato. Cassanti (2014) explica ainda que para se chegar a este resultado, primeiro deve-se acionar (via ordem judicial) o provedor de serviços, para que este informe os dados de conexão (IP, data, hora, fuso horário) da ocorrência do fato. Em seguida, deve-se acionar o provedor de acesso (também pela via judicial) para que este informe os dados físicos (nome, RG, CPF, endereço, telefone, etc.), chegando-se assim, à autoria do delito.

Wendt e Jorge (2012, p. 52-53) apresentam um interessante roteiro do que chamam de fase técnica da investigação:

- Análise das informações narradas pela vítima e compreensão do fato ocorrido na internet;
- Orientações à vítima com o intuito de preservar o material comprobatório do delito e sua proteção virtual;
- Coleta inicial de provas em ambiente virtual;
- Formalização do fato criminoso por intermédio de um registro ou boletim de ocorrência, com a conseqüente instauração do feito;
- Investigação inicial referente aos dados disponíveis na rede mundial de computadores sobre prováveis autores, origem de e-mails, registro e hospedagem de domínios;
- Formalização de relatório ou certidão das provas coletadas e apuração preliminar;
- Representação perante o Poder Judiciário para expedição da autorização judicial para quebra de dados, conexão ou acesso. Também poderão ser solicitados os dados cadastrais para os provedores de conteúdo;
- Análise das informações prestadas pelos provedores de conexão e/ou provedores de conteúdo.

Os procedimentos podem variar de acordo com a natureza da ação e o tipo de recurso da internet utilizado, por isso, na sequência serão examinadas situações específicas.

4.2.1 E-mails

Conforme orientam Wendt e Jorge (2012), na investigação de e-mails é necessário obter a exibição ou impressão do e-mail completo ou código fonte, pois todo e-mail possui uma parte denominada cabeçalho, que não é exibida na abertura normal do e-mail. O cabeçalho contém informações do remetente e do caminho percorrido pelo e-mail em todos os servidores até chegar ao destino, interessando principalmente a data e horário do envio e o endereço IP do remetente.

Quando não visível o endereço IP do remetente, será necessária a solicitação ao provedor que identifique o IP do usuário que enviou a mensagem. Uma vez obtido o endereço IP do remetente, por uma simples consulta na internet será obtido o nome do provedor responsável por aquele número de endereço IP, requisitando ao mesmo as informações do usuário titular da linha telefônica ou conexão à internet que utilizou aquele endereço IP no determinado dia e hora. No Brasil as informações cadastrais são protegidas por sigilo constitucional, devendo-se então representar perante o Poder Judiciário, para que, atendendo ao interesse da investigação determine às empresas que forneçam as informações necessárias.

4.2.3 Redes sociais

Wendt e Jorge (2012, p.95) definem as redes e mídias sociais como “diversas formas de relacionamento através das redes disponíveis na internet”, relacionando as mais populares no Brasil: Google+, Orkut, Facebook, LinkedIn, Quepasa, Sonico, Badoo e Twitter. As redes sociais têm sido muito utilizadas para prática de crimes contra a honra, sendo também comum a denuncia de criação de perfis “falsos”, onde o criminoso cria um perfil se fazendo passar por outra pessoa, inserindo fotos e dados pessoais, adicionando amigos, em seguida adotando condutas reprováveis por meio do perfil denegrindo a imagem da vítima.

Na investigação de crimes envolvendo perfis de redes sociais, deve-se observar que toda página possui uma url[9] única, através da qual, por meio de ordem judicial, se obterá junto à empresa responsável pela rede social os *logs* de acesso e criação da página, revelando assim dados de quem registrou e acessou o perfil, principalmente o endereço IP em cada acesso. Os *logs* são arquivos que armazenam informações como data e hora de acesso, endereço IP da estação que realizou o acesso, entre outros eventos. A partir do endereço IP, como já dito, poderá ser identificado o usuário titular da conexão de internet utilizada.

Wendt e Jorge (2013) alertam ainda que geralmente as empresas que administram as redes sociais disponibilizam no próprio site mecanismos para que os ofendidos solicitem a exclusão de páginas ou postagens impróprias, além de canais para contato e atendimento às forças da lei.

4.3 FORENSE COMPUTACIONAL

O artigo 159 do Código de Processo Penal (Decreto-Lei 3689/41) determina a atribuição para a realização de perícias:

> Art. 159. O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior.
> § 1º Na falta de perito oficial, o exame será realizado por 2 (duas) pessoas idôneas, portadoras de diploma de curso superior preferencialmente na área específica, dentre as que tiverem habilitação técnica relacionada com a natureza do exame.

[9] URL (*Uniform Resource Locator*), em português Localizador-Padrão de Recursos, é o endereço de um recurso disponível em uma rede (Disponível em: <http://pt.wikipedia.org/wiki/URL>. Acesso em: 05 nov. 2015.).

> § 2º Os peritos não oficiais prestarão o compromisso de bem e fielmente desempenhar o encargo.

A perícia forense aplicada à informática, também referenciada como forense computacional, é a aplicação de conhecimentos em informática e técnicas de investigação com a finalidade de obtenção de evidências. Utiliza de métodos científicos para identificar, preservar, analisar e documentar evidências localizadas em computadores e outros dispositivos eletrônicos (FREITAS, 2006). A perícia em sistemas computacionais é utilizada, quando necessário, para a realização das investigações digitais e tem como objetivo principal a compreensão dos eventos ocorridos, através das etapas tradicionais de forense: identificação, coleta, exame, análise e resultados.

No trabalho pericial, os peritos oficiais buscarão preservar as evidências em dados e equipamentos, em sistemas ligados ou desligados. Ao final do processo é lavrado um laudo pericial, que conterá a descrição do que foi apurado, especialmente com a resposta aos quesitos formulados pela Autoridade Policial (WENDT e JORGE, 2013).

5 ANÁLISE DOS RESULTADOS

A metodologia utilizada, pesquisa exploratória, proporcionou a elaboração do conteúdo teórico a partir da consulta a diversos autores. A pesquisa permitiu concluir que o combate ao cibercrime no Brasil está muito aquém de proporcionar resultados realmente eficientes. Para entender este quadro é preciso analisar alguns aspectos.

5.1 PRINCIPAIS DIFICULDADES NO COMBATE AO CIBERCRIME

5.1.1 A estrutura dos órgãos policiais

Conforme observado, as polícias civis dos estados arcam com a responsabilidade de investigar um grande número de crimes. Diariamente, as delegacias de polícia absorvem um grande número de ocorrências, que acabam por gerar inquéritos policiais, gerando um invencível acúmulo de trabalho, o que faz com que o esforço seja concentrado nas questões mais graves e urgentes.

Dentro deste universo de crimes sendo investigados, há uma parcela considerável, e crescente, de crimes de informática, os quais, nas delegacias não especializadas, estão longe de ser uma prioridade, dada a complexidade da investigação e despreparo técnico dos agentes, além, é claro, do grande volume de outros crimes considerados mais graves, requerendo maior urgência na elucidação.

Considerando que a investigação de crimes de informática, para obter resultados eficazes, precisa ser rápida, dada a necessidade de se obter dados de provedores e instituições que não têm a obrigação de manter estes dados armazenados por muito tempo, entre outros aspectos, pode-se concluir que o percentual de êxito nas investigações dos cibercrimes nas delegacias não especializadas (quando ocorrem) é próximo à zero.

As delegacias especializadas na investigação dos crimes cibernéticos também enfrentam grandes dificuldades e de acordo com jornais, revistas e sites especializados os principais problemas estão na necessidade de diligências em outros estados, cujo atendimento por parte das autoridades policiais deprecadas é muito demorado; também, na demora na realização de perícia que trabalham com casos de crimes virtuais que podem demorar vários anos para concluir um laudo pericial relativo à computação forense.

Outro ponto negativo é a falta de integração entre os estados brasileiros, para tratar com mais agilidade crimes envolvendo quadrilhas que atuam em vários estados, em atuação conjunta, e também, a falta de uma política nacional de combate aos crimes cibernéticos. Wendt e Jorge (2012) mencionam também o despreparo dos agentes policiais, havendo a necessidade de investir na capacitação destes e outros agentes da persecução penal, como o Ministério Público e o Poder Judiciário.

5.1.2 A burocracia provocada pela legislação

Um ponto que dificulta o trabalho da investigação é a necessidade de representações judiciais, toda vez que um delegado de polícia necessita de dados de clientes e usuários de provedores de acesso, operadoras de telefonia e internet, bancos, e quaisquer instituições que mantenham dados cadastrais. Muitas vezes mais de uma representação é necessária na mesma investigação. A representação pela quebra de sigilo de dados cadastrais, e a emissão do respectivo alvará pelo Poder Judiciário consome um tempo valioso, que, aliado à demora das empresas em responder à ordem judicial fornecendo as informações requeridas, prejudica e retarda a investigação. Acerca do sigilo de dados, trata o artigo 5º, inciso XII da Constituição Federal:

> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Há um ponto divergente na interpretação que se dá ao texto legal, referente ao que vem a ser protegido pelo sigilo constitucional. Algumas empresas entendem que dados cadastrais não são protegidos por sigilo, mas apenas o conteúdo das correspondências e comunicações. Assim, a Tim Celular, a Microsoft do Brasil e o site de compras Mercado Livre, por exemplo, fornecem as informações cadastrais sem a necessidade de ordem judicial (Wendt e Jorge, 2012). Mas a maioria das empresas exige a representação por quebra de sigilo para fornecer qualquer informação.

Soma-se ainda o fato de que os provedores de internet não têm a obrigação legal de guardar conteúdo dos usuários e *logs* de acesso por muito tempo, e

geralmente os mantém por cerca de três meses, tempo que pode ser insuficiente do ponto de vista da investigação.

Outro ponto crítico, é que muitas vezes o conteúdo requisitado está armazenado fora do Brasil, o que praticamente inviabiliza a investigação, devido à burocracia e morosidade dos procedimentos via cooperação internacional e cartas rogatórias.

Há casos ainda que uma investigação, mesmo percorrendo os caminhos adequados, não consegue chegar ao resultado, por exemplo: quando se obtém o endereço IP do computador que gerou o ato criminoso, representa-se em juízo para que o provedor de internet forneça os dados cadastrais do titular da conta que estabeleceu a conexão. No caso de ser uma *Lan house*, torna-se inviável descobrir-se o criminoso por esta via, devendo-se recorrer a outros meios, como por exemplo, examinar gravações de câmera de segurança do estabelecimento, caso exista. O mesmo se aplica a redes disponibilizadas a um grande público, como aeroportos, *shopping centers*, etc.

5.1.3 A criptografia

A criptografia e a esteganografia também são recursos que beneficiam os criminosos, dificultando a sua identificação e mesmo a interceptação do tráfego de seus dados. Wendt e Jorge (2012) definem criptografia como um processo utilizado para misturar dados e informações para garantir que apenas o destinatário possa ter acesso ao conteúdo produzido; e esteganografia como o ato de enviar uma mensagem oculta dentro de outra mensagem (permite esconder as informações de interesse no interior de uma mensagem, podendo ser um texto, vídeo ou áudio).

Wendt e Jorge (2012, p. 183) defendem a regulamentação do uso de softwares com criptografia, os quais só poderiam ser utilizados se devidamente registrados junto ao órgão competente e com depósito da chave correspondente.

5.2 PROVIDÊNCIAS NECESSÁRIAS À MELHORIA DA INVESTIGAÇÃO

Como podemos claramente observar, os crimes cibernéticos se proliferam muito rapidamente, e a resposta das forças de repressão é lenta e insuficiente,

sendo que a sensação de impunidade incentiva ainda mais o aumento dos índices de criminalidade.

Foi verificado, no curso das pesquisas, que, de acordo com os autores consultados e os profissionais de segurança pública, os principais pontos a serem melhorados – além do necessário aparelhamento do aparato policial, com melhorias nos recursos humanos, materiais e tecnológicos - são os seguintes:

5.2.1 Agilidade na expedição e cumprimento dos mandados judiciais

O processamento das requisições judiciais e deferimento dos mandados é um processo demorado, somando-se ao tempo que os provedores de conteúdo demoram para fornecer as informações. È necessário um dispositivo que obrigue as empresas a atender mais rapidamente. Um bom exemplo é a rede social Facebook, que criou em sua plataforma um ambiente exclusivo para auxílio às forças da lei, onde os agentes de segurança pública autorizados efetuam um cadastro e se comunicam com a empresa por meio de formulários e mensagens, podendo inclusive fazer *upload* de alvarás judiciais que são recepcionados e cumpridos pela empresa, que disponibiliza os dados requeridos com celeridade (WENDT e JORGE, 2013). Essa iniciativa do Facebook mostra que é perfeitamente viável uma comunicação rápida e eficaz entre as empresas digitais e as forças da lei. Um dispositivo legal poderia regulamentar a questão.

5.2.2 Celeridade da perícia forense computacional

Não é possível pensar em uma investigação exitosa, se esta depender de um laudo pericial que pode levar sete anos para ficar pronto. A solução passa por investimentos por parte do poder público, em contratação de peritos e capacitação de outros agentes que poderiam realizar exames periciais como peritos compromissados, agilizando o processo de investigação.

5.2.3 Instituir a integração entre as forças de segurança pública

Neste campo, os criminosos estão mais organizados. É comum a investigação policial se deparar com ação de quadrilhas, cujos indivíduos agem

espalhados por vários estados, e até mesmo no exterior. Já entre as forças policiais, não existe uma atuação integrada, nem padronização de procedimentos. Muitas vezes a falta de padronização se verifica dentro de um mesmo estado.

É fácil concluir que tal situação proporciona a ocorrência de diversas investigações paralelas, sobre a mesma quadrilha, em diferentes estados, que isoladamente não logram êxito, pois não conseguem avançar além das suas divisas territoriais. Wendt e Jorge (2012) defendem, como solução, a adoção de uma política pública específica para combater aos crimes cibernéticos, com criação de uma base de dados única ou compartilhamento das informações, padronização dos procedimentos, e todas as unidades especializadas no combate a estes crimes em sintonia para atuação conjunta a qualquer momento. Para tanto deveriam ser criadas unidades especializadas em todos os estados da federação, sendo que atualmente menos de cinquenta por cento dos estados possuem tais órgãos[10].

5.2.4 Promover melhorias na legislação

Apesar de algumas iniciativas legislativas aprovadas, ainda há muitos pontos a serem estabelecidos. Os agentes de segurança defendem a criação de uma legislação específica que abarque as condutas criminosas, deixando-se de enquadrar por analogia. Mais que isso, anseiam por um regulamento geral para o uso da internet, que defina claramente direitos e obrigações dos usuários e dos provedores de conteúdo. Wendt e Jorge (2012) defendem que os provedores de conteúdo deveriam ser obrigados por lei a manter os *logs* de conexão e outras informações dos usuários por período não inferior a um ano.

Esta regulamentação ocorreu com o advento da Lei n° 12.965 de 23 de Abril de 2014, também conhecido como Marco Civil da Internet. A lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil: os direitos e garantias dos usuários, a responsabilidade dos provedores e a atuação do poder público.

Esta lei possui pontos controversos, especialmente relacionados ao princípio da neutralidade de rede, que desagradou às empresas de telecomunicações porque limitou a oferta de promoções baseadas em restrições de pacotes de dados e velocidade de conexão. O princípio da neutralidade de rede prevê que todos os

[10] Fonte: SaferNet Brasil. Disponível em: <http://www.safernet.org.br/site/prevencao/orientacao/delegacias>. Acesso em: 07 nov. 2015.

dados que trafegam na rede devem ser considerados do mesmo jeito com acesso à mesma velocidade, sem nenhuma restrição de conteúdo, garantindo o livre acesso à qualquer informação na rede. Não pode haver interferência no conteúdo nem restrição de origem e destino. Esse princípio visa assegurar que todos possam acessar a rede em igualdade de condições, para qualquer conteúdo.

Do ponto de vista da investigação policial, o ponto mais importante da lei é a determinação de que os provedores de internet e de serviços devem preservar os registros (*logs*) de conexão pelo período de um ano e os registros de acesso a aplicações por seis meses, devendo fornecer as informações mediante ordemjudicial. Determina ainda que qualquer empresa que opere no Brasil, mesmo estrangeira, precisa submeter-se à legislação do país e cumprir as ordens judiciais. O marco civil da internet prevê ainda que as empresas que fornecem conexão não poderão ser responsáveis pelo conteúdos postados pelos usuários; já os provedores de serviços, como, por exemplo, os administradores de redes sociais, devem retirar do ar material considerado ofensivo, quando determinados pela Justiça.

CONCLUSÃO

O presente trabalho trouxe como problema central examinar a atuação dos órgãos de segurança pública do Brasil no combate aos crimes cibernéticos, a fim de enumerar os principais motivos que impedem uma ação eficiente, e que soluções devem ser buscadas.

O primeiro capítulo trouxe à definição do problema, a metodologia, a motivação para escolha do tema, os objetivos gerais e específicos e a descrição da estrutura do trabalho. No segundo capítulo foram apresentados os conceitos de redes de computadores, internet, segurança da informação, as principais ameaças e procedimentos de segurança. O terceiro capítulo trouxe o conceito de cibercrime, os tipos penais previstos na legislação e os sujeitos dos crimes de informática. O quarto capítulo tratou da investigação dos crimes cibernéticos no Brasil, como os órgãos policiais estão estruturados e como empreendem a investigação dos principais tipos de crime. No quinto capítulo procurou-se analisar o resultado da atuação das forças policiais frente às dificuldades presentes no combate ao cibercrime, além de descrever os principais problemas relacionados à investigação dos crimes de informática, e as providências que trariam melhorias neste campo.

Conclui-se que o resultado da pesquisa proporcionou o cumprimento dos objetivos propostos:

Identificar as ameaças à navegação na rede mundial de computadores: verificou-se que os ataques aos usuários de internet são empreendidos principalmente com o uso de dois artifícios: programas maliciosos e engenharia social, aproveitando-se de vulnerabilidades nos sistemas computacionais e imprevidência dos usuários.

Os crimes cibernéticos e legislação: foi possível identificar os crimes de informática, definidos por legislação própria ou tipificados na legislação penal convencional.

Investigação policial e resultados obtidos: verificou-se que no Brasil a investigação dos crimes de informática é empreendida pela Polícia Federal e pelas Polícias Civis dos Estados, com resultados insatisfatórios; os principais problemas

apontados são o excesso de burocracia, a falta de estrutura dos órgãos policiais, e a omissão da legislação em pontos importantes, como disciplinar que provedores de acesso e conteúdo colaborem com os órgãos de persecução penal.

Conclui-se que a investigação dos crimes cibernéticos no Brasil não proporciona resultados eficientes; o Brasil não está preparado para o combate ao cibercrime. Os próprios agentes públicos, ao falar sobre o assunto, enumeram sempre mais problemas do que resultados. A falta de estrutura e falta de integração dos órgãos policiais; as deficiências da legislação; a falta de regulamentação, que permite o uso livre e indiscriminado da internet, favorecendo a prática de atos ilícitos. Verificou-se que os agentes, no trabalho de investigação, convivem com uma série de empecilhos que dificultam e até inviabilizam a investigação (a demora na concessão de mandados judiciais, perícias, falta de integração entre os órgãos policiais, dificuldade em ver atendidas solicitações por alguns provedores de acesso e conteúdo, etc). E todos os pontos enumerados como sendo melhorias importantes, tratam-se tão somente das condições mínimas necessárias ao labor da persecução penal.

Wendt e Jorge (2012, p. 187) enfatizam a necessidade de criar mecanismos que calculem a incidência de ciberdelitos, favorecendo a análise criminal; a criação de políticas públicas preventivas, enfatizando a educação digital, e repressiva, baseada principalmente na formação de policiais investigadores de crimes cibernéticos; a regulamentação de redes abertas e sem controle, como *lan houses* e *cyber* cafés, bem como a obrigatoriedade de mecanismos que permitam a individualização de usuários de redes sem fio; além da criação de uma rede nacional de combate ao cibercrime.

Verificou-se que, quanto à tipificação dos atos ilícitos, houve ao longo dos últimos anos um esforço legislativo no sentido de enquadrar várias condutas, terminando mais recentemente com a aprovação da Lei 12.737/2012, que criminalizou a conduta de violar a segurança de computadores alheios, encerrando assim uma grave lacuna.

No decorrer dos procedimentos de pesquisa para elaboração do presente trabalho, verificou-se que um dos pontos carentes de regulamentação legal que trazia dificuldades à investigação policial, era a guarda e o fornecimento dos *logs* de

conexão e acesso pelos provedores de conexão e conteúdo. No dia 23 de abril de 2014 foi sancionada a Lei nº 12.965, originária do projeto de lei conhecido como“Marco Civil da Internet”, onde restou estabelecido que todos os provedores de conexão deverão guardar os registros pelo prazo de um ano, e os provedores de aplicações deverão guardar os registros de acesso pelo prazo de seis meses, e fornecidos à autoridade policial mediante ordem judicial, podendo, ainda, estes prazos serem dilatados por requerimento da autoridade policial ou administrativa ou o Ministério Público.

Resposta ao problema de pesquisa: “Quais os crimes virtuais que mais ocorrem e como se procede a investigação desses delitos no Brasil?”

Foram constatados que os tipos de delitos mais incidentes investigados pela Polícia Federal são pornografia infantil e fraudes bancárias; e pelas polícias civis, são crimes contra a honra (injúria, calúnia e difamação), fraudes bancárias e fraudes em comércio eletrônico.

No Brasil a atribuição constitucional da apuração das infrações penais é da Polícia Federal e das polícias civis dos Estados e do Distrito Federal. O instrumento de investigação é o inquérito policial, elaborado de acordo com as normas do Código de Processo Penal brasileiro. A Polícia Federal, nos crimes de sua competência, atua com melhor uso de inteligência policial, normalmente empreendendo investigações que visam atingir toda uma rede criminosa.

As polícias civis – com exceção de uns poucos órgãos especializados existentes em alguns Estados - geralmente não reúnem condições de dispensar a atenção necessária à investigação dos crimes de informática, especialmente pela falta de integração, sobrecarga de serviço, número insuficiente de agentes capacitados e órgãos especializados.

A pesquisa realizada permite concluir que o combate ao cibercrime no Brasil não atinge resultados satisfatórios, apontando-se, ainda, como pontos deficientes, a morosidade da perícia forense computacional e a falta de um decreto que regulamente de forma clara e objetiva os direitos e deveres dos usuários de internet e provedores de conexão e serviços, pois o marco civil da internet chegou cheio de lacunas e expressões ambíguas mostrando-se ineficiente em muitos aspectos.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF, 05 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em: 06 out. 2015.

Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal. **DiárioOficial [da] República Federativa do Brasil**, Brasília, DF, 31 dez. 1940. Disponívelem: <www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 06 out. 2015.

Decreto-Lei nº 3.689, de 03 de outubro de 1941 – Código de Processo Penal. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 13 out. 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 06 out. 2015.

Lei nº 11.829, de 25 de novembro de 2008**.** Altera a Lei nº 8.069, de 13 de julho de 1990. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 26 nov. 2008. Disponível em: <www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 06 out. 2015.

Lei nº 12.737, de 30 de novembro de 2012**.** Altera o Decreto-Lei nº 2848, de 7 de dezembro de 1940. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 03 dez. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm#art4>. Acesso em: 10 set. 2015.

Lei nº 12.965, de 23 de abril de 2014**.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial [da] RepúblicaFederativa do Brasil**, Brasília, DF, 24 abr. 2014. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 set. 2015.

CASSANTI, MOISÉS DE OLIVEIRA. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014.

CERT.br. **Cartilha de segurança para internet.** Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 05 out. 2015.

Estatísticas mantidas pelo CERT.br. Disponível em: <http://www.cert.br/stats/>. Acesso em: 03 out. 2015.

CETIC.br. **Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil.** Disponível em: <http://www.cetic.br/usuarios/tic/2012/apresentacao-tic-domicilios-2012.pdf>. Acesso em: 01 nov. 2015.

CGI.br. **O CGI.br e o Marco Civil da Internet**. Disponível em: <http://cgi.br/publicacoes/documentacao/CGI-e-o-Marco-Civil.pdf>. Acesso em: 06 out. 2015.

CORRÊA, GUSTAVO TESTA. **Aspectos jurídicos da internet**. São Paulo: Saraiva, 2007.

CRESPO, MARCELO XAVIER DE FREITAS. **Crimes digitais**. São Paulo: Saraiva, 2011.

FORUZAN, BEHROUZ A.; FEGAN, SOPHIA CHUNG. **Protocolo TCP/IP**. 3. ed. Porto Alegre: McGraw-Hill, 2010.

FREITAS, ANDREY RODRIGUES DE. **Perícia forense aplicada à informática:** ambiente Microsoft. Rio de Janeiro: Brasport, 2006.

JESUS, DAMASIO EVANGELISTA DE. **Direito penal–parte geral.** 31. ed. São Paulo: Saraiva, 2010.

KUROSE, JAMES F.; ROSS, KEITH W. **Redes de computadores e a internet:** uma abordagem top-down**.** 5. ed. São Paulo: Addison Wesley, 2010.

LYRA, MAURÍCIO ROCHA. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Ciência Moderna, 2008.

NAKAMURA, EMILIO T; GEUS, PAULO L. **Segurança de redes em ambientescooperativos**. São Paulo: Novatec, 2007.

OLIVEIRA, KARINA DE; REHDER, WELLINGTON. **Redes de computadores**. São Paulo: Viena, 2006.

PEREIRA, LEONARDO. **5 pontos essenciais para entender o Marco Civil da Internet**. 26 mar. 2014. Disponível em:<http://olhardigital.uol.com.br/noticia/41053/41053>. Acesso em: 27 out. 2015.

Polícia Federal – Agência de Notícias. **Operação Glasnot combate a pedofilia em 11 estados brasileiros**. 19 nov. 2013. Disponível em:<http://www.dpf.gov.br/agencia/noticias/2013/11/operacao-glasnost-combate-a-pedofilia-em-11-estados-brasileiros>. Acesso em: 01 nov. 2015.

ROSA, FABRIZIO. **Crimes de Informática**. 2. ed. Campinas: Bookselleer, 2006.

TANENBAUM, ANDREW S.; WETHERALL, DAVID. **Redes de computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2011.

TRF4 – Notícias. **Delegado da Polícia Federal garante mais eficiência no combate aos crimes de fraude bancária em seminário do TRF4**. 12 mar. 2013.Disponível em: <http://www.safernet.org.br/site/institucional/projetos/cnd/como-funciona>. Acesso em: 02 nov. 2015.

SAFERNET. Institucional – **Como funciona**. Disponível em: <http://www.safernet.org.br/site/institucional/projetos/cnd/como-funciona>. Acesso em: 02 nov. 2015.

SYMANTEC. **Trojan Horse (Cavalo de Troia).** Disponível em: <http://www.symantec.com/pt/br/security_response/glossary/define.jsp?letter=t&word=trojan-horse>. Acesso em: 10 nov. 2015.

WENDT, EMERSON. E-book. **Inteligência cibernética:** a (in)segurança virtual no Brasil. São Paulo: Delfos, 2011. Disponível em: <http://www.potti.com.br/home/detail/p/Mzg=>. Acesso em: 12 nov. 2015.

WENDT, EMERSON; JORGE, HIGOR V. NOGUEIRA. **Crimes cibernéticos:** ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.

Crimes cibernéticos: ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: Brasport, 2013.

HOLANDA FERREIRA, AURÉLIO BUARQUE DE. **Novo dicionário da língua portuguesa**. 2ª Ed. Rio de Janeiro: Nova Fronteira, 2000.p.1016

FERREIRA, IVETTE SENISE. A criminalidade Informática. In: LUCCS, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos relevantes. 2. ed. São Paulo: Quartier Latin.2005.

ROSA, FABRÍZIO. **Crimes de Informática**. Campinas: Bookseller,2002.

SILVA, RITA DE CÁSSIA LOPES. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003.