FACULDADE DE ADMINISTRAÇÃO E NEGÓCIO DE SERGIPE

FERNANDA LIMA DE SOUZA RAMOS

INVESTIGAÇÃO PENAL NOS CRIMES CIBERNÉTICOS

Aracaju
2014

FERNANDA LIMA DE SOUZA RAMOS

INVESTIGAÇÃO PENAL NOS CRIMES CIBERNÉTICOS

Monografia apresentada à Faculdade de Administração e Negócios de Sergipe - FANESE, como um dos pré-requisitos para obtenção de Grau de Bacharel em Direito, área de Ciências Humanas e Sociais.

Orientador: Professor Me. Sandro Luiz da Costa

Aracaju
2014

FERNANDA LIMA DE SOUZA RAMOS

INVESTIGAÇÃO PENAL NOS CRIMES CIBERNÉTICOS

Monografia apresentada à Faculdade de Administração e Negócios de Sergipe - FANESE, como um dos pré-requisitos para obtenção de Grau de Bacharel em Direito, área de Ciências Humanas e Sociais.

Aprovada em ____/____/____

BANCA EXAMINADORA

_____

Professor Me. Sandro Luiz da Costa

_____

Professor Esp. Matheus Dantas Meira

_____

Professor Esp. Fábio Brito Fraga

Aracaju
2014

AGRADECIMENTOS

A Deus, por ter me permitido nascer numa família tão maravilhosa, onde não falta amor, respeito, harmonia, cumplicidade, honra e dignidade, e, por estar sempre ao meu lado, dando-me sabedoria, paciência, perseverança, ânimo e humildade para enfrentar os desafios ao longo dessa árdua, mas compensadora jornada.

Aos meus filhos, IAN GABRIEL E DAVI EDUARDO, meus anjinhos, que ao chegarem ao mundo, me fizeram compreender e sentir o verdadeiro amor. Dedico essa graduação a vocês! Meus amores saibam que vocês foram minha inspiração e força para chegar até aqui. Amo vocês incondicionalmente!

A minha mãe, MARINALVA**,** mulher batalhadora, de sabedoria ímpar e coração imensurável. Por me ensinar os verdadeiros valores da vida. Com ela aprendi a perdoar, a perseverar, a ajudar o próximo sem exigir retorno, e, acima de tudo que família é o nosso bem mais precioso. Nela sempre encontrei o incentivo e a perseverança necessários para sobrepor os obstáculos da vida. Minha Mamusca, como é bom ter você comigo! Eu a amo demais!

Ao meu Pai, JOSÉ FERNANDES, sinônimo de trabalho, honradez e honestidade. Por me amar sem medida e se fazer presente em todos os momentos de minha vida. Com você eu sei que nunca vou estar só... Pai, você é o meu porto seguro! AMO VOCÊ!

Aos meus irmãos, EMERSON E FERNANDINHO, que sempre estiveram presentes com incentivos e exemplos próprios de determinação, força e superação.

Ao meu esposo, EMÍLIO EDUARDO, meu grande amor, que sempre me apoiou e incentivou a seguir nessa jornada acadêmica. Com ele eu aprendi a admirar e decifrar o mundo jurídico. Minha gratidão a você, por todas as aulas e dúvidas tiradas durante todo o curso. Nunca me esquecerei dos momentos, antes das provas, em que eu cansada e com sono sentia dificuldade de compreensão e memorização dos assuntos e ele pacientemente sentava ao meu lado e me explicava todo o conteúdo. O sucesso desse trabalho está intimamente ligado a você. Eu amo amar você!

Agradeço a todos da minha família, que de alguma forma, ajudaram nessa trajetória. Saibam que sempre estarei com vocês para o que der e vier! Obrigada por tudo! Amo vocês!

Agradeço também aos professores do curso de Direito da FANESE, pelas aulas que tão sabiamente ministraram no decorrer do curso, e em especial, ao Professor Me. SANDRO COSTA**,** por aceitar ser meu orientador nesse trabalho de conclusão de curso. Sua paciência e apoio ao me orientar, foram decisivos para que eu pudesse lograr êxito na conclusão desse estudo.

Não poderia deixar de agradecer aos meus colegas de trabalho, pelo apoio na minha jornada acadêmica, como também aos meus colegas de curso, em especial a minha amiga-irmã Shirley Costa, com os quais compartilhei esses anos de faculdade.

Por fim, agradeço a todos que, direta ou indiretamente, contribuíram para o término desta etapa.

RESUMO

O presente trabalho tem por objetivo analisar a investigação dos crimes cibernéticos frente às dificuldades existentes na sua persecução criminal. Para isso, foram abordadas questões relevantes referentes a conceitos, terminações e classificação desses delitos, procedimentos investigativos, produção de provas, legislação vigente e atuação do Estado, bem como da necessidade de profissionais capacitados nesta área. Tratou, ainda, da importância da existência de uma política de cooperação internacional para que haja uma maior celeridade e eficácia na investigação desses delitos. De uma forma geral, foram analisados os aspectos de uma investigação de crimes cometidos via e-mail, sites, redes sociais, dentre outros e como a utilização de técnicas de investigação especializadas interferem nessa inquirição. Nesse âmbito foi dado destaque aos cuidados necessários quando da produção de provas, em virtude do caráter efêmero dos dados e informações disponíveis na Internet. Deste modo, chegou-se a uma conclusão coerente, que o sucesso da investigação penal dos crimes cibernéticos independe de legislação específica, em outro termo, está intimamente ligado ao uso de recursos tecnológicos e de conhecimento em procedimentos investigativos especializados que devem ser passados aos profissionais que atuam nesta área.

PALAVRAS-CHAVE: crimes cibernéticos; investigação; provas; legislação.

ABSTRACT

This study aims to analyze the investigation of cyber crimes given the difficulties in its criminal prosecution. For this, the concepts relevant issues, terminations and classification of these offenses, investigative procedures, production of evidence, current legislation and state action as well as the need for trained professionals in this area were discussed. Also discussed the importance of a policy of international cooperation so that a faster and more efficient in investigating these crimes. In general, aspects of an investigation into crimes committed via email, websites, social networks, among others, and the use of specialist investigative techniques interfere with this inquiry were analyzed. In this context emphasis was given when necessary to the production of evidence, because of the ephemeral nature of the data and information available on the Internet care. Thus, we have reached a consistent conclusion that the success of the criminal investigation of cyber crimes independent of specific legislation, in other word, is closely linked to the use of technological resources and knowledge in specialized investigative procedures that should be passed to the professionals working in this field.

KEYWORDS: cyber crimes; investigation; evidence; legislation.

SUMÁRIO

INTRODUÇÃO 9

1 A REDE MUNDIAL DE COMPUTADORES 12

1.1 Histórico 12
1.2 Conceitos e características 15
1.3 Protocolo de Controle de Transmissão - TCP/IP 16
1.4 Sistema de Nome e Domínio - DNS 17
1.5 Provedor de Acesso e de Informação 17
1.6 Riscos na Internet 18

2 CRIMES CIBERNÉTICOS 23

2.1 Classificação 24
2.2 Sujeito Ativo e Passivo 25
2.3 Legislação Vigente 28
2.4 Convenção de Budapeste 34

3 DA INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS 36

3.1 Aspectos procedimentais 36
3.2 Procedimentos investigativos especializados 38

4 DESAFIOS NOS PROCEDIMENTOS INVESTIGATIVOS 49

4.1 Legislação vigente e a atuação do Estado 49
4.2 Profissionais Capacitados 51
4.3 Prova 51
4.4 Organização Criminosa 52
4.5 Cooperação Internacional 52

CONCLUSÃO 54

REFERÊNCIAS 56

INTRODUÇÃO

Os avanços tecnológicos dos últimos tempos, dentre outros aspectos, proporcionou à sociedade vivenciar um novo estágio de desenvolvimento: a Era da Informática. Nesse contexto, o advento da Internet, disponibilizou aos seus usuários acesso universal aos computadores e às informações neles contidas em questão de segundos. Com efeito, a sua utilização tem sido uma constante na vida das pessoas para as mais diversas formas de comunicação e produção do conhecimento.

Em que pesem os vários benefícios trazidos por essa rápida e crescente popularização da Internet, o uso dessa rede pode ocasionar diversos riscos aos seus usuários, pois que está sendo usada, com frequência, para a prática de crimes que trazem consequências danosas à sociedade.

Nesse diapasão surgem os crimes cibernéticos “que se caracterizam pela prática de delitos no ou por intermédio do ambiente cibernético, ou seja, da internet” (WENDT; JORGE, 2013).

Impende destacar que a terminologia usada neste trabalho, qual seja, crimes cibernéticos, será adotada como sinônimo de crimes virtuais cometidos na internet por entender que este é o termo mais adequado a conduta, natureza e o meio onde são praticados tais crimes, já que o objeto de estudo do delito ora em comento é a sua prática no ambiente da Internet.

A rede mundial de computadores é ambiente fértil para cometimento desse delito, pela falta de atenção dos seus usuários, ampla liberdade de comunicação e expressão que proporciona, ou diante da dificuldade de investigação gerada pelo anonimato que esta vem a oferecer.

Essa realidade trouxe um desafio para os profissionais que atuam nessa área, no tocante a sua investigação criminal, pela diversidade de tecnologias e termos técnicos que ambiente da internet dispõe.

Além disso, a investigação dos crimes cibernéticos não possui a mesma liberdade nem facilidade que aqueles praticados no mundo real. Exemplo disso são os procedimentos realizados para a produção de provas, em que, para conseguir informações do cadastro do usuário infrator se faz necessário que os prestadores de

serviços de acesso e de conteúdo à internet as forneçam para que a polícia judiciária ou outros órgãos de persecução criminal consigam investigar de maneira eficiente.

Dentro desse contexto, o trabalho justifica-se diante da dificuldade de investigação e da falta de padronização nos procedimentos investigativos para esses delitos, com o intuito de instrumentalizar e auxiliar os profissionais que atuam nessa área, para que possam combater com eficiência e proatividade o número crescente de crimes cometidos nessa rede, dando o correto encaminhamento às atividades investigativas dos casos que lhe chegarem ao conhecimento.

Analisando as metas propostas neste trabalho, a pesquisa realizada pode ser classificada, quanto ao objetivo do estudo, como explicativa, pois visa esclarecer quais fatores contribuem de alguma forma, para a ocorrência de determinado fenômeno. No que diz respeito ao procedimento técnico, será apresentada sob a forma de uma revisão da literatura, por apropriar-se de material já publicado em fontes secundárias impressas e digitais, associado à legislação vigente, desde que, contemplando a temática em estudo. Quanto a sua natureza, é classificada como teórica, sendo o conhecimento adquirido posto em análise para a solução do problema proposto para a pesquisa. Em relação a sua abordagem, é definida como qualitativa porque traz a realidade concreta relacionada, sem a preocupação com os dados estatísticos, observando ainda, os aspectos descritivo e interpretativo das informações obtidos com o estudo.

Para uma devida abordagem do tema, primeiramente será feito um estudo sucinto sobre a rede mundial de computadores para situar o leitor quanto a sua origem, conceitos, características e alguns termos técnicos necessários para uma melhor compreensão do objeto de estudo desse trabalho. Em seguida, aspectos relevantes aos crimes cibernéticos no tocante a conceitos, características e classificação, bem como dos seus fundamentos jurídicos, abrangência da normatização brasileira, tratados e convenções.

Superada a fase predominantemente teórica, será dada ênfase as principais questões de ordem técnica, que comumente dificultam a investigação dos crimes cibernéticos, quais sejam: aspectos procedimentais e os procedimentos investigativos especializados.

Por fim, será realizada uma abordagem crítica acerca dos desafios encontrados nos procedimentos investigativos dos crimes cometidos no ambiente da internet.

1 A REDE MUNDIAL DE COMPUTADORES

1.1 Histórico

Para uma melhor compreensão acerca do surgimento da Internet, convém de suma importância regressar às décadas de 60 e 70 para entender como ela se tornou o meio de comunicação mais popular da atualidade.

A Internet surgiu no auge da Guerra Fria, final da década de 60, diante da necessidade das forças armadas norte-americanas de preservar as comunicações em caso de ataques inimigos que destruíssem os seus meios convencionais de telecomunicações. A ideia central era o desenvolvimento de um sistema descentralizado que permitisse o funcionamento da rede ainda que uma ou mais máquinas fossem destruídas.

Assim, em 1969,surgiu a ARPANET desenvolvida pela empresa Advanced Research Projects Agency (ARPA), do Departamento de Defesa dos Estados Unidos, com a finalidade de aumentar a comunicação na sua força militar. Sua estrutura era baseada na comunicação descentralizadas das máquinas onde a remoção de uma ou mais delas na rede não comprometeria o seu funcionamento. A transmissão dos dados entre os computadores era feita através de comutação de pacotes, os quais continham todas as informações e dados que permitiam sua leitura pelos seus destinatários.

Assim assevera Fabrizio Rosa:

> O Departamento de Defesa dos EUA apoiou uma pesquisa sobre comunicações e redes que poderiam sobreviver a uma destruição parcial, em caso de guerra nuclear. A intenção era difundi-la de tal forma que, se os EUA viessem a sofrer bombardeiros, tal rede permaneceria ativa, pois não existiria um sistema central e as informações poderiam trafegar por caminhos alternativos até chegar ao seu destinatário. Assim, em 1962, a ARPA encarregou a Rand Corporation (um conselho formado em 1948) de tal mister, que foi apresentar seu primeiro plano em 1967. Em 1969, a rede de comunicações militares foi batizada de ARPANET (2005, p. 29).

Essa ferramenta ganhou novas finalidades, nas décadas de 70 e 80, sendo usada para objetivos diversos, sendo um importante meio de comunicação acadêmico para estudos científicos ou didáticos, bem como para comunicações

entre os usuários. Nesse período surgiu o protocolo TCP/IP (*Transmission Control Protocol/ Internet Protocol)*, protocolo este usado até os dias atuais e que será abordado com mais detalhes nos próximos tópicos deste capítulo.

Assim dispõe:

> Em 1974 surgiu o protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol*) que viria a ser utilizado até os dias de hoje. O seu surgimento está relacionado ao grande crescimento da rede ARPANET, de modo que seu protocolo de comutação de pacotes NCP (*Network Control Protocol*) veio a se tornar inadequado para os níveis de dados que seriam transmitidos. (BOLSONI, 2014, p. 33).

> Durante os anos 70, as universidades, principalmente dos Estados Unidos, estavam conectadas por meio da ARPANET, que, em 1975, contava com cerca de 100 sites, acessados por 25 (vinte e cinco) computadores interligados. Em 1983, após um vasto crescimento, a ARPANET se dividiu em duas redes para poder atender a demanda crescente e preservar os interesses estratégicos de defesa: a MILNet, de aplicação exclusivamente militar, e a ARPANet, com utilização no meio acadêmico (BOLSONI, 2014, p. 33).

Com o advento do “World Wide Web”, criado em Genebra, 1989, a internet tornou-se mundial, conectando países, e diminuindo as fronteiras geográficas, o uso da internet se popularizou, e com isso o número de usuários da rede. A inovação do “www” é a sua composição de hipertextos que permitem o relacionamento direto entre textos. Essa inovação permitiu que o usuário fizesse uso apenas de um clique no “*mouse*” para acessar toda a rede sem a necessidade de conhecimentos específicos sobre sua estrutura e funcionamento.

> Ate o inicio da década de 1990, a Internet era um verdadeiro reduto de pesquisadores ligados às universidades, ao governo e a indústria. Uma nova aplicação, a WWW (World Wide Web), mudou essa realidade e atraiu para a rede milhares de novos usuários, sem a menor pretensão acadêmica. (TANENBAUM, 2003, p. 59)

Assim, a internet atingiu o seu objetivo, que era facilitar a navegação, tornando-a mais agradável, além de inserir sons e imagens aos textos, cansativos e monótonos.

> Durante a década de 1990, muitos outros países e regiões também construíram redes nacionais de pesquisa, com frequência moldadas de acordo com a ARPANET e a NSFNET. Na Europa, essas redes incluíram EuropaNET e EBONE, que começaram com linhas de 2 Mbps e depois foram atualizadas com linhas de 34 Mbps. Mais tarde, a infraestrutura de rede na Europa também foi entregue a indústria. (TANENBAUM, 2003, p. 60)

A década de 90 tornou-se a era de expansão da Internet. Nesse período surgiram vários navegadores (browsers) como, por exemplo, o Internet Explorer da Microsoft e o Netscape Navigator. Além disso, o aparecimento de provedores de acesso e portais de serviços online fez com que a rede mundial de computadores fosse utilizada por vários segmentos sociais.

No Brasil, a Internet surgiu em 1988, com as comunidades acadêmicas de São Paulo e do Rio de Janeiro. No ano seguinte, O Ministério de Ciência e Tecnologia criou a Rede Nacional de Pesquisa, para disponibilizar os serviços de acesso à Internet.

Não obstante, apenas em 1995, a Rede Mundial de Computadores tomou maiores proporções em nosso País, através do Comitê Gestor de Internet (CGI), criado com a finalidade de promover o desenvolvimento de serviços desse conjunto de redes, estabelecendo padrões e procedimentos técnico-operacionais. Ressalte-se ainda, que o referido Comitê foi criado pela Portaria Interministerial nº 147, de 1995, e alterado pelo Decreto Presidencial nº 4.829, de 3de setembro de 2003.

Destarte,

> A Internet surgiu precisamente no Brasil em 1988, com as comunidades acadêmicas de São Paulo e do Rio de Janeiro. Em 1989, O Ministério de Ciência e Tecnologia criou a Rede Nacional de Pesquisa, tendo a finalidade de disponibilizar os serviços de acesso à Internet. Somente no ano de 1994 foi iniciada a exploração comercial da Internet neste País. Existe no Brasil um Órgão responsável pela administração da Internet. Este Órgão denomina-se Comitê Gestor de Internet, criado para fomentar o desenvolvimento de serviços na Internet, recomendar padrões e procedimentos técnicos e operacionais para a Internet, coordenar a atribuição de endereços na Internet, o registro de nomes de domínios, a interconexão de espinhas dorsais e, por fim, coletar, organizar e disseminar informações sobre os serviços da Internet. (ANDRADE, 2006, p.10)

A popularização mundial da “Rede das Redes” se deu com a chegada da internet banda larga que aumentou a velocidade de transmissão de dados. Hoje é possível navegar de forma mais rápida e assim realizar um número maior de tarefas em um curto espaço de tempo, bem como fazer downloads de programas maiores, como filmes, músicas, etc.

Enfim, é difícil imaginar o mundo atual sem a Internet. Ela tomou parte da vida das pessoas de tal forma, que estar conectado nela passou a ser um requisito precípuo à inserção do cidadão na sociedade da era digital.

1.2 Conceitos e características

Passados os conhecimentos acerca da história e desenvolvimento da internet, necessário se faz apresentar alguns conceitos e características acerca dessa ferramenta, para situar o leitor acerca do ambiente que será investigado no presente trabalho.

De acordo com TANENBAUM (2003, p. 53), “A Internet não é de modo algum uma rede, mas sim um vasto conjunto de redes diferentes que utilizam certos protocolos e fornecem determinados serviços comuns”.

Nesse sentido, a internet, pode ser definida como um conjunto de redes que conecta milhões de equipamentos computacionais em todo mundo. Não faz muito tempo, esses equipamentos eram apenas computadores, porém, hoje, existem outros dispositivos que usam que dispõem de tecnologia para usufruir dessa ferramenta, a exemplos dos celulares de terceira geração (3G), televisores, automóveis, equipamentos de sensoriamento ambiental, dentre outros. Cumpre salientar, que, na linguagem virtual, esses equipamentos são chamados de “hospedeiros” ou “sistemas finais”.

Dentre as suas características, LORENZETTI (2005 *apud* GEMIN, 2010, p. 17) destaca:

a) É uma rede aberta, visto que qualquer um pode ter acesso a ela;
b) É interativa já que o usuário gera dado, navega e estabelece relações;
c) É internacional, no sentido de que permite superar as barreiras nacionais;
d) Há uma multiplicidade de operadores.

Seguindo essa linha de pensamento, importante transcrever o ensinamento de MARTINS (2003 *apud* GEMIN, 2010, p. 17):

> [...] a Internet, também conhecida como a grande rede, traz consigo a era do tempo real, permitindo a disposição instantânea de uma informação, de uma imagem ou som através do mundo, com diversas aplicações possíveis, tais quais os ensino e trabalho à distância, a medicina pela via cibernética ou as relações de consumo travadas no espaço virtual[...]

Como já foi demonstrado, é inconteste a gama de benefícios que a Internet trouxe à sociedade, proporcionando entre as pessoas uma rápida interação das mais diversas formas.

1.3 Protocolo de Controle de Transmissão - TCP/IP

A arquitetura da Internet possui uma família de protocolos organizados em camadas, sendo os mais importantes o TCP e o IP, também chamados de protocolos de comunicação, responsáveis pelo encaminhamento e transporte de dados na rede, desde a sua origem até o destino.

> O protocolo TCP/IP (Transmission Control Protocol/Internet Protocol – Protocolo de Controle de Transmissão / Protocolo de Internet) é um conjunto de protocolos utilizado na Internet atualmente, e de uso bem difundido em redes locais , até as de uso doméstico. É um protocolo disponível praticamente todos os sistemas operacionais, e resultou de um projeto da DARPA (Defense Advanced Research Projects Agency – Agência de Projetos de Pesquisa Avançada de Defesa), que o criou para permitir comunicação de dados em rede, de forma confiável e resistente à queda de partes da rede.(COSTA, Sampaio Lemos; ANTONIO, Marcelo, 2003)

Zaniolo (2012, p. 139) define protocolo de comunicação como sendo “um conjunto de regras que torna possível a comunicação entre computadores de uma mesma rede, permitindo que as informações sejam enviadas e recebidas”.

> Assim como as nossas residências têm endereços, utilizados para receber correspondências, os computadores que fazem parte da Internet também precisam de um endereço para receber as suas “correspondências digitais”. Esse endereço é chamado de endereço IP, ou simplesmente IP, que a abreviatura de Internet Protocol (TANENBAUM, 2003, p. 54)

Da afirmação do renomado autor, depreende-se que uma vez realizada uma conexão de um computador ou dispositivo similar à Internet, um endereço IP (Protocolo de Internet) é atribuído exclusivamente para aquele equipamento. Desse modo não é possível que dois dispositivos tenham o mesmo IP quando da navegação na Internet no mesmo dia e horário.

Assim, para que ocorra a troca de informações entre esses dispositivos, na rede mundial de computadores, é necessário que o aparelho transmissor conheça o endereço do IP do seu destinatário e vice-versa.

Convém de suma importância esclarecer que esses endereços são controlados por entidades mundiais. No Brasil, o responsável pelo controle e manutenção desses endereços é o Registro.br.

1.4 Sistema de Nome e Domínio - DNS

Como já afirmado, os dispositivos computacionais conectados à internet são identificados pelo IP, tendo em vista a complexidade de memorização desses números, esses endereços são associados a um domínio, que nada mais é do que o endereço do site. Logo, para criação de um site é imprescindível o registro do seu domínio na Internet.

Nesse contexto, surge o servidor DNS (Domain Name System), responsável pela transformação de domínios em endereços IPs e vice-versa. Sem ele seria necessário a memorização de uma sequência de números dos mais de 4 bilhões de endereços únicos que o protocolo IP dispõe.

> O Domain Name System, ou DNS, é um serviço simples, mas muito importante para os usuários dos serviços da Internet. Sua função é mapear os endereços IP em nomes, tecnicamente chamados de domínio, e vice-versa (KUROSE, 2006 *apud* ELEUTÉRIO; MACHADO, 2013, p. 107).

Desse modo, quando o usuário digita um domínio em seu brownser[1], este é automaticamente traduzido para seu endereço numérico (IP), através do seu servidor DNS (Sistema de Nome e Domínio), ou seja, os domínios, quaisquer que sejam, são, na verdade, endereços associados aos endereços IP do servidor da Internet. Isso significa que ao digitar www.ssp.se.gov.br, na verdade, é um nome associado ao endereço IP 187.17.2.5.

1.5 Provedor de Acesso e de Informação

Antes de discorrer sobre provedores, para familiarizar o leitor acerca de alguns termos utilizados na Internet, será apresentado o significado das expressões

[1]Programa utilizado para navegar na internet.

“Internautas” e “site, a primeira diz respeito ao nome dado aos seus usuários, já a segunda, também chamada de sítio (tradução em português), se refere ao conjunto de páginas hospedadas na Internet interligadas através de links que ao acessá-lo, direcionam o usuário a página solicitada.

Cumpre esclarecer que esses sites são hospedados e gerenciados por servidores, ou seja, computadores que disponibilizam serviços e suporte para o armazenamento desses sites. Aqui, surge à figura do provedor, que nada mais é do que a empresa ou organização que disponibiliza tais serviços aos usuários de Internet.

Ao se falar em provedor, convém de suma importância fazer a distinção entre o que vem a ser provedor de acesso e provedor de informação. O primeiro disponibiliza o acesso direto do usuário à Internet, o segundo abastece a grande rede com informações.

Assim,

> o conceito de provedor de acesso contempla, exclusivamente, a disponibilidade de conexão à rede, não incluindo acessórios, dependentes dessa conexão, como o gerenciamento de contas de correio eletrônico ou a disponibilização de espaços destinados ao armazenamento de dados, com ou sem divulgação a terceiros.(PARENTONI, 2009, p.28)

Logo, a função do provedor de acesso é intermediar a conexão entre o usuário e a rede mundial de computadores. Com a conexão o usuário receberá um número de IP e ficará estabelecido um log de acesso, sendo possível armazenar informações no provedor de acesso como horário e tempo de conexão.

Já o provedor de informações é o responsável pela pelo armazenamento e disponibilização dos dados na Internet, sejam estes, imagens, textos, áudios ou vídeos, ou seja, ele tem o papel de proporcionar ao usuário abastecer a rede com os mais variados tipos de informações.

1.6 Riscos na Internet

Ao passo em que a internet vem ganhando cada vez mais espaço no mundo como um sistema de comunicação, traz consigo uma gama de riscos à sociedade.

Neste tópico serão abordadas as principais ameaças existentes no ciberespaço[2] que contribuem para prática de crimes cibernéticos.

1.6.1 Engenharia Social

Utilizada em praticamente todas as ações criminosas da “rede das redes”, nessa técnica o agente criminoso usa da persuasão para ter acesso não autorizado a computadores ou informações.

Para WENDT (2013), a engenharia social é um conjunto de técnicas destinadas a ludibriar a vítima, de forma que ela acredite nas informações prestadas e se convença a fornecer dados pessoais nos quais o criminoso tenha interesse ou a executar alguma tarefa e/ou aplicativo.

Nessa situação, o criminoso concentra-se nas vulnerabilidades que por ventura a vítima possa ter ou apresentar frente a determinadas ações do cotidiano. Logo, suas ações são baseadas na manipulação da emoção de seus “alvos”. Assim, trabalham principalmente com o medo, a ganância, a simpatia e, por último, a curiosidade.

Impende destacar que essa técnica também é usada na investigação criminal, a qual é denominada de engenharia social contra o crime. Nesses casos os investigadores se infiltram em uma organização criminosa, através dessa técnica, para que seja coletado o maior número de informações.

1.6.2 Phishing Scam

Caracteriza-se pelo envio de mensagens falsas aos usuários (normalmente por e-mail) que forjando pertencer a uma instituição conhecida como banco ou algum site do governo. Nesse tipo de e-mail,há normalmente links que apontam para páginas falsas onde são solicitados nossos dados. Alguns desses links também são

[2] Ciberespaço: espaço das comunicações por redes de computação(Dicionário Eletrônico Houais. Editora Antonio Houaiss. 2009).

usados para que o usuário ao clicar faça download de arquivos infectados, ou seja, arquivos maliciosos que provocaram danos ao computador.

Uma das formas de evitar ser vítima desse tipo de ataque é, ao receber um e-mail desse tipo, não clicar no link, ao invés disso, ir diretamente à pagina da instituição e lá verificar se as solicitações ou ofertas daquele e-mail são verídicas.

1.6.3 Pharming

Técnica muito parecida com o Phishing Spam, porém mais elaborada. A diferença deste golpe é o seu *modus operandi,* aqui o criminoso altera as configurações de um servidor DNS, fazendo com que um domínio qualquer aponte para um endereço IP de um servidor falso, mas com o site visualmente idêntico ao original. Por exemplo, o agente criminoso altera as configurações de DNS do site da Caixa Econômica, quando o usuário digitar o endereço do referido site aparecerá página do site, porém o seu endereço IP estará apontado para um servidor falso.

Na classificação do Centro de Estudos, Resposta e Tratamento de Incidentes e Segurança no Brasil (CERT.br, [s.d] [n.d]):

> Pharming e um tipo específico de phishing que envolve a direção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS (Domain Name System). Neste caso, quando você tenta acessar um ˆ site legítimo, o seu navegador Web e redirecionado, de forma transparente, para uma pagina falsa. Este redirecionamento pode ocorrer:
> - por meio do comprometimento do servidor de DNS do provedor que você utiliza;
> - pela ação de códigos maliciosos projetados para alterar o comportamento do serviço de DNS do seu computador;
> - pela ação direta de um invasor, que venha a ter acesso às configurações do serviço de DNS do seu computador ou modem de banda larga.

1.6.4 Deface

Técnica que consiste na desfiguração de páginas na Internet, também conhecida com defacement, ou seja, o agente criminoso invade a página e altera o seu conteúdo.

Esse tipo de ação geralmente é usada para o autor apresentar algum destaque ao grupo a que pertence, com o intuito de defender suas convicções religiosas, filosóficas ou políticas.

1.6.5 Malware

São programas com códigos maliciosos desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Uma vez instalados, passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, como por exemplo, obtenção de vantagens financeiras e coleta de informações confidenciais.

Segue os principais tipos e suas ações de acordo com a CERT.br:

- **Bot -** programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. É capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores. A comunicação entre o invasor e o computador infectado pelo bot pode ocorrer via canais de IRC, servidores Web e redes do tipo P2P, entre outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar spam. Um computador infectado por um bot costuma ser chamado de zumbi (zombi e computer), pois pode ser controlado remotamente, sem o conhecimento do seu dono.
- **Botnets -** uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots. O atacante que a controlar, além de usá-la para seus próprios ataques, também pode alugá-la para outras pessoas ou grupos que desejem que uma ação maliciosa específica seja executada. Algumas das ações maliciosas que costumam ser executadas por intermédio de botnets são: ataques de negação de serviço (Distributed Denialof Service – DdoS), propagação de códigos maliciosos (inclusive do próprio bot), coleta de informações de um

grande número de computadores, envio de spam e camuflagem da identidade do atacante (com o uso de proxies instalados nos zumbis).

- **Cavalo de Troia –** permite que o seu autor (agente criminoso) obtenha dados pessoais do computador da vítima através de acesso remoto.
- **Keylogger –** também conhecido como registrador de teclado, tem a função de registrar tudo que o usuário digita no computador e também o que aparece na tela do computador.
- **Rootkit –** conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.
- **Backdoor–**deixa o computador vulnerável a ataques e invasões.

2 CRIMES CIBERNÉTICOS

Não há dúvida que a inovação tecnológica trouxe uma série de benefícios para as pessoas e a comunidade em geral. Todavia, essas vantagens trouxeram, no âmbito da rede mundial de computadores, a possibilidade de realização de novas práticas ilegais e criminosas, quais sejam: os crimes cibernéticos.

Como já mencionado, apesar de existir várias qualificações quanto aos crimes praticados na internet, no presente trabalho, optou-se por adotar o termo “crimes cibernéticos”, por entender ser essa a nomenclatura mais adequada.

É conveniente para elucidar o conceito desse tipo de delito, trazer a lume o pensamento de alguns estudiosos no assunto:

> O conceito de crime cibernético no Brasil é exatamente o fato consistente na prática de crime contra uma pessoa ou sociedade, mediante o uso da internet, passível de enquadramento nas leis penais brasileiras, para fins de punição efetiva, ou seja, aquele que sai do virtual e entra na realidade de todos (AZEVEDO, 2011, p. 33).

Assim, de acordo com Pires Neto (2009, p. 11), “crimes cibernéticos são aqueles cometidos utilizando a Internet, ou seja, o crime cibernético é espécie do crime de informática, uma vez que se utiliza de computadores para acessar a Internet”.

Já, Lindolfo Neto (2009), considera esse tipo de delito como um ato típico, antijurídico, culpável e antiético, cometido sempre com utilização de dispositivos computacionais, para transmissão de dados através da Internet, com o intuito de copiar dados sem autorização, prejudicar outrem, atentar contra a liberdade individual, à privacidade, à honra, etc.

Destarte, pelo acima alinhavado, depreendem-se crimes cibernéticos como delitos praticados no ambiente da internet, onde para sua execução, é indispensável o uso de dispositivos computacionais. Frise-se ainda que, nesse tipo de delito os agentes criminosos são detentores de um vasto conhecimento na área de tecnologia da informação.

2.1 Classificação

Na classificação dos crimes cibernéticos, a questão principal é averiguar se a internet foi à peça fundamental para o cometimento do delito, ou seja, se esta foi utilizada como meio e como fim para determinada conduta delituosa ou se, apenas como meio.

Nesse sentido, WENDT e JORGE (2013, p. 19) os classificam em:

> - Crimes exclusivamente cibernéticos: praticados somente com a utilização de dispositivos computacionais que permitam acesso à internet. Ex: invasão de computadores, interceptação telemática ilegal, etc.
> - Crimes cibernéticos abertos: quando o computador é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele. Ex: crimes contra honra, de ameaça, estelionato, pornografia infantil, etc.

Insta salientar que a doutrina majoritária os classifica como: crime puro ou próprio e o impuro ou misto. No primeiro, os delitos são exclusivamente praticados no âmbito da Internet, onde o sistema de informática é compreendido como meio e fim, almejado pelo criminoso virtual. Já, no segundo, seria somente a utilização da rede mundial de computadores como meio, ou seja, como veículo para a prática de um delito que já está devidamente definido na legislação penal vigente.

Assim,

> Os crimes próprios são aqueles que só podem ser praticados na informática, ou seja, a execução e a consumação ocorrem nesse meio, trata-se de tipos novos em que o bem jurídico tutelado é a informática, apresenta como exemplos a violação de e-mail e o dano em arquivos causado pelo envio de vírus; e os crimes impróprios são aqueles já tipificados, que violam bens já protegidos pela legislação brasileira, podem ser praticados de qualquer forma e o computador é só mais um meio/instrumento de execução dessa conduta, como por exemplo, o crime de ameaça, de pedofilia, entre outros (MENDES; VIEIRA, 2012).

Para Viana (2003, p. 39), os crimes cibernéticos impróprios são aqueles praticados através do computador e da internet, todavia os mesmos não constituem o alvo da pratica delituosa, mas somente o meio pelo qual se dá a realização do delito. A principal característica desse tipo de infração é a não necessidade do uso do computador e da internet, ou seja, o crime pode ser praticado por outros meios que não o digital, e que necessariamente lesem bens jurídicos que se encontram também fora do mundo digital. Já, os crimes cibernéticos próprios são aqueles cujo

agente necessariamente se utiliza de um computador, uma vez que o sistema eletrônico é tanto o meio pelo qual se realiza o ilícito, quanto o objeto violado pela ilegalidade, ou seja, alem do criminoso se utilizar da internet, ele busca modos de ultrapassar a segurança do computador da vítima a fim de adquirir dados, alterná-los no sistema e usufruir de forma delituosa.

Numa classificação mais específica,

> O crime virtual puro seria toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas. Crime virtual misto seria aquele em que o uso da internet é condição *sine qua non* para a efetivação da conduta, embora o bem jurídico visado seja diverso do informático, como, por exemplo, as transferências ilícitas de valores em uma *home banking* ou no chamado *salamislacing*, onde o *cracker* retira de milhares de contas correntes, diariamente, pequenas quantias que correspondem a centavos e as transfere para uma única conta. Embora esses valores sejam ínfimos para o correntista, que, na maioria das vezes, nem se dá conta do furto, representam para o cibercriminoso uma expressiva quantia em seu montante. Por derradeiro, crime virtual comum seria utilizar a internet apenas como instrumento para a realização de um delito já tipificado pela lei penal. Assim, a Rede Mundial de Computadores acaba por ser apenas mais um meio para a realização de uma conduta delituosa (FURLANETO NETO; GUIMARAES, 2003, p. 69).

Extrai-se por meio do presente estudo que no tocante à classificação dos crimes cibernéticos, o cerne da questão é identificar se a internet serviu apenas como meio para prática delitiva, ou se esta serve como ferramenta indispensável à prática do ato delituoso. No primeiro caso, cumpre registrar, que são crimes já existentes e tipificados pela legislação pátria, sendo novo apenas o seu *modus operandi*[3].

2.2 Sujeito Ativo e Passivo

Levando em consideração os seus sujeitos, o direito penal classifica os crimes cibernéticos, em geral, como crime comum, visto que, podem ser praticados por qualquer pessoa. Assim preceitua Capez (2011, p. 268), “crime comum é o que pode ser cometido por qualquer pessoa. A lei não exige nenhum requisito formal”.

[3] Expressão em latim que significa "modo de operação", utilizada para designar uma maneira de agir, operar ou executar uma atividade seguindo sempre os mesmos procedimentos.

Diferentemente de outros crimes no qual o sujeito ativo e passivo do ato delituoso é facilmente identificado, nos crimes cometidos na Internet, a única certeza sobre o criminoso é que este é uma pessoa física ou jurídica ou uma entidade pública ou privada, e que sempre haverá o sujeito passivo, ou seja, alguém que está sendo lesado enfim o que sofre a ação.

2.2.1 Sujeito Ativo

No tocante ao sujeito ativo, numa análise mais apressada, imagina-se que esses crimes são praticados por pessoas com alto conhecimento na área de tecnologia da informação, porém com a popularização da Internet apareceram milhares de casos, como os de caráter difamatório, aliciamento de menores e o comércio sexual, que são praticados por pessoas com baixo conhecimento em informática.

Nesse sentido, a autoria delitiva, de forma simplificada, é imputada ao homem comum, havendo uma única necessidade, qual seja a disponibilidade de um dispositivo informático conectado à internet. De posse disso, o agente criminoso consegue atacar os diversos bens jurídicos tutelados no nosso ordenamento jurídico, violando inclusive às normas penais vigentes, sem a necessidade de preencher qualquer requisito subjetivo que o torne apto à prática desses delitos.

A definição do sujeito ativo, no caso dos crimes realizados no âmbito da Internet, encontra respaldo nas palavras de Mirabete:

> Sujeito ativo do crime é aquele que pratica a conduta descrita na lei, ou seja, o fato típico. Só o homem, isoladamente ou associado a outros (coautoria ou participação), pode ser sujeito ativo do crime, embora na Antiguidade e na idade média ocorressem muitos processos contra animais. A capacidade geral para praticar crime existe em todos os homens, é toda pessoa natural independente da sua idade ou de seu estado psíquico, portanto também os doentes mentais (MIRABETE, 2008, p. 15).

Assim, é de fundamental importância traçar um perfil desses agentes criminosos para se chegar à autoria do crime.

Primeiramente, destaca-se a figura do hacker que de acordo com o dicionário Michaelis quer dizer “pessoa que usa seu conhecimento técnico para ganhar acesso a sistemas privados”.

Cumpre esclarecer que esses indivíduos utilizam seus conhecimentos não necessariamente para práticas ilícitas. Nesse diapasão, depreende-se existir pessoas que usam o conhecimento técnico de forma positiva ou negativa. Neste ultimo caso, temos a figura do cracker, conhecido como o usuário de computador que usa seus conhecimentos, de forma premeditada, com fim criminoso de auferir vantagens ilícitas.

> A definição mais aceita é que *Hacker* é qualquer um que tenha grande conhecimento sobre computadores e faça invasões. Ou seja, apesar da fama de “criminosos virtuais”, nem todo *Hacker* deseja o prejuízo alheio. Existem aqueles que se dizem “*Hackers* do bem”, pois invadem os computadores e deixam mensagens informando a vítima do risco existente, aconselhando a providenciar uma proteção mais efetiva. Outros, ainda, passam a trabalhar em empresas a fim de desenvolver programas que sejam capazes de frear as invasões (CRESPO, 2011, p.95).

Sobre os criminosos virtuais, de acordo com Crespo (2011, p.96) ainda existem:

> ***Carders***: estelionatários típicos, assim chamados por fazerem compras pela rede com cartões de créditos alheios ou gerados por programas de computadores. Esse tipo de criminoso invade os computadores das administradoras de cartões de crédito e subtrai os números. Depois disso, distribui-os nas redes, a fim de não ser descoberto, porque, dessa forma, muitas pessoas podem ter acesso aos números, sendo muito difícil saber quem os subtraiu.
> ***Lammers***: pensam ser “Hackers”, embora não detenham muito conhecimento. São comparados àqueles que fazem uma ou duas aulas de artes marciais e já querem bater em todo mundo. Geralmente são insultados e depreciados pelos “Hackers”.
> ***Phreakers***: usam seus conhecimentos para fazer ligações gratuitas ou escutas telefônicas. Para isso, usam computadores e, quando um telefone toca, o dele também o faz, possibilitando ouça toda a conversa. Também são capazes de fazer ligações sem pagar a conta, por intermédio dos computadores, confundem as operadoras de telefonia quanto à origem de uma ligação. Assim, quem paga a conta é qualquer outra pessoa que tenha telefone daquela operadora.

Como já mencionado, também podem figurar como sujeito ativo deste tipo de delito, usuários básicos de internet, que fazem uso desta para caluniar, difamar,

dentre outros atos delituosos que violam bens jurídicos tutelados pelo ordenamento jurídico pátrio.

Feitos esses esclarecimentos, impende destacar, a problemática de identificar esse autor frente à sua ausência física, uma vez que na rede mundial de computadores, os indivíduos são livres para criar uma identidade que não corresponde à sua realidade, sendo a sua única identificação limitadas ao endereço eletrônico (IP- internet protocolo) do equipamento utilizado. Isso justifica a morosidade de identificação do sujeito ativo na prática.

2.2.2 Sujeito Passivo

Atua no polo passivo dos crimes cibernéticos qualquer pessoa, independente de uso de dispositivo informático, podendo haver mais de um individuo como conceitua Mirabete:

> Sujeito passivo do crime é o titular do bem lesado ou ameaçado pela conduta criminosa, nada impede que em um delito dois ou mais sujeitos passivos existam desde que tenham sido lesados ou ameaçados a seus bens jurídicos referidos no tipo, são vitimas de crime. (MIRABETE, 2008, p 114)

Portanto, qualquer pessoa, física ou jurídica, pode figurar como sujeito passivo desse tipo de delito. Bastando, para isso, ter seus bens jurídicos tutelados violados.

2.3 Legislação Vigente

Embora muito se fale na inexistência de leis que tipifiquem a condutas delitivas no âmbito da internet, grande parte dos crimes cibernéticos já se encontram devidamente tipificados no nosso ordenamento jurídico. A seguir serão apresentadas as normas penais incriminadoras, vigentes no Brasil, no tocante a esses delitos.

2.3.1 Legislação Penal

O Direito Penal, diante do número crescente de delitos praticados na Internet, vem constantemente buscando meios de coibir e tipificar tais delitos, o que não é surpresa, pois cabe ao Direito disciplinar e regulamentar as condutas da sociedade em geral independente do ambiente, ou seja, se real ou virtual.

Nesse sentido segue um amparado de condutas praticadas na Internet, que já são eficientemente tipificadas na nossa legislação penal.

> Com as atualizações da legislação penal desde 1940, foram criados tipos penais também para crimes praticados contra sistemas de informática ou tipos penais específicos para crimes cometidos por meio de tecnologias de informação, como, por exemplo, em 2008, com a criminalização específica da pornografia infantil, através de cinco tipos penais no Estatuto da Criança e do Adolescente (artigos 241 a 241-E). Outros exemplos podem ser citados como os delitos previstos nos artigos 153,§1º (violação de segredo), 313-A (inserção de dados falsos em sistema de informações), 313-B (modificação ou alteração não autorizada de sistema de informações) e 325, I (violação de sigilo funcional), todos do Código Penal. O ataque aos sistemas de informática da Justiça Eleitoral também foram criminalizados, com penas de até 10 anos de reclusão, através do art. 72 da lei 9.504/1997 (COSTA, 2012)

Código Penal Brasileiro:

> **Violação de Segredo**
> Art. 153, § 1°-A – Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública.
> Pena – detenção de 1 a 4 anos, e multa.
>
> **Violação dos Direitos Autorais**
> Art. 184 - Violar direitos de autor e os que lhe são conexos: (Redação dada pela Lei nº 10.695, de 1º.7.2003)
> Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa. (Redação dada pela Lei nº 10.695, de 1º.7.2003)
> § 1o Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente: (Redação dada pela Lei nº 10.695, de 1º.7.2003)
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 10.695, de 1º.7.2003)
> § 2o Na mesma pena do § 1o incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete

ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente. (Redação dada pela Lei nº 10.695, de 1º.7.2003)
§ 3o Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente: (Redação dada pela Lei nº 10.695, de 1º.7.2003)
Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 10.695, de 1º.7.2003)
§ 4o O disposto nos §§ 1o, 2o e 3o não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei nº 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto. (Incluído pela Lei nº 10.695, de 1º.7.2003)

Inserção de dados falsos em sistema de informação
Art. 313-A – 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.
Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.

Modificação ou alteração não autorizada de sistema de informações
Art. 313 – B – Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente.
Pena – detenção de 3 (três) meses a 2 (dois) anos, e multa.

Violação de sigilo funcional
Art. 325, § 1°, incisos I e II - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação:
Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.
§ 1º Nas mesmas penas deste artigo incorre quem:
I – permite ou facilita, 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;
II – se utiliza, indevidamente, do acesso restrito.

2.3.2 Estatuto da Criança e do Adolescente (Lei 8.069/1990)

Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008)
Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008)
§ 1o Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena. (Redação dada pela Lei nº 11.829, de 2008)
§ 2o Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime: (Redação dada pela Lei nº 11.829, de 2008)

I – no exercício de cargo ou função pública ou a pretexto de exercê-la; (Redação dada pela Lei nº 11.829, de 2008)
II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou (Redação dada pela Lei nº 11.829, de 2008)
III – prevalecendo-se de relações de parentesco consanguíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento. (Incluído pela Lei nº 11.829, de 2008)

Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008)
Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008)
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: (Incluído pela Lei nº 11.829, de 2008)
Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
§ 1o Nas mesmas penas incorre quem: (Incluído pela Lei nº 11.829, de 2008)
I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; (Incluído pela Lei nº 11.829, de 2008)
II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.(Incluído pela Lei nº 11.829, de 2008)
§ 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. (Incluído pela Lei nº 11.829, de 2008)
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: (Incluído pela Lei nº 11.829, de 2008)
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
§ 1o A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
§ 2o Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por: (Incluído pela Lei nº 11.829, de 2008)
I – agente público no exercício de suas funções; (Incluído pela Lei nº 11.829, de 2008)
II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo; (Incluído pela Lei nº 11.829, de 2008)
III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário. (Incluído pela Lei nº 11.829, de 2008)
§ 3o As pessoas referidas no § 2o deste artigo deverão manter sob sigilo o material ilícito referido. (Incluído pela Lei nº 11.829, de 2008)
Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou

> modificação de fotografia, vídeo ou qualquer outra forma de representação visual: (Incluído pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
> Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
> Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: (Incluído pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
> Parágrafo único. Nas mesmas penas incorre quem: (Incluído pela Lei nº 11.829, de 2008)
> I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso; (Incluído pela Lei nº 11.829, de 2008)
> II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita. (Incluído pela Lei nº 11.829, de 2008)
> Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais. (Incluído pela Lei nº 11.829, de 2008).

2.3.3 Crime contra ordem tributária (Lei 8.137/1990)

> Art. 2°, V – Lei n. 8.137/90 – utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública.

2.3.4 Interceptação ilegal de comunicações (Lei 9.296/1996)

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de justiça, sem autorização judicial ou com objetivos não autorizados em lei.
> Pena – reclusão, de dois a quatro anos, e multa.

2.3.5 Legislação Eleitoral (Lei 9.504/1997)

> Art. 72 – Constituem crimes, puníveis com reclusão, de cinco a dez anos:
> I – obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos;
> II – desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral;
> III – causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.

2.3.7 Lei de crimes cibernéticos (Lei 12.737/2012)

Também conhecida como “Lei Carolina Dieckmann”, pois foi sancionada depois que a referida atriz sofreu invasão, subtração e exposição na internet de suas fotografias íntimas. A Lei 12.737/12 alterou o Código Penal para tipificar os crimes exclusivamente cibernéticos, ou seja, aqueles somente praticados com o uso de dispositivos informáticos que dispõem de acesso à internet, quais sejam:

- Invasão de dispositivo informático

> 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.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

- Ataque de denegação de serviço telemático ou de informação.

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
>
> Parágrafo único - Aplicam-se as penas em dobro, se o crime é cometido por ocasião de calamidade pública.

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

Aqui resta configurada a conduta denominada **ataque de denegação de serviço (DOS/DDOS)**, quando o agente do delito lança, por meio de seu computador, vulnerabilidades ou programas maliciosos em outros computadores, fazendo com que estes, sem o conhecimento dos seus usuários, acessem simultaneamente um serviço com o intuito de travá-lo. Tal prática é usada, por exemplo, para tornar sites governamentais indisponíveis.

- Falsificação de documento particular/cartão

> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
> Pena - reclusão, de um a cinco anos, e multa.
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

2.4 Convenção de Budapeste

Por se tratar de delitos de alcance mundial, tendo em vista a sua efetiva coação e punibilidade, os crimes cibernéticos carecem de uma atuação combinada entre os países.

Nesse sentido, impende destacar a Convenção sobre Cibercrime, elaborada em 2001, em Budapeste, na Hungria, pelo Conselho da Europa, também conhecida como Convenção de Budapeste. Na ocasião, foi consolidado o acordo entre os 43 Países, formado por países da Europa, Estados Unidos, Canadá e Japão. Tem como objetivo precípuo introduzir nos ordenamentos jurídicos, dos países signatários e aderentes, tipificações penais e normas processuais que visam uma maior celeridade e eficiência na persecução penal, bem como na cooperação internacional do combate aos crimes cibernéticos.

Essa cooperação resta cristalina no artigo 23, da referida Convenção:

> Princípios gerais relativos à cooperação internacional
> As Partes cooperarão entre si, em conformidade com as disposições do presente capítulo, em aplicação dos instrumentos internacionais pertinentes sobre a cooperação internacional em matéria penal, de acordos celebrados com base nas legislações uniformes ou recíprocas, e do seu direito nacional, na medida mais ampla possível, para efeitos de investigações ou

> de procedimentos relativos a infrações penais relacionadas com sistemas e dados informáticos, ou para recolher provas sob a forma eletrônica de uma infração penal.

A Convenção dispõe sobre regras penais (tipificação de delitos informáticos), processuais e de cooperação internacional. De início aborda conceitos e terminologias ligados aos delitos cometidos na rede mundial de computadores. Em seguida, trata os casos de infrações contra a confidencialidade, integridade e disponibilidade de sistema de dados e informáticos assim discriminados: acesso e interceptação ilegítimos; interferência em dados e sistemas e uso abusivo de dispositivos. Posteriormente, trata dos crimes cibernéticos abertos, ou seja, crimes comuns já tipificados no nosso ordenamento jurídico e que também podem ser cometidos com o uso de dispositivos computacionais. Já no terceiro momento prioriza as ofensas relacionadas à pornografia infantil. Por fim, trata de disposições processuais para fins de investigação e procedimentos penais.

Ainda sobre a referida Convenção, impõe ressaltar a criação do Protocolo Adicional à Convenção de Budapeste, em março de 2006, para inserir a esta, a criminalização dos atos de racismo e xenofobia praticados mediante sistemas informáticos.

3 DA INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

Antes mesmo de se falar em investigação dos crimes cibernéticos, é importante lembrar a delimitação dada à ferramenta utilizada para o cometimento desses delitos, qual seja, a rede mundial de computadores.

Nas palavras de Wendt e Jorge (2013), existem duas fases nesse processo investigativo, são elas:

- Fase técnica: onde são analisadas e executadas tarefas com o objetivo único de localizar o computador que foi utilizado para ação criminosa. Nessa fase verifica-se a narração da vítima sobre o fato ocorrido; é feita a coleta de provas e orientação ao sujeito passivo do delito, no tocante a conservação e proteção destas no ambiente virtual; formaliza-se o registro ou boletim de ocorrência do fato criminoso e instauração do feito; inicia-se a investigação sobre os dados disponíveis na internet dos prováveis criminosos; elaboração de relatório ou certidão do que foi apurado; é feita a representação perante o poder Judiciário para expedição de autorização judicial para quebra de dados, conexão e acesso, sendo possível solicitar dados cadastrais dos provedores de conteúdo e; por fim, analisa-se às informações obtidas destes.
- Fase de campo: nessa fase há o deslocamento de agentes policiais para realização de diligências com o intuito de promover o reconhecimento operacional no local. Ressalta-se que essa diligência deverá ser discreta, em virtude de uma eventual necessidade de solicitar uma medida processual penal cautelar, por exemplo, um mandado de busca e apreensão.

3.1 Aspectos procedimentais

No tocante aos procedimentos investigativos dos crimes cibernéticos, há de se considerar o caráter global da internet. Nesse sentido, os delitos dessa natureza

podem ser praticados de qualquer lugar do mundo, o que dificulta sobremaneira a sua inquirição.

Diante dessa característica, os delitos praticados nessa esfera, demandam uma investigação mais aparelhada, com profissionais especializados, com conhecimentos técnicos de informática, para que possam reunir as evidências necessárias para se chegar à autoria e materialidade do delito.

A seguir, serão feitas algumas considerações importantes e indispensáveis para obtenção de êxito na investigação desses delitos.

3.1.1 Evidências eletrônicas

Como nos crimes comuns, os delitos praticados na internet deixam “rastro”, não obstante, essas evidências são intricadas e de difícil leitura, demandando conhecimentos técnicos especializados, tendo em vista a diversidade de recursos, que servem de meio à prática desses atos delituosos, disponíveis nessa rede.

Quando se buscam os vestígios dos crimes cibernéticos, há de se levar em consideração as suas características, são elas:

> a) volatilidade, ou seja, podem ser apagados, alterados ou perdidos facilmente;
> b) possuem formatos complexos e variados (arquivos, fotos, dados digitalizados etc.);
> c) aparecem misturados aos dados legítimos, e;
> d) requerem uma análise apurada dos técnicos e peritos que participam da persecução penal. (ELEUTÉRIO, 2013, p. 51)

No tocante a esses vestígios, impende salientar, a existência dos registros de login (logs), ferramenta essencial à investigação dos crimes que são objeto de estudo deste trabalho, responsáveis por armazenar dados de acesso do usuário toda vez que este realiza alguma ação na internet.

Nesses logs são encontrados registros referentes a: hora de início, duração da sessão, e o endereço IP da máquina do usuário atribuído à operação.

Dessa forma, resta evidente que, quase toda atividade na rede é de alguma maneira registrada, seja em relação ao conteúdo dos dados acessados, ou nas informações de quando, onde e como se acessou estes conteúdos. Essa é uma informação importante para o perito, pois lhe dá subsídios para indicar quais dados solicitar ao provedor de acesso à internet ou ao provedor de conteúdo.

Ainda sobre as evidências, cumpre ressaltar que, a simples existência de um documento impresso da Internet, por si só não servirá como prova. Estes devem vir amparados por outros instrumentos, os quais lhes conferem presunção de veracidade.

3.1.2 Interceptação telemática

Nos casos em que se deseje obter todo o conteúdo e o trâmite das comunicações telemáticas do investigado, pode-se recorrer a sua interceptação, desde que preenchidos os requisitos previstos na Lei nº 9.296/1996. Ou seja, para lançar mão desse instrumento, são necessários indícios razoáveis da autoria ou da participação na infração penal; ausência de outros meios comprobatórios da conduta delituosa; e, por fim, só é admissível nos crimes punidos com reclusão.

Além disso, é preciso que o investigador tenha a informação de todos os dispositivos computacionais que o criminoso dispõe para acessar a internet, seja o computador da empresa ou o de sua residência, seu smartphone, ou qualquer outro meio, para que se possa direcionar a solicitação da interceptação telemática aos seus respectivos provedores de acesso.

No caso de interceptação das contas de e-mail, todas as mensagens enviadas e recebidas da conta do investigado são encaminhadas para uma conta fornecida pelo investigador.

3.2 Procedimentos investigativos especializados

Tendo em vista as diversas formas de cometimento dos crimes cibernéticos, o ponto de partida do trabalho do investigador é a descoberta da ferramenta utilizada pelos criminosos para a execução do ato delituoso.

Nesse diapasão, serão abordados, neste tópico, os procedimentos investigativos dos principais meios de comunicação, da rede mundial de computadores, que são ambientes favoráveis à prática de delitos cibernéticos.

Primeiramente, será abordado como se dá esta investigação em sites, pois, esta servirá de base para as demais.

3.2.1 Sites

Devido ao número crescente de conteúdo ilícito nas páginas da internet, a investigação de sites tem sido uma tarefa corriqueira entre os profissionais de combate à criminalidade cibernética. Nesse sentido, o exame tem como foco verificar o conteúdo e encontrar o responsável por sua publicação.

- Verificação de conteúdo

Para guardar o conteúdo do site investigado, há que se fazer a impressão das páginas que contém os indícios de crime e o download do conteúdo de interesse da investigação, antes que essas páginas sejam modificadas ou apagadas. Esse é um cuidado fundamental que o investigador deve ter para não perder as provas necessárias que servirão de apoio para a localização e condenação dos autores dos delitos.

Outro fator importante é a manutenção da originalidade do conteúdo do site investigado para evitar possíveis questionamentos, na esfera judicial, sobre a integridade destas informações, em razão da possibilidade de terem sido alteradas no curso da investigação.

Nesse sentido, Wendt (2013) ensina:

> [...] o uso conjuntos dos programas HTTrack Website Copier e do MD5summer. O primeiro software é uma ferramenta extremamente útil e fácil de ser utilizada, atentando-se para que a cópia seja gerada incluindo-se os links vinculados e que interessam à investigação, ou seja, a profundidade e os limites na cópia, já que a cópia da simples mascara do site pode não trazer informações importantes à investigação policial. O próprio software, quando da realização da cópia do site, gera um log da gravação feita em um arquivo “índex”, possibilitando-se gravar todo o conteúdo em um CD para ser anexado ao inquérito policial e/ou processo judicial. No caso de sites com acesso por login e senha, o HTTrack não pode ser utilizado.

Ainda sobre esse assunto, o autor supracitado destaca a veracidade da certidão elaborada pela polícia civil:

> [...] O agente policial, na condição de “Escrivão”, tem fé pública sobre seus atos e pode, acessando uma página na internet, promover a sua impressão e certificar data e existência. Assim, também pode e deve usar todos os meios disponíveis (WENDT, 2013).

Nesse sentido, nada impede que o escrivão de polícia, caso não possua conhecimentos técnicos para fazer uso do programa HTTrack, faça a cópia dos conteúdos do site com a tecla “print screen” e cole o seu texto no conteúdo da sua certidão. Esse é um procedimento, também deve ser feito nos casos de sites que solicitam login e senha, pois, como já mencionado, o referido programa não consegue realizar a cópia.

Além disso, é importante frisar que o investigador deve está atento a todo conteúdo publicado no site investigado, tendo em vista a possibilidade de existir informações importantes, como o email e números de telefone dos responsáveis pelo site, ou até mesmo conteúdo de conversas que podem facilitar o trabalho policial.

- Identificação do responsável pelo conteúdo

É importante esclarecer que, para a compreensão do tema aqui abordado, será necessário retomarmos a assuntos de capítulos anteriores, a exemplo do IP (*Protocol Internet*) e DNS (*Domain Name System*).

Assim, para o desenvolvimento da investigação nos sites, o passo inicial e mais importante é descobrir onde está registrado o seu domínio, ou seja, o nome ou endereço de acesso dado ao site.

Convém esclarecer que todo site para ser publicado na “grande rede”, precisa ter o seu domínio registrado na mesma. Cada país dispõe de um órgão responsável para gerenciar esses registros, sendo que, no Brasil, o órgão responsável por esse controle é o Comitê Gestor da Internet, por meio do Registro.br.

Sobre isso, Wend e Jorge (2013) assevera:

> Registrar um domínio na internet é bastante fácil e nada burocrático, em sítios[4] internacionais basta, em regra, o cadastro de e-mail (login e senha) e o pagamento do valor exigido que pode variar. No Brasil, há uma exigência maior, qual seja a de acrescentar um CPF ou CNPJ (Cadastro de Pessoa Física ou Cadastro Nacional de Pessoa Jurídica). Atualmente, o valor anual de um domínio com terminação ".br" é R$ 30,00, mas anteriormente esse valor era maior. Em ambos os casos, sites brasileiros ou fora do Brasil, não há necessidade de envio de documentos, circunstância que aumenta a possibilidade de inserção de informações falsas com a finalidade de praticar os mais variados crimes.

Ainda sobre esse registro, para fazê-lo, a única exigência é que ele esteja disponível, ou seja, não podem existir dois nomes de domínio iguais. Impende destacar a existência de regras para a criação desses domínios, uma delas é que cada país possuir sua terminação, no caso do Brasil o ".br". Para saber as terminações de outros países, basta acessar o site da IANA (Internet Assigned Numbers Authority) no endereço http://www.iana.org.

No site supracitado, também é possível encontrar o órgão de registro de domínios. Dessa forma, em uma investigação de um site com terminação do país ".pt", para identificar a sua origem, basta acessar o endereço http://www.iana.org/domains/root/db e fazer a pesquisa. A figura abaixo ilustra essa pesquisa:

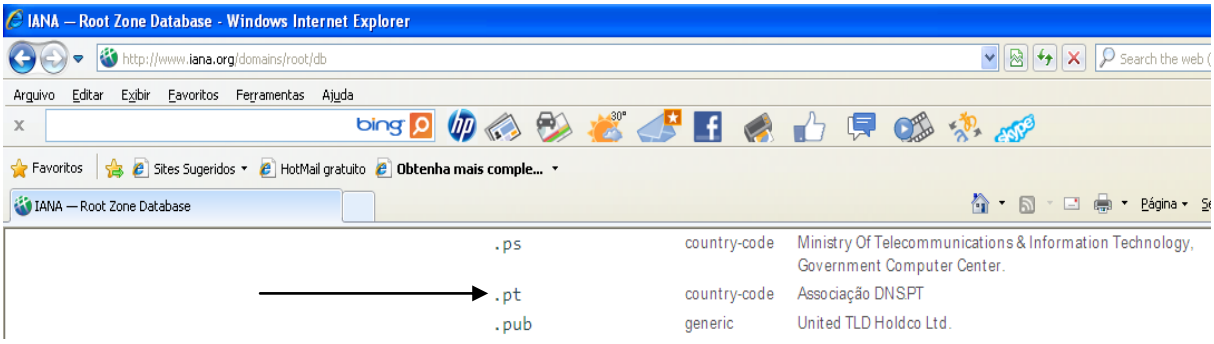

Figura 1. Pesquisa por país pela terminação

Para descobrir o site responsável pelo registro e controle de domínios desse país, dê um clique sobre a terminação ".pt" que será aberta uma página com os dados de cadastro do responsável do país, conforme figura abaixo:

[4] Tradução da palavra sites em português

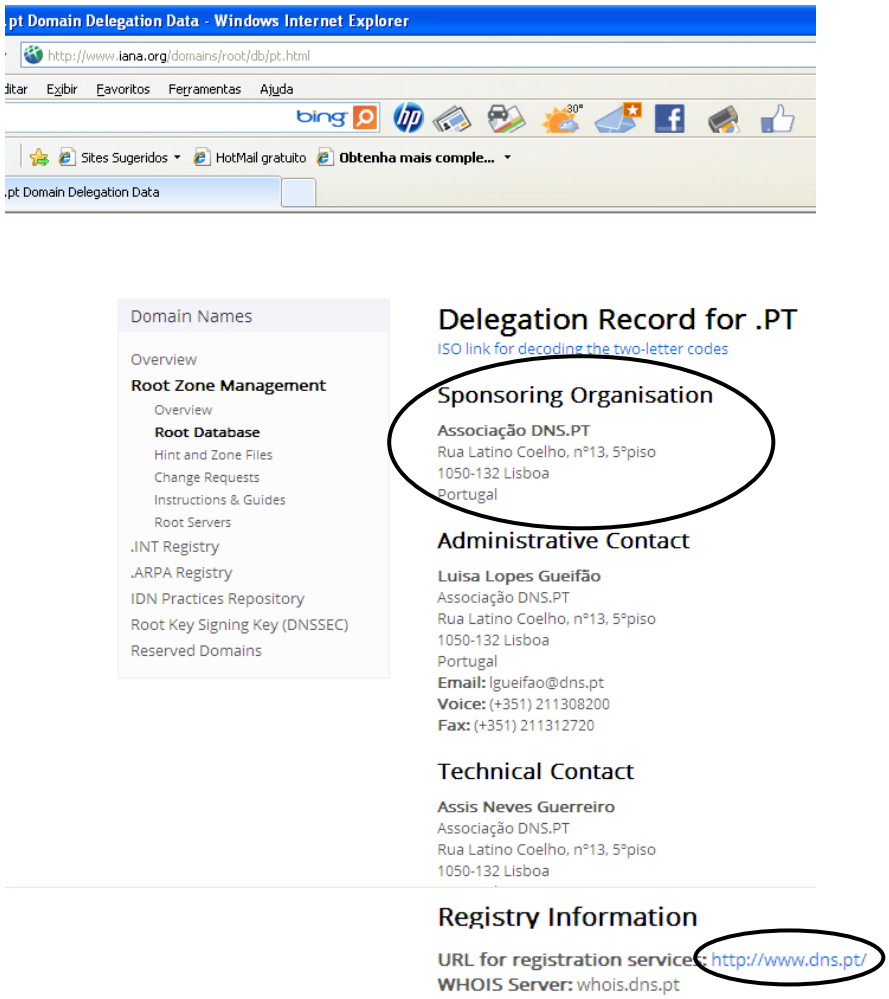

Figura 2. Responsável pelo registro do domínio “.pt”.

Descoberto o órgão responsável pelo registro do domínio, o próximo passo é a obtenção dos dados cadastrais do responsável pelo site. Este acesso também é feito através dos sites de registros de domínios. No caso do Brasil, basta acessar o endereço www.registro.br, em tecnologia/ferramentas/serviço de diretório whois e digitar o endereço do site que deseja obter os dados de cadastro. Com isso, é possível obter dados do investigado, seja para informações dos provedores, de conexão ou conteúdo e os servidores DNS vinculados ao domínio. Veja, nas figuras abaixo, uma pesquisa feita sobre o site FANESE com domínio em www.registro.br.

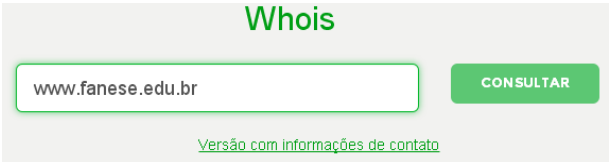

Figura 3. Pesquisa dos dados do responsável pelo site da FANESE

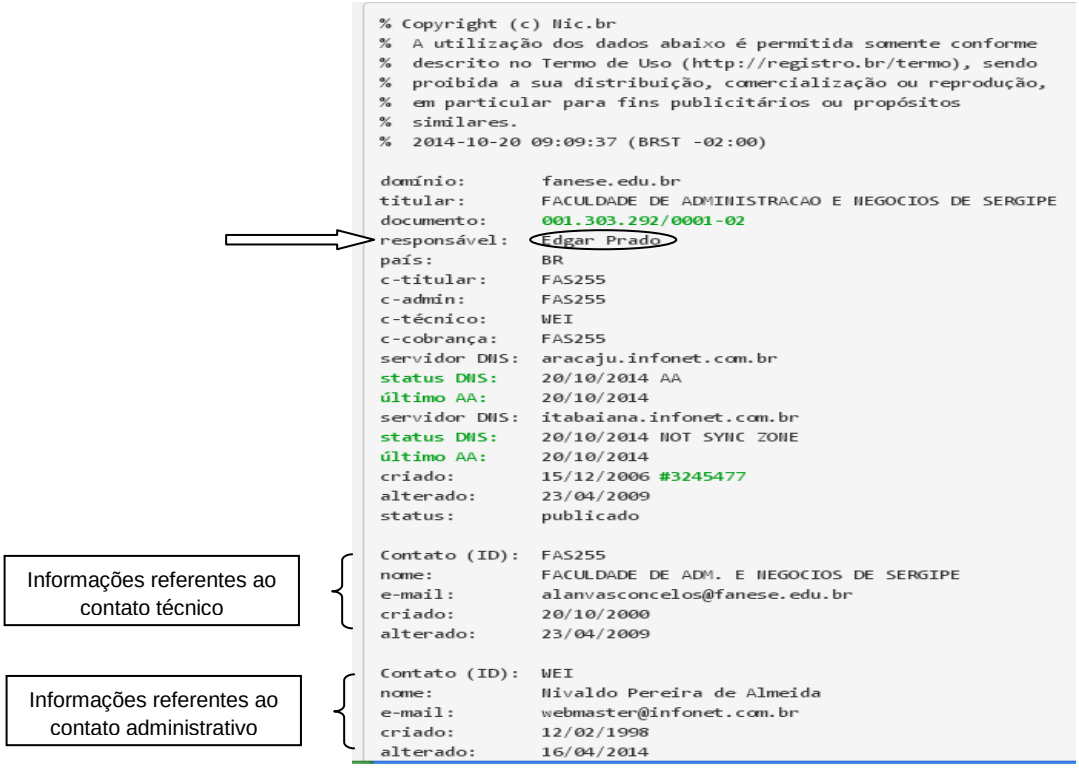

Figura 4. Dados do responsável pelo site

A referida ferramenta também oferece outras opções de pesquisa, dentre as mais usadas destacam-se: por domínio, por IP e pelo cadastro de pessoas físicas ou jurídicas. Da pesquisa extraem-se: os dados do proprietário do domínio, o contato administrativo, o contato técnico, os servidores DNS, dentre outros.

O ultimo passo da investigação é descobrir o responsável pela hospedagem do site, ou seja, o seu provedor de informação. Como já mencionado, no capítulo 1, o site fica hospedado em um servidor (computador) da empresa que disponibiliza este tipo de serviço. Para se chegar ao responsável por esse serviço, primeiramente será feito a busca do endereço IP deste servidor. Essa pesquisa é feita com o comando PING, do prompt de comando. Para isso, basta acessar o prompt de comando do windows (Iniciar – Executar – digite cmd – Enter). Na tela que se abre, digite: PING – espaço – nome de domínio – enter, como na imagem a seguir.

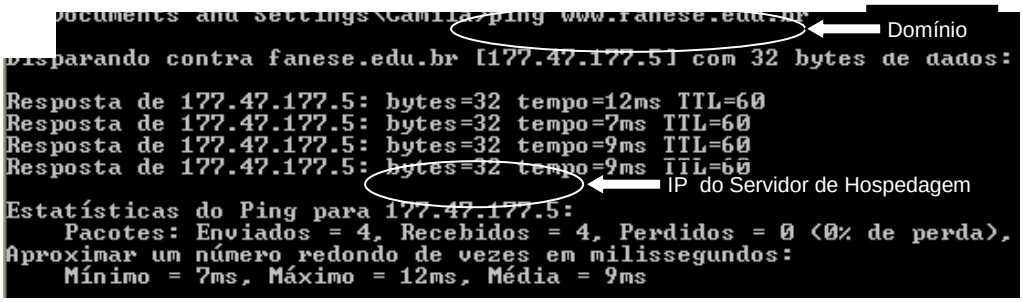

Figura 5. Prompt de Comando para descobrir IP do servidor do site.

Da leitura feita da imagem acima se depreende: o nome do domínio “fanese.edu.br” está hospedado no servidor com endereço IP 177.47.177.5. Com essa informação é possível, através da ferramenta whois do Registro.br, obter os dados do provedor de hospedagem.

De posse dessas informações (identificação do proprietário do site; dos servidores DNS e do responsável por sua hospedagem), pode-se chegar à identidade do investigado, solicitando aos provedores os registros de acesso, bem como outros dados necessários para a identificação do agente criminoso. Com esses dados será possível fazer uma busca eletrônica em fontes abertas, como no site do Google.

3.2.2 Fraudes eletrônicas

Nas palavras de Gil (1999), fraude é todo ato intencional de omissão ou manipulação de transações, adulteração de documentos, registros e demonstrações contábeis. Em um ambiente informatizado, tal ato é resultado de procedimentos e informações de pessoa jurídica ou física, que tem como finalidade alcançar benefício ou satisfação psicológica, financeira e material apropriado, indevidamente de outra pessoa física ou jurídica, através de software e bancos de dados.

Nesse tipo de fraude, os criminosos capturam os dados das vítimas, a exemplo da clonagem de cartões de crédito, nos casos de vítimas de sites de compras.

Em virtude desse tipo de delito ser ter como meio para o seu cometimento sites, a exemplo e-commerce e internet banking, a sua investigação se dá no mesmo modo do tópico anterior.

3.2.3 Redes sociais

Diante da ocorrência de crimes cibernéticos, no âmbito da rede social da internet, o responsável pela investigação deverá solicitar, à pessoa jurídica responsável pelo site, em regra, com a necessidade de ordem judicial, os logs de

acesso[5] do autor do delito, bem como os referentes ao perfil dos usuários e grupos envolvidos, e, sendo necessário, à interceptação telemática do fluxo de dados.

Ao serem resgatados, os LOGs geralmente apontam para um endereço IP que o usuário utilizou para acessar a rede na data e horário do fato delituoso.

De posso dessas informações, em relação à busca dos responsáveis pelas ações criminosas, seguem-se os procedimentos do item 3.1.1 deste capítulo.

3.2.4 E-mails

A tentativa de identificar o responsável pelo envio e de uma mensagem eletrônica de conteúdo criminoso, tem sido uma prática comum no âmbito dos profissionais de investigação dos crimes cibernéticos, haja vista o número crescente de denúncias de pessoas vítimas de mensagens de emails com injúrias, difamações, calúnias, pornografia infantil, programas maliciosos, etc.

Convém esclarecer que, para acessar um serviço de e-mail, o usuário deverá está conectado à Internet por um Provedor de Serviços de Internet (PSI). Nesse sentido, quando da investigação, primeiramente busca-se informações, sobre o usuário da mensagem de correio eletrônico, no provedor de e-mail, e em seguida, junto ao PSI.

O sucesso dessa investigação está intimamente ligado à preservação de todos os dados contidos no e-mail, ou seja, o conteúdo da mensagem e o seu cabeçalho completo (dados do destinatário e remetente da correspondência). Fazer essa cópia da mensagem original recebida é indispensável, nela pode conter algumas informações, como o endereço de email, o endereço IP do remetente e a data/hora, incluindo informações de fuso horário (GMT) em que a mensagem foi enviada.

Nesse sentido, Wendt e Jorge (2013) ensina:

[5] Histórico dos usuários da internet denominado “registros de eventos”, guardado pelos seus provedores de acesso e de serviços.

> [...] Para a completa apuração da origem de uma mensagem de e-mail é necessário que obtenhamos acesso ao chamado “cabeçalho completo” ou “código fonte” dele.
> Assim, a origem do e-mail pode ser determinada pela parte de um cabeçalho completo chamado de *“Received”.* Esse item normalmente não é exibido, mas é facilmente revelado pela opção de “Exibir todos os cabeçalhos”, “Exibir código fonte”, “Cabeçalho completo”, ou algo semelhante, presente em muitos webmails e em todos os clientes de e-mail, seguindo o protocolo RFC 822.

Veja a seguir, destacadas em negrito, a exibição de dados relevantes para investigação, retirados de cabeçalho completo de uma mensagem de e-mail:

From "FANESE" Fri Oct 17 18:46:32 2014
X-Apparently-To: souzananda@yahoo.com.br; Fri, 17 Oct 2014 18:46:34 +0000
Return-Path: <do-not-reply@fanese.edu.br>
Received-SPF: none (domain of fanese.edu.br does not designate permitted sender hosts)

X-Originating-IP: [209.85.216.176]
Authentication-Results:mta1545.mail.gq1.yahoo.comfrom=fanese.edu.br; domainkeys=neutral (no sig); from=fanese.edu.br; dkim=neutral (no sig)
Received: from 127.0.0.1 (EHLO mail-qc0-f176.google.com) (209.85.216.176)
by mta1545.mail.gq1.yahoo.com with SMTPS; Fri, 17 Oct 2014 18:46:33 +0000
Received: by mail-qc0-f176.google.com with SMTP id r5so1055863qcx.7
for <souzananda@yahoo.com.br>; Fri, 17 Oct 2014 11:46:33 -0700 (PDT)

X-Received: by 10.224.7.129 with SMTP id d1mr15084695qad.70.1413571593012;
Fri, 17 Oct 2014 11:46:33 -0700 (PDT)
Return-Path: <do-not-reply@fanese.edu.br>
Received: from AQUILES ([177.159.239.44])
by mx.google.com with ESMTPSA id e52sm1491282qge.42.2014.10.17.11.46.31
for <souzananda@yahoo.com.br>
(version=TLSv1 cipher=ECDHE-RSA-AES128-SHA bits=128/128);
Fri, 17 Oct 2014 11:46:32 -0700 (PDT)
Message-ID: <54416408.371f8c0a.0465.ffffbef4@mx.google.com>
Date: Fri, 17 Oct 2014 11:46:32 -0700 (PDT)
X-Google-Original-Date: 17 Oct 2014 15:46:16 -0300
MIME-Version: 1.0
From: "FANESE" <do-not-reply@fanese.edu.br>
To: souzananda@yahoo.com.br
Reply-To: "FANESE" <do-not-reply@fanese.edu.br>
Subject: =?utf-8?B?QXZpc28gZGUgZGV2b2x1w6fDo28=?=

Figura 6. Cabeçalho completo de uma mensagem de e-mail

A leitura do cabeçalho em regra ocorre de baixo para cima, tendo destaque para as informações descritas a seguir:

- Return Path - contém o endereço de e-mail do servidor que deu origem ao e-mail. Não é o endereço de e-mail do remetente, mas o endereço de e-mail do programa de computador que foi usado para transmiti-lo.
- Received (Recebido) - " from" é o endereço de e-mail da pessoa que lhe enviou o e-mail. Em alguns casos identifica o IP do computador ou dispositivo informático de onde partiu a mensagem. É comum um cabeçalho possuir várias linhas de “received”. Isso acontece para

especificar por quantas estações (ou servidores) a mensagem passou antes de chegar ao destinatário. O parágrafo que interessa é sempre o último “received”; é ele quem indica a primeira máquina que originou a mensagem, isto é, o computador do remetente.

- Date – é a data e a hora que um e-mail foi enviado.

Pode-se perceber que a forma como os dados estão dispostos neste tipo de cabeçalho é um tanto embaraçosa, contudo, para facilitar a leitura dessas informações, aconselha-se o uso da ferramenta Trace_email, disponível no endereço eletrônico http://www.ip-adress.com/trace_email/. Ao acessá-la, basta copiar o cabeçalho expandido e colar na caixa de texto da referida ferramenta, em seguida clicar no botão trace email sender.

Veja, na imagem abaixo, o resultado do uso dessa ferramenta:

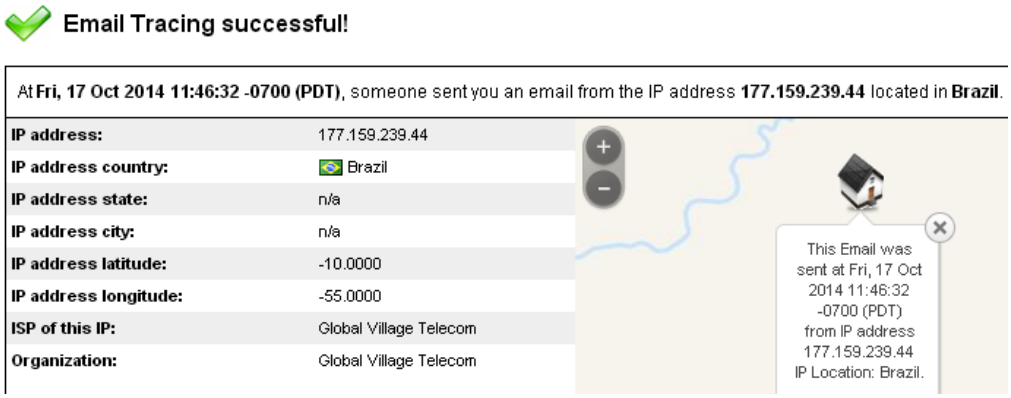

Figura 7. Informações retiradas do cabeçalho completo de e-mail com a ferramenta trace_email

De posse dessas informações, o investigador pode solicitar ao provedor, através de ordem judicial, os dados cadastrais do usuário a quem foi disponibilizado o número IP, na data e horário obtidos.

Essa solicitação é amparada pela Lei nº 12965/2014 (Marco Civil da Internet), nos seus artigos 15 e 22, que assim dispõem:

> **Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.**
> § 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
> **§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de**

> **internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.**
> **§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.**
> **[...]**
> **Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.**
> Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
> I - fundados indícios da ocorrência do ilícito;
> II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
> III - período ao qual se referem os registros.

O art. 22, da lei supracitada, também abrange os casos em que não se consiga acessar o cabeçalho completo de um e-mail. Para esses casos, a solicitação judicial deve ser direcionada ao provedor do serviço de correio eletrônico (ex: Yahoo, Bol, etc), requisitando deste, informações cadastrais e registros de eventos (logs de acesso) da conta de email investigada.

Nesses registros, estarão disponíveis os endereços IPs que tiveram acesso à conta, com data e hora. Para descobrir qual o provedor de internet que forneceu esses IPs, basta acessar, nos endereços eletrônicos https://registro.br/cgi-bin/whois/ ou http://whois.domaintools.com/

Logo, uma vez levantados esses dados, é possível ter uma noção de qual o caminho percorrido pela mensagem virtual e, com isso, localizar o individuo que fez uso de uma conta de email, para prática de um ato delituoso.

4 DESAFIOS NOS PROCEDIMENTOS INVESTIGATIVOS

Durante a investigação criminal relacionada aos crimes ocorridos no âmbito da internet, muitos são os desafios encontrados pelo investigador na busca por evidências que comprovem a autoria e a materialidade do delito.

A seguir serão abordados os principais entraves, acerca das investigações dos crimes cibernéticos, considerando as peculiaridades enfrentadas nestes tipos de delitos.

4.1 Legislação vigente e a atuação do Estado

Embora, a ocorrência de crimes cibernéticos tenha crescido consideravelmente, tendo como principal fator o avanço da tecnologia e o advento da rede mundial de computadores, este acontecimento não tem sido acompanhado por uma atuação diligente e eficaz do Estado Brasileiro.

Essa situação encontra respaldo na crença de que é necessária a criação de uma legislação específica, que tipifique as condutas delitivas e dê subsídios operacionais aos órgãos do Poder Público quando no âmbito da Internet.

Alguns operadores do direito adotam essa ideia com respaldo na proibição ao uso da analogia, no direito penal, para suprir eventuais lacunas da lei quando esta atuar em desfavor do réu.

Há também quem defenda essa ideia com base no principio da legalidade, previsto na Carta Magna, em seu art. 5º, XXXIX, que assevera “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”.

Diante dessa discussão, vale lembrar, a existência de leis nacionais e internacionais suficientes para aplicação às diversas condutas criminosas no âmbito da internet. Além disso, pode-se recorrer aos princípios gerais e fundamentais dos institutos normativos vigentes nas diversas áreas do Direito, bastando enquadrar as condutas em um ou mais instrumento normativo.

É esse o pensamento de Pinheiro:

> Não devemos achar, portanto que o Direito Digital é totalmente novo. Ao contrário, tem sua guarida na maioria dos princípios do Direito atual, além de aproveitar a maior parte da legislação em vigor. A mudança está na postura de quem a interpreta e faz sua aplicação. É errado, portanto, pensar que a tecnologia cria um grande buraco negro, no qual a sociedade fica à margem do Direito, uma vez que as leis que estão em vigor são aplicáveis à matéria, desde que com sua devida interpretação. O Direito tem de partir do pressuposto de que já vivemos uma sociedade globalizada. (PINHEIRO, 2010 p. 77).

Em matéria penal, GRECO esclarece:

> [...] focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da Internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, como, por exemplo, o homicídio. O crime, no caso, é provocar o resultado morte, qualquer que tenha sido o meio ou a ação que a causou. Na Europa conta-se que já ocorreu um homicídio por meio da informática: um *hacker* invadiu os computadores da UTI de um hospital e, manipulando os dados, provocou a morte do paciente (GRECO, 2000)

Nessa linha de raciocínio, Sandro Costa assevera:

> [...] o Código Penal ainda é adequado para muitos delitos praticados por meio do computador. A maior parte dos tipos penais (conduta criminosa prevista na norma) é de ação livre, não exigindo uma forma específica de execução para sua caracterização. Dessa forma, não há diferença, em termos de definição de crime, de um homicídio praticado com uma faca ou por meio de sistemas de informática (COSTA, 2012).

Nesse diapasão, podem-se destacar os crimes de pedofilia, estelionato, homicídio, racismo, falsa identidade, crimes contra honra, dentre outros, que são crimes já tipificados no nosso ordenamento jurídico, que quando cometidos na internet não deixam de ser enquadrados como tal, ou seja, a incriminação independe do meio utilizado para praticá-lo.

Greco (2000) completa:

> Como se vê, as ditas situações modernas não são tão modernas assim. Podem as circunstâncias torná-las mais importantes, mais danosas e, até,

> mais interessantes, mas não cabe ao Direito Penal entendê-las como um fenômeno diferente do comportamento irregular na humanidade.

Logo, o obstáculo de punibilidade desses delitos está intimamente ligado à atuação precária do Estado, tendo em vista a ineficiência técnica e insuficiência de recursos tecnológicos dos entes públicos, e não da inexistência de normas penais.

4.2 Profissionais Capacitados

Tendo em vista a diversidade de recursos tecnológicos disponíveis na rede mundial de computadores, a investigação dos crimes cibernéticos requer profissionais que além de embasamento jurídico, possuam conhecimentos técnicos de informática.

Dentro desse contexto, pode-se afirmar que, o sucesso da persecução penal desses delitos possui relação intrínseca com o grau de capacitação dos profissionais que atuam nesta área.

De outro lado, a falta de habilitação dos policiais, representantes do Ministério Público e demais atores dessa investigação, comprometem a sua persecução penal, na medida em que pode impedir a punição dos criminosos virtuais e, por consequência, causar impunidade.

É necessário, portanto, um esforço perante os entes judiciários e policiais em aprimorarem seus conhecimentos na área de informática, principalmente nos termos relevantes à internet, para que possam se adequar as exigências sociais da investigação eficaz dos crimes cibernéticos.

4.3 Prova

No tocante as evidências probatórias, o ponto crítico diz respeito à necessidade de requisição de ordem judicial para obtenção dos dados de conexão do usuário da internet, sendo este uma afronta ao princípio da celeridade exigido, nas investigações dos crimes cibernéticos.

Sobre esse assunto Wend e Jorge (2013) dispõem:

> O requisito de ordem judicial para obtenção de toda e qualquer informação relativa ao crime cibernético é outra questão que atravanca a investigação e representa uma das facetas do excesso de burocracia, que apenas prejudica e/ou retarda o esclarecimento desse delito.

Os renomados autores lembram ainda, que muitos provedores de conexão ou de acesso a conteúdo não fazem exigência quanto à ordem emanada do Poder Judiciário para o fornecimento dos dados cadastrais de seus clientes, sendo necessária apenas a representação firmada pelo Delegado de Polícia.

4.4 Organização Criminosa

Tem sido comum na investigação dos crimes em comento, a existência de criminosos, espalhados em diversas localidades, que realizam ações criminosas em parceria e de me maneira organizada. Isso acontece devido ao caráter transnacional da internet, onde criminosos espalhados em todo do mundo, se reúnem, sem a necessidade de se conhecerem ou até mesmo estarem presentes fisicamente no mesmo lugar, para prática de tais atos delituosos.

Essa interação do mundo criminoso com o uso de recursos tecnológicos por vezes dificulta a investigação desses delitos, não pelo desconhecimento dos processos investigativos, mas pela infinidade de evidências que precisam ser apuradas num crime desse porte.

4.5 Cooperação Internacional

O princípio da cooperação jurídica internacional é considerado um dos mais importantes do direito internacional público, tendo em vista, a necessidade de cooperação entre os Estados para combater os crimes de caráter transnacionais.

Nesse diapasão, se enquadram os crimes cometidos na rede mundial de computadores, onde há a necessidade de cooperação internacional entre polícia e judiciário de diferentes países para o seu enfrentamento.

Assim, resta evidente, a necessidade de adesão do Brasil à Convenção de Budapeste, já mencionada no tópico 2.6 deste trabalho, pois o referido tratado traz como princípio norteador da cooperação internacional, assegurando que os Estados participantes cooperarão entre si, instrumentos e medidas pertinentes à nível internacional, de meios destinados a investigação ou recolhimento de provas relacionados a práticas de ilícitos informáticos.

CONCLUSÃO

O presente trabalho monográfico se propôs a mostrar as dificuldades encontradas pelos órgãos da persecução penal frente aos crimes cibernéticos, precipuamente no que diz respeito aos procedimentos investigativos direcionados a esclarecer a autoria e comprovar a materialidade desses delitos com a maior eficácia possível.

Cumpre salientar, que o sucesso da persecução penal desses crimes independe da existência de uma legislação específica, uma vez que estes já se encontram devidamente tipificados no ordenamento jurídico pátrio, sendo diferente apenas o meio, instrumento para a prática do mesmo.

Nesse diapasão, destaca-se a importância da atuação dos profissionais desta área, sendo devido a eles o papel de investigar e buscar, através de meios e instrumentos, respostas para solucionar os delitos praticados no âmbito da Internet, tendo em vista que a adequada investigação e consequente punição dos autores são consideradas as principais inibidoras da sua incidência.

Assim, fica evidente, a necessidade de capacitação e especialização de todos aqueles que se defrontam, na sua atuação profissional, com crimes dessa natureza.

Outro aspecto relevante é a atenção especial dada na busca e armazenamento das evidências deixadas pelos criminosos desses delitos, tendo em vista o caráter efêmero das provas no mundo virtual. Portanto, a coleta e o modo como serão guardados os dados, as informações ou equipamentos em si, devem seguir rotinas e procedimentos próprios que evitem perecimento das provas.

Ainda sobre a aquisição de provas, se faz necessária a criação de uma norma com a capacidade de diminuir a burocracia na obtenção dos dados de conexão dos usuários da internet quando o foco for à identificação dos autores dos crimes cibernéticos.

Demais disso, cumpre salientar, quanto ao cenário internacional, à necessidade de uma política internacional, que estabeleça a cooperação entre os países, no sentido de propiciar maior facilidade e eficiência na investigação e

punição dos delitos cibernéticos, haja vista o seu caráter supranacional. Nesse sentido, resta cristalino a importância do Brasil se tonar um país signatário da Convenção de Budapeste que dentre outros assuntos relacionados aos crimes cibernéticos, trata veementemente essa questão.

Por fim, dentre os aspectos aqui apontados, resta evidente, a importância do profissional que atua contra a criminalidade cibernética, devendo este ser devidamente habilitado e dispor de recursos de alta tecnologia para o enfretamento efetivo dos crimes cometidos no âmbito da rede mundial de computadores.

REFERÊNCIAS

ANDRADE, Wesley Almeida. **Crimes na Internet: uma realidade na sociedade da informação**. São Paulo, 2003. Disponível em: http://intertemas.unitoledo.br/revista/ index.php/ Juridica/article/view/486/480 Acesso em: 28 de setembro de 2014.

ANTONIO, Marcelo; COSTA, Sampaio Lemos. **Computação Forense.** São Paulo: Millennium, 2003.

ARAS, Vladimir. **Uma análise do substitutivo ao PL sobre crimes de informática.** Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/4225-4219-1-PB.htm>. Acesso em: 30 de setembro de 2014.

AZEVEDO, Robson Barbosa de. **O combate à criminalidade cibernética no Brasil: parâmetros objetivos de tipicidade**. Revista Jurídica Consulex, ano XV, nº 343, 1º de maio de 2011.

BOLSONI, Evandro Paulo. **Sociabilidade em Redes Digitais Sociais.** Maringá-PR: Linkania, 2014.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.

Cartilha de Segurança para Internet - CERT.br. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em 14/09/2014)

COSTA, Sandro Luiz. **Crimes Cibernéticos.** Disponível em: <http://www.infonet.com.br/sandrocosta/ler.asp?id=136677>. Acesso em: 05 de outubro de 2014.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

ELEUTÉRIO, Pedro M. da Silva; MACHADO, Marcio Pereira. **Desvendando a Computação Forense.** São Paulo: Novatec, 2013.

FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. **Crimes na internet: elementos para uma reflexão sobre a ética informacional.** Brasília: Revista do Centro de Estudos Judiciários, 2003. Disponível em: <http://daleth.cjf.jus.br/revista/numero20/artigo9.pdf>. Acesso em: 18 de setembro de 2014.

GATTO, Victor Henrique Gouveia. **Tipicidade penal dos crimes cometidos na internet**. In: **Âmbito Jurídico**, Rio Grande, XIV, n. 91, ago 2011. Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10065&revista_caderno=17>. Acesso em 27 de setembro 2014.

GEMIN, André. **Crimes Cibernéticos: Tecnologia a Serviço da Criminalidade**. Disponível em: http://siaibib01.univali.br/pdf/andre%20gemin.pdf. Acesso em 10 de setembro de 2014.

GIL, Antonio de Loureiro. **Fraudes Informatizadas**. 2ª edição. São Paulo: Atlas, 1999.

GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet**. São Paulo: Revista Direito Mackenzie nº 1, 2000.

MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges. **Os Crimes Cibernéticos no Ordenamento Jurídico Brasileiro e a Necessidade de Legislação Específica**. Disponível em: <http://www.viajus.com.br/viajus.php?pagina=artigos&id=4696>. Acesso em: 22 de setembro de 2014.

MIRABETE, Julio Fabbrini. **Manual do Direito Penal, Volume 1: parte geral**. São Paulo: Atlas, 2008.

MOURA, Douro. **Crimes virtuais no Brasil**. 2000. Disponível em: <http://www.brasil.discovery.com/features/000908vcrimen/pg1.html>.Acesso em: 30 de agosto de 2014.

PARENTONI, Leonardo Netto. **Responsabilidade Civil dos Provedores de Serviços na Internet: Breves Notas**, in *Revista Magister de Direito Empresarial Nº 25*, fev-mar/2009.

PINHEIRO, P. P**. Direito Digital.** Saraiva: São Paulo, 2010.

PIRES NETO, Lindolfo. **Crimes Cibernéticos: necessidade de uma legislação específica no Brasil.** Disponível em: <http://www.fespfaculdades.com.br/painel/uploads/arquivos/trabArquivo_11052010080523_LINFOLFO.pdf>. Acesso em: 20 de setembro de 2014.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **Crimes virtuais**. Disponível em: <http://www.advogadocriminalista.com.br>. Acesso em: 25 de agosto de 2014.

ROSA, Fabrízio. **Crimes de informática**. Campinas: Bookseller, 2005.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal.** São Paulo: Memória Jurídica, 2004.

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**. Rio de Janeiro: Forense, 2003.

TANENBAUM, Andrew S. **Redes de Computadores.** Rio de Janeiro: Campus, 2003.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação**. Rio de Janeiro: Brasport, 2013

ZANIOLO, Pedro Augusto. **Crimes Modernos: o impacto da tecnologia no direito**. Curitiba: Juruá, 2012.