FACULDADE DOCTUM DE CARANGOLA
CURSO DIREITO

ARTHUR OLIVEIRA DOS SANTOS

CRIMES CIBERNÉTICOS: ANÁLISE DA LEGISLAÇÃO PENAL

CARANGOLA
2016

ARTHUR OLIVEIRA DOS SANTOS

CRIMES CIBERNÉTICOS: ANÁLISE DA LEGISLAÇÃO PENAL

Monografia apresentada ao curso de direito das faculdades Doctum de Carangola como requisito parcial a obtenção do titulo de bacharel em direito.
Área de concentração: Direito Civil

Orientador: Julio Cesar Simbra Soares

CARANGOLA
2016

FOLHA DE APROVAÇÃO

Título do Trabalho: **Crimes cibernéticos: análise da legislação penal**

Elaborada pelo Aluno: Arthur Oliveira dos Santos

Foi aprovada por todos os membros da Banca Examinadora e aceita pelo curso de Direito das Faculdades Integradas de Caratinga – FIC, como requisito parcial da obtenção do título de

BACHAREL EM DIREITO

Carangola_____ de _____ de _____

_____

Orientador

_____

Examinador 1

_____

Examinador 2

_____

Agradecimentos

Agradeço primeiramente a Deus por ter me concedido sabedoria para chegar até aqui.

Agradeço a meus familiares e amigos por tudo.

Agradeço a minha orientadora pelos conhecimentos repassados.

“Liberdade é o direito de fazer tudo o que as leis permitem”

Barão de Montesquieu

RESUMO

A internet cada vez ganha mais espaço na sociedade, sendo um dos meios de comunicação mais utilizados. Nesse contexto surge o mundo virtual, que diminui fronteiras, facilita a comunicação, transforma as relações, sendo um espaço onde as pessoas se sentem livres, e sob a condição do anonimato. Entretanto, o espaço virtual, é um lugar que tem sido palco de inúmeras condutas danosas, os denominados crimes virtuais ou crimes cibernéticos. Os crimes virtuais aumentam cada dia mais, e se tornam uma preocupação constante da população. Entretanto, essa se vê a mercê dos criminosos virtuais, pois não existem meios legais específicos que atuem com o intuito de coibir, e aplicar sanções aos infratores. Diante disso o presente trabalho tem como objetivo analisar os crimes virtuais, e a legislação brasileira, abordando os principais meios de proteção contra os crimes cibernéticos. Objetivou-se também realizar um breve histórico sobre o surgimento da internet para melhor compreender a difusão dos crimes virtuais. Como proposta metodológica, utilizou-se a pesquisa bibliográfica, tendo como base artigos, leis, documentos que trazem argumentos que facilitem a compreensão do tema abordado.

Palavras-chave: Crime virtual; Internet; Direito.

ABSTRACT

The internet increasingly gains more space in society, being one of the most used means of communication. In this context emerges the virtual world, which reduces borders, facilitates communication, transforms relationships, being a space where people feel free, and under the condition of anonymity. However, virtual space is a place that has been the scene of numerous harmful behaviors, so-called virtual crimes or cyber crimes. Virtual crimes increase every day, and become a constant concern of the population. However, this is at the mercy of virtual criminals, as there are no specific legal means that act to restrain, and apply sanctions to violators. In view of this the present work aims to analyze the virtual crimes, and the Brazilian legislation, addressing the main means of protection against cyber crimes. The objective was also to make a brief history about the emergence of the Internet to better understand the dissemination of virtual crimes. As a methodological proposal, bibliographical research was used, based on articles, laws, documents that bring arguments that facilitate the understanding of the topic addressed.

Keywords: Virtual crime; Internet; Right.

ABREVIATURAS E SIGLAS

SAGE - Semi-Automatic Ground Environment

ARPA - Advanced Research Projects Agency-

ARPANET - Agência de Pesquisas em Projetos Avançados na Rede

CSNET - Computer Science Research Network

CONTEL - Conselho Nacional de Telecomunicações

SUMÁRIO

INTRODUÇÃO **8**

CAPÍTULO I – A REDE MUNDIAL DE COMPUTADORES: INTERNET **10**

1.1Breve histórico do surgimento da internet 10

1.2 Internet no Brasil 12

CAPÍTULO II: CRIMES CIBERNÉTICOS **15**

2.1 Conceitos 15

2.2 Formas de prevenção dos crimes virtuais 20

CAPÍTULO III – A LEGISLAÇÃO PENAL APLICADA AOS CRIMES CIBERNÉTICOS **22**

CONSIDERAÇÕES FINAIS **27**

REFERÊNCIAS BIBLIOGRÁFICAS **28**

INTRODUÇÃO

A internet devido a seu alcance infindável, a cada dia ganha mais espaço na sociedade, sendo considerada um dos maiores meios de comunicação na atualidade. Através da internet laços são criados, informações importantes são repassadas, sendo capaz de possibilitar a comunicação universal, sem fronteiras. A internet se tornou uma ferramenta essencial no mundo globalizado, entretanto, é nesse mundo conectado que os crimes também podem ocorrer, esse é o caso do denominado crime virtual, ou crime cibernético.

O ambiente virtual proporciona ao usuário um sentimento de liberdade, devido ao anonimato que esse ambiente traz, nesse sentido oferece um mundo sem fronteiras, “onde tudo é permitido”, o que possibilita as ocorrências dos crimes virtuais.

Os crimes virtuais são crimes que acontecem por intermédio de um computador, e que causam alguma lesão a outrem, esse tipo de crime assume posição de destaque dentro do cenário penal brasileiro, a cada dia novos criminosos são atraídos a utilizar o meio virtual para cometer seus delitos, pois nesse meio o anonimato se faz presente, e se torna mais fácil enganar as vítimas.

Entretanto, esses crimes ainda não possuem legislação específica, sendo encaixados em crimes já tipificados no ordenamento jurídico, o que dificulta muitas das vezes a punição dos delitos.

Diante disso, considerou-se necessário conhecer um pouco mais sobre os crimes cibernéticos, e como estes vem crescendo cada vez mais juntamente com a tecnologia, e as medidas legais que abrangem tais delitos.

O presente trabalho monográfico tem por objetivo tratar dos crimes virtuais e analisar como o direito penal age diante do crescimento da tecnologia, sendo a prevenção da criminalidade informática, uma temática central, uma vez que esses avanços não trouxeram apenas vantagens, pois aumentou crimes praticados com o uso da internet, como a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas e outros.

Para alcançar tais objetivos, será utilizado o método dedutivo, através de um estudo das legislações que tratem do tema. Será feito também um levantamento dos principais crimes que ocorrem na internet, demonstrando que a cada dia cresce o

número de usuários que buscam no ambiente virtual propagar seus crimes de uma maneira desenfreada, seja aplicando golpes como estelionatários, iludindo a vítima, ou aplicando golpes fraudulentos, com o uso por exemplo, de falsos sites, em que a vítima achando se encontrar no site de um determinado banco, digita todos os seus dados, senha, número da conta, cartão de crédito, e todos os dados digitados são encaminhados aos bandidos.

CAPÍTULO I – A REDE MUNDIAL DE COMPUTADORES: INTERNET

1.1 Breve histórico do surgimento da internet

Para compreendermos o histórico dos crimes cibernéticos primeiramente considera-se essencial fazer um breve levantamento histórico sobre o surgimento da internet e as transformações tecnológicas trazidas a sociedade.

Segundo Feitoza (2012) a internet é o meio de comunicação em massa mais difundido na sociedade nos últimos tempos, devido a sua capacidade infindável, e ilimitada, capaz de facilitar e modernizar a vida das pessoas. Nesse sentido, a internet se tornou o meio universal de informação e comunicação.

O primeiro computador digital foi construído em 1946, denominado computador integrador numérico eletrônico, no entanto, é somente em 1957 que pode ser considerado o marco inicial da tecnologia, quando então as forças aéreas dos Estados Unidos, diante da repercussão da explosão causada pela primeira bomba de hidrogênio da União Soviética, em 1953, cria um sistema de defesa contra aviões bombardeiros inimigos, chamado Semi-Automatic Ground Environment (SAGE), “esse sistema operava de maneira distribuída por vinte e três centros de processamento de dados instalados em bunkers gigantescos, cada qual contendo dois computadores de grande porte” (CARVALHO, 2006, p.15).

O SAGE trouxe avanços tecnológicos a sociedade, surgiu o uso do modem, monitores de vídeos interativos, uso de computação gráfica, além de servir de modelo para a criação de vários outros sistemas. Nesse sentido, o sistema ligado de computadores surge a partir de uma necessidade de proteção, enquanto uma arma norte americana de informação militar.

De acordo com Rosa (2005, p.31)

> A fagulha que acabaria por acender a revolução da conectividade ocorreu em 1957, quando a União Soviética pôs em orbita o primeiro satélite espacial, o Sputnik: quatro meses depois, o presidente americano Dwight Eisenhower anunciava a criação de uma agencia federal norte-americana, nos moldes da NASA, conhecida como Advanced Research Projects Agency- ARPA, com a missão de pesquisar e desenvolver alta tecnologia para as forças armadas.

A ARPA tinha como função realizar pesquisas militares de cunho tecnológico, tendo como intuito proteger o território estadunidense, evitando surpresas tecnológicas de outros países, como foi o caso da União Soviética.

Na década de 1960 consolidou-se a ideia de se criar uma rede capaz de integrar computadores que estivessem distantes, e por meio dessa, seria possível a transmissão de dados, nesse período é criada a Agência de Pesquisas em Projetos Avançados na Rede (ARPANET) (LIMA, 2014).

A ARPANET operava por intermédio de diversos e inúmeras redes locais privadas e de baixo alcance chamadas e LAN (Local Area Network), seu objetivo era agrupar informações contidas no banco de dados e no departamento de pesquisa, enviando-as as partes interessadas (FEITOZA, 2012).

Inellas (2009, p. 1) destaca que

> a partir dessa preocupação, o Departamento de Defesa dos Estados Unidos elaborou um Sistema de Telecomunicações, desenvolvido pela Agência de Projetos e Pesquisas Avançadas, a ARPA, criando assim uma rede denominada ARPANET, que operaria através de inúmeras e pequenas redes locais, denominadas LAN (Local Area Network), que significa rede local responsável em ligar computadores num mesmo edifício, sendo instaladas em locais estratégicos por todo o País, os quais foram interligadas por meios de redes de telecomunicação geográficas, denominadas WAN (Wide Area Network), que significa rede de longo alcance, responsáveis pela conexão de computadores por todo o mundo, e assim, caso houvesse um ataque nuclear contra os Estados Unidos da América, as comunicações militares e governamentais não seriam interrompidas, podendo permanecer interligadas de forma contínua

Segundo Carvalho (2006, p. 16-17) uma das estratégias que viabilizaram a construção da ARPANET foi “a implantação de uma arquitetura que permitisse dividir as complexas tarefas de conectividade em um conjunto de funções discretas que interagissem entre si através de regras específicas; [...] o estilo de gerenciamento do projeto”.

Nos anos 70, a ARPANET passou a ser disponibilizada para o uso acadêmico no âmbito das instituições, funcionado como auxiliadora para troca de mensagens e compartilhamento de informações. Nesse contexto, surge o primeiro padrão de protocolo diferente do até então fornecido. Protocolo, segundo Inellas (2009, p. 2) “é a designação dada aos formatos de mensagens e suas regras, entre dois computadores, para que possa haver troca de mensagens [...] ele permite a comunicação entre os dois comunicadores”.

Em 1972, foi criado o correio eletrônico, hoje denominado e-mail.

> Correio eletrônico ou ainda *e-mail* ou *correio-e* é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação. O termo *e-mail* é aplicado tanto aos sistemas que utilizam a Internet e são baseados no protocolo SMTP, como aqueles sistemas conhecidos como *intranets*, que permitem a troca de mensagens dentro de uma empresa ou organização e são, normalmente, baseados em protocolos proprietários (FEITOZA, 2012, p. 28).

No início dos anos 80, a ARPANET, interligava somente algumas redes, nesse período um grupo de seis universidades norte-americanas começam a se organizar para criar uma rede acadêmica que pudesse atender a mais departamentos, criando a CSNET (Computer Science Research Network), essa perdurou de 1982 a 1985, obtendo sucesso, sendo a primeira a oferecer acesso às redes de outros países (CARVALHO, 2006).

Dessa forma, apesar de não ter tido o resultado esperado, a CSNET, trouxe mudanças no cenário da tecnologia, dando um maior acesso a diversas universidades de outros países a redes de computadores.

Em 1986, a ARPANET passa a ser chamada de Internet, com a criação da Teia Mundial (*World Wide Web* - WWW)

> que é um conjunto de documentos em hipermídia, da Linguagem de Marcação de Hipertexto (*HyperText Markup Language* - HTML), que é uma linguagem para a produção de páginas de internet, visualizados através de programas de computador chamados de *browsers* (programas para navegação pela internet, como o *Internet Explorer* ou o *Firefox*). Tal evolução trouxe como grande vantagem a melhoria na interface gráfica (LIMA, 2014, s/p).

1.2 Internet no Brasil

No Brasil o processo de introdução da internet se deu de forma lenta e progressiva, sendo introduzida a partir de iniciativas dos governos federais para iniciar o desenvolvimento das telecomunicações no Brasil. Em 1961, início do Governo de Jânio Quadros, foi criado o Conselho Nacional de Telecomunicações (CONTEL) e em 1964 foi aprovado o Código Brasileiro de Telecomunicações (CBT) (FEITOZA, 2012).

Esses meios criados, entretanto, só atendiam a uma parcela da população, pois o setor de telecomunicações era dominado por empresas privadas, enquanto isso a população pobre continuava desprovida de toda essa tecnologia.

Em 1964, o governo militar promoveu a implantação do Código Brasileiro de Telecomunicações (CBT), regulamentado pela lei 4.117, a estruturação da CONTEL, e a construção da Empresa Brasileira de Telecomunicações (EMBRATEL), criada para implantar a rede nacional, passou “a adquirir o controle das concessionárias privadas e assumir os serviços nacionais e internacionais prestados pelas multinacionais” (FEITOZA, 2012, p.31).

Em 1967, a CONTEL é substituída pelo Ministério das Comunicações (Minicom). Em 1979, foi criada a Secretaria Especial de Informática (SEI) que tinha como função cuidar das diretrizes relacionadas com o fluxo internacional de dados, essa secretaria estava subordinada ao Conselho de Segurança Nacional, o que dificultava o seu desenvolvimento (*idem*).

Nesse contexto, o Brasil viveu sob o regime militar, o que dificuldade a liberdade de informação, diante disso, o Brasil juntamente com outros países e a UNESCO criaram um órgão “Intergovernamental Bureau for informatics” (IBI), que tinha como objetivo conscientizar a sociedade da importância da livre informação e comunicação.

Em 1984, foi aprovada a “Lei de Informática”, lei nº 7.232, que “referendou os princípios básicos de capacitação tecnológica e reserva do mercado e democratizou o processo decisório através da criação do Conselho Nacional de Informática e Automação (CONIN)” (FEITOZA, 2012, p. 33).

A partir desse contexto começou a disseminação do uso de computadores em todos os âmbitos da sociedade, nas residências, nas empresas, e em 1994, com o lançamento da Teia Mundial, as empresas que ofereciam serviços de rede isolados passam a atuar como provedores, nesse momento a internet passa a ser disponibilizada para assinantes da rede.

> A internet comercial só chegou ao Brasil em 1996, totalmente obsoleto com uma infraestrutura insuficiente para atender às demandas de seus provedores de acesso e, principalmente dos seus usuários, essa cresceu rapidamente, não somente em números de usuários, mas em transações por meio do comércio eletrônico. Em decorrência surgiram diversas lojas virtuais, portais de conteúdo e máquinas de busca, como *Booknet*, Universo *On Line* (UOL), Brasil *On Line* (BOL) (FEITOZA, 2012, 34).

A partir disso, o mundo passa a viver interligado por um conglomerado de redes que permite o acesso a todo tipo de informação e transferência de dados, surge assim o denominado “mundo virtual”, que veio a reduzir distâncias, a modificar as relações, a criar os vínculos virtuais.

Entretanto, apesar de tantos benefícios trazidos por essa crescente tecnologia, surge um “ambiente convidativo para a prática de delitos e fraudes” (CARVALHO, *et al,* 2013), é nesse contexto que surgem os chamados crimes virtuais ou crimes cibernéticos, realizados por sujeitos criminosos especializados na linguagem da informática.

Rosa (2005,p. 33), diante desse contexto, posiciona-se

> Com a expansão do uso de computadores e com a difusão da internet, tem-se notado, ultimamente, que o homem está se utilizando dessas facilidades para cometer atos ilícitos, potencializando, cada vez mais, esses abusos cometidos na rede. Como todos os recursos de disponibilidade do ser humano, a informática e a telecomunicação não são utilizadas apenas para agregar valor. O abuso (desvalor), cometido por via, ou com assistência dos meios eletrônicos não tem fronteiras. De um terminal eletrônico instalado num país se poderá manipular dados, cujos resultados fraudulentos poderão ser produzidos noutro terminal, situado em país diverso.

Destarte, os crimes virtuais surgem junto com o avanço da tecnologia, sendo uma consequência negativa da internet, trazendo malefícios aqueles que utilizam da rede.

CAPÍTULO II: CRIMES CIBERNÉTICOS

2.1 Conceitos

Segundo Silveira (2015) os crimes virtuais retomam à década de 70, quando foi definido o termo “hacker”, sendo considerado aquele indivíduo dotado de conhecimentos técnicos, que promove a invasão de sistemas operacionais.

Os crimes virtuais, também denominados de crimes cibernéticos, crimes digitais, crimes de alta tecnologia, entre outras nomenclaturas, possui várias definições, diante disso se torna essencial trazer os conceitos dados a esse termo por alguns estudiosos do assunto.

De acordo com Filho (2012) os crimes virtuais referem-se aos crimes contemporâneos praticados por criminosos por intermédio da internet, esses possuem conhecimento tecnológico ou de sistema de informação, podendo figurar como um crime formal, onde tem por finalidade infiltrar no sistema de um computador, ou somente arquitetar a criação de um vírus, pode estar relacionado a degradação da integridade ou da imagem do usuário, ou a invasão de dados confidenciais de empresas ou pessoais.

Nigri (2000) define crime virtual, como um ato lesivo cometido através de um computador, com a intenção de se obter uma vantagem indevida.

Pinheiro (2006, p. 16) afirma que o

> crime virtual é qualquer ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão em que um computador conectado à rede mundial de computadores – Internet – seja o instrumento ou o objeto do delito.

Segundo Rosa (2002, p. 53), a Organização para cooperação econômica e de desenvolvimento (OECD) crime virtual é considerado “qualquer conduta ilegal não ética, ou não autorizada que envolva processamento de dados e/ou transmissão de dados”.

Rosa (2002, p. 53-54), conceitua o crime de informática como sendo

> 1. É a conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. o 'Crime de Informática' é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. assim, o 'Crime de Informática' pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. a expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc

De acordo com Ramalho Terceiro

> Os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas. (TERCEIRO, 2002, p. 1)

Destarte, independente dos muitos conceitos em torno de crimes virtuais, todos tem por base que esses são crimes que acontecem por intermédio de um computador, e que causam alguma lesão a outrem.

> Os crimes de informática possuem como pré-requisito a presença de apenas três fatores fundamentais para que sejam executados: (1)- agente capaz de cometer o ilícito (2)- um computador em pleno funcionamento e, (3)- acesso a rede mundial de computadores. Preenchido estes requisitos, qualquer um pode incidir sobre esta modalidade criminosa (FEITOZA, 2012, p 37).

Assim, os crimes virtuais podem ser cometidos por qualquer sujeito, capazes de cometer o ato ilícito. Em relação ao agente delitivo, o hacker merece destaque.

> Hacker é aquela pessoa dotada de conhecimentos aprofundados de sistemas operacionais e tipos de linguagens programacionais, ele conhece com perfeição as falhas de segurança existentes nos programas e está sempre em busca de novas outras falhas. O *hacker* invade os sistemas pelo

> simples prazer de provar para si mesmo que é capaz de fazê-lo, sem alterar nada (FEITOZA, 2012, p. 37).

Os infratores com conhecimento avançado no que diz respeito a informática, são chamados de crackers, definidos por Rosa (2005, p. 61) como

> *Cracker* é o mesmo que *hacker*. A diferença entre um e outro está em utilizar o seu conhecimento para o mal. Destruir e roubar são suas palavras de ordem. Assim, o *cracker* usa os seus conhecimentos para ganhar algo, rouba informações sigilosas para fins próprios e destrói sistemas para exibir.

Existem ainda o preaker, que ao contrário dos outros dois usuários maliciosos, não emprega o computador e a internet como ferramentas para atingir seu ataque, mas sim o telefone, é conhecedor da rede de telefonia. Atua na obtenção de escutas telefônicas gratuitas (FEITOZA, 2012).

O Loser, é outro personagem no meio virtual, refere-se a um operador de internet novo, sem experiência técnica, mas que tem como objetivo se tornar um hacker. O *wannabe* é o usuário de computador comum, “entretanto, aprendeu a manusear diversos programas produzidos e disponibilizados por hackers na internet e os usa para facilitar suas tarefas privadas” (FEITOZA, p. 47).

O expert em informática e navegação na rede é chamado de guru, sendo a pessoa que possui conhecimentos superiores em tecnologia, sendo considerado o pai dos hackers.

No que diz respeito ao sujeito passivo dos crimes virtuais, Rosa (2005, p. 61) define o “sujeito passivo dos crimes de informática pode ser qualquer pessoa, física ou jurídica, de natureza pública ou privada, pouco importando se é capaz ou não de entender o que possa estar acontecendo”

Os crimes cibernéticos podem ser classificados em próprios e impróprios, os primeiros são aqueles que podem ser praticados na informática, ou seja, a execução e a consumação ocorrem nesse meio, tem-se como exemplo a violação de emails, danos em arquivos causado pelo envio de vírus; o segundo, os crimes impróprios são aqueles já tipificados, que violam bens protegidos pela legislação, podem ser praticados de qualquer forma, sendo o computador só mais um instrumento, tem-se como exemplo a pedofilia, ameaças (MENDES e VIEIRA, 2012).

Outra classificação seria a tripartida, citada por Castro (2003, s/p):

> a) os crimes de informática puros, onde o agente objetiva atingir o computador, o sistema de informática ou os dados e as informações neles

> utilizadas; b) os crimes de informática mistos, onde o agente não visa o sistema de informática e seus componentes, mas a informática é instrumento indispensável para consumação da ação criminosa e c) os crimes de informática comuns, onde o agente não visa o sistema de informática e seus componentes, mas usa a informática como instrumento (não essencial, poderia ser outro o meio) de realização da ação.

Quanto aos métodos utilizados para invasão dos computadores e sistemas operacionais, Feitoza (2012) destaca os seguintes:

- Chave mestra: uso indevido e não autorizado de programas criados parra modificar , copiar, utilizar ou inserir o uso de algumas informações arquivadas em bancos de dados informáticos;
- Sniffer: programa incumbido de captar e interceptar a informação que está trafegando pela rede de computadores;
- Cavalo de Tróia: programa que objetiva sabotar, alterar dados, cópia de arquivos com a finalidade de obter ganhos monetários;
- Vírus: fragmento de programa de computador que é capaz de mudar totalmente a estrutura do *software* do sistema operacional, destruindo ou inutilizando dados e outras informações;
- *Spyware:* programa que tem como finalidade monitorar os hábitos recorrentes no computador;
- *Key logger:* registra todos os toques dados no teclado e em outras atividades no sistema;
- *Cookie:* uma espécie de arquivo utilizada por alguns sites que põem no computador do usuário para autorizar a personalização dos conteúdos contidos na web.

É importante ressaltar que o sujeito ativo no crime cibernético pode ser qualquer pessoa, assim como sujeito passivo, “que pode ser qualquer pessoa passível de sofrer dano moral ou material decorrente da violação de seu sistema de informática” (SILVEIRA, 2015, s/p).

São muitos os tipos de crimes possíveis de se praticar no meio virtual, sendo os mais praticados segundo Takushi e Aquotti (2009, p. 5-9) e Pinheiro (2014, p. 17):

- Crime de dano: a conduta nesse tipo de crime é apagar, modificar, destruir ou inutilizar, parcial ou completamente, dados ou programas de computador

- Crime de Veiculação de pornografia através da internet: esse crime consiste em dois tipos de conduta, a de oferecer serviço e/ou oferecer informação, de caráter pornográfico, via rede de computadores.
- Estelionato e fraude: estelionato seria a obtenção de vantagem ilícita, para si ou para outrem, levando ao prejuízo alheio; fraude está relacionada a lesão ao patrimônio por meio enganoso, tendo como fim o prejuízo alheio;
- Crime contra a privacidade: refere-se à vida íntima, privada;
- Espionagem e sabotagem informática: a sabotagem configura-se na alteração de programas ou de peças, modificando a programação originária, nesse caso o autor se aproveita de falhas no sistema e através de programas específicos invadi e subtrai dados da máquina;
- Crimes contra a honra: são exemplos de crime de calúnia, injúria e difamação;
- Crime contra a liberdade individual: crimes de ameaça, inviolabilidade de correspondência, divulgação de segredos;
- Crimes contra o patrimônio: crimes de furto, extorsão, dano e estelionato.

Como uma forma de orientar sobre os crimes virtuais, destacam-se, de acordo com Carvalho (*et al,* 2012) duas organizações: nacional SaferNet Brasil e Uniys.

A Safer Net Brasil (Central Nacional de Denúncias) foi fundada em 2005 tendo como objetivo “oferecer uma resposta eficiente para os problemas relacionados ao uso indevido da internet na prática de crimes virtuais e violações contra os Direitos Humanos” (CARVALHO *et al,* 2012, p. 4).

Segundo os indicadores da SaferNet, em 10 anos já foram recebidas 3.746.062 denúncias envolvendo 628.848 páginas distintas da internet (das quais 201.066 foram removidas). Os crimes monitorados pela organização são: intolerância religiosa, racismo, neo nazismo, tráfico de pessoas, pornografia infantil, maus trato contra animais, xenofobia, apologia e incitação a crimes contra a vida, homofobia (SAFERNET, 2016).

A organização Unysis “é uma empresa mundial de tecnologia da informação, especializada em ajudar grandes empresas e organizações governamentais no ambiente de segurança”. A organização fornece uma medida estatística sobre quatro áreas de segurança: segurança nacional de epidemias, segurança financeira, segurança na internet, segurança pessoal (CARVALHO, *et al,* 2012, p. 6).

Segundo os índices de segurança Unysis a grande preocupação da maioria das pessoas está voltada para a segurança virtual, principalmente no que se refere a fraudes, a compras na internet.

Destarte, os crimes virtuais vem se tornando algo preocupante, sendo necessário, nesse sentido, avaliar as legislações que tipificam esse crime.

2.2 Formas de prevenção dos crimes virtuais

Diante dos inúmeros crimes virtuais, alguns mecanismos de proteção e prevenção de abusos foram criados. Segundo Feitoza (2012, p. 56-57 *apud* SILVA, 1995) podem ser visualizadas três categorias gerais no ambiente de proteção do computador:

a) *Softwares,* dados e informações – esses programas tem como intuito preservar a confidência, integridade e disponibilidade
b) Serviços de processamento de dados – é considerado um dos recursos mais importantes para requerer proteção em casos onde a segurança é dependente dos sistemas de computador;
c) Equipamento de processamento de dados eletrônicos e instalações – esta categoria envolve a propriedade tangível.

Além desses meios, é importante que os usuários busquem outras formas de proteção, como o uso de senhas, estas não devem estar contida “em nenhuma espécie de dicionários, idiomas estrangeiros ou temas correlatos, não utilizar informações pessoais como data de aniversário, apelido ou sobrenome, usar variações de caracteres e de pontuação” (FEITOZA, 2012, p. 57 *apud* ZANIOLO, 2007).

Outro mecanismo que também pode ser utilizado são os *softwarees antimalware*, são ferramentas que procuram detectar, e então anular ou remover esses arquivos maliciosos do seu computador. Dentre os mecanismos tem-se também o *Firewal*, protege a rede interna contra hackers maliciosos, isola as ameaças dos computadores (FEITOZA, 2012).

> Também tem os filtros *antispam,* que são integrados aos e-mails e programas correlatos, permitindo a separação de e-mails que não sejam desejados (*spams*), podendo assim, os usuários classificá-los conforme

> desejar. Outro recurso que pode o usuário fazer uso é os *Honeypots* e os *Honetnets*, sendo que estes são recursos computacionais de segurança destinado à serem sondados, atacados ou comprometidos, cujo valor esta na capacidade de reunir a maior quantidade de informações importantes sobre tendências, comportando assim, o aperfeiçoamento na segurança das redes (FEITOZA, 2012, p. 58-59).

O teste de reputação do site é um dos mecanismos mais importante, pois é a partir desse que pode se determinar a confiabilidade dos sites, onde essa aferição pode ser feita de diversas formas, conforme explica Feitoza (2012, p. 59)

> por meio de esquemas de cores, onde o programa indica a reputação do *site*, em verde escuro (excelente), verde claro (boa), amarelo (insatisfatório), vermelho (má) e vermelho escuro (péssima). Outra maneira de verificar é valendo-se de informações que estejam na página de acesso, é certificar que sua url (*Uniform Resource Locator)* que em tradução livre que dizer Localizador-Padrão de Recursos, que nada mais é que um localizador de recurso disponível em uma rede, podendo ela ser de internet ou intranet, esse recurso pode ser uma impressora, um arquivo.

É importante ressaltar que tais mecanismos são eficientes, porém, são apenas medidas preventivas contra os ataques cibernéticos, servindo para amenizar os casos, mas é essencial que o usuário tenha todo o cuidado, para que não acabe sendo mais uma vítima do crime virtual.

CAPÍTULO III – A LEGISLAÇÃO PENAL APLICADA AOS CRIMES CIBERNÉTICOS

Diante das ameaças surgidas decorrentes da revolução tecnológica, são muitos os desafios apresentados que o direito penal precisa transpor. Por ser um mundo sem leis, os atos ilícitos praticados pela internet, acabam sendo inseridos na esfera jurídica, surgindo assim os crimes virtuais.

Segundo Feitoza (2012, p. 44) qualquer crime virtual para que seja passível imputação de penalidade legal é necessário três requisitos essenciais de validade:

> O primeiro requisito diz respeito à tipificação expressa do crime em lei, ou seja, sua denominação legal e precisa do ato volitivo contributivo do infrator para o resultado finalístico. Se não houver tal tipificação, a materialidade para o delito simplesmente irá desaparecer, o tornando atípico e consequentemente não punível pela legislação jurídica penal brasileira.
> A próxima condição fundamental que se encaixa ao delito é a conduta do autor, que pode se dar de forma comissiva ou omissiva, dolosa ou culposa. A conduta comissiva se aduz em uma ação positiva desencadeada pelo transgressor, ocorrendo quando a ação for expressamente proibida por lei [...].
> Já na hipótese de ato omissivo, o indivíduo age negativamente, deixando de praticar algo que lhe era devido por obrigação ou que poderia fazer para amenizar a consequência derradeira.

Os crimes cibernéticos, diante da falta de uma legislação mais rigorosa, se enquadram em crimes já tipificados no ordenamento brasileiro. Em sua maioria esses crimes são julgados com base no artigo 171 do Código Penal “obter para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento”. No caso de crimes de pedofilia, pornografia infantil, é reprimida pelo Código Penal em seu artigo 234 e pelo Estatuto da Criança e do Adolescente. Os crimes de danos se enquadram no PL nº84-A/99, sua ementa dispõe sobre os crimes cometidos na área da informática. No caso do racismo cometido no meio virtual, encontra-se inserido na lei nº 7.716/89 e tem como punição a reclusão de dois a cinco anos e multa. O crime de furto eletrônico é predito no artigo 155, *caput,* visa proteger o bem alheio móvel (FEITOZA, 2012).

Entretanto, existem casos que não se aplicam as leis existentes, o que transforma o mundo virtual em um mundo sem lei, de acordo com Lima (2014 *apud* BASSO e ALMEIDA, 2007, p. 123)

> quando afirmam que em vários casos, as leis existentes são também aplicáveis aos novos pressupostos do contexto virtual. Em outros, uma nova regulamentação é necessária para se ter mais segurança no emprego das ferramentas eletrônicas e maior certeza quanto a validade e eficácia das transações celebradas por meio eletrônico.

Ao enquadrar os crimes virtuais em crimes já tipificados, a interpretação feita está baseada na ideia de que apesar do crime não ser propriamente físico, a equiparação existe a partir do resultado buscado pelo criminoso ao cometer tal conduta na internet.

Feitoza (2012) destaca alguns projetos de lei importantes no que diz respeito a punição a crimes virtuais, como o PL nº84/1999, esse projeto tem como proposta a tipificação de alguns crimes de informática, dentre eles o estelionato.

Rosa (2002, p. 90) faz a seguinte ponderação sobre o PL nº84/99

> O PL nº 84/99 foi aprovado na forma do substitutivo da comissão de segurança pública. O relatório aprovado, do deputado Nélson Pellegrino (PT-BA), acrescenta nova seção do Código Penal para tipificar diversos crimes relacionados aos sistemas informatizados, como a difusão de vírus eletrônico, de pornografia infantil na internet e o acesso indevido a meio eletrônico ou sistema informatizado, entre outros. Também está prevista no texto a tipificação do crime de falsificação de telefone célula ou de meio de acesso a sistema eletrônico, como cartão inteligente, transmissor ou receptor de radiofrequência. Para os efeitos penais, serão considerados meios eletrônicos elementos como computador, processador de dados, disquete e CD-ROM. A rede de computadores, base de dados e o programa de computador são classificados como sistema informatizado.

Esse projeto sofreu algumas alterações de 2008 para 2010, sob a responsabilidade do então senador Eduardo Azevedo. O senador Eduardo Azevedo afirmou em seu vasto parecer em relação aos crimes virtuais, a necessidade urgente de uma norma que regulasse esses crimes, afirmando que o avanço da tecnologia era capaz de gerar vazios na lei, o que acaba por gerar a proliferação de fraudes e danos aos usuários (FEITOZA, 2012).

Foi somente a partir de fatos importantes na sociedade, que considerou-se necessário criar normas mais eficazes e específicas sobre os crimes virtuais. Em 2011, sites oficiais do governo e de empresas públicas, sofreram uma onda de ataques de *hackers* e *crackers* e ficaram fora do ar temporariamente, tal fato

influenciou na criação da lei 12.737/2012, resultante do PL 84/1999. Outro fator que influenciou a criação da lei foi a publicação de fotos íntimas da atriz Carolina Dieckmann. Segundo Oliveira, segundo a atriz sua conta de email havia sido hackeada, os invasores postaram imagens em sites de pornografia (LIMA, 2016).

A Lei 12.737/2012, altera o código penal, criando o artigo 154-A que trata da invasão de dispositivo informático, e altera a redação dos artigos 266 e 298 para adequá-los a realidade cibernética.

> 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.
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos (BRASIL, 2012).

Porém, é importante ressaltar que no Congresso Nacional tramitam incontáveis projetos de leis referentes aos delitos informáticos, mas nenhum ainda foi sancionado ou aprovado definitivamente para que passe a ser revestido de uma norma *erga omnes.*

Entretanto, ao pensar em crimes cibernéticos, é importante ressaltar que os desafios encontrados para extinguir esse problema está muito além de uma

disposição legislativa, é importante que os profissionais de investigação tenham técnicas especializadas para facilitar na identificação dos agentes delituoso, porém, existem grandes dificuldades nesse sentido. Segundo Rocha (2004) um dos problemas encontrados para a resolução de problemas é identificar a autoria dos atores que comente o crime no sistema de informação.

No entendimento de Atheniense (2004, p. 1)

> as soluções legais a serem buscadas deverão objetivar a circulação de dados pela internet, controlando a privacidade do indivíduo sem cercear o acesso a informação. Neste sentido é necessário aprimorar nossas leis de proteção de dados, inclusive com a regulamentação da atividade dos provedores que controlam a identificação do infrator, bem como um maior aparelhamento das delegacias especializadas.

Nesse sentido, é necessário que sejam fornecidos melhores condições e treinamentos a policiais, capacitando-os a investigar os crimes que ocorrem no ambiente virtual. Sendo essencial ainda a aquisição de equipamentos capazes de prever e analisar os novos crimes, assim como maneiras de viabilizar condutas preventivas e de correção.

Segundo Pinheiro (2006, p. 26)

> A impunidade dos criminosos virtuais é uma conseqüência mais da fragilidade das informações de rastreamento do que da falta de legislação específica. Pela natureza da Internet, com seu ciberespaço, é muito difícil fiscalizá-la. O transito de dados é livre e veloz, é instantâneo, e como todas esses dados são traduzidos em bits, facilmente manipulados pelos experts, a prova da conduta ilícita é frágil, isso quando resta alguma.

Nesse sentido, um dos problemas é identificar os autores dos crimes virtuais, pois, como afirma Feitoza (2012, p. 48)

> A grande problemática de se identificar os autores dos fatos é que a rede mundial de computadores interliga em seu seio pessoas do mundo inteiro, e em alguns casos é praticamente impossível se determinar o local em que o ato ilícito foi gerado, sabendo-se que o mesmo criminoso pode-se valer de inúmeros computadores e locais diferentes de acesso para exaurir o fato. Devido ao computador e a internet serem objetos móveis, muitas vezes um único crime cometido por apenas um autor “viaja” por diversos lugares, impossibilitando o trabalho investigatório de identificação de autoria.

Outro fator que dificulta a resolução do crime, diz respeito a delimitação do local onde o mesmo foi cometido. A identificação do local exato do crime é de suma

importância para se delimitar a competência jurisdicional e a origem da ocorrência criminosa, que será de grande valia no processo acusatório (FEITOZA, 2012, p. 49).

Portanto, os crimes cibernéticos ainda continuam em um mundo sem lei, faltando respaldo para que possam haver punições adequadas ao crime, assim como é necessário equipes capacitadas, para que dessa forma as investigações sejam feitas de maneira efetiva. Como afirma Amadeu Robalinho Dantas da Gama Neto, da coordenadoria de Operações e Recursos Especiais da Polícia Civil de Pernambuco “o crime evolui, e a lei não acompanha a evolução” (CARVALHO *et al*, 2012).

Nesse sentido, é possível afirmar que o estado encontra-se vulnerável perante os novos criminosos virtuais, pois esses em sua grande maioria são mais rápidos que os legisladores. Inellas (2009, p. 100) afirma

> sei que infelizmente, os criminosos são mais rápidos que os legisladores. Isso acontece em todo o mundo e o Brasil não é exceção. Ainda mais, em se tratando de internet, que passou a ser largamente utilizada em nosso país a pouco tempo e que possui peculiaridades que outros meios de comunicação não tem. A facilidade que a internet oferece para a prática de crimes, deixou os juristas completamente assarapantados. Não possuímos legislação específica a respeito de crimes virtuais em nosso Código Penal de 1940. Evidentemente, no combate aos crimes virtuais, a justiça utiliza o Código Penal, pois a grande maioria das infrações penais cometidas através da internet, pode ser capitulada nas condutas criminosas previstas no Código Penal. Todavia, o ideal seria a existência de lei especial, onde estivessem capituladas as condutas especificas, isto é, as condutas criminosas, praticadas através da internet

Dessa forma, é essencial, que sejam criadas leis específicas para combater o crime virtual, para que esse não cresça cada vez mais em nossa sociedade.

CONSIDERAÇÕES FINAIS

O crime cibernético é uma problemática atual e deve ser vista com cuidado pelos legisladores, pois por mais que esses sejam julgados com base no código penal de 1940, existe uma grande diferença entre os crimes cometidos na internet e os crimes cometidos em ambiente real. Nesse sentido, nesse mundo virtual sem lei, a cada dia os criminosos cibernéticos se especializam mais, enquanto as leis de proteção permanecem estagnadas. A elaboração da lei 12.737/2012 foi importante, entretanto insuficiente no que concerne a punição sob os crimes virtuais, dessa forma, cabe ao Direito Penal a obrigação de estruturar mecanismos que venham prevenir e punir esses criminosos de forma efetiva.

Destarte, pode-se constatar ainda que uma das dificuldades da resposta estatal aos crimes virtuais é pelo fato desses ocorrerem de maneira ágil, sem quaisquer pistas, não havendo território fixo, além disso não existem profissionais capacitados para lidar com esse tipo de crime, não tendo sucesso em investigações por não possuírem recursos necessários para deter tais crimes.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Lei nº 12.737, de 30 novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto Lei 2848, de 7 de dezembro de 1940, e dá outras providências. Disponível em: <http://www.planalto.gov.br> Acesso em 20 nov 2016.

BRASIL. **Decreto Lei nº 2.848, de 07 de dezembro de 1940**. Código Penal. Brasília. Disponível em <www.planalto.gov.br> Acessado em 16 de nov de 2016.

CARVALHO, Marcelo S. R. M. **A trajetória da internet no Brasil:** do surgimento das redes de computadores à instituição dos mecanismos de governança. Dissertação de Mestrado. Universidade Federal do Rio de Janeiro, 2006.

CARVALHO, D. L.; SOUZA, M. A.;COSTA, H. R. **Crime Virtual:** crescimento e falta de leis específicas. 2012. Disponível em: <http://www.viajus.com.br> Acesso em 20 nov 2016.

CASTRO, Aldemario Araújo. **Internet e os Tipos Penais que Reclamam Ação Criminosa em Público.** In: Webly. Disponível em <http://www.webly.com.br> Acesso em 20 nov 2016.

FEITOZA, L. G. M. **Crimes Cibernéticos: o estelionato virtual.** Monografia apresentada ao curso de Direito. Universidade Católica de Brasília, 2012.

FILHO, D. C. A. N. **Crime virtual:** crime contra o patrimônio no âmbito da internet, suas pecularied ades e controvérsias a luz do Código Penal de 1940. 2012. Disponível em: <http://ambitojuridico.com.br> Acesso em 20 nov 2016

INELLAS, G. C. Z. **Crimes na Internet.** 2 ed. São Paulo: Editora Juarez de Oliveira, 2009.

LIMA, S. P. **Crimes virtuais:** uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade. 2014. Disponível em: <http://www.ambitojuridico.com.br> Acesso em 20 nov 2016.

NIGRI, Débora Fisch. **Crimes e segurança na internet.** Rio de Janeiro: Instituto dos Magistrados do Brasil, 2000.

PINHEIRO, E. P. **Crimes Virtuais:** uma análise da criminalidade da informática e da resposta estatal. 2006. Disponível em: <http://www.egov.ufsc.br> Acesso em 20 nov 2016

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

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **Crimes virtuais**. 2005. Disponível em:<http://www.advogadocriminalista.com.br> Acesso em 18 nov 2016.

SAFERNET. **Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos.** 2016. Disponível em: <http://indicadores.safernet.org.br> Acesso em 22 nov 2016.

SILVEIRA, A. B. **Os crimes cibernéticos e a lei nº 12.737/2012.** 2015. Disponível em: <http://www.conteudojuridico.com.br> Acesso em 20 nov 2016

TAKUSHI, T. T.; AQUOTTI, M. V. F. **Crimes Virtuais.** 2005. Disponível em: <http://intertemas.unitoledo.br> Acesso em 20 nov de 2016.

ATHENIENSE, A. R. **Crimes virtuais, soluções e projetos de Lei**. DNT. [s.l.]. 29 out. 2004. Disponível em: <http://www.dnt.adv.br/noticias/direito-penal-informatico/crimes-virtuais-solucoes-e-projetos-de-lei/>. Acesso em: 20 nov. 2016.