UNIVERSIDADE DE PASSO FUNDO
FACULDADE DE DIREITO

Fabrícia de Matos

CRIMES VIRTUAIS: UMA ANÁLISE À LUZ DO ORDENAMENTO JURÍDICO PÁTRIO.

Lagoa Vermelha
2016

Fabrícia de Matos

CRIMES VIRTUAIS: UMA ANÁLISE À LUZ DO ORDENAMENTO JURÍDICO PÁTRIO.

Monografia apresentada ao curso de Direito, da Faculdade de Direito da Universidade de Passo Fundo, como requisito parcial para a obtenção do grau de Bacharel em Ciências Jurídicas e Sociais, sob a orientação do professor Me. Henrique Rech Neto.

Lagoa Vermelha
2016

Fabrícia de Matos

CRIMES VIRTUAIS: UMA ANÁLISE A LUZ DO ORDENAMENTO JURÍDICO PÁTRIO.

Monografia apresentada ao curso de Direito, da Faculdade de Direito da Universidade de Passo Fundo, como requisito parcial para a obtenção do grau de Bacharel em Ciências Jurídicas e Sociais, sob a orientação do professor Me. Henrique Rech Neto.

Aprovado em _____ de _____ de _____.

BANCA EXAMINADORA:

_____

Prof. Me. Henrique Rech Neto

_____

Prof.

_____

Prof.

Lagoa Vermelha
2016

A minha família que, mesmo diante dos obstáculos impostos pela vida, me oportunizaram cursar o ensino superior e por todo carinho, dedicação e incentivo proporcionado durante todos esses anos, para que este sonho fosse concretizado.

AGRADECIMENTOS

Agradeço primeiramente a meus pais e minha irmã pela oportunidade em cursar o ensino superior, pelo apoio e incentivo desmedido, mesmo diante de todas as dificuldades que a vida lhes impôs.

Ao Vantuir Dutra, que de bom grado me incentivou e prestou seu apoio e auxilio para que o presente trabalho fosse realizado, meus singelos agradecimentos.

Ao Cleber Melo da Silva, fiel amigo, que sempre ofereceu palavras e gestos de incentivo nos momentos de dificuldades, mostrando que era possível concluir com sucesso o presente trabalho.

Ao Professor Mestre Henrique Rech Neto, merecedor do meu prestígio e admiração, por aceitar a tarefa de orientar este trabalho, meus sinceros agradecimentos.

Por fim, agradeço também a todos que, de algum modo, contribuíram para a minha formação, principalmente, aos professores da Universidade de Passo Fundo, Campus Lagoa Vermelha/RS e aos meus amigos que sempre estiveram ao meu lado me dando apoio e acreditando na realização deste sonho.

RESUMO

A presente monografia tem por objetivo analisar minuciosamente as circunstâncias determinantes dos delitos perpetrados com o uso da internet. Para tanto, será realizado uma exposição a respeito do surgimento da informática, bem como considerações pertinentes a evolução dos sistemas informatizados a partir da interconectividade e transmissão de dados entre os computadores, hoje conhecida como internet. Também, serão abordados aspectos relevantes a respeito dessa nova criminalidade, analisando o perfil dos delinquentes virtuais, demonstrando suas principais formas de atuação, destacando-se os artifícios maliciosos que usam para ludibriar as vítimas ou manipular dispositivos informáticos e, com isso, obter vantagens indevidas. Versa a respeito das condutas danosas que possam ser praticadas em ambiente virtual mencionado suas principais características e classificando-as conforme o bem jurídico lesado. Por fim, busca-se fazer referência à legislação nacional e internacional, com o escopo de compreender como os países vêm se posicionando diante dessa criminalidade moderna, bem como ressaltar a importância do fortalecimento do ordenamento jurídico pátrio, para tipificar e punir os indivíduos que cometem tais atos, bem como desenvolver formas de prevenção contra os criminosos virtuais.

Palavras-chave: Bem Jurídico. Crimes Digitais. Criminosos Virtuais. Internet. Legislação. Sistemas informatizados.

SUMÁRIO

INTRODUÇÃO

O direito sempre esteve presente na sociedade, intervindo em diversos seguimentos e contribuindo para a resolução de conflitos que surgem a partir das relações e interesses interpessoais. Ocorre que a sociedade não é estática, constantemente mudam-se hábitos, costumes, tecnologias, sendo que a partir dessas mudanças podem advir situações conflituosas, as quais nem sempre serão abarcadas pela legislação vigente.

Ao longo do tempo a sociedade desenvolveu novas tecnologias que lhes permitiu maior comodidade em suas tarefas diárias, traçando novos paradigmas culturais impostos pela virtualização das relações humanas em decorrência do uso da internet, a qual invadiu todos os setores da sociedade, sendo amplamente difundida, de modo que nos tornamos a sociedade da informação.

Assim, podemos dizer que a internet é um campo vasto, ainda não desbravado completamente e desconhecido em muitos aspectos pelos seus usuários, os quais podem tornar-se alvos de pessoas mal intencionadas, que veem no suposto anonimato que a internet proporciona uma oportunidade para cometer atos ilícitos.

Nesse sentido, o presente trabalho tem por objetivo demonstrar que conjuntamente aos avanços científicos em relação aos dispositivos informatizados surge a figura de um delinquente ágil e habilidoso, que usa de artifícios maliciosos para manipular pessoas e máquinas com o objetivo de causar algum dano ou prejuízo a outrem e, por consequência, auferir qualquer vantagem indevida.

Dito isto, o primeiro capítulo será dedicado a analise da evolução dos dispositivos informáticos, abrangendo desde o surgimento dos primeiros computadores, suas especificações, utilidades e sua evolução ao longo do tempo, incluindo o desenvolvimento e aperfeiçoamento de sistemas que permitiam a conectividade entre essas máquinas, hoje denominado mundialmente como internet.

Ainda, nesse capítulo foram efetuadas algumas considerações a respeito dos protocolos de comunicação na rede mundial de computadores, dando ênfase ao protocolo TCP/IP, bem como uma analise dos criminosos virtuais, destacando-se

duas figuras comuns ao universo da informática, os *hackers* e os *crackers,* distinguindo-os conforme sua forma de atuação e abordando aspectos históricos e comportamentais desses indivíduos.

No segundo capítulo, procuramos abordar as condutas típicas praticadas por intermédio do computador, classificando cada crime digital conforme sua natureza e forma de execução, distinguindo-os doutrinariamente em impróprios, próprios e mistos, sendo realizada uma breve explanação a respeito de cada tipo penal, demonstrando suas particularidades.

Por fim, no terceiro capítulo realizamos uma breve exposição a respeito da legislação nacional e internacional a respeito dos crimes praticados com o uso da internet, mencionando tratados internacionais que versem sobre o tema, procurando demonstrar o posicionamento de diferentes nações a respeito dos crimes praticados por computador.

Ainda, nesse capitulo demos ênfase a analise do ordenamento jurídico pátrio, destacando projetos de lei que tramitaram no congresso nacional e como os tribunais brasileiros vem se manifestando diante desses delitos, fazendo referência a questões de competência para apuração e julgamento de crimes dessa natureza. Ao final, destacamos a importância da cooperação entre países na atuação repressiva e punitiva dos crimes cibernéticos, dando maior importância a colaboração internacional na investigação desses delitos.

2 ASPECTOS RELEVENTES DOS CRIMES PRATICADOS ATRAVÉS DO COMPUTADOR

O presente capítulo tem por objetivo demonstrar a evolução histórica da informática, desde o surgimento do computador até o implemento da internet como instrumento de comunicação, bem como realizar uma breve análise dos crimes virtuais e seus sujeitos.

2.1 Surgimento e evolução da informática e breves considerações a respeito da internet como instrumento de comunicação

Para a realização de suas tarefas o homem sempre recorreu ao um conjunto de objetos ou técnicas que mediavam sua relação com a natureza. Nesse sentido, paralelamente à mecânica e a energia, o homem buscou aprimorar tecnologias inteligentes que lhes permitisse a manipulação das informações. Primeiramente, a escrita representou ao poder estatal das grandes civilizações um controle sobre a administração de seus domínios territoriais, mas somente o desenvolvimento científico possibilitou a universalização da informação com a criação da informática.[1]

Inicialmente o desenvolvimento dos computadores sofreu influências da cibernética, ciência voltada para o estudo das relações entre máquinas e seres vivos, já que para a realização de seu trabalho o homem não dispunha mais de simples ferramentas, mas sim de máquinas sofisticadas que superavam a capacidade intelectual.[2]

Assim, o advento da informática pode ser explicado através de condições de ordem técnica, social e ideológica. A informática, portanto é a ciência de produção, armazenamento e distribuição de informação dada através de um código binário ou *bits.* Introduzido pelo pesquisador Claude Shannon, o termo *bit* serve para designar

---

[1] FRANCO, Marcelo Araujo. Ensaios Sobre as Tecnologias Digitais da Inteligência. São Paulo: Editora Papirus, 1997, p. 90/91.
[2] LEMOS, André. Cibercultura: Tecnologia e Vida Social na Cultura Contemporânea. Porto Alegre: Sulina, 210, p. 101-102.

a quantidade mínima da informação e quantos *bits* eram necessários para transmiti-la.[3]

Dessa forma, o computador é uma máquina formada por um sistema eletrônico apto a receber instruções, chamado de *hardware*, conforme uma série de programas nele contidos, os softwares. Portanto, os sistemas dos computadores são formados por dispositivos físicos interconectados, os quais são comandados por dispositivos lógicos.[4]

Através desses dispositivos o computador moderno é capaz de receber, armazenar e criar informações de forma rápida e com grande precisão. Motivo pelo qual, os computadores foram ligeiramente incorporados às diversas atividades cotidianas, passando a ser instrumento indispensável à sociedade moderna.

Contudo, para se chegar ao computador foi necessário aprimorar a tecnologia usada nessas máquinas, uma vez que o uso dos primeiros computadores estava atrelado basicamente à realização de cálculos aritméticos. Por isso, a expressão computador, *"computer"*, aquele que conta, ou ainda *"ordinateur"*, aquele que põe ordem, classifica.[5]

Na verdade, a ideia de programa de computador como conhecemos hoje, surgiu com as pesquisas do matemático Von Neumann, o qual se baseou na programação por algoritimos desenvolvido pelo estudioso Alan Turing, que havia desenvolvido uma máquina que deveria resolver problemas formulados em termos de algoritimos. A calculadora de Turing abriu caminho para a construção de máquinas que realizariam o processamento automático de informações.[6]

Além disso, os primeiros computadores a ser fabricados destinavam-se apenas ao uso militar, científico ou de engenharia, tomamos como exemplo o Eniac. Sendo que o marco inicial dos computadores produzidos com cunho comercial deu-se entre os anos de 1951 a 1958, a partir de uma versão modificada do Eniac,

---

[3] FRANCO, Marcelo Araujo. Ensaios Sobre as Tecnologias Digitais da Inteligência. São Paulo: Editora Papirus, 1997, p. 21.
[4]VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 23.
[5] LEMOS, André. Cibercultura: Tecnologia e Vida Social na Cultura Contemporânea. Porto Alegre: Sulina, 210, p. 103.
[6] FRANCO, Marcelo Araujo. Ensaios Sobre as Tecnologias Digitais da Inteligência. São Paulo: Editora Papirus, 1997, p. 22.

batizado pelo nome de Univac. Iniciava-se, assim a primeira geração dos computadores, os quais eram compostos por válvulas a vácuo.[7]

As válvulas a vácuo eram componentes internos do computador e se assemelhavam a lâmpadas, sendo necessário muitas dessas para o funcionamento da máquina. Ocorre que essas válvulas produziam muito calor e queimavam com frequência causando diversos problemas e dificultando o uso do computador, além de consumiam muita energia.[8]

Posteriormente, no ano de 1947 os cientistas John Bardeen, Walter H. Brattain e William Shockley desenvolveram um pequeno dispositivo que transfere sinais eletrônicos através de um resistor, o qual fora denominado de transistor, sendo este, posteriormente aplicado em diversos equipamentos eletrônicos, entre eles o computador.[9]

Assim, a segunda geração dos computadores deu-se entre os anos de 1959 a 1964, já adaptados ao uso do transistor, equipamento proporcionou inúmeras vantagens, já que os transistores eram menores que as válvulas a vácuo e consequentemente consumiam menos energia e geravam menos calor.[10]

Outra grande transformação foi o desenvolvimento da linguagem simbólica, a qual proporcionou mudanças na programação da máquina, já que durante a primeira geração a linguagem usada para programar os computadores baseava-se unicamente em números, necessitando de muito tempo para sua realização.

Durante esse período, os computadores eram usados basicamente para fins comerciais, em universidades e organizações governamentais. Ainda não havia a comercialização do computador com o objetivo de atingir o público em geral, tal máquina ainda não estava direcionada a realização de atividades domésticas.

Por fim, a terceira geração dos computadores teve inicio no ano de 1965, estendendo-se até o ano de 1970, quando o sistema de circuito integrado, um circuito eletrônico completo, formado por uma substância cristalina conhecida como silício, capaz de conduzir corrente elétrica, passou a substituir o uso dos transistores. Dessa forma, o uso dos chips de silício foi considerado um avanço em

---

[7] CAPRON, H. L.; JOHNSON, J. A., Introdução à Informática. São Paulo: Pearson Prentice Hall, 2004, p. 260.
[8] CAPRON, H. L.; JOHNSON, J. A., Introdução à Informática. São Paulo: Pearson Prentice Hall, 2004, p. 260.
[9] CAPRON, H. L.; JOHNSON, J. A., Introdução à Informática. São Paulo: Pearson Prentice Hall, 2004, p. 261.
[10] CAPRON, H. L.; JOHNSON, J. A., Introdução à Informática. São Paulo: Pearson Prentice Hall, 2004, p. 261.

termos de geração, pois possibilitou desenvolver sistemas mais confiáveis, assim como reduzir o tamanho da máquina o que acarretou a baixa dos custos de produção.[11]

Nota-se que em um curto espaço de tempo a informática transformou-se rapidamente, sendo que a cada nova geração ocorria o desenvolvimento de sistemas mais baratos e ao mesmo tempo mais sofisticados com maior capacidade de assimilação de tarefas. Ao longo do tempo o computador passou de uma simples máquina de calcular para um sistema complexo, apto a facilitar as atividades humanas.

Tem-se também a chamada quarta geração, a qual iniciou por volta do ano de 1971 estendendo-se até os dias atuais. A quarta geração foi uma expansão da terceira geração, já que nesta haviam sido desenvolvidos chips especializados para memória e lógica de computador, permitindo assim, o avanço tecnológico da informatização.[12]

Esse progresso tecnológico deu origem ao primeiro processador de uso geral em apenas um chip, denominado microprocessador. Computadores menores, com apenas um único chip, com capacidade de armazenamento e de resolução de tarefas muito maior que seus gigantes antepassados.

O primeiro computador de uso pessoal disponível ao público foi produzido no ano de 1975, chamado de MITS Altair, era uma máquina composta por chaves e botões, embora ainda não possuísse o teclado e a tela. Posteriormente, Steve Jobs e Steve Wozniak projetaram o primeiro computador Apple para uso doméstico, sendo o primeiro a oferecer teclado e tela, conhecido por Aplle I.[13]

Dessa forma, a indústria da informática ganhou cada vez mais espaço, a companhia Aplle criou e inseriu no mercado o modelo Aplle II, versão modificada do modelo Aplle I. Também, a empresa IBM, no ano de 1981 revolucionou o mercado da informática apresentando um computador com 80 caracteres, teclado com letras maiúsculas e minúsculas, além da possibilidade de acrescentar memória. Contudo, o

---

[11] CAPRON, H. L.; JOHNSON, J. A., Introdução à Informática. São Paulo: Pearson Prentice Hall, 2004, p. 262.
[12] CAPRON, H. L.; JOHNSON, J. A., Introdução à Informática. São Paulo: Pearson Prentice Hall, 2004, p. 262.
[13] CAPRON, H. L.; JOHNSON, J. A., Introdução à Informática. São Paulo: Pearson Prentice Hall, 2004, p. 262/263.

grande destaque da indústria da informática foi a Microsoft Corporation, que ofereceu um sistema operacional sofisticado denominado de Windows.[14]

No Brasil, o primeiro computador foi produzido pela Universidade de São Paulo (USP) em parceria com a PUC do Rio de Janeiro, a partir do projeto G-10, visando à criação de *hardwares* e *softwares* para o uso exclusivo da Marinha.[15]

Cabe salientar, que atualmente estão disponíveis no mercado diversos equipamentos eletrônicos dotados de sistemas computacionais, desde equipamentos para uso pessoal como *smartphones, tablets*, até equipamentos para indústria, área da saúde, dentre outros.

Por fim, a grande revolução da informática ocorreu ao final do século XX, quando se expandiu a conectividade desses sistemas por meio de uma rede mundialmente interligada, conhecida por internet, a qual possibilitou a constante troca de informações entre os usuários interligados pelo sistema.[16]

Todavia, assim como o computador a internet surgiu durante a Segunda Guerra Mundial, a partir de um investimento militar realizado pelo Departamento de Defesa dos Estados Unidos, com o intuito de dar uma resposta ao programa *Sputnik,* da então, extinta União Soviética.[17]

Frisa-se que inicialmente a internet fora denominada de Arpanet, em virtude de ter sido desenvolvida pela Arpa (*Advenced Research Projects Agency*), agência americana responsável pela primeira transmissão de dados entre computadores. Somente em 1969, a Arpanet, até então de domínio militar passou a ser usada nas universidades, esse foi o marco inicial para que a internet se propagasse, tornando-se um instrumento global de comunicação.[18]

Em relação ao Brasil, a história da internet remota ao ano de 1988, tendo como precursores o Laboratório Nacional da Computação Cientifica do CNPQ e a Fapesp. No mesmo ano, o Laboratório Nacional da Computação Cientifica do CNPQ conseguiu o acesso a uma rede americana de computadores denominada de Bitnet.

---

[14] CAPRON, H. L.; JOHNSON, J. A., Introdução à Informática. São Paulo: Pearson Prentice Hall, 2004, p. 263.

[15] Surgimento da Informática. Disponível em http://www.portaleducacao.com.br/iniciacao-profissional/artigos/47410/o-surgimento-da-informatica-e-sua-chegada-ao-brasil#ixzz3qMKAE5F1, acessado em 01/11/2015.

[16] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos. Curitiba: Juruá Editora, 2010, p. 32.

[17] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos. Curitiba: Juruá Editora, 2010, p. 32

[18] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos. Curitiba: Juruá Editora, 2010, p. 33.

Posteriormente, a Fapesp efetuou a primeira conexão brasileira utilizando protocolo de comunicação, permitindo a troca de informações entre computadores.[19]

Mas, somente no ano de 1995, a partir da criação e instituição do Comitê Gestor da Internet/BR, órgão responsável por coordenar e incentivar a implantação da internet no país é que ocorreu a liberação da internet com fins comerciais, atingindo o público em geral.

Salienta-se que a globalização da internet deu-se pela sua capacidade de transcender o mundo material, não se atribuindo como elemento fundamental a presença física, permitindo que fossem criadas comunidades *on-line*, das quais o internauta poderá participar onde quer que esteja, desde que conectado a internet, sendo que a interatividade do individuo com os demais membros da comunidade *on-line* ocorre mediante mensagens de textos e imagens.[20]

Ademais, a internet possibilitou ao internauta a criação de uma realidade virtual, distinta do mundo físico, acessível a um simples toque. É como se fosse possível estar presente e ao mesmo tempo ausente em diversos lugares, pois a internet facilita a comunicação sem que haja necessidade de fazer-se presente fisicamente.

Neste sentido, cabe destacar, que a internet modificou drasticamente o comportamento das pessoas, assim como a forma de comunicação entre elas, possibilitando a interatividade de um individuo com sujeitos de diferentes culturas, nacionalidades e perfis. Em suma, a internet eliminou a distância entre as pessoas.

Neste aspecto, o posicionamento de Maciel Colli:

> O uso da internet possibilitou a superação da dificuldade ocasionada pela distância territorial e pela limitação comunicativa entre as pessoas em locais distantes. A voz e o papel foram desbancados do *ranking* instrumental de intercâmbio de mensagens. O texto exibido nas telas de computadores, produtos de linguagem binária interpretada e transmutada pelas plataformas dos computadores, elimina a distância e o tempo.[21]

---

[19] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos. Curitiba: Juruá Editora, 2010, p. 33.
[20] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos. Curitiba: Juruá Editora, 2010, p. 33.
[21] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos. Curitiba: Juruá Editora, 2010, p. 39.

No entanto, o desenvolvimento tecnológico que propiciou avanços positivos, também proporcionou aspectos negativos, permitindo que desenvolvedores se utilizassem de tal ferramenta com fins escusos, diversos do objetivo inicial, de sorte que o conhecimento da informática proporcionou ao criminoso perpetuar condutas ilícitas comuns de uma forma mais sofisticada. Dessa forma, embora os computadores e a internet sejam instrumentos voltados para finalidades positivas, muitas vezes, são usados para atividades que sendo ou não de caráter antijurídicas, acabam causando um dano ou prejuízo alheio.

2.2 Sistemas de transmissão de dados na internet.

O objetivo das redes de computadores é permitir a troca de informações entre várias máquinas que estejam conectadas entre si, sendo que tais redes são formadas por dispositivos eletrônicos com microprocessadores capazes de compartilhar dados e recursos, como impressoras e e-mails.[22]

Dessa forma, os sistemas computacionais podem ser interligados por fios, cabos, ondas de rádio, infravermelho ou via satélite. As redes locais (LAN) geralmente são usadas em residências e escritórios, enquanto que as redes de áreas ampliadas (WAN) são utilizadas para interligar redes locais.[23]

A internet, por sua vez é uma rede global que permite a conexão de sistemas informatizados em todo o planeta através do uso de protocolos, dispositivos informáticos que permitem o envio e recebimento de informações entre os computadores conectados, sendo que cada um desses sistemas recebe um endereço que os identifica.[24]

Podemos definir protocolo como uma espécie de linguagem utilizada para que os computadores estabeleçam uma conectividade e possam trocar informações e dados, já que duas máquinas, embora conectadas a mesma rede se não possuírem

---

[22] Rede de Computadores. Disponível em: https://pt.wikipedia.org/wiki/Rede_de_computadores, acesso em 24 de fevereiro de 2016.
[23] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 24.
[24] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 25.

a mesma linguagem não conseguirão realizar entre si a transmissão dos dados informatizados[25].

Assim, é necessário que cada computador que acessa a rede tenha um endereço pelo qual poderá ser localizado, sendo denominado endereço IP ou Internet Protocol. O endereço IP pode apresentar-se de forma estática ou ser dinâmico, será estático quando for atribuído um número permanente ao computador, podendo ser modificado somente por ação manual, já o dinâmico representa um número dado ao computador toda vez que ele se conecta a internet, mudando a cada nova conexão.[26]

Nesse contexto, assim como as pessoas usam documentos com expressões numéricas que as identificam e distinguem umas das outras, o endereço IP atribuído a um computador quando se conecta na rede visa efetuar um cadastramento da máquina, promovendo o registro da mesma e tornando possível a partir desse código a monitoração das atividades desenvolvidas pelo usuário.

Para tanto, os endereços IP são distribuídos por organizações competentes como a IANA (Internet Assigned Numbers Authority ou Autoridade para Atribuição de Números da Internet) e a LACNIC (Registro Regional da Internet para a Região da América Latina e Caribe), sendo que cada país pode determinar a faixa de IP que deseja utilizar, assim é possível auferir a localização de um determinado endereço de IP, pois se verifica em que faixa o IP pertence.[27]

Na verdade, cada endereço IP está vinculado a um provedor de acesso, o qual é responsável por promover o acesso de um computador a internet, fornecendo, consequentemente o número do endereço IP a máquina para que dessa forma seja possível a conexão com a rede.

Além disso, cada um desses endereços é relacionado a um nome específico que se denomina domínio, o qual foi concebido com o intuito de facilitar a memorização dos endereços de computadores na internet. Nesse aspecto, cada

---

[25] O que é TCP/IP. Disponível em: http://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-htm, acesso em 24 de fevereiro de 2016.
[26] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro: Editora Brasport, 2014, p. 86.
[27] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro: Editora Brasport, 2014, p. 87.

domínio obedece a uma hierarquia, iniciando pela direita e diminuindo progressivamente até a esquerda.[28]

Interessante notar, que o conjunto de números que formam o endereço IP é estabelecido por uma série de quatro números separados por pontos, assim a representação destes por um nome específico ou domínio permite aos usuários acessar os recursos da internet.

Tulio Viana e Felipe Machado explicam que quando o usuário digita o endereço www.dominio.com.br, por exemplo, tem-se como maior hierarquia o domínio “br”, na segunda hierarquia o domínio “com”, como terceira hierarquia a palavra “domínio” e como quarta hierarquia o “www”. Assim, quando digitado o endereço acima o navegador ira procurar na rede o servidor responsável por gerenciar o domínio br, o qual remetera ao gerenciador dos domínios .com.br, que por sua vez acionará o domínio .dominio.com.br, que por fim, indicará o endereço IP do computador www.[29]

Os domínios de maior hierarquia são identificados por duas letras que representam o código do país de origem. No Brasil usa-se o domínio br, o qual, segundo sua finalidade encontra-se subdividido em outros domínios como: com.br, usados por empresas, org.br adotado por entidades não governamentais, mon.br usado por pessoas físicas, ind.br por industrias entre outros.[30]

O TCP/IP por sua vez, é um dispositivo que une dois protocolos de comunicação de computadores em rede, sendo que a sigla TCP significa *Transmission Control Protocol,* ou seja, protocolo de controle de transmissão e o endereço IP *Internet Protocol*, ou protocolo de internet, protocolo de interconexão.[31]

O protocolo TCP/IP foi desenvolvido em 1969 pela agência americana Deparment Of Defense Advenced Research Projects Agency como um recurso para o projeto Arpanet, com o escopo de facilitar a comunicação entre um grande número de sistemas de computadores das organizações militares caso ocorresse uma guerra nuclear. Posteriormente, com a expansão do projeto Arpanet na comunidade internacional, mais precisamente no ano de 1983 ficou definido que todos os

---

[28] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 25

[29] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 25

[30] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 25-26.

[31] História do TCP/IP. Disponível em https://pt.wikpedia.org/wik/TCP/IP, acesso em 24 de fevereiro de 2016.

computadores conectados a Arpanet passariam a usar o protocolo de transmissão TCP/IP.[32]

Assim, o protocolo TCP/IP tornou-se de domínio público, o que permitiu aos fabricantes de processadores informatizados instalarem o protocolo TCP/IP aos seus sistemas operacionais de rede. Atualmente, o TCP/IP é usado em qualquer sistema operacional que tenha a capacidade de conectar-se a internet, incluindo-se celulares e handhelds.[33]

Embora, inicialmente o protocolo de comunicação TCP/IP tenha exigido muita memória e hardware em sua utilização, este oferece alguns benefícios se comparado a outros protocolos, fazendo com que desenvolvedores de sistemas operacionais buscassem evoluir os processadores de dados com o intuito de oferecê-lo em suas plataformas.[34]

Ademais, o conjunto de protocolo TCP/IP é composto por quatro camadas, aplicação, transporte, de rede e de interface, sendo que cada uma delas é responsável pela execução de tarefas distintas. Essa organização em camadas permite que os dados que são transmitidos na rede possam manter sua integridade.[35]

Na camada de aplicação ocorre o processamento dos dados e consequentemente o envio dessas informações as camadas subsequentes, nela encontram-se demais protocolos, como o SMTP, usado para envios de e-mails, FTP para realizar transferência de arquivos e o HTTP, usado para navegar na internet.[36]

Assim, uma vez que a informação contida na camada de aplicação ser codificada nos padrões de um protocolo haverá a passagem para a próxima camada, a qual se denomina camada transporte, responsável por receber os dados, verificar a integridade e dividi-los em pacotes com o posterior envio para a internet.[37]

---

[32] História do TCP/IP. Disponível em https://pt.wikipedia.org/wik/TCP/IP, acesso em 24 de fevereiro de 2016.
[33] TCP/IP. Disponível em http://www.harware.com.br/termos/tcp-ip, acesso em 24 de fevereiro de 2016.
[34] História do TCP/IP. Disponível em https://pt.wikipedia.org/wik/TCP/IP, acesso em 24 de fevereiro de 2016.
[35] O que é TCP/IP. Disponível em: http://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-htm, acesso em 24 de fevereiro de 2016.
[36] O que é TCP/IP. Disponível em: http://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-htm, acesso em 24 de fevereiro de 2016.
[37] O que é TCP/IP. Disponível em: http://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-htm, acesso em 24 de fevereiro de 2016.

Após serem encaminhados pela camada de transporte os dados são recebidos na camada de rede, onde são anexados ao endereço virtual do computador ou endereço IP do computador remetente e destinatário para serem distribuídas na internet.[38]

Por fim, os dados passam para a camada interface, responsável pelo recebimento e envio de pacotes pela rede, ela determina a rota que os dados seguirão entre o computador remetente até chegar ao computador de destino. [39]

Assim, constata-se que o protocolo TCP/IP é de suma importância, já que além de permitir a conexão com a internet e o envio de informações por meio de pacotes, permite localizar o endereço físico da máquina, com a qual foi cometido um delito em ambiente virtual.

2.3 Aspectos históricos dos crimes virtuais.

Crimes informáticos, crimes cibernéticos, cibercrimes, crimes eletrônicos, crimes virtuais ou digitais são todos termos usados para se referir as atividades delituosas praticadas através de um computador ou rede de computadores, os quais servem como as ferramentas base ou meios necessários à consecução do crime.[40]

A palavra *ciber* deriva do grego *Kubernétés* e correlato ao latim *gubernator*, sendo o prefixo *ciber* é utilizado na língua portuguesa para atribuir novos sentidos a palavras já existentes, o termo pode ser associado à arte de pilotar, de governar uma nau (máquina). Assim, a arte de governar uma máquina com um crime gera a expressão *cibercrime.*[41]

Historicamente, os primeiros indícios de delitos praticados com o uso da internet ocorreram ainda no século XX, mais precisamente por volta dos anos 60, sendo nessa época mais comum a incidência de sabotagem e manipulação dos dados do equipamento informático.

---

[38] O que é TCP/IP. Disponível em: http://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-htm, acesso em 24 de fevereiro de 2016.
[39] História do TCP/IP. Disponível em https://pt.wikpedia.org/wik/TCP/IP, acesso em 24 de fevereiro de 2016.
[40] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro: Editora Brasport, 2014, p. 3.
[41] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos. Curitiba: Juruá Editora, 2010, p. 20.

Logo após, na década de 70, ainda associado à ideia de roubo e invasão de sistemas surge à figura do *hacker*, individuo que possui conhecimento amplo e habilidade para lidar com programas de computador, mas esses indivíduos não possuíam a intenção de causar danos ou prejuízos aos usuários do dispositivo informático que foi invadido.[42]

Nesse aspecto, Olavo José Anchieschi Gomes define *hackers* como:

> Hacker é a pessoa interessada em testar e recondicionar qualquer tipo de sistema operacional. Muitos deles são programadores e possuem alto grau de conhecimentos em sistemas operacionais e linguagem de programação. Eles descobrem falhas nos sistemas e as razões pelas quais foram detectadas. Hackers constantemente procuram por conhecimento, compartilham gratuitamente o que descobrem e nunca têm a intenção de destruir arquivos ou sistemas.[43]

Em primeiro momento os *hackers,* jovens apaixonados pela computação, pretendiam demonstrar as falhas que as redes de computadores possuíam, levando, através do envio e recebimento de simples mensagens a invasão do sistema do computador.

Para André Lemos, os *hackers* eram indivíduos que buscavam denunciar a racionalidade tecnológica, tentando de todas as maneiras desvendar os mistérios digitais e os códigos secretos. Os *hackers* foram, portanto*,* os desbravadores dos sistemas informatizados.[44]

O primeiro caso de invasão de sistemas computacionais que resultou em um processo penal ocorreu no ano de 1983, envolvendo adolescentes americanos que penetraram nos sistemas de dados da Ciments Lafarge, no Canadá. Nesta ação os adolescentes enviaram mensagens irônicas que apagaram diversos arquivos da instituição.[45]

Ressalta-se, que apesar dos *hackers* serem eméritos conhecedores de programas de computador, estes não almejavam um resultado danoso, seus objetivos não era violar, destruir ou espionar dados alheios, mas revelar as falhas da suposta segurança dos sistemas.

---

[42] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro: Editora Brasport, 2014, p. 2.
[43] GOMES, Olavo José Anchieschi. Segurança Total: Protegendo-se Contra os Hackers. São Paulo: Editora Makron, 2000, p. 24.
[44] LEMOS, André. Cibercultura: Tecnologia e Vida Social na Cultura Contemporânea. Porto Alegre: Sulina, 210, p. 204.
[45] LEMOS, André. Cibercultura: Tecnologia e Vida Social na Cultura Contemporânea. Porto Alegre: Sulina, 210, p. 207.

Além disso, que os *hackers* possuem um código de ética e conduta, propondo o compartilhamento de informações sem bagunçar ou destruir dados alheios. Sua motivação é o desafio de testar sistemas digitais, de resolver problemas técnicos. A exemplo, cita-se a ação do *Caos Computer Club,* que em 1984 desviaram 135.000 DM da Caixa Econômica de Hamburg, mas que no dia seguinte, procuraram o banco e efetuaram a devolução do dinheiro.[46]

Contudo, concomitantemente aos *hackers* surge a figura dos *crackers,* criminosos que tem por objetivo invadir os sistemas informáticos para inserir poderosos vírus que irão apagar, roubar e destruir as informações e dados contidos no computador atacado. [47]

Nesse prisma, a definição de Olavo José Anchieschi Gomes:

> Cracker é um individuo que utiliza de sua sabedoria para comprometer a segurança da rede. Muitos deles possuem alto grau de conhecimento em linguagens de programação e sistemas operacionais. Suas atividades incluem acesso não autorizado, danificar todo e qualquer tipo de sistema, espionagem etc. Geralmente tais atividades são tidas como ilegais e possuem sanções previstas em lei.[48]

Os *crackers* são considerados os verdadeiros criminosos da internet, basicamente aqueles que conseguem quebrar um sistema de segurança e o invadir. Fanáticos pelo vandalismo, muitas vezes também deixam em páginas da internet mensagens de conteúdo agressivo e racista. Assim, a diferença entre *hackers* e *crackers* é o ato criminoso, os primeiros não destroem ou roubam aleatoriamente, enquanto que os *crakers* não respeitam regras, praticam atividades ilegais por meio de um computador, possuem um instinto destrutivo particular.

Cabe mencionar, que criminosos como os *crackers* geralmente fazem uso da chamada engenharia social, um conjunto de técnicas usadas para ludibriar a vítima de forma que esta acredite na veracidade das informações prestadas pelo criminoso e execute determinada tarefa ou forneça os dados que interessem a este, vindo a sofrer algum dano ou prejuízo.[49]

---

[46] LEMOS, André. Cibercultura: Tecnologia e Vida Social na Cultura Contemporânea. Porto Alegre: Sulina, 210, p. 206-209.
[47] LEMOS, André. Cibercultura: Tecnologia e Vida Social na Cultura Contemporânea. Porto Alegre: Sulina, 210, p. 221.
[48] GOMES, Olavo José Anchieschi. Segurança Total: Protegendo-se Contra os Hackers. São Paulo: Editora Makron, 2000, p. 27.
[49] WEND, Emerson; Higor Vinicius Nogueira Jorge. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação. Rio de Janeiro: Brasport, 2013, p. 21.

A engenharia social tornou-se uma técnica de grande valor estratégico para os criminosos virtuais, já que esses sujeitos demostram muita habilidade ao desenvolver e usar mecanismos psicológicos que manipulam as vítimas, fazendo com que estas respondam ao solicitado pelo meliante, sem que haja uma análise minuciosa sobre informações pessoais a serem disponibilizadas, bem como com que finalidade essas informações serão usadas.[50]

A esse conjunto de meios ardis podemos destacar algumas características, como a *ancoragem*, consistente na vinculação de uma instituição respeitável para que a vítima acredite na informação prestada pelo criminoso; a *saliência,* que são informações que chamam a atenção da vítima com base em fatos atuais e de repercussão; e, principalmente a *manipulação das emoções* em que o delinquente usa dos sentimentos da vítima para conseguir seu objetivo.[51]

Usando essas técnicas o criminoso costuma enviar para seus alvos diversos e-mails contendo algum artifício para despertar a curiosidade destes e, por consequência convencê-los a realizar alguma atividade de seu interesse. Não raras vezes, estes e-mails possuem anexos ou *links* que redirecionam o usuário ao artefato malicioso.[52]

Dessa forma, a vítima inconscientemente, sem imaginar a situação de risco em que se encontra, acaba obedecendo ao comando do criminoso virtual, disponibilizando na falsa página informações de cunho pessoal, como senhas de contas bancárias ou números de documentos, sendo que esses dados serão automaticamente conhecidos pelo manipulador que os usará para atividades ilícitas.

Contudo, no inicio da década de 90 houve um aumento vertiginoso de usuários da internet e em decorrência disso a propagação dos mais variados delitos cometidos a partir do computador. A adequação deste as mais diversas atividades cotidianas tornou-se um campo vasto, a ser explorado por pessoas mal intencionadas.[53]

---

[50] Engenharia Social: As Técnicas de Ataque Mais Utilizadas. Disponível em http://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/ acesso em 18 de setembro de 2015.

[51] JORGE, Vinicius Nogueira; WENDT. Fraudes Eletrônicas e Engenharia Social. Revista Jurídica Consulex. n.º 386, 15 de fevereiro de 2013, p. 63.

[52] JORGE, Vinicius Nogueira; WENDT. Emerson. Fraudes Eletrônicas e Engenharia Social. Revista Jurídica Consulex. n.º 386, 15 de fevereiro de 2013, p. 63.

[53] FILHO, Adilson Paulo Prudente do Amaral. Crimes Cibernéticos. Revista Jurídica Consulex n.º 343, maio de 2011, p.37.

Hoje, é possível, através da internet acessar os mais diversos serviços, o comércio eletrônico, os serviços bancários, os programas de comunicação em tempo real, tudo ao alcance das mãos, fazendo com que situações semelhantes ao mundo real venham a incidir nas relações virtuais.

Assim, do mesmo modo em que hoje temos criminosos tradicionais andando pelas ruas a procura de possíveis vítimas, temos a figura do delinquente virtual, aquele que navegando pela internet aproveita-se da constante troca de informações entre usuários para o cometimento de crimes.[54]

Ademais, ao longo do tempo, o perfil das pessoas que praticam crimes virtuais foi mudando, hoje estamos diante de crimes meramente informatizados e outros em que o computador é o instrumento para a realização do delito. Não se exige mais o amplo conhecimento da informática, hoje qualquer pessoa conectada a internet tem o potencial de ser um cibercriminoso.

3 CLASSIFICAÇÃO DOS CRIMES VIRTUAIS E SUAS ESPÉCIES.

Neste capítulo abordaremos as condutas ilícitas praticadas por meio do computador, descrevendo as principais características de cada crime, bem como promovendo a classificação dos mesmos conforme sua forma de atuação.

3.1 Dos crimes virtuais impróprios.

Podemos descrever como crimes virtuais impróprios toda conduta ilícita nas quais o computador serviu de instrumento para o cometimento de um delito, sem, contudo, lesar a inviolabilidade do sistema de informação. Nesse caso, o computador é o mecanismo de atuação, o meio empregado para a consumação do crime já existente.[55]

Já para Emerson Wend os crimes tradicionais praticados pelo computador recebem a denominação de crimes cibernéticos abertos, já que podem ser

[54] NETO, José Matias. Criminalidade Insegurança na Rede. Revista Jurídica Consulex n.º 343, maio de 2011, p.37.
[55] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 30.

cometidos sem o uso da máquina, são aqueles abarcados pela legislação penal e que são realizados por qualquer agente, não necessitando de habilidades intelectuais. Em geral, são crimes de fácil execução, que não exigem muitos conhecimentos informáticos, os quais podem ser cometidos perfeitamente através das redes sociais, das denominadas salas de bate papo, ou ainda por qualquer página da internet.[56]

Entre os crimes virtuais impróprios podemos destacar:

Crimes contra a honra: são aqueles com previsão legal nos artigos 138, 139 e 140 todos do Código Penal, correspondendo respectivamente à calúnia, difamação e injúria. São delitos que afetam diretamente a honra subjetiva e objetiva das pessoas, sendo crimes comuns também na internet, devido ao número elevado de usuários que navegam na rede.

A honra subjetiva caracteriza-se pelo sentimento que cada pessoa nutre por seus atributos individuais, sejam eles físicos, intelectuais ou morais. Enquanto que a honra objetiva é a reputação, aquilo que os outros pensam a respeito da pessoa no que refere a esses atributos. Assim, os delitos de calúnia e difamação atingem a honra objetiva da pessoa e a injuria ofende a honra subjetiva.[57]

São condutas que podem ser praticadas por meio da internet, já que é possível através das redes sociais ou salas de bate papo em imputar falsamente um fato criminoso a alguém, atingir a reputação do agente ou ainda, atribuir qualidade negativa a honra subjetiva, aos sentimentos individuais.

Crimes contra a liberdade individual: são aqueles que ferem a liberdade legalmente garantida, consistente na faculdade de o individuo se autodeterminar, de fazer o que quiser dentro dos ditames legais.[58] Nestes, inclui-se o delito de ameaça, tipificado no artigo 147 do Código Penal, podendo ser perpetrado por ações simples, como envio de mensagens por e-mail ou publicações em páginas da internet que visem intimidar alguém.

Ainda, com relação aos crimes contra a liberdade individual, temos o crime de violação de correspondência, previsto legalmente no artigo 151 do Código Penal, sendo um tipo aplicável à interceptação e violação de e-mails, se considerarmos a

---

[56] WEND, Emerson; Higor Vinicius Nogueira Jorge. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação. Rio de Janeiro: Brasport, 2013, p. 19.
[57] JESUS, Damásio. Código Penal Anotado. São Paulo: Editora Saraiva, 2004, p. 138.
[58] Crimes contra a Liberdade Pessoal: Disponível em http://www.direitonet.com.br/guias-de-estudo/exibir/141/Crimes-contra-a-liberdade-pessoal, acesso em 06 de fevereiro de 2016.

evolução dos meios de comunicação e aplicarmos analogicamente a correspondência eletrônica, pois tal dispositivo visa proteger o sigilo das informações contidas em uma correspondência. Frisa-se que tal garantia é prevista também em nossa Carta Magna, nos termos do artigo 5º, inciso XII.[59]

Diante disso, podemos dizer que ocorre a equiparação entre a correspondência eletrônica e a tradicional, pois o bem jurídico a ser protegido nesse caso é a confidencialidade das informações a ser transmitidas, independentemente da forma em que tais informações foram remetidas ao destinatário.

Crimes patrimoniais: são aqueles que lesam o interesse econômico, atingem o conjunto de bens apreciáveis economicamente ou não que cada pessoa possui. Merecendo destaque estelionato e furto mediante fraude, previstos respectivamente nos artigos 171 e 155, § 4°, inciso II, ambos do Código Penal.

Podemos conceituar o estelionato como um crime onde o agente emprega meio enganoso para obter vantagem econômica da vítima, seja para si ou para outrem (terceira pessoa), mantendo ou induzindo esta em erro.

No estelionato empregado por meio informático, o criminoso para induzir ou manter a vítima em erro necessita conquistar a confiança desta, sendo muito comum nesses casos, o delinquente enviar e-mail a seus alvos, persuadindo-os a efetuar depósitos em dinheiro com a promessa de que após algum tempo receberão em troca vantagens financeiras, geralmente altos valores em dinheiro.[60]

Outra forma de estelionato virtual são as páginas falsas de comércio eletrônico, nas quais a vítima realiza o pagamento pelos produtos oferecidos, mas não chega a receber o bem que havia adquirido. Nesse caso, as vítimas são atraídas para páginas falsas em razão do baixo valor dos produtos se comparado às lojas mais conhecidas.[61]

Destacam-se como aspectos comuns ao delito de estelionato virtual em sites de comércio eletrônico o baixo preço das mercadorias, bem como a forma estabelecida para o pagamento dos produtos adquiridos, uma vez que geralmente é realizado a vista, através de boleto bancário ou ainda por meio de depósitos

---

[59] COIMBRA, Márcio C. A inviolabilidade dos e-mails. Disponível em https://jus.com.br/artigos/1787/a-inviolabilidade-dos-e-mails?secure=true, acesso em 06 de fevereiro de 2016.
[60] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 31.
[61] WENDT, Emerson. Compras Online e o “Estelionato Virtual”. Disponível em http://www.emersonwendt.com.br/2010/06/compras-online-e-estelionato-virtual.html, acesso em 08 de fevereiro de 2016.

bancários em contas de pessoas físicas, muitas vezes sem qualquer relação com a suposta empresa.[62]

O estelionato praticado em ambiente virtual amolda-se perfeitamente na tipificação já prevista em lei, uma vez que a conduta descrita no verbo é realizada pelo infrator, entretanto, este usa dos meios de comunicação disponíveis na internet para convencer a vítima a realizar tarefa que venha a lhe proporcionar vantagem econômica de maneira ilícita, sem manter contato pessoal com a mesma.

Quanto ao delito de furto, é plenamente possível executá-lo no meio virtual, desde que em sua modalidade qualificada pelo emprego de fraude. O furto consiste basicamente na subtração de coisa alheia móvel, para si ou para outrem, com a finalidade de apoderar-se do bem de maneira definitiva, sem que haja violência ou grave ameaça durante a realização do delito.[63]

O meio de execução empregado nesses casos é a manipulação de dados bancários do correntista, com o intuito de desviar depósitos bancários, bem como a obtenção de senhas para a manipulação de contas bancárias com o objetivo de auferir vantagem econômica com a diminuição do patrimônio da vítima que ficará em poder do criminoso.

Para tanto, o delinquente virtual usa de diversas formas para obter as informações bancárias da vítima. As técnicas mais usadas nesses casos são os envios de e-mails contendo o vírus denominado Cavalo de Troia ou Trojan, ou ainda, através do *phishing scams* que direcionam o usuário a páginas falsas de bancos ou administradoras de cartões de crédito. Assim, quando a vítima insere seus dados na pagina falsa, o criminoso os cópias para seu computador.[64]

Observa-se que estamos diante de dois delitos, um informático onde o criminoso invade o dispositivo eletrônico da vítima para obter informações e outro patrimonial, sendo que o delito informático é apenas o crime-meio para que se possa executar o delito-fim, ou seja, o furto. Dessa forma, pelo princípio da consunção o delito informático será absorvido pelo furto.

---

[62]WENDT, Emerson. Compras Online e o “Estelionato Virtual”. Disponível em http://www.emersonwendt.com.br/2010/06/compras-online-e-estelionato-virtual.html, acesso em 08 de fevereiro de 2016.

[63] Delito de furto Conceituação. Disponível em https://pt.wikipedia.org/wiki/Furto, acesso em 08 de fevereiro de 2016.

[64] WEND, Emerson; Higor Vinicius Nogueira Jorge. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação. Rio de Janeiro: Brasport, 2013, p. 92.

Para alguns doutrinadores, como Cassanti, o crime de dano previsto no artigo 163 do Código Penal é perfeitamente praticável por meio da internet, já que é possível o envio de poderosos vírus que irão atacar e destruir equipamentos informáticos.[65]

Analisando minuciosamente a questão, percebe-se que os verbos inutilizar pressupõe tornar o objeto imprestável, inútil e que deteriorar indica arruiná-lo, estragá-lo, modificar para a pior. Nesse aspecto, se considerarmos que não necessariamente deve haver contato físico entre o agente e o objeto, o crime pode ser executado virtualmente.

No entanto, para Gomes o objeto material do crime de dano é a coisa móvel ou imóvel, devendo ser necessariamente corpórea ou real, sendo danificada somente por ação física. Desse modo, segundo o doutrinador os dados do computador são propriedades intelectuais, não sendo possível punir quem destrói dados informáticos alheios, haja vista não haver previsão legal.[66]

Crimes resultantes de preconceito de raça ou cor: a Lei n.º 7.716/1989 define quais são os crimes decorrentes de discriminação religiosa, de raça, cor, etnia ou procedência nacional, estabelecendo como punição pena de até cinco anos de reclusão e multa. A internet proporciona a sensação de liberdade, como se fosse possível expressar-se mantendo tais pensamentos no anonimato, de maneira que as pessoas publicam na rede comentários, vídeos ou matérias discriminatórias, sem imaginar que podem ser punidas por esses atos.[67]

Ao analisarmos a questão tomamos ciência de que o racismo quando praticado verbalmente nem sempre será compartilhado por muitas pessoas, enquanto que na modalidade virtual tem repercussão maior. Além disso, internet também proporciona ao sujeito agir individualmente ou ainda associar-se a uma organização criminosa com o fim veicular conteúdo racista na internet.[68]

Menciona o artigo 20 da referida lei que praticar, induzir, ou incitar a discriminação ou preconceito são fatos punidos com reclusão de um a três anos e multa. Nesse sentido, é plenamente aceitável que a disseminação de conteúdo

---

[65] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro: Editora Brasport, 2014, p. 25.
[66] GOMES, Olavo José Anchieschi. Segurança Total: Protegendo-se Contra os Hackers. São Paulo: Editora Makron, 2000, p. 221.
[67] AZEVEDO, Robson Barbosa de. O Combate a Criminalidade Cibernética no Brasil.Revista Jurídica Consulex. n.º 343, maio de 2011, p. 34.
[68] WEND, Emerson; Higor Vinicius Nogueira Jorge. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação. Rio de Janeiro, Brasport: 2013, p. 101.

discriminatório na internet, seja através de e-mails, chats ou comentários pejorativos constitua o crime de racismo praticado virtualmente.

Salienta-se que o racismo é considerado crime grave, punido com reclusão, sendo, inclusive, imprescritível e inafiançável nos termos do artigo 5º, inciso XLIII da Constituição Federal[69]. Nesse interim, não ocorre à perda do direito de punir pelo estado (*jus puniend*), podendo este atuar sem limite de tempo diante da ocorrência do crime.

Crime de pornografia infantil: primeiramente há que se fazer uma breve distinção entre pedofilia e pornografia infantil, a primeira deriva do grego, simbolizando a união de duas palavras *pedo* que quer dizer infância, criança, juventude e *filia* que significa filiação, amizade ou gosto. Portanto, a pedofilia é uma perversão sexual caracterizada pela atração sexual compulsiva por crianças e adolescentes, enquanto que a pornografia infantil é a representação sexual, através de imagens eróticas de crianças ou adolescentes.[70]

Desse modo, a pornografia infantil em meio digital consiste na produção de fotos ou vídeos em que crianças e adolescentes aparecem em cenas eróticas, com a sua posterior publicação ou comercialização na internet, sem que haja qualquer forma de relação sexual entre adultos e crianças ou adolescentes.

No Brasil, a Lei n.º 11.829/2008 acrescentou vários dispositivos ao Estatuto da Criança e do Adolescente (Lei n.º 8.069/90), com o intuito de criminalizar a pornografia infantil, inclusive aquela praticada através de computadores, considerando como crime qualquer registro que contenha cenas de sexo ou imagens pornográficas com crianças e adolescentes.[71]

Trata mais especificadamente o artigo 241-A do Estatuto da Criança e do Adolescente da pornografia infantil por meio informatizado, dispondo que quem: 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

---

[69] VADEMECUM. Editora Verbo Jurídico, 8º Edição, 2012, p. 28.

[70] Glossários dos Direitos Humanos. Disponível em: http://www.safernet.org.ber/site/prevenção/glossarios/direitos-humano#pedo, acesso em 16 de fevereiro de 2016.

[71] WEND, Emerson; Higor Vinicius Nogueira Jorge. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação. Rio de Janeiro, Brasport: 2013, p. 99.

criança ou adolescente, será punido com pena de reclusão de três a seis anos e multa. [72]

Ainda, conforme o § 1º, incisos I e II do mesmo artigo, incorrem nas mesmas penalidades quem de qualquer modo assegurar os meios necessários para o armazenamento do conteúdo pornográfico, assim como assegurar ou facilitar o acesso por redes de computadores às fotografias, imagens ou cenas contendo pornografia infantil.

O artigo 241-B do mesmo dispositivo legal criminaliza a conduta de quem adquire, possui ou armazena, por qualquer meio, as fotografias, vídeos ou outras formas de registro que contenha sexo explícito ou pornográfica envolvendo criança ou adolescente, com pena de reclusão de um a quatro anos e multa.[73]

Tal norma passou a considerar como crime a simples posse de material pornográfico, vindo a punir o usuário, ou seja, aquele que adquire, possui ou armazena, ainda que em pequena quantidade imagens ou cenas eróticas com crianças e adolescentes, mesmo que o individuo não tenha o intuito de publicar, comercializar ou trocar o conteúdo pornográfico.

O artigo 241, § 1º, também elenca as causas de diminuição da pena, incluindo a pequena quantidade do material pornográfico, mas não especifica quanto vem a ser pequena quantidade. Já os § 2º e 3º apresentam os casos especiais de exclusão da tipicidade do fato, em razão de o agente praticar a conduta ilícita com o escopo de entregar tal material a autoridade competente para que esta possa apurar a existência do crime.

Frisa-se, que a falsa sensação de anonimato atribuída aos meios de comunicação informatizados representa um campo fértil para comportamentos que os indivíduos não realizariam se fosse necessário expor-se. Dessa forma, o uso da internet incentivou a pratica de crimes com enfoque sexual contra crianças e adolescentes, sendo que estes podem ser difundidos com facilidade, já que a internet proporciona ao criminoso a ampliação de seu meio de atuação.

Falsa identidade: crime previsto no artigo 307 do Código Penal consiste basicamente em atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem, punido com

[72] VADEMECUM. Editora Verbo Jurídico, 8º Edição, 2012, p. 1288.
[73] VADEMECUM. Editora Verbo Jurídico, 8º Edição, 2012, p. 1288.

detenção de três meses a um ano ou multa, se o fato não constitui elemento de crime mais grave.[74]

Em se tratando de crimes virtuais, são frequentes os casos em que indivíduos mal intencionados criam perfis falsos, ou perfis fakes, em redes sociais ou sites de relacionamentos com o intuito de enganar as vítimas ou ainda praticar delitos como ameaça ou contra a honra.[75]

Notório, que a globalização permitiu que criminosos valendo-se da velocidade em que as informações são propagadas junto à rede mundial de computadores, em razão da sensação de impunidade criassem perfis falsos para praticar atos criminosos como ameaças, difamações, calunias ou injúrias contra seus desafetos. Ou ainda, em sites de relacionamentos, com o intuito de enganar a vítima, fazendo-se passar por outra pessoa.

Cabe mencionar, que muitas vezes pedófilos usam falsos perfis na internet com o intuito de conquistar a confiança de crianças e adolescentes para obter vantagens de cunho sexual, tentando marcar encontros virtuais ou convencer a vítima a realizar fotos ou vídeos pornográficos.[76]

Apologia ao crime ou criminoso: fazer apologia significa enaltecer, elogiar, defender determinada conduta típica. Trata-se de crime de forma livre, podendo ser realizada por qualquer meio eleito pelo agente, sendo requisito necessário para a consumação do delito que a manifestação seja tornada pública, de modo a atingir várias pessoas, em local de acesso ao público.[77]

Portanto, é um tipo praticável por meio da internet, já que é possível publicar, principalmente através de redes sociais públicas como *facebook, twiter* ou ainda em sites comentários que simpatizam com a pratica de crimes ou com a figura do criminoso. Geralmente, são postados vídeos ou imagens em redes sociais, nas quais indivíduos exibem armas ou drogas, fazendo clara referência a criminosos ou facções, demonstrando apoiando e enaltecendo moralmente condutas ilícitas.[78]

---

[74] VADEMECUM. Editora Verbo Jurídico, 8º Edição, 2012, p. 549.
[75] WEND, Emerson; Higor Vinicius Nogueira Jorge. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação. Rio de Janeiro: Brasport, 2013, p. 104.
[76] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro: Editora Brasport, 2014, p. 30.
[77] NUCCI, Guilherme de Souza. Código Penal Comentado. Rio de Janeiro: Editora Forense, 2014, p. 1192-1193.
[78] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro: Editora Brasport, 2014, p. 33-34.

Induzimento, instigação ou auxílio ao suicídio: embora o suicídio não seja fato punível, prestar auxílio a este, mesmo que moralmente constitui crime tipificado no artigo 122 do Código Penal. Trata-se de delito cometido por qualquer sujeito e não exige forma especifica para seu cometimento, sendo que a conduta dolosa é a vontade de induzir, instigar ou prestar auxílio ao suicídio.[79]

Nesse sentido, a internet apresenta-se como meio para a realização do delito, já que é possível induzir ou instigar uma pessoa a efetuar tais atos através de conversas nas salas de bate papo disponíveis nas redes sociais.

Para alguns doutrinadores como Túlio Viana e Felipe Machado, delitos como favorecimento a prostituição previsto no artigo 228 do Código penal e o rufianismo tipificado no artigo 230 do Código Penal, podem ser considerados como delitos virtuais impróprios, uma vez que podem ser criadas páginas na internet com anúncios de profissionais do sexo, havendo a possibilidade de contratar tais serviços virtualmente.[80]

Se analisarmos minuciosamente os tipos penais acima referidos, perceberemos que as condutas necessárias para que haja a ocorrência de tais delitos podem ser praticadas através da internet, uma vez que qualquer cidadão, sem muitas dificuldades pode criar uma página com anúncios de tais serviços.

3.2 Dos crimes virtuais próprios.

São aqueles em que o bem jurídico protegido é a inviolabilidade dos dados informatizados, são delitos que somente podem ser praticados com a utilização de dispositivos que possam se conectar com a internet. Nestes incluem-se:

Invasão de dispositivo informático: incluído no Código Penal através da Lei n.º 12.737/2012, após polêmica envolvendo a atriz global Carolina Dickmann, a qual teve fotografias íntimas roubadas através de dispositivos eletrônicos e disponibilizadas na internet, o artigo 154-A dispõe a respeito da inviolabilidade dos sistemas de informação. Vejamos:

---

[79] NUCCI, Guilherme de Souza. Código Penal Comentado. Rio de Janeiro: Editora Forense, 2014, p. 684-685.

[80] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 31.

> 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 prefeitosII - 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;
>
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Objetiva-se com a norma proteger os sistemas informatizados e, por consequência os direitos previstos na Constituição Federal em seu artigo 5º, inciso X que versa sobre a inviolabilidade da intimidade, vida privada, a honra e imagens das pessoas, já que a conduta criminosa lesa informações de caráter sigiloso e pessoais.[81]

Assim, o objeto material do delito são os dispositivos informáticos, incluindo-se todo e qualquer equipamento que possa processar dados automaticamente, como computadores de mesa, notbook, tablet, smartphones ou quaisquer outros dispositivos similares. Sendo que as condutas típicas consistem em invadir, que supõe violar ou transgredir sistema de segurança de dispositivo informático alheio, não havendo diferenças se este esteja ou não conectado a internet, já que é possível obter ou alterar dados constantes em equipamentos desconectados e, em instalar vulnerabilidades para futura obtenção de vantagens ilícitas.[82]

---

[81] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 95.

[82] NUCCI, Guilherme de Souza. Código Penal Comentado. Rio de Janeiro: Editora Forense, 2014, p. 812.

Salienta-se que é pressuposto da consumação do delito a violação indevida de mecanismo de segurança, tais como senhas, antivírus, firewalls, de modo que, se o agente conseguir acessar o computador da vítima sem que haja qualquer violação de sistemas de segurança a conduta será atípica. [83]

Da mesma forma, a conduta deve ser realizada sem autorização expressa ou tácita do titular do dispositivo. Será expressa quando formalizada através de documento assinado ou por qualquer outro registro de manifestação de vontade, enquanto que a tácita dar-se-á por atos que demonstrem tal permissão, como fornecimento de *login* e senha para pessoas de seu convívio.[84]

Ademais, não se vislumbra o cometimento do delito na forma culposa, já que o agente pratica o ato de forma livre e consciente, objetivando o resultado final, ou seja, a obtenção, adulteração ou destruição dos dados informatizados, bem como a obtenção de vantagem ilícita com a instalação de vulnerabilidades.[85]

Criação e divulgação de programas de computador destrutivos: tal delito vem tipificado no § 1º do artigo 154-A, que dispõe a respeito de quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática de invasão de dispositivo informático, previsto no *caput*.

Trata o dispositivo legal de abranger os vírus de computador, os quais são programas desenvolvidos com o propósito de causar um dano ao computador, sendo que geralmente utilizam de ferramentas de comunicação para se espalharem pelo sistema, sendo enviados por mensagens eletrônicas ou ainda por acesso a *web sites* e arquivos infectados.[86]

O legislador pretendia ao incluir tal parágrafo punir por equiparação os atos preparatórios do crime de invasão de dispositivo informático, em virtude de que para a consumação da violação é fundamental a existência de mecanismo apto a viabilizá-la. Nesses termos, a figura típica abrange aquele que de qualquer forma,

---

[83] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 95-97.
[84] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 96.
[85] NUCCI, Guilherme de Souza. Código Penal Comentado. Rio de Janeiro: Editora Forense, 2014, p. 813.
[86] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro: Editora Brasport, 2014, p. 8.

permite o acesso a mecanismos ou programas que proporcionem a invasão de dispositivo informático alheio.[87]

Contudo, conforme leciona Nucci, as condutas descritas no § 1º do artigo 154-A, não possui sujeito passivo determinado, afinal consiste na preparação do delito previsto no *caput*, de maneira que a punição estatal volta-se a proteção da sociedade. Ora, se o sujeito passivo é a sociedade, é inviável a punição do delito, já que o artigo 154-B estipula a necessidade de representação da vítima, salvo se for cometido contra a administração pública direta ou indireta.[88]

Dessa forma, para que se possa efetivar a punição ao agente que produz, oferece, vende, distribui ou difunde dispositivo de computador destinado a pratica do delito referido no *caput,* é mister que o crime seja praticado contra a administração pública ou que ocorra a apuração conjunta com o delito do *caput* e, ainda que o sujeito passivo seja o mesmo em ambos os delitos.[89]

Nota-se que se houver a perpetração das condutas elencados no § 1º do referido dispositivo, mas não houver invasão concretizada, ou não houver nexo com uma possível invasão, inexiste quem possa oferecer representação, não sendo possível prosseguir com a persecução penal com o intuito de oferecer denúncia.

No entanto, há que se fazer uma ressalva quanto à criação e divulgação de vírus, já que a norma, nesse caso, deveria prever como elemento normativo o dolo específico no momento em que o sujeito pratica uma das condutas previstas no verbo, uma vez que poderia estar proibindo programadores bem intencionados de promover vírus com a finalidade de estudá-los.

Interceptação telemática ilegal: trata-se de delito previsto no artigo 10 da Lei n.º 9.269/1996, o qual visa garantir a inviolabilidade e o sigilo das comunicações, conforme prerrogativa do artigo 5º, inciso XII da Carta Magna de 1988, consistente no direito de liberdade de comunicação, sem que fosse lícito a outrem intrometer-se.

Vejamos o que refere tal dispositivo de lei:

> 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 2 (dois) a 4 (quatro) anos, e multa.

---

[87] NUCCI, Guilherme de Souza. Código Penal Comentado. Rio de Janeiro: Editora Forense, 2014, p. 814-815.
[88] NUCCI, Guilherme de Souza. Código Penal Comentado. Rio de Janeiro: Editora Forense, 2014, p. 815.
[89] NUCCI, Guilherme de Souza. Código Penal Comentado. Rio de Janeiro: Editora Forense, 2014, p. 815.

Analisando o tipo penal nos confrontamos com duas condutas, a primeira refere-se a realização de interceptação de comunicações telefônicas, de informática ou telemática, sem que haja autorização judicial ou com objetivos não previstos em lei, enquanto que a segunda trata-se da quebra de segredo de justiça.

No que tange a realização de interceptação telefônica, de informática ou telemática estar-se-á diante de um crime comum, praticado por qualquer sujeito, sem nenhuma condição especial, já no que diz respeito à quebra do sigilo trata-se de crime próprio, pois só pode ser cometido por quem deveria assegurar o sigilo.[90]

A nós, interessa a realização de interceptação, que nesse caso significa captar mensagem enviada por terceiro e por qualquer meio de comunicação, incluindo o informático, sem que o interlocutor tenha ciência do ocorrido. Nota-se, que durante a interceptação ilegal o agente não tem acesso direto ao sistema informático da vítima, ele apenas captura as informações enviadas entre dois dispositivos, fazendo a leitura dos dados que estão sendo transmitidos.[91]

Tal delito não possui previsão de forma culposa, já que o elemento subjetivo das figuras típicas é o dolo, consistente na vontade livre de praticar o crime, sendo que sua consumação ocorre no momento em que se inicia a interceptação dos dados, não se exigindo gravação das comunicações alheias.

Observa-se que o Código Penal Brasileiro não tipifica a conduta de interceptação ilegal, punindo apenas a divulgação, transmissão ou utilização indevida de comunicação alheia, conforme disposição do artigo 151, §1º, inciso II, já a Lei mostra-se mais abrangente, ela antecipa a conduta delitiva, considerando como crime a interceptação dos dados, independente do uso que seja dado a essas informações.[92]

No entanto, a Lei não possui o condão de revogar o disposto no Código Penal, já que tratam de objetos distintos. O objetivo da lei é regulamentar a interceptação dos meios de comunicação, segundo a qual, somente pode haver interceptação quando necessário em investigações criminais e em instrução processual penal. Nesse sentido, a interceptação de dados para fins não fundados

---

[90] CABETTE, Eduardo Luiz Santos. Interceptação telefônica. São Paulo: Editora Saraiva, 2011, p. 154.
[91] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 33.
[92] CABETTE, Eduardo Luiz Santos. Interceptação telefônica. São Paulo: Editora Saraiva, 2011, p. 153.

em ordem judicial será um crime cibernético, já que ocorre a violação de informações de terceiros.

Falsificação informática: trata-se do delito conhecido popularmente como “pirataria digital”, onde o individuo procura reproduzir ilegalmente programas de computador com fins comerciais, sem que haja autorização expressa do proprietário do *software* para a realização de tal pratica.

Dito isto, passamos a analise da Lei n.º 9.609/1998 que dispõe sobre a propriedade intelectual de programa de computador, definindo, conforme o artigo 1ª programa de computador como a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.

Nesse ponto, visa a Lei tutelar os direitos autorais e intelectuais dos criadores de *softwares* com o intuito de evitar a reprodução ou distribuição de cópias não autorizadas de programas de computador, uma vez que quando se adquire o *software* não se adquire a propriedade deste, apenas uma permissão para uso, não podendo, portanto, realizar qualquer exploração financeira como cópias para revenda ou aluguel, exceto se autorizado pelo titular.[93]

Confere também a Lei aos programas de computador, independente de registro a mesma proteção dos direitos intelectuais assegurados às obras literárias, com exceção as relativas a danos morais, ressalvado o direito do autor de reivindicar a paternidade do programa ou de opor-se a alterações não autorizadas, quando estas impliquem em modificações, mutilações que possam prejudicar sua honra ou reputação.

Assim, a chamada pirataria digital ou de *software* vem criminalizada no artigo 12 da referida lei, a qual prevê sanções para aquele que violar direitos inerentes à propriedade intelectual dos programas de computador. Vejamos:

> Art. 12. Violar direitos de autor de programa de computador:
> Pena - Detenção de seis meses a dois anos ou multa.
> § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:

[93]Propriedade Intelectual: Pirataria de Software. Disponível em: http://www.abessoftware.com.br/propriedade-intelectual/saiba-mais-sobre-pirataria-de-software, acesso em 19 de março de 2016.

> Pena - Reclusão de um a quatro anos e multa.
> § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.
> § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:
> I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;
> II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.
> § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação.

Percebe-se, que o objetivo da lei é proteger os direitos autorais de programadores ou criadores de *softwares*, culminando penas a todos que de qualquer forma possam contribuir para que ocorra violação aos programas de computador, seja através da reprodução, venda, aquisição ou ocultação com fins comerciais de programas originais ou cópias.

3.3 **Dos crimes virtuais mistos**.

São delitos em que além da inviolabilidade dos dados informáticos a norma visa tutelar bem jurídico de natureza diversa, são crimes complexos que representam a fusão de dois tipos penais diferentes. Primeiramente esses delitos derivam da invasão de um dispositivo informático, mas o objetivo final é atingir outro bem jurídico.[94]

Doutrinadores como Túlio Viana e Felipe Machado defendem que a invasão de dispositivos informáticos vinculados com o sistema eleitoral constituem delitos informáticos mistos. Para tanto, citam dispositivos legais, como as Leis n.º 9.100/1995 e n.º 9.504/1997 que referem à conduta de quem invadisse os sistemas de informações ligados à urna eletrônica.[95]

Analisemos a seguir o que dispõe a Lei n.º 9.100/1995:

> Art. 67. Constitui crime eleitoral:
> (...)

[94] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 35.
[95] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012. Belo Horizonte: Editora Fórum, 2013, p. 35.

> VII obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizados pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos.
> Pena: reclusão, de um a dois anos e multa.

Após, no ano de 1997 a Lei n.º 9.504 dispôs em seu artigo 72, inciso I o seguinte:

> 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.

Observa-se que tais dispositivos são praticamente idênticos, havendo apenas uma elevação considerável no tocante a aplicação das penas e pequenas alterações no que refere à revogação da lei anterior, uma vez que a segunda não disciplina os casos em que houvesse o delito na modalidade tentada, restando, portanto, vigente de forma parcial a Lei n.º 9.100/95. Além disso, o próprio artigo 107 da Lei 9.504/97 traz o rol dos dispositivos por ela revogados, não incluindo o artigo 67 da Lei n.º 9.100/95.

Nesse aspecto, o que se discussão é segurança da urna eletrônica, já que o código fonte do programa usado no dispositivo não é aberto, sendo conhecido apenas pelo grupo de programadores responsáveis pelo desenvolvimento do *software.* Assim, se um programador se corrompesse poderia colocar em situação de risco a legitimidade de uma eleição, pois não havendo publicidade, não seria possível saber se o programa utilizado pela urna estaria funcionando sem alguma alteração.

Contudo, o Tribunal Superior Eleitoral (TSE) afirma que o processo eleitoral é totalmente inviolável, garantindo a segurança da urna eletrônica, uma vez que além do lacre físico a urna eletrônica é lacrada digitalmente através da assinatura digital que busca assegurar que o programa não será modificado intencionalmente, bem como são realizadas auditorias junto a órgãos de pesquisa para buscar encontrar vulnerabilidades.[96]

Ademais, o TSE argumenta que a urna eletrônica durante o processo eleitoral colhe os votos em *offiline,* ou seja, sem que esteja conectada a internet, evitando assim ataques remotos ao seu sistema. Dessa forma, a urna eletrônica

[96]Principais Dispositivos de Segurança da Votação Eletrônica. Disponível em: http://www.justicaeleitoral.jus.br/arquivos/tre-se-seguranca-da-urna-eletronica, acesso em 19 de março de 2016.

estaria resguardada de qualquer crime digital, já que esses geralmente ocorrem quando há interconectividade do sistema a internet.[97]

No entanto, sempre insurgem dúvidas quanto à inviolabilidade da urna eletrônica, já que todo o sistema de segurança de dispositivos informáticos pode apresentar falhas. Nesse aspecto, cabe mencionar a quebra de sigilo da urna eletrônica realizada pela Universidade de Brasília durante um teste de segurança organizado pelo TSE para aprimorar o sistema eleitoral.[98]

Durante a realização do teste a equipe do Departamento da Ciência da Computação da Universidade, sob o comando do professor Diego Aranha conseguiu identificar fragilidades no sistema de segurança da urna, sendo possível descobrir através dessas falhas a ordem cronológica em que 474 eleitores haviam votado na urna que estava sendo realizado o teste. Não foi possível identificar os eleitores, mas foi obtido o horário exato de cada voto e qual foi o candidato escolhido.[99]

Embora tal teste tenha ocorrido sob a supervisão do TSE e justamente para por em prova a confiabilidade da urna eletrônica e aprimorar seu sistema, fica evidente que é possível haver falhas na segurança do dispositivo, por isso a necessidade de constantes melhorias nos sistemas desses equipamentos, com o objetivo de evitar que possam ocorrer alterações nos dispositivos eletrônicos das máquinas e a manipulação do resultado eleitoral.

4 ASPECTOS PENAIS E PROCESSUAIS DOS CRIMES VIRTUAIS NO DIREITO NACIONAL E INTERNACIONAL.

Neste último capítulo serão trabalhados os aspectos penais e processuais dos crimes virtuais, observando o posicionamento internacional a cerca de delitos

[97]Principais Dispositivos de Segurança da Votação Eletrônica. Disponível em: http://www.justicaeleitoral.jus.br/arquivos/tre-se-seguranca-da-urna-eletronica, acesso em 19 de março de 2016.
[98]UNB quebra sigilo de urna eletrônica em testes organizados pelo TSE. Disponível em: http://www.unb.br/noticias/print_email/imprimir.php?u=http://www.unb.br/noticias/unbagencia/unbagencia.php?id=6375, acesso em 19 de março de 2016.
[99] UNB quebra sigilo de urna eletrônica em testes organizados pelo TSE. Disponível em: http://www.unb.br/noticias/print_email/imprimir.php?u=http://www.unb.br/noticias/unbagencia/unbagencia.php?id=6375, acesso em 19 de março de 2016.

dessa natureza, bem como a legislação nacional a respeito do assunto, fazendo uma analise critica da falta de normatização uniforme do ambiente virtual.

Por fim, analisaremos brevemente as consequências que a carência legislativa influencia na obtenção probatória, uma vez que os delitos praticados com o uso da internet podem ser executados em um determinado local e sua consumação ocorrer em outro e a necessidade da cooperação entre países nas investigações desses delitos.

4.1 Legislação nacional em relação aos crimes virtuais.

O direito penal tem por objetivo regular as relações humanas que sejam contrarias aos valores indispensáveis a organização do corpo social. Desse modo, as condutas que tenham potencial de lesar ou que violem um bem jurídico protegido pela norma sofrerão repressão na esfera penal através de uma sanção previamente especificada em um aparato normativo. Nesse sentido, o direito penal encontra-se vinculado com as relações existentes no meio digital, já que estas são entre indivíduos e, consequentemente devem ser disciplinadas para evitar o uso indevido dessas tecnologias.

No ordenamento jurídico brasileiro toda a conduta que produz resultados danosos e que contrariam os atos disciplinados na esfera penal são denominados como fatos típicos, ou seja, todas as ações ou omissões conscientes e voluntarias que previamente são criminalizadas pela lei por possuírem um potencial lesivo. Sobremaneira, quando alguém pratica um ato ainda não disciplinado pela norma, não incorre em nenhum fato típico, portanto não há como responsabilizá-lo[100].

Nesse sentido, a Constituição Federal de 1988 assegura em seu artigo 5º, inciso XXXIX que “não há crime sem lei anterior que o defina, nem pena sem previa cominação legal”. Portanto, para que seja possível punir os crimes praticados através das mídias digitais, faz-se mister que as ações decorrentes desses dispositivos sejam compreendidas por um tipo penal já existente, ou ainda, no caso

[100] STEFAM, André. Direito Penal Parte Geral: São Paulo, Editora Saraiva, ano 2010, p. 159.

de lacunas que por ventura ainda existem, sejam estas preenchidas, incorporando-se conceitos de informática em seu texto normativo.

Ao passo que analisamos os delitos virtuais, tomamos consciência que muitas das condutas ilícitas praticadas em ambiente virtual já estão abrangidas pela legislação pátria, o que as diferencia como uma nova criminalidade e a sua forma de execução, ou seu *modus operandi*, já que são realizadas através da internet e geralmente por pessoas que tenham notável conhecimento em informática. A dificuldade que se apresenta nesse ponto é como compreender e proteger de forma eficaz direitos existentes em um mundo imaterial.[101]

Embora, ainda não exista legislação que compreenda a matéria como um todo, em nosso país há normas que disciplinam diversas situações decorrentes do ambiente virtual, de sorte que a maioria dos crimes cometidos através da internet são compreendidos por leis esparsas já em vigor.[102]

Além, para outras situações peculiares ao ambiente informático há diversos Projetos de Lei que objetivam garantir a segurança dos usuários da rede mundial de computadores, reprimindo as praticas ilícitas que possam ser cometidas nesse espaço ainda não totalmente conhecido pelos juristas.

Há, contudo, aqueles que afirmam que a inexistência de regulamentação especifica em relação aos crimes cibernéticos dificulta a investigação criminal de delitos dessa natureza, de forma que na falta de previsão legal muitos bens jurídicos relevantes continuam desprotegidos, sobretudo em relação aos delitos virtuais próprios, já que muitas das violações aos dados informatizados dos sistemas computacionais ainda não se encontram tipificadas.[103]

Segundo essa corrente, no que refere aos delitos virtuais impróprios, embora, a estes sejam aplicadas por analogia normas penais vigentes, não se pode olvidar que a falta de regulamentação própria produza controvérsias doutrinarias e

---

[101] VAINZOF, Roni e JIMENE, Camila do Vale. Segurança no Ambiente Eletrônico e Suas Implicações Jurídicas: Revista Jurídica Consulex, Ano XV, n.º 343, 1 de maio de 2011, p. 31.
[102] VAINZOF, Roni e JIMENE, Camila do Vale. Segurança no Ambiente Eletrônico e Suas Implicações Jurídicas: Revista Jurídica Consulex, Ano XV, n.º 343, 1 de maio de 2011, p. 31.
[103] ARAS, Vladimir. O Projeto de Lei dos Cibercrimes (PLS 76/200): Critica ao Substitutivo Aprovado no Senado. Disponível em Https://blogdovladimir.files.wordpress.com/2010/01/artigo_projeto-de-lei-dos-cibercrimes-pls-76-de-2000.pdf, acesso em 19 de março de 2016.

jurisprudências a respeito da tipificação exata desses delitos.[104] A respeito, podemos citar o entendimento do Supremo Tribunal Federal em julgamento que versava sobre a tipificação correta em relação à subtração de valores depositados em instituições financeiras. Vejamos:

> CONFLITO NEGATIVO DE COMPETÊNCIA. FURTO MEDIANTE FRAUDE QUE NÃO SE CONFUNDE COM ESTELIONATO. FRAUDE ELETRÔNICA NA INTERNET. TRANSFERÊNCIA DE NUMERÁRIO DE CONTA DA CAIXA ECONÔMICA FEDERAL. CONSUMAÇÃO. SUBTRAÇÃO DO BEM. APLICAÇÃO DO ART. 70 DO CPP. PRECEDENTES DA 3.ª SEÇÃO. COMPETÊNCIA DA JUSTIÇA FEDERAL DO RIO DE JANEIRO

Versa a decisão sobre o conflito de competência, uma vez que não havia consenso em relação a qual delito se tratava, se estelionato ou furto mediante fraude. O STF ao examinar a questão entendeu que as transações bancárias para a obtenção de vantagem patrimonial caracteriza o crime do artigo 155, § 4º, inciso II do Código Penal, afastando dessa forma o enquadramento pelo delito de estelionato.

No mesmo sentido, temos o entendimento do Tribunal de Justiça do Rio Grande do Sul. Vejamos:

> CONFLITO DE JURISDIÇÃO. CRIMES CONTRA O PATRIMÔNIO. SUBTRAÇÃO DE VALORES DA CONTA CORRENTE DA VÍTIMA VIA INTERNET. FATO EM INVESTIGAÇÃO QUE CARACTERIZA FURTO MEDIANTE FRAUDE, E NÃO ESTELIONATO. Caso em que se observa a subtração de dinheiro depositado em conta bancária da vítima mediante transferência via internet, e não o emprego de ardil contra a vítima para, com a sua manutenção em erro, obtenção de vantagem ilícita. Logo, não há falar em estelionato, mas sim em furto mediante fraude, mostrando-se evidente a competência do juízo do local onde a vítima mantinha a conta corrente da qual foi subtraída a quantia em dinheiro. CONFLITO JULGADO PROCEDENTE. (Conflito de Jurisdição Nº 70050578194, Sétima Câmara Criminal, Tribunal de Justiça do RS, Relator: José Conrado Kurtz de Souza, Julgado em 29/11/2012).

Percebe-se que ambos os delitos furto mediante fraude ou estelionato quando praticados por meio eletrônico mantem certas semelhanças, fazendo com que houvesse dúvidas em relação ao enquadramento típico do fato, sendo necessário que os tribunais realizassem minuciosa analise quanto a conduta realizada pelo agente.

No entanto, é pacifico que o legislador brasileiro tem buscado se antever e promover a normatização do uso da internet em nosso país, uma vez que uma das

---

[104] ARAS, Vladimir. O Projeto de Lei dos Cibercrimes (PLS 76/200): Critica ao Substitutivo Aprovado no Senado. Disponível em Https://blogdovladimir.files.wordpress.com/2010/01/artigo_projeto-de-lei-dos-cibercrimes-pls-76-de-2000.pdf, acesso em 19 de março de 2016.

primeiras normatizações a respeito do tema surgiu com o advento do Plano Nacional de Informática e Automação, a Lei 7.232/84 que versava sobre os objetivos e diretrizes da Politica Nacional da Informática e instituía o Conselho Nacional de Informática e Automação, (Conin).

Em seguida, surgiu a Lei 9.609/98, sendo a primeira a disciplinar questões relacionadas ao uso indevido dos meios informatizados, criminalizando condutas decorrentes de reproduções ilegais de programas de computador com o fim de obter vantagem econômica, lesando os direitos autorais do programador responsável pelo desenvolvimento da tecnologia.

Posteriormente, muitos outros Projetos de Leis foram propostos com o intuito de normatizar situações advindas do uso da internet no país. Nesse sentido, destacamos o Projeto de Lei n.° 84/99, o qual alterou ou incorporou ao Código Penal Brasileiro alguns tipos penais que tratam de delitos promovidos por meio da internet.

Também tramitou no Senado o Projeto de Lei 89/2003, de autoria do Senador Eduardo Azeredo, em substituição ao projeto apresentado pelo senador Luiz Piauhylino. Sendo aprovado no ano de 2008, o projeto versa sobre os crimes cometidos através da internet, modificando diplomas legais como o Código Penal, Código Penal Militar, Estatuto da Criança e Adolescente, criando novos tipos penais em consonância com os parâmetros estabelecidos pelo Conselho da Europa em relação à matéria.[105]

Tal Projeto de Lei buscou incorporar novas condutas ilícitas a legislação já existente, criando treze tipos penais, dentre eles podemos destacar a disseminação de vírus, o racismo e a pedofilia praticados através da internet, as clonagens de cartões de crédito e de aparelhos celulares, o roubo de senhas e de dados pessoais. Além disso, a proposta determina que os provedores de acesso a internet mantenham sob sua guarda dados de conexão como data, hora e endereço eletrônico do acesso, visando transformar o provedor em um colaborador, uma vez que essas informações são necessárias a apuração da autoria delitiva durante uma investigação criminal que tenha por objeto crimes virtuais.[106]

---

[105] NETO, José Matias. Cibercriminalidade: Insegurança na Rede. Revista Jurídica Consulex, Ano XV, n.º 343, 1 de maio de 2011, p. 29.
[106] NETO, José Matias. Cibercriminalidade: Insegurança na Rede. Revista Jurídica Consulex, Ano XV, n.º 343, 1 de maio de 2011, p. 28-29.

Ademais, o Projeto de Lei adequou outras condutas aos tipos penais já existentes, prevendo o estelionato eletrônico, o qual consiste em roubar senhas através de mensagens contendo *phisching scam,* a destruição, inutilização e deterioração de dados e dispositivos informáticos como crime de dano, a difusão e inserção de códigos maliciosos ou vírus, a inserção de código malicioso seguido de dano, as falsificações de dados de documentos eletrônicos públicos ou particulares, bem como a interrupção de serviço telegráfico, telefônico, informático, telemático de dispositivos de comunicação através de sistemas informatizados.[107]

Contudo, embora o legislador tenha tido por objetivo estabelecer meios de combater essas espécies de delitos, se observa a falta de conhecimentos técnicos e específicos a respeito do assunto, já que não a referência a termos técnicos utilizados por especialistas da área. Essa imprecisão técnica se torna mais evidente quando da simples leitura dos dispositivos, principalmente no que concerne a restrição aos provedores da internet, sem, contudo mencionar os servidores.

Além disso, se considerarmos a gravidades das lesões ao bem jurídico atingido por um crime virtual, as penas cominadas nesse dispositivo de lei são absolutamente ínfimas, sendo alguns crimes de competência do Juizado Especial Criminal, procedimento que é inviável frente a complexidade da produção probatória necessária a elucidação desse tipo de delito,

Ademais, em 24 de agosto de 2011 a então presidente Dilma Rousseff encaminhou ao Congresso Nacional o Projeto de Lei n.º 2.126/11, o qual visa estabelecer o marco civil da internet no Brasil, estabelecendo princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.[108]

Vindo a ser aprovado no ano de 2014, o projeto regulamentou questões importantes a respeito das relações entre usuários da internet e servidores de acesso, sendo inclusive reconhecido pela ONU como projeto exemplo para o resto do mundo. Além disso, regulamentou os serviços prestados pelos servidores da

---

[107] NETO, José Matias. Cibercriminalidade: Insegurança na Rede. Revista Jurídica Consulex, Ano XV, n.º 343, 1 de maio de 2011, p. 29.

[108] MOREIRA, Fabio Lucas. Da “Sociedade Informática” de Adam Schaff ao Estabelecimento dos Fundamentos e Princípios do Marco Civil da Internet (PL 2.126/2011): Porto Alegre. Livraria do Advogado Editora, 2012, p. 22.

internet, estipulando o fornecimento com segurança e garantia de funcionalidade, concedendo importantes meios de proteção ao consumidor.[109]

No entanto, o que se observa com o citado Projeto de Lei é que o legislador vislumbrou como disciplinar as relações civis dos usuários da internet e a atuação dos provedores de acesso, ficando evidente que não há em seu bojo a fixação de norma penal, motivo pelo qual a unificação dos projetos de leis anteriormente analisados representasse uma solução adequada para maior controle estatal frente aos delitos da internet.

Ademais, se observa que em nosso ordenamento jurídico não possuímos uma legislação específica em relação ao tema, mas tão somente leis esparsas, que tentam solucionar alguns delitos, assim como a aplicação a essas condutas dos crimes previstos no Código Penal, ficando evidente a necessidade de legislação própria para os cibercrimes.

4.2 Legislação internacional em relação aos crimes virtuais.

Todas as atividades desenvolvidas em sociedade necessitam de regulamentação que venham a prevenir e/ou resolver os litígios surgidos dos divergentes anseios socias. A internet seria, portanto, um novo mundo, onde as leis dos Estados não se aplicariam, sendo necessário desenvolver uma nova legislação para compor os problemas decorrentes das relações pessoais no ciberespaço.[110]

Embora as condutas ilícitas sejam executadas através de um meio digital, seus efeitos são verificáveis no mundo real, pois é induvidoso que a lesão ocorra no país ou nos países em que a vítima vive e não apenas no espaço digital, já que o criminoso embora execute os atos necessários à consumação do delito por meio da internet, as consequências vão incidir no mundo real.[111]

---

[109] MOREIRA, Fabio Lucas. Da “Sociedade Informática” de Adam Schaff ao Estabelecimento dos Fundamentos e Princípios do Marco Civil da Internet (PL 2.126/2011): Porto Alegre. Livraria do Advogado Editora, 2012, p. 23.

[110] FURTADO, Roberto Wilson. Dano Transnacional e Internet. Direito Aplicável e Competência Internacional: Curitiba, Editora Jaruá, 2010, p. 21

[111] FURTADO, Roberto Wilson. Dano Transnacional e Internet. Direito Aplicável e Competência Internacional: Curitiba, Editora Jaruá, 2010, p. 21.

Preocupados com o crescimento dos delitos praticados com o uso de dispositivos informáticos, os quais, inclusive podem causar danos transnacionais, muitos países tem buscado adaptar essas novas situações conflituosas a seus ordenamentos jurídicos, ou ainda criar regras específicas para regulamentar os problemas que possam surgir a partir dessa nova tecnologia.

Após sofrerem grandes prejuízos com o ataque de um vírus desenvolvido por Robert Tappans Morris, um estudante que visava demonstrar falhas de segurança, os Estados Unidos foi um dos primeiros países a buscar tipificar e punir penalmente problemas surgidos com o uso da internet. Nesse sentido, cabe lembrar que nos Estados Unidos cada estado tem liberdade legislativa, assim, o combate a criminalidade deu-se através de leis estaduais e federais. [112]

No âmbito federal podemos destacar as seguintes disposições legislativas: a Lei de Proteção aos Sistemas Computacionais (Federal Computer System Protection Act Of 1981), que visa coibir fraudes, furtos ou espécies de apropriação indébita. No ano seguinte, surgiu uma lei que versa sobre transferências eletrônicas e de fundos, (Eletronic Funds Transfer Act 1982). Por fim, em 1986 criou-se a Lei de Fraude e de Abuso Computacional, que busca proteger a acessibilidade dos sistemas para obtenção de segredos nacionais com o objetivo de obter vantagens econômicas.[113]

A França embora não apresente legislação especifica para tratar de delitos decorrentes da internet, em 1988 elaborou a Lei n.° 88-19 que efetuou algumas alterações no Código Penal, acrescentando um capítulo especial, que versa sobre alguns delitos informáticos, incriminando o acesso fraudulento a sistema de elaboração de dados, sendo considerados como crime tanto o acesso quanto manter-se ilegalmente no sistema, sendo que a pena é aumentada caso haja supressão ou modificação de dados, ou ainda alteração no funcionamento do sistema, a sabotagem informática, que pune a conduta de quem apaga ou falsifica o funcionamento de sistema eletrônico, a destruição de dados, responsabilizando aquele que introduz, suprime ou modifica dados, a falsificação de documentos

[112]SILVA, Ana Karolina. Internet e Informática. Disponível em http://www.ambito-jurídico.com.br/site/index.php/?n link=revistaartigosleitura&artigo id=12778&revistacaderno=17, acesso em 25 de fevereiro de 2016.
[113]SILVA, Ana Karolina. Internet e Informática. Disponível em http://www.ambito-jurídico.com.br/site/index.php/?n link=revistaartigosleitura&artigo id=12778&revistacaderno=17, acesso em 25 de fevereiro de 2016.

informatizados com a intenção de causar prejuízos a outrem, bem como aquele que utiliza os referidos documentos.[114]

A Alemanha editou em 1986 a Lei de Combate a Criminalidade Econômica, a qual traz em seu texto normas que disciplinam alguns crimes virtuais, não havendo previsão legal para casos em que ocorrerem simples invasões aos sistemas informatizados. Há, contudo, previsão de delitos de maior gravidade como espionagem de dados, extorsão informática, falsificação de elementos probatórios, sabotagem informática e alterações de dados.[115]

O direito penal italiano também possui previsão para delitos praticados no âmbito da internet, sendo que o título que tutela a inviolabilidade de domicilio faz referência no artigo 615 para o acesso abusivo ao sistema informático ou telemático. Também, no artigo 617 o código penal italiano é punível a conduta de instalação de equipamentos com o fim de interceptação, interrupção ou até mesmo de impedimento ilícito de comunicação informática.[116]

Nota-se que o Código Penal Italiano preocupou-se em penalizar condutas que venham a violar o funcionamento de sistemas informáticos ou telemáticos, reconhecendo a necessidade de adaptar a seus dispositivos legais já vigentes as fraudes realizadas através do uso da internet.

O Japão possui sistema jurídico baseado no modelo da Civil Law de tradição europeia, mas possui influencia anglo-americana, principalmente no que concerne o sistema de revisão judicial dos atos legislativos pela suprema corte. Em relação aos delitos virtuais o Código Penal Japonês incorporou alguns dispositivos que tipificam fraudes como a sabotagem informática e a interferência em sistemas.[117]

A Argentina possui sistema jurídico de natureza híbrida, sendo adepta a institutos da Civil Law e da Common Law, sendo a administração da justiça exercida

---

[114]SILVA, Ana Karolina Internet e Informática. Disponível em http://www.ambito-jurídico.com.br/site/index.php/?n link=revistaartigosleitura&artigo id=12778&revistacaderno=17, acesso em 25 de fevereiro de 2016.
[115]SILVA, Ana Karolina. Internet e Informática. Disponível em http://www.ambito-jurídico.com.br/site/index.php/?n link=revistaartigosleitura&artigo id=12778&revistacaderno=17, acesso em 25 de fevereiro de 2016.
[116]SILVA, Ana Karolina. Internet e Informática. Disponível em http://www.ambito-jurídico.com.br/site/index.php/?n link=revistaartigosleitura&artigo id=12778&revistacaderno=17, acesso em 25 de fevereiro de 2016.
[117] WEND, Emerson; Higor Vinicius Nogueira Jorge. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação: Rio de Janeiro, Brasport, 2013, p. 313.

de maneira concorrente entre o Poder Judiciário do país e pelos Poderes Judiciários exercidos pelas províncias. Em relação aos delitos virtuais a Argentina também aderiu as Convenções Internacionais, como a Lei de Cooperação Internacional em Matéria Penal e ao Protocolo de Assistência Jurídica Mútua em Assuntos Penais do Mercosul.[118]

Em relação à legislação a Argentina dispõe em seu Código Penal dispositivos que punem crimes virtuais dentre eles merecem destaque a incriminação de mensagens que contenham conteúdo pornográfico, o acesso não autorizado aos sistemas informáticos, a publicidade de informações, inclusive as obtidas através de mensagens eletrônicas, desde que causem prejuízos a terceiros e a punição aquele que abre ou se apropria, sem autorização de comunicação eletrônica.[119]

Os países que fazem parte do Reino Unido possuem sistemas jurídicos regidos pelo princípio da Common Law, sendo a lei estabelecida por precedentes jurídicos, tendo como principal fonte legal a jurisprudência, seguindo também o posicionamento doutrinário, mas cada membro possui sua própria legislação. [120]

Na Espanha o sistema judiciário é composto pela jurisdição penal, trabalhista, militar, civil e contencioso administrativo, sendo orientado pelo sistema da Civil Law, baseado em leis codificadas e no direito romano. O código penal espanhol também incrimina condutas como interceptar telecomunicações, criminalizando condutas como apoderar-se de mensagens, incluindo as eletrônicas com o intuito de descobrir ou violar intimidade de outrem. Também prevê o direito penal espanhol punição para a fraude informática e o estelionato cometido com o uso da tecnologia eletrônica.[121]

Portugal também criminaliza condutas ilícitas cometidas através de dispositivos eletrônicos como as que envolvem sabotagem informática, danos aos sistemas de computador, acesso ilegítimo aos sistemas de computador,

---

[118] WEND, Emerson; Higor Vinicius Nogueira Jorge. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação: Rio de Janeiro, Brasport, 2013, p. 318-319.

[119]SILVA, Ana KAROLINA. Internet e Informática. Disponível em http://www.ambito-jurídico.com.br/site/index.php/?n link=revistaartigosleitura&artigo id=12778&revistacaderno=17, acesso em 25 de fevereiro de 2016.

[120] WEND, Emerson; Higor Vinicius Nogueira Jorge. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação: Rio de Janeiro, Brasport, 2013, p. 310.

[121] WEND, Emerson; Higor Vinicius Nogueira Jorge. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação: Rio de Janeiro, Brasport, 2013, p. 333.

interceptação ilegítimas em ambiente eletrônico, a falsificação de programas de computador e a reprodução ou divulgação sem autorização de programas ou *softwares*.[122]

Nesse sentido, observa-se que a maioria dos países se mostram atentos aos crimes virtuais, buscando desenvolver um aparato normativo que busque coibir, bem como prevenir condutas ilícitas praticadas com o uso da tecnologia, sendo que muitos desses têm buscado além de legislar sobre a matéria, aderir a tratados e acordos internacionais para dar mais efetividade à apuração dos crimes cometidos nesse ambiente.

4.3 Da cooperação internacional diante da dificuldade de obter provas nos crimes digitais.

Inicialmente cabe esclarecer que o termo prova advém do Latim *probatio* e significa verificação, exame, comprovação, sendo que de tal termo deriva o verbo *probare*, ou seja, provar, demonstrar. Nesse interim, a prova é um conjunto de elementos que podem levar a conhecimento de algo, cuja finalidade é auxiliar na reconstrução de um fato passado, com o objetivo de apurar se o agente cometeu ou não a infração penal e como ocorreram os fatos.[123]

No direito penal brasileiro prova é todo elemento pelo qual se procura demonstrar a veracidade de uma alegação ou de um fato, buscando com isso, influenciar o convencimento do julgador. Portanto, no processo penal prova é tudo aquilo que é trazido pelas partes para auxiliar na elucidação de um fato e que pode influenciar na formação da convicção do juiz.

Como regra geral, quando chega ao conhecimento da autoridade policial a respeito da ocorrência de um delito, o meio mais adequado para a realização das investigações preliminares é o Inquérito Policial, no qual se busca através de um

---

[122] WEND, Emerson; Higor Vinicius Nogueira Jorge. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação: Rio de Janeiro, Brasport, 2013, p.
[123] VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012: Belo Horizonte, Editora Fórum, 2013, p. 70-71.

conjunto probatório mínimo auferir a materialidade delitiva, assim como apurar a autoria do crime.[124]

Nesse aspecto, fica evidente que a investigação criminal de delitos praticados através da internet apresenta uma série de dificuldades e restrições se comparada as investigação de delitos comuns, haja vista que a internet não possui um endereço físico, pois se trata de um conglomerado de redes, na qual milhares de computadores podem se conectar, sendo que sob essas condições o delinquente virtual não precisa usar da sua identidade real para cometer o crime.[125]

Ademais, para que se possa descobrir a autoria do crime e posteriormente vir a punir o delinquente, a policia necessita identificar primeiramente o endereço eletrônico da máquina que foi utilizada para cometer o delito, para após, conhecendo o número IP do computador proceder a localização do provedor de acesso a internet e determinar através de ordem judicial que esse forneça as informações necessárias para a identificação do autor do delito. As dificuldades se tornam maiores quando o IP identificado pertence a um computador de uso coletivo, como os disponíveis em estabelecimentos denominados *Lan House*, já que nesses casos será necessário localizar o usuário do computador no exato momento em que o delito foi cometido.[126]

Além disso, muitas vezes para o esclarecimento dos delitos virtuais é necessário a analise técnica e especifica dos dispositivos de informática. Assim, em havendo necessidade deve a autoridade policial mediante mandado judicial realizar a busca e apreensão dos equipamentos de informática para a realização de perícia por meio de profissional especializado, já que qualquer dano causado ao *hardware* ou ao *software* da máquina pode comprometer o material probatório.[127]

Outra dificuldade em relação à obtenção de provas é o caráter transnacional dos delitos cometidos com o uso da internet, já que muitas vezes o país que hospeda o provedor da internet é diverso daquele em que o delito se consumou. Dessa forma, uma da medida a ser adotada é a cooperação internacional, devendo

---

[124] SILVA, Mauricio Faria. O Procedimento Investigatório dos Crimes Praticados Pela Internet: Porto Alegre. Livraria do Advogado Editora, 2012, p. 123.
[125] SILVA, Mauricio Faria. O Procedimento Investigatório dos Crimes Praticados Pela Internet: Porto Alegre. Livraria do Advogado Editora, 2012, p. 127.
[126] SILVA, Mauricio Faria. O Procedimento Investigatório dos Crimes Praticados Pela Internet: Porto Alegre. Livraria do Advogado Editora, 2012, p. 129.
[127] SILVA, Mauricio Faria. O Procedimento Investigatório dos Crimes Praticados Pela Internet: Porto Alegre. Livraria do Advogado Editora, 2012, p. 131.

os países envolvidos na investigação de um delito virtual buscar alternativas para garantir meios para a prevenção e investigação de um cibercrime.[128]

Sob essa ótica, a dificuldade na realização de investigação de delitos virtuais que possuam repercussão transnacional consiste basicamente nas diferenças estruturais dos sistemas processuais penais dos países envolvidos, sendo que cada país adota um sistema de investigação criminal próprio, assim como uma legislação penal, sendo provável que dessas diferenças surjam divergências na forma de conduzir as investigações a respeito de um mesmo fato.[129]

Diante disso, com o escopo de facilitar a averiguação, o controle e estabelecer alternativas de prevenção aos crimes digitais, diplomas internacionais tem buscado estabelecer princípios gerais, os quais garantem a cooperação entre os países durante as investigações de um cibercrime. A Convenção de Cibercrimes de Budapeste, firmada em 23 de novembro de 2001 pelo Conselho da Europa é um bom exemplo de diploma internacional de cooperação mútua entre os países signatários, uma vez que estabelece as diretrizes que devem ser aplicadas na investigação desses delitos.[130]

Dividia em quatro capítulos a Convenção de Budapeste procurou aproximar leis nacionais de diferentes países e permitir o uso de sistemas práticos de investigação, bem como dispõe que cada Estado tome as medidas cabíveis para criminalizar condutas que lesem os sistemas de informática. Aduziu também a possibilidade de uso da tecnologia para auxiliar a colheita de prova e a identificação do autor do delito durante a investigação preliminar de um cibercrime.[131]

Percebe-se que medidas de cooperação entre países para combater delitos, principalmente de caráter virtual é sem duvida uma maneira eficaz de enfrentar essas praticas, já que muitas vezes as informações necessárias para se auferir a autoria do delito encontram-se armazenadas em um provedor estrangeiro que não possui escritório ou representação no país em que ocorreu o ilícito.

---

[128] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos: Curitiba, Juruá Editora, 2010, p. 173.
[129] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos: Curitiba, Juruá Editora, 2010, p. 173.
[130] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos: Curitiba, Juruá Editora, 2010, p. 174.
[131] FLOR, Roberto. Perspectiva Para Novos Modelos de “Investigação Tecnológica” e Proteção de Direitos Fundamentais na Era da Internet: Revista Brasileira de Ciências Criminais, Editora dos Tribunais, 2012. p. 72.

Nesse sentido, a Convenção de Budapeste editou em seu corpo normativo regras que disciplinam a atuação dos servidores e provedores da internet diante da investigação de um delito virtual, dispondo que estes órgãos devem reter pelo prazo máximo de 90 dias as informações armazenadas, quando houver uma solicitação por ordem judicial que visa apurar um cibercrime.[132]

Em especial para o Brasil, um dos diplomas internacionais de maior relevância no que diz respeito à cooperação internacional na investigação e combate aos crimes digitais é a Convenção Interamericana sobre Assistência Mútua em Matéria Penal. Conhecida popularmente como Convenção de Nassau, tal diploma visa facilitar a cooperação jurídica e administrativa em matéria penal entre os países membros da Organização dos Estados Americanos.[133]

Além disso, tal diploma legal tem por proposito procurar soluções para dirimir os problemas jurídicos, políticos e econômicos entre seus países membros, trazendo em seu bojo uma série de diretrizes que orientam os estados integrantes na busca de maior cooperação entre as partes, devendo haver assistência mútua nas investigações, processos e procedimentos em matéria penal.

Ainda, no âmbito internacional podemos citar como principal órgão de atuação investigativa em face aos delitos virtuais a Interpol. Considerada como maior órgão policial internacional, a Interpol tem garantido assistência aos diversos órgãos policiais pertencentes aos países a ela ligados, visando coibir e auxiliar na investigação de delitos que possuem caráter transnacional. Dentre as principais funções da Interpol destacamos a função de garantir a troca de informações entre órgãos policiais internacionais, bem como armazenar e fornecer essas informações, prestar suporte operacional e treinar equipes policiais.[134]

Sem duvidas, que em se tratando de delitos que transpõe as fronteiras territoriais entre países, existe a necessidade de haver entre as nações envolvidas colaboração no sentido de fornecer as informações necessárias para auxiliar nas investigações, bem como se busque através de tratados e acordo internacionais estabelecer padrões legislativos no combate e prevenção dos delitos virtuais.

---

[132] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos: Curitiba, Juruá Editora, 2010, p. 178.
[133] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos: Curitiba, Juruá Editora, 2010, p. 175.
[134] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos: Curitiba, Juruá Editora, 2010, p. 176.

Essa necessidade decorre das dificuldades de obter provas mínimas durante as investigações preliminares dos crimes cibernéticos, já que muitas vezes os dados necessários à identificação do criminoso encontram-se armazenados em provedores e servidores de internet situados fora do país. Nesse prisma, a colaboração entre países, assegurando que os provedores e servidores da internet e os órgãos policiais do local onde ocorreu o delito tem se mostrado como medida indispensável para a obtenção de evidências de materialidade e autoria.[135]

Sobre a adoção de procedimentos de armazenamento de informações em servidores e provedores da internet, mais uma vez destacamos os dispositivos legais da Convenção de Budapeste, já que as artigos 16 a 17 e 29 a 34 estabelecem uma série de orientações, as quais os países signatários do tratado devem seguir quando for necessário a colaboração investigativa entre eles. Embora tal diploma internacional não estipule prazo para o armazenamento de dados, prevê um prazo máximo de 90 dias para a retenção das informações solicitadas através de ordem judicial.[136]

Com objetivo semelhante agiu o legislador brasileiro, quando estabeleceu no projeto de Lei 89 de 2003 algumas obrigações aos provedores de acesso a internet, dispondo em seu artigo 22 a obrigatoriedade destes em reter os dados a serem utilizados em favor de eventuais investigações preliminares que envolvam crimes virtuais.

Embora, o projeto tivesse por objetivo resguardar as informações necessárias a investigação de um possível delito, o que se vislumbra na pratica é a imprecisão técnica, uma vez que se encontram dificuldades para armazenar todas as informações de acesso a internet pelos usuários de um mesmo provedor, já que o período de três anos estipulado para o armazenamento desses dados mostra-se inviável frente ao espaço que deveria ser dispendido para reter tanta informação.

Sem duvidas, que responder a essa nova criminalidade, que modifica constantemente sua forma de atuação mediante o uso de recursos disponíveis na internet, faz com que os Estados se mostrem incapazes de sozinhos conseguirem conter as condutas danosas perpetuadas pela rede mundial de computadores e que muitas vezes possuem caráter transnacional, ou seja, avançam sobre os limites

[135] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos: Curitiba, Juruá Editora, 2010, p. 177.
[136] COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos: Curitiba, Juruá Editora, 2010, p. 178.

territoriais. Diante disso, impõe-se a necessidade dos países buscarem criar uma rede global, de cooperação internacional no combate a criminalidade virtual.

CONCLUSÃO

Ao fim da pesquisa, pode-se comprovar a relevância do tema tratado, uma vez que vivemos hoje a era da informação e que em decorrência do caráter transnacional da internet, tem emergido inúmeros litígios, dos quais, muitos ainda não foram abarcados pelo direito, exigindo-se do estado à busca pela normatização do ambiente virtual.

Embora muitas das condutas típicas praticadas com o uso da internet possuam semelhanças com tipos penais já existentes, sendo possível aplicar o direito penal em vigor, há aquelas que ainda são totalmente desprovidas de previsão legal, ou que tal previsão se mostra insuficiente. Devendo, assim o estado agir de forma a regulamentar essas situações, visando disciplinar as relações decorrentes do acesso à internet.

No primeiro capítulo, procuramos fazer uma breve analise histórica do surgimento e evolução dos dispositivos de informática, bem como mencionar aspectos pertinentes a rede mundial de computadores, fazendo referência aos protocolos de comunicação, bem como ao endereço IP usados pelos computadores durante o acesso a internet.

Outrossim, ainda nesse capítulo estudou-se os primeiros crimes digitais e suas motivações, assim como o perfil dos criminosos virtuais, distinguindo-os conforme sua forma de atuação entre “*hackers e crackers*”, demonstrando as principais técnicas que usam para escolher e ludibriar as suas possíveis vítimas, o que nos leva a concluir que geralmente são pessoas inteligentes, hábeis e que possuem bom conhecimento em informática.

No segundo capítulo, buscamos apresentar as particularidades de cada delito cometido através da internet, haja vista que doutrinariamente são divididos em impróprios, próprios e mistos, sempre observando as características essenciais a forma de consumação de cada um e fazendo referência as disposições legais pertinentes.

Por fim, no terceiro capítulo realizou-se uma analise da legislação nacional e internacional a respeito dos crimes cibernéticos, buscando refletir sob o posicionamento de cada país frente a esses delitos, dando ênfase aos tratados e

acordos internacionais que funcionam como parâmetros estruturais, orientando a elaboração e aplicação da legislação. Também, buscou orientar-se através das decisões proferidas pelos nossos tribunais a cerca da tipificação dos delitos.

Discorremos também a respeito da dificuldade de obtenção de provas nos delitos virtuais e da necessidade de manter-se um clima de cooperação mútua durante a coleta de provas, já que muitos desses delitos possuem caráter transnacional e possam envolver países com legislação e meios de investigação divergentes. Nesse ponto, salientamos a importância das convenções realizadas entre países com o intuito de procurar harmonizar seus ordenamentos jurídicos, seguindo diretrizes previamente estabelecidas nesses acordos, bem como manter a cooperação investigativa diante da ocorrência de um delito que envolva mais que um país.

Diante disso, ressaltamos a importância da Convenção de Budapeste que buscou estabelecer entre os países membros formas de ajuda mútua, bem como informar princípios gerais para a confecção de normas jurídicas. Para o Brasil, demonstramos a importância da adesão a Convenção Interamericana sobre Assistência Mútua em Matéria Penal, a qual dispõe sobre a cooperação entre países americanos.

Por fim, pode-se concluir que embora o legislador brasileiro tenha aprovado projetos de leis que versem sobre os delitos virtuais, estes possuem deficiências, já que a informática é um ambiente mutante, havendo nos projetos de leis apresentados falta de conhecimentos técnicos sobre o assunto, bem como muitos desses delitos são punidos com pena inferior a lesão causada ao bem jurídico protegido pela norma, sendo muitos desses processados junto ao Juizado Especial Criminal.

Ademais, importante referir que embora alguns tipos penais, principalmente nos crimes classificados como impróprios ocorre certa similaridade com os delitos comuns, havendo aplicação de leis já existentes, a falta de regulamentação especifica para esses crimes dificulta a apuração e punição desses. O ideal nesse caso seria a criação de uma lei especifica que busca não apenas inserir novos tipos penais, mas estabelecer critérios para a utilização dessa tecnologia.

Nesse interim, ressaltamos a importância da Convenção de Budapeste, diploma internacional, cuja finalidade é fixar princípios universais de orientação aos países para a criação de normas penais que versem sobre delitos virtuais, sendo que a adesão a esse tratado representasse para o Brasil o avanço em termos legislativos, uma vez que poderia seguir os princípios nela estabelecidos e criar uma legislação harmônica e coerente com a cooperação jurídica internacional em relação a esses delitos, evidentemente desterritorializados.

Cabe salientar, que o objeto dessa reflexão é desenvolver um novo pensar sobre o direito penal, tendo em vista que as transformações trazidas pelo uso da tecnologia implicam no surgimento de uma nova criminalidade, já que os delitos consumados através da internet podem ocorrer em qualquer lugar, desde que tenha acesso a rede mundial de computadores. Nesse ponto, impera a necessidade do direito penal acompanhar essas mudanças, razão pela qual necessitamos de um ordenamento jurídico abrangente, já que no Brasil o que se observa é a criação de leis esparsas que não conseguem por si só disciplinar as situações ocorridas nesse meio.

REFERÊNCIAS

ARAS, Vladimir. O Projeto de Lei dos Cibercrimes (PLS 76/200): Critica ao SubstitutivoAprovado no Senado. Disponível em Https://blogdovladimir.files.wordpress.com/2010/01/artigo_projeto-de-lei-dos-cibercrimes-pls-76-de-2000.pdf, acesso em 19 de março de 2016.

AZEVEDO, Robson Barbosa de. O Combate a Criminalidade Cibernética no Brasil.Revista Jurídica Consulex. n.º 343, maio de 2011, p. 34.

CABETTE, Eduardo Luiz Santos. Interceptação telefônica. São Paulo, Editora Saraiva, 2011.

CAPRONH, H. L.; JOHNSON, J. A., Introdução à Informática. São Paulo, Pearson Prentice Hall, 2004.

CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais: Rio de Janeiro, Editora Brasport, 2012.

COIMBRA, Márcio C. A inviolabilidade dos e-mails. Disponível em https://jus.com.br/artigos/1787/a-inviolabilidade-dos-e-mails?secure=true, acesso em 06 de fevereiro de 2016.

COLLI, Maciel. Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos: Curitiba, Juruá Editora, 2010.

Crimes contra a Liberdade Pessoal: Disponível em http://www.direitonet.com.br/guias-de-estudo/exibir/141/Crimes-contra-a-liberdade-pessoal, acesso em 06 de fevereiro de 2016.
Delito de furto Conceituação. Disponível em https://pt.wikipedia.org/wiki/Furto, acesso em 08 de fevereiro de 2016.

Engenharia Social: As Técnicas de Ataque Mais Utilizadas. Disponível em http://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/ acesso em 18 de setembro de 2015.

FILHO, Adilson Paulo Prudente do Amaral. Crimes Cibernéticos. Revista Jurídica Consulex. Ciber Criminalidade Insegurança na Rede: n.º 343, maio de 2011.

FRANCO, Marcelo de Araujo. Ensaios Sobre as Tecnologias Digitais da Inteligência. São Paulo: Editora Papirus, 1997.

FLOR, Roberto. Perspectiva Para Novos Modelos de “Investigação Tecnológica” e Proteção de Direitos Fundamentais na Era da Internet. Revista Brasileira de Ciências Criminais, Editora dos Tribunais, 2012.

FURTADO, Roberto Wilson. Dano Transnacional e Internet. Direito Aplicável e Competência Internacional: Curitiba, Editora Jaruá, 2010.

GOMES, Olavo José Anchieschi. Segurança Total: Protegendo-se Contra os Hackers. São Paulo, Editora Makron, 2000.

Glossários dos Direitos Humanos. Disponível em: http://www.safernet.org.ber/site/prevenção/glossarios/direitos-humano#pedo, acesso em 16 de fevereiro de 2016.

História do TCP/IP. Disponível em https://pt.wikpedia.org/wik/TCP/IP, acesso em 24 de fevereiro de 2016.

JESUS, Damásio. Código Penal Anotado. São Paulo, Editora Saraiva, 2004.

JORGE, Vinicius Nogueira; WENDT. Emerson. Fraudes Eletrônicas e Engenharia Social. Revista Jurídica Consulex. n.º 386, 15 de fevereiro de 2013.

LEMOS, André. Cibercultura: Tecnologia e Vida Social na Cultura Contemporânea. Porto Alegre: Sulina.

MORREIRA, Fabio Lucas. Da "Sociedade Informática" de Adam Schaff ao Estabelecimento dos Fundamentos e Princípios do Marco Civil da Internet (PL 2.126/2011): Porto Alegre. Livraria do Advogado Editora, 2012.

NETO, José Matias. Cibercriminalidade: Insegurança na Rede. Revista Jurídica Consulex, Ano XV, n.º 343, 1 de maio de 2011.

NUCCI, Guilherme de Souza. Código Penal Comentado. Rio de Janeiro, Editora Forense, 2014.

O que é TCP/IP. Disponível em: http://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-htm, acesso em 24 de fevereiro de 2016.

Principais Dispositivos de Segurança da Votação Eletrônica. Disponível em: http://www.justicaeleitoral.jus.br/arquivos/tre-se-seguranca-da-urna-eletronica, acesso em 19 de março de 2016.

Propriedade Intelectual: Pirataria de Software. Disponível em: http://www.abessoftware.com.br/propriedade-intelectual/saiba-mais-sobre-pirataria-de-software, acesso em 19 de março de 2016.

Rede de Computadores. Disponível em: https://pt.wikipedia.org/wiki/Rede_de_computadores, acesso em 24 de fevereiro de 2016.

SILVA, Ana Karolina. Internet e Informática. Disponível em http://www.ambito-jurídico.com.br/site/index.php/?n link=revistaartigosleitura&artigo id=12778&revistacaderno=17, acesso em 25 de fevereiro de 2016.

SILVA, Mauricio Faria. O Procedimento Investigatório dos Crimes Praticados Pela Internet: Porto Alegre, Livraria do Advogado Editora, 2012.

STEFAM, André. Direito Penal Parte Geral: São Paulo, Editora Saraiva, ano 2010.

TCP/IP. Disponível em http://www.harware.com.br/termos/tcp-ip, acesso em 24 de fevereiro de 2016.

UNB quebra sigilo de urna eletrônica em testes organizados pelo TSE. Disponível em:http://www.unb.br/noticias/print_email/imprimir.php?u=http://www.unb.br/noticias/unbagencia/unbagencia.php?id=6375, acesso em 19 de março de 2016.

VADEMECUM. Editora Verbo Jurídico, 8º Edição, 2012, p. 549.

VAINZOF, Roni e JIMENE, Camila do Vale. Segurança no Ambiente Eletrônico e Suas Implicações Jurídicas: Revista Jurídica Consulex, Ano XV, n.º 343, 1 de maio de 2011.

VIANNA, Tulio; MACHADO, Felipe. Crimes Informáticos - Conforme a Lei n.º 12737/2012: Belo Horizonte, Editora Fórum, 2013.

WEND, Emerson; Higor Vinicius Nogueira Jorge. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação: Rio de Janeiro, Brasport, 2013.

WEND, Emerson: Compras Online e o “Estelionato Virtual”. Disponível em http://www.emersonwendt.com.br/2010/06/compras-online-e-estelionato-virtual.html, acesso em 08 de fevereiro de 2016.