SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DO SUL E SUDESTE DO PARÁ
CAMPUS UNIVERSITÁRIO DE MARABÁ
INSTITUTO DE ESTUDO EM DIREITO E SOCIEDADE
FACULDADE DE DIREITO

CRIMES CIBERNÉTICOS PATRIMONIAIS: A DIFICULDADE DE PRODUÇÃO PROBATÓRIA

RENATA GUIMARÃES AZEVEDO

MARABÁ/PA
2015

RENATA GUIMARÃES AZEVEDO

CRIMES CIBERNÉTICOS PATRIMONIAIS: A DIFICULDADE DE PRODUÇÃO PROBATÓRIA

Trabalho de Conclusão de Curso apresentado como requisito para a obtenção do título de Bacharel em Direito pela Universidade Federal do Sul e Sudeste do Pará, Campus Universitário de Marabá.

Orientador: Prof.° Me. Marco Alexandre da Costa Rosário

MARABÁ/PA
2015

Dados Internacionais de Catalogação-na-Publicação (CIP)
(Biblioteca Josineide Tavares, Marabá-PA)

Azevedo, Renata Guimarães.

Crimes cibernéticos patrimoniais: a dificuldade de produção probatória. /Renata Guimarães Azevedo; Orientador, Marco Alexandre da Costa Rosário. – 2015.

Trabalho de Conclusão de Curso (Graduação) Universidade Federal do Pará, Faculdade de Direito, 2015.

1.Crime de informática– Brasil. 2. Internet– Aspectos jurídicos– Brasil. 3. Direito penal – Brasil. 4. Ciberespaço. I. Título.

Doris: 340.0285

RENATA GUIMARÃES AZEVEDO

CRIMES CIBERNÉTICOS PATRIMONIAIS: A DIFICULDADE DE PRODUÇÃO PROBATÓRIA

Banca Examinadora:

_____
Prof.º Me. Marco Alexandre da Costa Rosário
(Orientador)

_____
Prof.ª Me. Olinda Magno Pinheiro

Aprovado em: ___/___/___.

Conceito: _____.

AGRADECIMENTOS

Primeiramente a Deus nosso pai, o qual é digno de toda honra e toda glória.

A todos da minha família que sempre torceram e incentivaram não somente pelo meu sucesso profissional como para o alcance de todos os meus objetivos, fazendo-me acreditar na minha potencialidade e dando-me força para perseverar em mais essa trilha da vida.

"Mas buscai primeiro o reino de Deus e sua justiça, e todas estas coisas vos serão acrescentadas."

(Mateus 6:33)

RESUMO

A criação e a popularização da internet no Brasil e no mundo fizeram surgir novos crimes, bem como crimes tradicionais que migraram sua execução do mundo real para o virtual e demandam a devida repressão estatal. A essência do presente trabalho é um estudo sobre os crimes cibernéticos, especificamente os de cunho patrimonial como furto e estelionato, com o objetivo de ampliar o debate democrático sobre o tema. Ao longo do trabalho são analisados: o advento da rede mundial de computadores, a relação gênero/espécie dos crimes cibernéticos, sua conceituação, bem como os sujeitos ativos e passivos, as legislações existentes e projetos de lei em tramitação no congresso, e o fenômeno da prova com suas peculiaridades. O trabalho busca discutir as questões processuais que dificultam a responsabilização dos autores dos crimes cibernéticos, qual seja relativos à autoria ou produção da prova. Analisa-se igualmente os requisitos das provas, sua autenticidade e sua aplicação na apuração de tais crimes. Logrou-se, deste modo, tratar de um tema atual e demonstrar sua relevância para a seara penal.

Palavras-chave: Internet; Crimes Cibernéticos; Provas.

ABSTRACT

The creation and the popularization of the Internet in Brazil and the world have created new crimes and traditional crimes that migrated its real-world performance for virtual and require proper state repression. The essence of this work is a study on cybercrime, specifically the balance of nature such as theft and embezzlement, in order to broaden the democratic debate on the subject . Throughout the work are analyzed: the advent of the World Wide Web, the gender ratio / kind of cyber crimes, its concept as well as the subject assets and liabilities, existing laws and bills pending in Congress, and the phenomenon of proof with its peculiarities. The job search discuss procedural issues that hinder the accountability of perpetrators of cyber crimes, namely concerning authorship or of evidence. It also looks up the requirements of the evidence, its authenticity and its application in the investigation of such crimes. Was achieved, thus it is a current theme and demonstrate its relevance to the criminal harvest.

Keywords: the Internet; Cybercrime; evidence.

LISTA DE ABREVIATURAS

ARPAnet - Advanced Research Projects Agency ou Agência de Projetos de Pesquisa Avançada.

CC – Código Civil

CERT.br - O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CF – Constituição Federal

CPB - Código Penal Brasileiro

DNS - Domain Name System – Sistema de Nomes de Domínios

EUA – Estados Unidos da América

HDD - hard disk drive

MP – Ministério Público

MPF – Ministério Público Federal

MS – Mato Grosso do Sul

MT – Mato Grosso

NCP - Network Control Protocol

OECD – Organização para Cooperação Econômica e Desenvolvimento

PLC – Projeto de Lei da Câmara

PLS – Projeto de Lei do Senado

PSDB – Partido da Social Democracia Brasileira

PT – Partido dos Trabalhadores

SEN – Senador

SEPFIN - Serviço de Perícia em Informática

SP – São Paulo

TCP/IP - Transmission Control Protocol/Internet Protocol

URL - Uniform Resource Locator, ou Localizador Uniforme de Recursos

WWW - World Wide Web

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho objetiva uma abordagem acerca de uma das mais novas modalidades de prática criminal, qual seja: "Crimes Cibernéticos". Tais práticas ilícitas são realizadas através da Rede Mundial de Computadores - Internet, em suas mais variadas, como uso indevido da imagem, pedofilia, plágio, calúnia, difamação, clonagem de cartões e etc. Trataremos especificamente dos crimes cibernéticos patrimoniais como furto e estelionato ocorridos através da internet.

A pesquisa teve como base os principais autores que discorrem sobre a relação do Direito Penal com os crimes que ocorrem em ambientes virtuais, utilizando para tanto o método dedutivo, sendo que foi feita uma pesquisa bibliográfica a partir de um material que já versava sobre o assunto, constituído de livros e artigos disponíveis em sítios na internet.

Entre os numerosos clientes da rede que se utilizam dessa facilidade para auferir lucros, concretizando negócios, para lazer pessoal ou em grupos, estão aqueles que vêem ali uma oportunidade de praticar ilícitos penais, haja vista a facilidade com a qual podem realizar suas atividades virtuais delitivas, tanto pela velocidade, como pela dificuldade em identificar o agente causador dos danos.

Embora muitos se utilizem desses meios de maneira adequada, aumenta o número de casos onde os agentes, aproveitando-se deste anonimato e a impunidade, cometem ilícitos contra as outras pessoas que também utilizam a rede.

Muitas vezes, o que atrai os criminosos no setor digital, é o fato de estarem amparados pela falta de legislação adequada sobre o tema, mas a esmagadora maioria é atraída pela ausência de meios adequados de prova, que identifiquem os autores do delito, uma vez que o sistema ainda não se adequou à nova realidade digital, e por vezes não tem equipamentos, nem peritos capacitados, que os levem aos criminosos.

O debate sobre os crimes cibernéticos se torna relevante haja vista que a revolução tecnológica da informática, em especial a ferramenta internet, se tornou

um meio hábil e eficaz de comunicação e informação, ocasionando uma transformação profunda do cotidiano do homem moderno. Sucede que esta modernização estendeu-se também sobre o Direito especificamente sobre o Direito Penal.

No limiar dessa evolução tecnológica é possível constatar que, atualmente, o Código Penal de 1940[1] lida com situações criminosas que vão além do plano físico. Hoje, o agente delituoso não necessita ir às ruas para cometer determinados ilícitos como fraude, furto ou estelionato, e por vezes, o diploma legal torna-se retrógrado para os tipos penais atuais.

[1] BRASIL. Decreto-Lei nº 2.848/40: Código Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 10 out. 2014.

2 ANTECEDENTES HISTÓRICOS DA INTERNET E SUAS AMEAÇAS

2.1 A INTERNET NO MUNDO E NO BRASIL

No período da guerra fria, pesquisadores americanos começaram a imaginar um sistema imune a ataques aéreos, que fosse capaz de interligar inúmeros computadores e permitindo o compartilhamento de dados entre eles. Em 1969, a primeira versão deste sistema ficou pronta e recebeu a denominação de Advanced Research Projects Agency ou Agência de Projetos de Pesquisa Avançada (ARPAnet). Sua principal característica era não possuir um comando central, que em caso de destruição de um ou mais computadores, todos os outros equipamentos ligados ao sistema continuariam operando. Esse avanço tecnológico era capaz de evitar a perda de informações em caso de bombardeio, por exemplo, ficando resguardado o que já estava armazenado no banco de dados[2].

Com a divulgação dessa tecnologia para a sociedade a ARPAnet passou a ser utilizada para todos os tipos de comunicação, para todos os tipos de usuários, sem distinção de uso militar e civil. Fez-se necessário uma subdivisão, ficando a ARPAnet exclusiva para uso acadêmico e a MILnet, criada posteriormente, para uso exclusivo das forças militares[3].

No início da década de 70, universidades e outras instituições que faziam trabalhos envolvidos à defesa, tiveram permissão para se conectar à Arpanet, e em meados de 1975, existiam aproximadamente 100 sites. Pesquisadores que trabalhavam na Arpanet estudaram como o crescimento da rede alterou o modo como as pessoas a utilizavam. No final dos anos 70, a Arpanet tinha crescido tanto que o seu protocolo de comutação de pacotes original, chamado de Network Control Protocol (NCP), tornou-se inadequado. Foi então que a ARPANET começou a usar um novo protocolo chamado TCP/IP (Transmission Control Protocol/Internet Protocol). Atualmente, há cerca de 400 milhões de computadores permanentemente

---

[2] HISTÓRIA. **História da internet**. Disponível em: <http://www.slideshare.net/guest06f3c/historia-da-internet-1162354>. Acesso em: 16 jul. 2014.

[3] GOUVEIA, Sandra Medeiros Proença. **O direito na era digital**: Crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997. Disponível em: <http://books.google.com.br/books>. Acesso em: 16 jul. 2014.

conectados à Internet, além de muitos sistemas portáteis e de desktops que ficavam online por apenas alguns momentos[4].

Gabriel César Zaccaria descreve em que consiste o protocolo utilizado pela rede mundial de computadores[5]:

> Protocolo é a designação dada aos formatos de mensagens e suas regras, entre dois computadores, para que possa haver troca de mensagens. Vale dizer que o protocolo permite a comunicação entre os dois comunicadores.

Foi somente em 1990 que a internet alcançou a população em geral, já que o Engenheiro inglês Tim Bernes - Lee desenvolveu a World Wide Web que possibilitava a utilização de uma interface gráfica e a criação de sites dinâmicos e mais interessantes visualmente. A partir dai a internet cresceu aceleradamente e muitos dizem ser a maior criação tecnológica, depois da televisão na década de 50. A década de 90 foi a era de expansão da internet, pois foi aí que surgiram vários navegadores como o Internet Explorer da Microsoft e o Netscape Navigator, bem como o surgimento de provedores de acesso e portais de serviços online[6].

Com o desenvolvimento tecnológico o sistema foi usado na interligação das universidades americanas e posteriormente em institutos de pesquisas com sede em outros países, no entanto, a idéia central de ser uma espécie de associação mundial de computadores interligados por meio de um conjunto de regras padronizadas que especificariam o formato, a sincronização e a verificação de erros em comunicação de dados, permaneceu intacta.

Em geral, as informações na Web estão agrupadas em sites, que são coleções de páginas a respeito de um determinado assunto. Há, hoje, aproximadamente 800 milhões de sites publicados na rede. Todos eles podem ser acessados por intermédio de programas de navegação (browsers) como o Internet

---

[4] HISTÓRIA. **História da internet**. Disponível em: <http://www.slideshare.net/guest06f3c/historia-da-internet-1162354>. Acesso em: 16 jul. 2014.

[5] INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**.São Paulo: Editora Juarez de Oliveira, 2009.

[6] GOUVEIA, Sandra Medeiros Proença. **O direito na era digital**: Crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997. Disponível em: <http://books.google.com.br/books>. Acesso em: 16 jul. 2014.

Explorer, o Netscape ou o Mozilla Firefox. O “endereço” que digitamos nesses programas de navegação para acessar algum site (por exemplo, www.stf.gov.br) é chamado de URL, abreviação de Uniform Resource Locator, ou “Localizador Uniforme de Recursos”[7].

Os endereços da Web seguem uma estrutura ordenada, composta por domínios. No URL do Supremo Tribunal Federal, por exemplo, após a sigla www, há o nome do site (“.stf”), um sufixo que indica o tipo de organização (no caso, “.gov”), e duas letras finais para designar o país de origem (“.br”). Essas três partes que compõem o endereço eletrônico receberam, respectivamente, a denominação de “nomes de domínio” ou domain names (como “google”, “yahoo”, “uol”, “globo”); “domínios de nível superior” (“.gov”, “.com”, “.edu”, “.org” etc.); e “domínios de países” (.br, .fr., .it, .pt etc.). Sites sediados nos Estados Unidos não possuem a extensão final porque, no princípio, a Web estava restrita àquele país e não se julgou necessário acrescentar o domínio específico[8].

Os URLs que digitamos nos programas de navegação precisam ser “traduzidos” para um endereço numérico, denominado “endereço IP”. Dissemos mais acima que as comunicações entre os computadores conectados à rede são feitas por intermédio de regras padronizadas, chamadas de “protocolos”. Pois bem, a abreviação “IP” refere-se justamente a esses protocolos da Internet. Cada site ou página que acessamos está hospedado em um computador permanentemente ligado à rede, chamado de servidor, o qual é identificado apenas pelo endereço numérico IP. Por exemplo, o URL da Procuradoria da República em São Paulo (www.prsp.mpf.gov.br) é identificada na rede pelo endereço IP 200.142.34.3, que é um número único em toda a rede mundial. A “tradução” dos nomes de domínio para

---

[7] MINISTÉRIO PÚBLICO FEDERAL - PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO - GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. **Crimes Cibernéticos:** Manual Prático de Investigação. São Paulo, 2006. Disponível em: < http://www.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1ticaversaofinal .pdf >. Acesso em: 15 out. 2014.

[8] MINISTÉRIO PÚBLICO FEDERAL - PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO - GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. **Crimes Cibernéticos:** Manual Prático de Investigação. São Paulo, 2006. Disponível em: < http://www.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1tica-versaofinal.pdf >. Acesso em: 15 out. 2014.

um endereço IP é feita por meio de um computador chamado servidor DNS (sigla de Domain Name System – Sistema de Nomes de Domínios)[9].

Como é sabido, para que um usuário possa “navegar” nas páginas da Internet, e também receber e enviar e-mails, trocar arquivos de áudio ou vídeo, participar de grupos de discussão ou conversar com outras pessoas em chats, é preciso que esteja conectado à rede. A conexão é feita por intermédio de um modem, ligado a uma linha telefônica ou a um cabo. As concessionárias de telefone comercializam linhas especiais para a Internet, popularmente conhecidas como “banda larga”[10].

A conexão com a Internet depende ainda da assinatura de um provedor de acesso como UOL, Globo, IG, Terra, AOL, USP, Procuradoria da República. A regulação estatal da atividade desses provedores é mínima, o que dificulta as investigações criminais desenvolvidas no Brasil e, consequentemente, contribui para a impunidade de alguns crimes cibernéticos. Para reduzir o problema, as Procuradorias da República de alguns Estados vêm celebrando “termos de compromisso” com os provedores, pelos quais estes se obrigam a preservar os dados dos usuários pelo prazo mínimo de seis meses e a informar a polícia e o Ministério Público, tão logo tomem conhecimento de algum crime cometido em suas páginas[11].

Quando o usuário faz a conexão à rede, recebe um número – o Internet Protocol (IP) já referido. Esse número, durante o tempo de conexão, pertence

[9] MINISTÉRIO PÚBLICO FEDERAL - PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO - GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. **Crimes Cibernéticos:** Manual Prático de Investigação. São Paulo, 2006. Disponível em: < http://www.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1tica-versaofinal.pdf >. Acesso em: 15 out. 2014.

[10] MINISTÉRIO PÚBLICO FEDERAL - PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO - GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. **Crimes Cibernéticos:** Manual Prático de Investigação. São Paulo, 2006. Disponível em: < http://www.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1tica-versaofinal.pdf >. Acesso em: 15 out. 2014.

[11] MINISTÉRIO PÚBLICO FEDERAL - PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO - GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. **Crimes Cibernéticos:** Manual Prático de Investigação. São Paulo, 2006. Disponível em: < http://www.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1tica-versaofinal.pdf >. Acesso em: 15 out. 2014.

exclusivamente ao usuário, pois é graças a ele que o internauta pode ser "encontrado" na rede. A identificação do IP é o primeiro e mais importante passo para a investigação de um crime cibernético, como veremos adiante. Convém, desde logo, lembrar que o investigador deve ainda identificar a hora exata da conexão e o fuso horário do sistema, pois um número IP pertence ao usuário apenas durante o período em que ele está conectado; depois, o número é atribuído a outro internauta, aleatoriamente[12].

Conforme Bogo[13]:

> A internet surgiu no Brasil em 1991 trazida pela RNP – Rede Nacional de Pesquisas, no intuito de conectar redes de universidades e centros de pesquisas. Em 1994 a Embratel lança o serviço experimental e somente em 1995 é que por meio da iniciativa do Ministério das Telecomunicações e Ministério da Ciência e Tecnologia foi realizada a abertura ao setor privado da Internet para exploração comercial para a população brasileira.

Carla Rodrigues de Araújo de Castro[14] conceitua internet da seguinte maneira:

> Internet é uma grande rede de comunicação mundial, onde estão interligados milhões de computadores, sejam eles universitários, militares, comerciais, científicos ou pessoais, todos interconectados. É uma rede de redes, que pode ser conectada por linhas telefônicas, satélites, ligações por microondas ou por fibra ótica.

2.2 HISTÓRICO SOBRE AS PRIMEIRAS AMEAÇAS

Com o passar dos anos e com a evolução dos recursos tecnológicos as ameaças praticadas via computador foram aprimoradas. A informação sobre programas de computador que se autoreplicassem remontam à década de 50,

---

[12] MINISTÉRIO PÚBLICO FEDERAL - PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO - GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. **Crimes Cibernéticos:** Manual Prático de Investigação. São Paulo, 2006. Disponível em: < http://www.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1tica-versaofinal.pdf >. Acesso em: 15 out. 2014.

[13] BOGO, Kellen Cristina. **A história da Internet: como tudo começou.** 2000. Disponível em < http://www.portalguia.com.br >. Acesso em 09 jun. 2014.

[14] CASTRO, Carla Rodrigues Araujo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003.

oriunda do matemático John Von Neumam e na década seguinte é que se tem notícias dos pioneiros em ameaça[15].

Tudo começou quando um grupo de programadores desenvolveu um jogo chamado Core Wars, capaz de se reproduzir cada vez que era executado, sobrecarregando a memória da máquina do outro jogador. Os inventores desse jogo também criaram o primeiro antivírus, batizado de Re eper, com capacidade de destruir as cópias geradas pelo Core Wars. A existência desse jogo, seus efeitos e forma de desativá-lo, no entanto, vieram a público somente em 1983, por um artigo escrito por um de seus criadores, publicado em uma revista científica da época[16].

Os primeiros crimes ocorreram na década de 70, e eram praticados, na maioria das vezes, por especialistas em informática cujo principal objetivo era driblar os sistemas de segurança, principalmente de instituições financeiras[17].

A literatura científica internacional demonstra que o universo dos crimes informáticos teve seus primeiros indícios na década de 60, onde se deu as primeiras referências sobre essa modalidade de crimes, nas mais diversas denominações, com maiores incidências em casos de manipulação e sabotagem de sistemas de computadores[18].

Na década de 70 a figura do Hacker já era citada com o advento de crimes como invasão de sistema e furto de software, mas foi em 1980 que houve maior propagação dos diferentes tipos de crimes como a pirataria, pedofilia, invasão de sistemas, propagação de vírus, surgindo então com isso a necessidade de se despender maiores preocupações com a segurança virtual que exige uma atenção especial para identificação e punição dos responsáveis, que a essa altura estão em todos os lugares do mundo como foi o caso da caça desesperada do governo

[15] HISTÓRIA. **História da internet**. Disponível em: <http://www.slideshare.net/guest06f3c/historia-da-internet-1162354>. Acesso em: 16 jul. 2014.
[16] PCWORLD**. A Epidemia Via internet**. Disponível em: <http://www.cin.ufpe.br/~rdma/documentos/revistapcworldseguranda.pdf>. Acesso em 15 Jul. 2014.
[17] CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <http://www.cert.br>. Acesso em: 20 out. 2014.
[18] HISTÓRIA. **História da internet**. Disponível em: <http://www.slideshare.net/guest06f3c/historia-da-internet-1162354>. Acesso em: 16 jul. 2014.

americano atrás de Kevin Mitnick, um dos hackers mais famosos do planeta e que hoje trabalha para o governo americano na área da segurança da informação[19].

Em relação ao assunto, não existe uma posição pacífica sobre o surgimento do primeiro vírus de computador, para alguns, foi o *Elk Cloner* e para outro o *Brain*. Convém lembrar que em 1986 surgiram os primeiros cavalos de tróia que se tem notícias[20].

[19] CARNEIRO, Adeneele Garcia. **Crimes Virtuais:** elementos para uma reflexão sobre o problema na tipificação. Disponível em: http://www.ambito-juridico.com.br/. Acesso em: 02 ago.2014.
[20] WENDT, Emerson; Jorge, Higor Vinícius Nogueira. Crimes ciberneticos: Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2013.

3 CRIMES CIBERNÉTICOS

3.1 CONCEITO

A internet, como comunicação contemporânea, é umas das melhores formas de tráfego de informações, no entanto, tais avanços permitem que os chamados ataques cibernéticos se alcem em uma escala mundial e crescente, apresentando-se como grande desafio assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação de modo que esforços são empreendidos objetivando a segurança da sociedade.

Com o avanço crescente e desordenado da criminalidade, criminosos reais passaram a utilizar a internet para o cometimento de crimes virtuais, como estelionato, calúnia, furto e o racismo. Analisando a relação estabelecida entre o meio eletrônico e o homem, a probabilidade de haver cometimentos de delitos no Cyber espaço é maior, tendo em vista que o usuário se sente inatingível pela punição decorrente de um delito praticado pelo meio eletrônico, tamanha a insegurança jurídica e o respectivo despreparo por parte do Estado para dar continuação às investigações, bem como da inabilidade nos procedimentos investigatórios de tais delitos.

Ivette Senise Ferreira[21] conceitua e sugere a seguinte classificação dos crimes Cibernéticos:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio.

De acordo com Castro[22] “crime de Informática é aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador.

---

[21] FERREIRA, Ivette Senise. **Direito e Internet**: Aspectos jurídicos relevantes. 2 ed.São Paulo: Quartier Latin, 2005, p.26.
[22] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 09.

Inclui-se neste conceito os delitos praticados através da Internet, pois pressupostos para acessar a rede é a utilização de um computador".

O Professor João Marcello de Araújo Junior *apud* Castro[23] conceitua crime cibernético como sendo uma conduta lesiva, dolosa, a qual não precisa, necessariamente, corresponder à obtenção de uma vantagem ilícita, porém praticada, sempre, com a utilização de dispositivos habitualmente empregados nas atividades de informática.

As denominações quanto aos crimes praticados em ambiente virtual são diversas, não havendo consenso sobre a melhor denominação para os delitos que se relacionam com a tecnologia, crimes de computação, delitos de informática, abuso de computador, fraude informática, enfim, os conceitos ainda não abarcam a totalidade dos crimes ligados à tecnologia e, portanto, faz-se necessária a atenção quando da conceituação de determinado crime, visto que existem muitas situações complexas no ambiente virtual.

3.2 ENGENHARIA SOCIAL

É a utilização de um conjunto de técnicas destinadas a ludibriar a vítima, de forma que ela acredite nas informações prestadas e se convença a fornecer dados pessoais nos quais o criminoso tenha interesse ou a executar alguma tarefa e/ou aplicativo[24].

Geralmente os criminosos simulam fazer parte de alguma instituição confiável como órgãos do governo, grandes lojas, grandes bancos fazendo com que a vítima acredite nos dados apresentados, ora falsos, que será usado como isca para que as informações que eles necessitem sejam fornecidas.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) conceitua engenharia social como:

---

[23] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 09.
[24] WENDT, Emerson; Jorge, Higor Vinícius Nogueira.Op. Cit., p. 21.

> um método de ataque , onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações[25].

As principais técnicas utilizadas pelos engenheiros sociais são baseadas na manipulação de emoção dos alvos, daí trabalham com o medo, a ganância, a simpatia, e a curiosidade. O usuário da rede motivado por estes sentimentos acabam prestando informações que não deviam, bem como acessam links que direcionam a sites de conteúdo malicioso e/ou para execução de algum código maléfico em seu computador.

Outro aspecto a destacar sobre a engenharia social é a utilização do chamado efeito *saliência*: quando o criminoso usa, para chamar a atenção de suas potenciais vítimas, algum assunto que está em destaque na mídia mundial, nacional, regional. Outra característica da engenharia social é ancoragem, quando os criminosos utilizam, para dar credibilidade aos seus atos, imagens de empresas de mídia, de bancos, de órgãos públicos, usando assim, por exemplo, imagens das Polícia Civil, Polícia Federal, Supremo Tribunal Federal, Ministério Público Federal, Globo, Record, SBT[26].

3.3 SUJEITOS ATIVO E PASSIVO

Segundo Júlio Mirabete[27], sujeito ativo “é aquele que pratica a conduta descrita na lei, ou seja, o fato típico”.

Face à ausência física do sujeito ativo a imputação objetiva ao autor do crime e sua comprovação é extremamente difícil, mas diante da necessidade da identificação do autor é que surgiu determinados perfis traçados para denominar grupos que praticam alguns crimes virtuais, dentro dessa denominação temos a figura do *hacker*.

---

[25] CERT.br. **Cartilha de Segurança para Internet**. Disponível em: <http://cartilha.cert.br>. Acesso em: 15 set.2014.
[26] WENDT, Emerson; Jorge, Higor Vinícius Nogueira.Op. Cit., p. 24.
[27] MIRABETE, Júlio Fabbrini. **Manual de Direito Penal**: Parte Geral. 19 ed. São Paulo: Atlas, 2003, p. 122.

O significado da palavra *Hacker* segundo tradução do dicionário Michaelis quer dizer em um de seus resultados “pessoa que usa seu conhecimento técnico para ganhar acesso a sistemas privados”. Ou seja, tecnicamente pessoas com conhecimentos impares sobre informática e sistemas que se utilizam de seus conhecimentos não necessariamente para praticas ilícitas. A partir do momento que se vislumbra que *hackers* são pessoas com grande conhecimento é possível haver conhecimento técnico de forma positiva e negativa[28].

A princípio, qualquer pessoa pode ser sujeito ativo dos crimes de informática. Um estelionato praticado através da Internet, por exemplo, não requer nenhuma qualidade especial do agente. Como este, a maioria dos crimes de informática é comum em relação ao sujeito. Existem, porém, alguns delitos que normalmente são praticados pelos representantes legais das pessoas jurídicas relacionadas com a rede. Por exemplo: um provedor de acesso à internet que, diante de uma ordem judicial, se recusa a informar o endereço de um usuário[29].

Os agentes responsáveis pelo cometimento de crimes de informática recebem diversas nomenclaturas, entre elas podemos destacar o *Cracker*, indivíduos que possuem conhecimento de informática e o utiliza para quebrar sistemas de segurança, de forma ilegal ou sem ética, para furtar informações sigilosas, em proveito próprio ou de outrem; e há o *Hacker*, que é aquele que tem conhecimento profundo de sistemas operacionais e linguagens de programação e o utiliza para invadir sistemas pelo simples prazer de provar a si mesmo que é capaz, sem causar danos a outrem.

Genericamente Hacker é uma denominação para alguém que possui uma grande habilidade em computação. Cracker, black-hat ou script kiddie neste ambiente denomina-se os hackers que tem como hobby invadir computadores. Portanto, a palavra Hacker é gênero, e o cracker é a espécie.

---

[28] CARNEIRO, Adeneele Garcia. **Crimes Virtuais:** elementos para uma reflexão sobre o problema na tipificação. Disponível em: <http://www.ambito-juridico.com.br/>. Acesso em: 02 ago.2014.
[29] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 12.

Dentre essas espécies temos ainda os chamados *lamers*, chamados de *wannabes* ou *script-kid* são *hackers* que atuam em pequenos feitos limitando seus conhecimentos e não representam tanto perigo sendo classificados como leigos frente às grandes posições de *hackers*, ainda nas espécies temos os *phreakers* que comentem crimes específicos voltados para a área de telecomunicações e os *defacers* que registram suas marcas ao invadirem páginas na internet e desfigurá-las[30].

Assim, um indivíduo tecnicamente experiente em informática tem condição de apropriar de senha alheia, utilizando-a para o cometimento de diversos atos ilícitos que se estendem desde a simples navegação virtual, a aplicação de pequenos golpes, a invasão e destruição de dados, a divulgação de pornografia infantil e adolescente, culminando com apropriação indébita, furtos e outros delitos que a imaginação do criminoso virtual se propuser a executar[31].

Frente à classificação desses perfis de criminosos temos uma ideia de quem eles são como agem e o que querem de uma forma genérica, mas a pergunta é como identificá-los antes de eles cometerem condutas ilícitas que os identifiquem já que quando falamos em sujeito ativo sabemos que realmente os dados obtidos para identificação do sujeito é o endereço da máquina que envia as informações, ou seja, o IP, seu *login* e senha portanto com a possibilidade de camuflagem dos dados e a utilização de dados inverídicos dificilmente há uma rápida identificação do sujeito ativo na prática[32].

Quando falamos de um crime específico logo sabemos quem é o sujeito ativo e passivo da conduta, quem realizou e em quem recaiu a ação ou omissão, no caso dos crimes virtuais de forma generalizada a única afirmação cabível é que será sempre uma pessoa física ou jurídica ou uma entidade titular seja pública ou privada

---

[30] CARNEIRO, Adeneele Garcia. **Crimes Virtuais:** elementos para uma reflexão sobre o problema na tipificação. Disponível em: <http://www.ambito-juridico.com.br/. Acesso em: 02 ago.2014.
[31] DARÓS MALAQUIAS, Roberto Antonio. **Crime cibernético e prova:** A investigação criminal em busca da verdade.Curitiba: Juruá, 2012, p. 64.
[32] CARNEIRO, Adeneele Garcia. **Crimes Virtuais:** elementos para uma reflexão sobre o problema na tipificação. Disponível em: <http://www.ambito-juridico.com.br/. Acesso em: 02 ago.2014.

titular do bem jurídico tutelado, sempre haverá o sujeito passivo, ou seja, alguém que está sendo lesado enfim o que sofre a ação[33].

Em relação ao sujeito passivo, também pode ser qualquer pessoa. Seja quem for conectado a Internet, pode receber um vírus e ter destruídos seus programas[34].

O sujeito passivo da infração penal pode ser qualquer indivíduo normal, pessoa física, ou até mesmo uma pessoa jurídica, haja vista poder, por exemplo, ter seus bens desviados, seu patrimônio deteriorado ou mesmo ter informações violadas. Ambas são capazes de determinar a ação do agente criminoso[35].

E, aqui, surge um dos maiores empecilhos para conhecimento e apuração dos crimes. Na maioria das vezes a empresa lesada prefere arcar com os prejuízos causados pela infração, do que tornar público o fato de ter sido vítima deste tipo de delito. A publicidade da vulnerabilidade do sistema de informática da empresa pode causar prejuízos maiores do que os efetivamente sofridos[36].

Ocorre que atualmente a maioria dos crimes praticados ainda não são divulgados, seja por conta da não disseminação dessas informações ou pela falta de denuncia, como, por exemplo: grandes empresas evitam a divulgação sobre possíveis ataques virtuais ou mesmo invasões para não demonstrarem fragilidade quanto à segurança; quanto às pessoas físicas vemos que por falta da devida punibilidade aos infratores e a falta de mecanismos de denuncia, apesar de já existirem, as vítimas acabam não denunciando, o que facilita a propagação desses crimes[37].

---

[33] CARNEIRO, Adeneele Garcia. **Crimes Virtuais:** elementos para uma reflexão sobre o problema na tipificação. Disponível em: <http://www.ambito-juridico.com.br/. Acesso em: 02 ago.2014
[34] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 12.
[35] CARNEIRO, Adeneele Garcia. **Crimes Virtuais:** elementos para uma reflexão sobre o problema na tipificação. Disponível em: <http://www.ambito-juridico.com.br/. Acesso em: 02 ago.2014
[36] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 12.
[37] CARNEIRO, Adeneele Garcia. **Crimes Virtuais:** elementos para uma reflexão sobre o problema na tipificação. Disponível em: <http://www.ambito-juridico.com.br/. Acesso em: 02 ago.2014

3.4. ESPÉCIES

A espécie "crimes cibernéticos" subdividem-se em "crimes cibernéticos abertos" e "crimes exclusivamente cibernéticos". Com relação aos crimes cibernéticos abertos, são aqueles que podem ser praticados da forma tradicional ou por intermédio de computadores, ou seja, o computador é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele. Já os crimes exclusivamente cibernéticos são diferentes, pois eles somente podem ser praticados com a utilização de computadores ou de outros recursos que permitem o acesso à internet. Um exemplo é o crime de aliciamento de crianças praticados por intermédio de salas de bate papo na internet, previsto no artigo 241-D do Estatuto da Criança e Adolescente(Lei 8.069/90). Também são exemplos os crimes de interceptação telemática ilegal e o recém aprovado crime de invasão de computadores[38].

Os crimes de informática também podem ser classificados como próprios e impróprios. Os primeiros são aqueles que só podem ser praticados através da informática. São os típicos crimes do mundo virtual, tendo em vista que existem única e exclusivamente em razão da informática[39].

Os impróprios são aqueles que podem ser praticados de qualquer forma, ou seja, o agente utiliza a informática para praticar o crime, no entanto, dispunha de outros meios para atingir o fim criminoso[40].

De acordo com Marco Aurélio Rodrigues da Costa (1995) citado por Castro[41], os crimes são divididos em crimes de informática puros, crimes de informática misto e crime de informática comum.

Segundo o citado autor os crimes de informática puros seriam aqueles que atingem especificamente o sistema de informática, os crimes mistos se consubstanciam nas condutas que lesionam bens jurídicos diversos da área da informática, no entanto, para que o fim seja alcançado é necessário utilizar o sistema

[38] WENDT, Emerson; Jorge, Higor Vinícius Nogueira.Op. Cit., p. 19.
[39] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 10.
[40] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 10.
[41] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 11.

de informática. Por fim, os crimes de informática comum são aqueles que podem ser praticados por qualquer meio, inclusive pelo sistema de informática[42].

Greco Filho adota a seguinte divisão: condutas perpetradas contra um sistema informático e condutas perpetradas contra outros bens jurídicos, segue observação do autor:

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou[43].

O autor Vladimir Aras[44] tem sua classificação da seguinte forma: a) uma primeira, onde estão substancialmente unidos pela circunstância que o computador constitui a necessária ferramenta de realização pela qual o agente alcança o resultado legal; b) a segunda categoria de crimes do computador, poderia incluir todos aqueles comportamentos ilegítimos que contestam os computadores, ou mais precisamente, seus programas; c) a última categoria deveria juntar todas as possíveis violações da reserva sobre a máquina, aqui entram em consideração as habilidades de colheita e elaboração de todo tipo de dados.

Ivete Senise Ferreira, apud Carla Rodrigues[45], divide os crimes de informática em duas categorias: na primeira, os atos são dirigidos contra o sistema de informática, divididos em atos contra o computador e atos contra os dados ou programas de computador. Na segunda categoria estão os atos cometidos por intermédio do sistema de informática, que podem ser contra o patrimônio, contra a liberdade individual e contra a propriedade imaterial.

---

[42] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 11.
[43] GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. **Boletim do IBCCrim**. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.
[44] ARAS, Vladimir**.**Crimes de Informática.Uma nova criminalidade. **Jus Navigandi**, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/artigos/2250>. Acesso em: 8 jul. 2014.
[45] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 11.

Em todas as classificações há distinções e pontos em comum a considerar, algumas posições atribuem os meios eletrônicos como bem jurídico protegido e meios eletrônicos como meio ou instrumento de se lesionar outros bens, sendo esta última a classificação mais oportuna por abarcar um número maior de opções acerca destas práticas delitivas. Mas essas classificações são eficazes didaticamente para se entender e classificar alguns crimes, mas por conta da rapidez na evolução e dinâmica da rede de computadores e internet fica quase impossível acompanhar e afirmar categoricamente que não há modalidades que não estejam elencadas nas classificações adotadas.

4 FRAUDE ELETRÔNICA: ESTELIONATO E FURTO

A utilização cada vez mais frequente e cotidiana dos correios eletrônicos, dos sítios de instituições financeiras que oferecem atividades bancárias *online*, dos produtos e serviços disponibilizados pelas empresas virtuais por meio do comércio eletrônico (*e-commerce*), geram também a catalisação de atividades criminosas nesse mesmo ambiente virtual.

Nas fraudes o usuário é induzido a fornecer seus dados pessoais e financeiros, na maioria das vezes mascarada por trás de páginas duvidosas, o qual o usuário e encaminhado para páginas fraudulentas, na maioria das vezes os fraudadores utilizam as mídias sociais, e tentam de todas as maneiras persuadir o usuário a fornecer seus dados pessoais[46].

A fraude, segundo Eduardo Valadares de Brito, apud Carla Rodrigues[47], costuma ocorrer:

> [...]quando o indivíduo ao comprar, vender ou investir via Internet é enganado de alguma forma. O vendedor pode descrever produtos ou serviços de maneira enganosa ou pode, ainda, receber o pedido e o dinheiro, mas não entregar o bem o qual estava obrigado.

Surgem os estelionatarios cibernéticos que são indivíduos com as mesmas características delituosas da sociedade tradicional que buscaram aperfeiçoar suas técnicas e "*modus operandi*" para atuarem no espaço cibernético[48].

Em linhas gerais, o crime de estelionato é configurado quando alguém obtém, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento. O artigo 171 do Código Penal[49] versa que:

---

[46] CERT.br. **Cartilha de Segurança para Internet**. Disponível em: <http://cartilha.cert.br>. Acesso em: 15 set.2014.
[47] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 32.
[48] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.80.
[49] BRASIL. Decreto-Lei nº 2.848/40: Código Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 10 out. 2014.

> Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> pena – Reclusão, de 1 (um) a 5 (cinco) anos, e multa.

O crime de estelionato pressupõe dois resultados: vantagem ilícita e prejuízo alheio. Este resultado deve ser obtido mediante artifício, ardil ou qualquer outro meio fraudulento. É exatamente aqui que entra a informática. O agente pode utilizar *homepages*, *sites*, conversas *on line* e *e-mails* para induzir o lesado a erro, seja mediante ardil, artifício ou qualquer meio[50].

Na lição do mestre Paulo José da Costa Júnior apud Carla Rodrigues[51], o ardil se distingue do artifício na medida em que o primeiro opera sobre a realidade externa, criando uma falsa aparência material e o último atua diretamente sobre o psiquismo do enganado.

Esses citados estelionatários virtuais utilizam a grande disponibilidade existente nos sistemas informatizados para se criar e manusear uma caixa de correio eletrônico gratuito, sem identificação positiva ou cadastro, forjando situações fictícias e ardilosas com a finalidade de ludibriar a boa-fé do indivíduo e obter para si vantagens indevidas[52].

O estelionato cibernético ocorre também com o envio de spam, arquivos executáveis, serviços de hospedagem, com a utilização de listas e cadastros de usuários e servidores públicos, utilizando como estratégia criminosa o envio de mensagens eletrônicas falsas, simulando atividades de instituições bancárias em cadastramento de dados e informações pessoais, números e códigos de contas correntes, cartões bancários e senhas que são capturadas, ludibriando os cidadãos inexperientes, por intermédio do manuseio de sistemas operacionais e *programas-fantasmas*.

---

[50] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 31.
[51] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 31.
[52] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.81.

As fraudes eletrônicas têm crescido em escala exponêncial, especialmente no que diz respeito à modalidade de furto mediante fraude (Art. 155 do Código Penal[53]), que se caracteriza pelo envio de um email falso (*phishing)* para um usuário, e são capturados dados de sua conta bancária, mediante a instalação de um programa em seu equipamento de acesso à internet.

Tratando-se o phishing de uma fraude eletrônica, através do qual o agente obtém informações da vítima, senhas e dados pessoais, levando-a a erro, fazendo-se passar por terceiro, como por um banco ou um estabelecimento comercial ou levando o lesado a confiar em arquivos informáticos infectados por softwares daninhos, que capturam ou copiam dados. Verifica-se que o objetivo do agente é a obtenção de vantagem patrimonial ilícita[54].

O crime de furto está previsto no artigo 155, e seus parágrafos, do Código Penal[55], sendo que a sua forma simples consiste em “subtrair, para si ou para outrem, coisa alheia móvel”.

Tal figura delitiva é classificada como crime de informática impróprio, pois pode ser praticado por outros meios alheios à informática.

Costuma-se fazer uma distinção entre crime de informática praticado contra o sistema de informática ou através deste. Quando o agente furta o computador ou um de seus acessórios, o crime é contra o sistema de informática. Exemplo: furto de um disquete. Por outro lado, se o agente utiliza o computador para praticar a subtração, ele utiliza a informática como instrumento do crime, trata-se de crime através do sistema de informática. São os casos de subtração de valores de conta bancária[56].

---

[53] BRASIL. Decreto-Lei nº 2.848/40: Código Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 10 out. 2014.

[54] FERNANDES, David Augusto. **Crimes Cibernéticos: O descompasso do Estado e a realidade.**Disponivel em: http://www.direito.ufmg.br/revista/index.php/revista/article/view/P.0304-2340.2013v62p139 . Acesso em 17. Set. 2014.

[55] BRASIL. Decreto-Lei nº 2.848/40: Código Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 10 out. 2014.

[56] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 26.

Enormes valores são subtraídos diariamente de contas bancárias através da internet e tem preocupado as Instituições Financeiras de todo o mundo, fazendo com que eles invistam cada vez mais em tecnologia.

Quase não se vê notícias desses furtos em Instituições Bancárias, o que não significa inocorrência desses fatos. Como bem exposto por Carla Rodrigues[57], os Bancos não costumam divulgar os furtos em contas correntes de seus clientes, pois preferem arcar com o prejuízo a tornar pública a vulnerabilidade de seu sistema tecnológico e gerar um marketing negativo.

Para praticarem o crime, os agentes violam o sistema de informática de um Banco e transferem valores para suas contas-correntes. É comum ocorrer também a hipótese do agente conseguir a senha do correntista, através de spams ou e-mails, e invadir a própria conta bancária do mesmo, subtraindo valores.

Ao praticar subtração de valores de uma conta corrente através da Internet, o sujeito incorrerá nos preceitos do artigo 155, do Código Penal[58], conforme o entendimento de Alexandre Jean:

> [...] a inovação está no *modus operandi*. O resultado alcançado com a conduta independe da abrangência jurídica atribuída a res. O dinheiro rapinado de uma conta corrente via Internet é furto como outro qualquer, diferenciando-se apenas quanto a maneira e quanto ao agente que pratica o delito[59].

A causa de aumento de pena prevista no § 1º, do artigo 155, do Código Penal[60], não tem aplicação, eis que o fundamento da qualificadora reside na circunstância da maior facilidade que pode ter o sujeito quando pratica o furto em altas horas da noite. Ora, tanto faz para o hacker agir durante o período diurno ou noturno, pois a dificuldade será a mesma.

---

[57] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 26.

[58] BRASIL. Decreto-Lei nº 2.848/40: Código Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 10 out. 2014.

[59] DAOUN, Alexandre Jean. **Os novos crimes de informática**. Disponível em: <http://www.advogado.com/internet/zip/novocrim. Acesso em 05. nov.2014.

[60] BRASIL. Decreto-Lei nº 2.848/40: Código Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 10 out. 2014.

De outro lado, nada impede que o privilégio do § 2º, do artigo supra seja aplicado, desde que o criminoso seja primário e o valor da coisa furtada seja de pequeno valor[61].

Em relação às qualificadoras do § 4º, é facilmente perceptível que os incisos I (destruição ou rompimento de obstáculo) e III (emprego de chave falsa) não terão relevância para os cybercrimes. Nada impede que a qualificadora relativa ao abuso de confiança e mediante fraude tenha aplicabilidade[62]. Exclui-se a qualificadora referente à escalada e destreza.

Por fim, dois agentes podem agir em conluio para praticar subtrações em contas bancárias por intermédio da informática. Estaria caracterizada a qualificadora de concurso de agentes[63].

Ainda que o Código Penal Brasileiro (CPB) faça menção ao estelionato e furto em seu texto, vale ressaltar que a conduta descrita diz respeito apenas ao delito praticado de forma direta pelo infrator, isto é, obtendo vantagem ilícita em prejuízo alheio em pleno contato com a vítima, não sendo necessário o intermédio do computador e da internet para que reste consumada sua atividade criminosa.

O impasse surge quando da tipificação do estelionato e do furto virtual na legislação penal, que se mostra inerte quanto a isso. A Constituição Federal (CF/88)[64] traz no inciso 39 do artigo 5º o princípio da legalidade, que também encontra-se no CPB, *in verbis:*

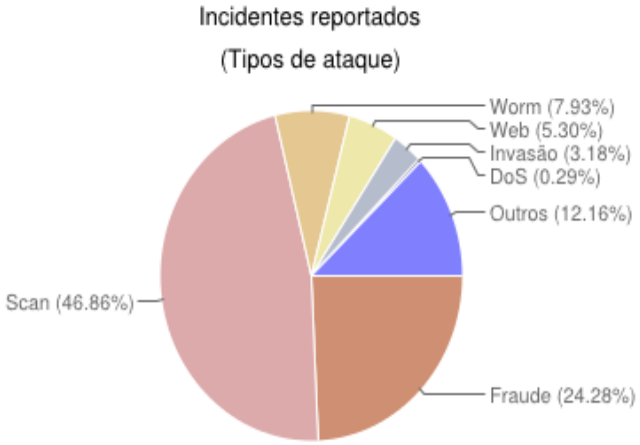
> Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)

[61] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 26.
[62] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 26.
[63] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 27.
[64] BRASIL. Constituição Federal de 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em 10 out. 2014.

> XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal.

Por esse princípio, todo e qualquer indivíduo que cometa crime deve ser punido tendo como base esse princípio norteador, portanto, para que o processo penal seja normal, o fato deve se adequar perfeitamente na legalidade estrita da lei, não podendo ser reprovável sem que cumpra os requisitos de validade. A natureza jurídica deste dispositivo legal acaba por limitar a pretensão punitiva estatal, e por inexistir a tipificação expressa do estelionato e furto virtual em diploma legal, em alguns casos seus adeptos são absolvidos devido a esta “brecha” deixada pelo Código antiquado aos dias atuais, código este datado no ano de 1940.

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2013



Legenda:

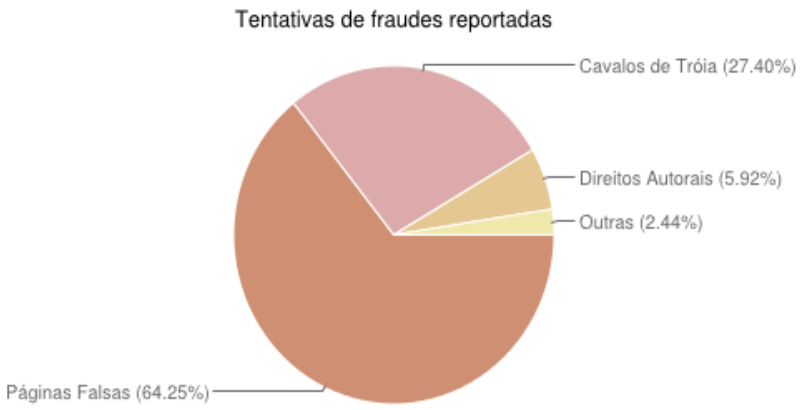
- **worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as

notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

- **outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

Obs.: Vale lembrar que **não se deve confundir scan com scam**. Scams (com "m") são quaisquer esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras. Ataques deste tipo são enquadrados na categoria fraude.

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2013



Legenda:

- **Cavalos de Tróia**: Tentativas de fraude com objetivos financeiros envolvendo o uso de cavalos de tróia.
- **Páginas Falsas**: Tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas.
- **Direitos Autorais**: Notificações de eventuais violações de direitos autorais.
- **Outras**: Outras tentativas de fraude.

5 LEGISLAÇÃO NACIONAL EM RELAÇÃO AOS CRIMES CIBERNÉTICOS

O espaço virtual, que se mostra tão propício para a prática dos mais variados crimes, apesar da falta de legislação específica, é relativamente protegido juridicamente, pois se encontram no ordenamento jurídico brasileiro algumas normas que tratam da matéria, como por exemplo: a Lei nº 11.829/08, que combate a pornografia infantil na internet; a Lei nº 9.609/98, que trata da proteção da propriedade intelectual do programa de computador; a Lei nº 9.983/00, que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da Administração Pública; a Lei nº 9.296/96 disciplinou a interceptação de comunicação telemática ou informática; e a Lei nº 12.034/09, que delimita os direitos e deveres dentro da rede mundial, durante as campanhas eleitorais[65].

Além disso, os aplicadores do direito têm aplicado a legislação já existente, como o Código Penal, aos crimes cometidos no meio virtual. Exemplos de crimes cibernéticos já tipificados na legislação penal que são cometidos através de computadores e outros meios tecnológicos são, entre outros, o crime de calúnia, ameaça, difamação, apologia a crime ou criminoso, injúria, constrangimento ilegal, falsa identidade.

O ato legislativo mais recente relativo aos crimes cibernéticos realizou-se no dia 15.05.2012, no plenário da Câmara dos Deputados, aprovando o Projeto de Lei 2.793/11, de iniciativa do Deputado Federal Paulo Teixeira (PT-SP) e outros parlamentares, que define tipos penais para os delitos virtuais no Código penal (Decreto-lei 2.848/40)[66].

Nesse projeto a invasão de sistemas no sentido de obter conteúdos de caráter privado ou obter segredos comerciais e industriais fazendo uso de técnicas remotas não autorizadas e violando mecanismos de segurança, tem a previsão de uma pena de reclusão que vai de 6 meses a 2 anos e multa, com a agravante nos

---

[65] MENDES, Eugenia Gonçalves Mendes; VIEIRA, Natalia Borges. **Os Crimes cibernéticos no ordenamento jurídico brasileiro e a necessidade de legislação específica**. Disponível em: http://www.gcpadvogados.com.br/artigos/ . Acesso em: 31 Out. 2014.

[66] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.205.

casos de divulgação, comercialização ou transmissão a terceiros os dados obtidos ilegalmente.

A invasão de dispositivo informatizado ou rede local com a finalidade de destruir ou alterar dados ou informações, além de instalar vulnerabilidades (*trojan horse*) para obter vantagem ilícita ou simplesmente por vandalismo e exibicionismo, será penalizado com 3 meses a 1 ano de detenção e multa. Em contrapartida, será enquadrado no mesmo crime o indivíduo que produzir, oferecer, distribuir, vender ou difundir programa de computador destinado a executar crimes cibernéticos em computadores, *smart phones*, *tablets* ou em quaisquer outros dispositivos computacionais e em redes locais[67].

Vale ressaltar que o referido projeto de lei foi objeto de crítica pelos demais parlamentares, tendo em vista que, segundo eles, o governo foi omisso durante anos acerca do tema e por conta do vazamento das fotos da atriz Carolina Dieckman votou um projeto sem a discussão necessária. No entanto a Lei nº 12.737/2012[68] foi sancionada pela presidente no dia 30 de novembro de 2012 alterando o Código Penal e tipificando alguns delitos informáticos.

A nova legislação aborda questões importantes como invasão de dispositivo eletrônico, acesso remoto não autorizado, interrupção de serviços telemáticos e outros pontos interessantes. Entretanto, as penas cominadas são pouco inibidoras, ocorrendo exatamente o oposto da tendência internacional, que segundo noticiários, a Justiça da Califórnia, Estados Unidos da América (EUA) condenou a 10 anos de prisão, além do pagamento do valor de indenização no valor de 76 mil dólares, o hacker acusado de subtrair fotos de celebridades pela internet.

Primeiro ponto para reflexão: a lei restringe a tipicidade da invasão aos casos em que há a violação indevida de mecanismos de segurança. Assim, os dispositivos informáticos não dotados de ferramenta de proteção estariam excluídos da aplicação legal. Ademais, as expressões mecanismo de segurança e dispositivo informático

---

[67] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.205.

[68] BRASIL. Lei 12.737/2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 10 out. 2014.

(só hardwares? E os softwares?) não foram definidas na lei, restando dúvidas sobre o completo enquadramento de certos casos. Também é possível antever discussão sobre quem poderá ser considerado o "titular do dispositivo" invadido - expressão da lei para indicar a vítima. Será que o possuidor ou o mero usuário eventual também estão protegidos? O texto não esclarece, mas há a impressão de o tipo direcionar-se somente ao proprietário[69].

5.1 PROJETO DE LEI E MARCO CIVIL DA INTERNET

É interessante listar os projetos de lei oriundos da Câmara dos Deputados e do Senado Federal que se encontram em andamento ou aguardando entrar em pauta de votação, com o objetivo de normatizar as áreas temáticas referentes ao espaço cibernético, qual sejam relacionados a crimes cibernéticos exclusivamente patrimoniais, a seguir descritos.

PLS 383/05[70], apresentado em 10.11.2005 (Sen. Delcidio Amaral, PT/MS). Acrescenta ao Código Penal o artigo 308-A, prevendo os crimes de "Fraude sobre cartão ou chave de identificação pessoal automatizada" e de "Petrechos para obtenção indevida".

PLS 6.024/05[71], apresentado em 06.10.2005 (Dep. Mendes Thamé, PSDB/SP). Dispõe sobre crimes informáticos, alterando o Código Penal e regulando a disponibilidade dos arquivos dos provedores.

PLS 463/03[72], apresentado em 13.11.2003 (Sen. Serys Slhessarenko, PT/MT). Obriga os provedores de hospedagem da Rede Mundial de Computadores (Internet) a fornecer relação das páginas sob seu domínio.

---

[69] BLUM, Renato Opice. **Crimes Eletrônicos**: A nova lei é suficiente? Disponível em <http://www.opiceblum.com.br/lang-pt/02_artigos_a001.html?ID_ARTIGO=119#>. Acesso em 11. nov. 2014.

[70] BRASIL. Projeto de Lei do Senado nº 385/2005. Disponível em: < http://www.senado.gov.br/atividade/materia/Consulta>. Acesso em: 11 nov. 2014.

[71] BRASIL. Projeto de Lei do Senado nº 6.024/2005. Disponível em: < http://www.senado.gov.br/atividade/materia/Consulta>. Acesso em: 11 nov. 2014.

[72] BRASIL. Projeto de Lei do Senado nº 463/2003. Disponível em: < http://www.senado.gov.br/atividade/materia/Consulta>. Acesso em: 11 nov. 2014.

PLC 3.891/00[73], apresentado em 06.12.2000 (Dep. Julio Semeghini, PSDB/SP). Dispõe sobre o registro de usuários pelos provedores de serviços de acesso a rede de computadores, inclusive à Internet. Obriga os provedores de serviço da Internet a manterem registros de seus usuários, e dados referentes a cada transação atendida pelo provedor, para solucionar o problema de identificação do usuário em caso de utilização ilícita da rede, cometidas, em geral, por *hackers* ou *crakers*.

PLS 76/00[74], apresentado em 27.03.2000 (Sem. Renan Calheiros, PMDB/AL). Define e tipifica os delitos informáticos, e dá outras providências.

A lei do Marco Civil da Internet (12.965/2014[75]), aprovada em 23 de Abril de 2014, regulamenta a internet, com um texto que garante direitos de privacidade, neutralidade na rede, garantia de liberdade de expressão, bem como obrigações de responsabilidade civil aos usuários e provedores.

O Marco Civil da Internet obriga que os registros de conexão dos usuários devem ser guardados pelos provedores de acesso pelo período de um ano, sob total sigilo e em ambiente seguro. Essas informações dizem respeito apenas ao IP, data e horas inicial e final da conexão. O texto ainda faculta aos provedores a guarda de registros de Acesso a Aplicações de Internet - que ligam o IP ao uso de aplicações da internet – por seis meses.

A lei também estabelece que a guarda de registros seja feita de forma anônima. Ou seja, os provedores poderão guardar o IP, nunca informações sobre o usuário. A disponibilização desses dados, segundo o texto, só poderá ser feita mediante ordem judicial.

---

[73] BRASIL. Projeto de Lei da Câmara nº 3.891/2000. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=20405>. Acesso: em 11 nov. 2014.

[74] BRASIL. Projeto de Lei do Senado nº 76/2000. Disponível em: < http://www.senado.gov.br/atividade/materia/Consulta>. Acesso em: 11 nov. 2014.

[75] BRASIL. Lei 12.965/2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 out. 2014.

5.2. CONVENÇÃO DE BUDAPESTE

Tendo em vista essa modalidade de crimes ter abrangência internacional o Conselho da Europa, em 21 de Setembro de 2001 firmou a Convenção de Budapeste, visando a discutir as normas a serem utilizadas no combate ao crime cibernético, nos Estados membros e demais países que fizessem a adesão, dando ênfase a uma legislação adequada, à cooperação internacional e questão da extraterritorialidade que envolve esses crimes.

O mencionado acordo tem por objetivo principal a estruturação, em caráter prioritário, de uma política criminal internacional, protegendo a sociedade contra a criminalidade no espaço cibernético por intermédio da adoção de normas adequadas, visando a melhoria da cooperação internacional, tendo em vista que as profundas mudanças provocadas por meio da informatização, convergência e globalização permanente das redes e sistemas informatizados contribuem para aumentar o risco de que a informação digital seja utilizada para cometer inúmeros delitos, principalmente por intermédio do armazenamento e da divulgação criminosa dessas mencionadas informações, fotografias, vídeos, dados diversos, além dos conteúdos acessados e tratados ilicitamente por meio da invasão aos sistemas de redes com capilaridade regional e nacional[76].

A Convenção de Budapeste veio a tipificar as seguintes condutas:

> Infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos: a) acesso doloso e ilegal a um sistema de informática; b) interceptação ilegal de dados ou comunicações telemáticas; c) atentado à integridade dos dados (conduta própria de um subgrupo hacker, conhecido como cracket; d) atentado à integridade de um sistema; e) produção, comercialização, obtenção ou posse de aplicativos ou códigos de acesso que permitam a prática dos crimes acima indicados.
>
> Infrações informáticas: a) falsificação de dados; b) estelionatos eletrônicos
>
> Infrações relativas ao conteúdo: a) pornografia infantil (produção, oferta, procura, transmissão e posse de fotografias ou imagens realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito); b) racismo e xenofobia (difusão de imagens, ideias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência

[76] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.212.

> contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica; injúria e ameaças qualificadas pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade);
>
> Atentado à propriedade intelectual e aos direitos que lhe são conexos[77].

Na América Latina não há fonte emergente de doutrina que trate sobre os *crimes cibernéticos* e a produção legislação é insignificante. A grande diretriz que surge no direito internacional, como já mencionada anteriormente, é a Convenção de Budapeste contra o Cibercrime*,* que permanece em sua diretriz fundamental e aguarda a aderência do Brasil e demais países remanescentes a esse tratado para que surta os efeitos desejados nos sistemas normativos de cada nação, objetivando criar uma solução jurídica internacional eficaz aos delitos voltados para o ambiente digital[78].

[77]Disponível em: <http://www.wirelessbrasil.org/wirelessbr/secoes/crimes_digitais/texto_convencao.pdf>. Acesso em: 03 nov. 2014

[78] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.215.

6 PROVA

No direito, durante os procedimentos processuais existentes no ordenamento jurídico, a parte envolvida no litígio deverá não apenas alegar os fatos de que tem convicção, mas também comprová-los, demonstrando ao magistrado a veracidade das afirmações feitas em juízo. A ferramenta utilizada para tanto se trata das provas, que uma vez produzidas, em geral na fase instrutória do processo, serão acostadas aos autos.

Desta feita, a prova é o somatório entre o material ora juntado ao processo e o estado psíquico causado ao magistrado, levando-o a entender os fatos alegados como verdadeiros, os quais são denominados objetos da prova, enquanto a busca pelo convencimento do juiz é chamado de finalidade da prova, sendo ele o destinatário desta ferramenta processual.

Em relação à valoração dada à prova apresentada durante o procedimento, existem três sistemas históricos no Brasil. O primeiro é o do critério legal, onde o magistrado está restrito ao valor determinado pela própria legislação pátria, que elencava as diversas formas de se comprovar um determinado fato, e hierarquizava-as, hoje não mais utilizado.

O segundo sistema era chamado de livre convicção, e também não é mais utilizado atualmente. Oposto ao primeiro sistema, ele determinava que a íntima convicção do juiz como a maneira para valorar as provas, extremando mais uma vez uma regra que possibilitava até mesmo a julgamento da lide contrário às provas dos autos, se assim entendesse correto o julgador.

Por fim, o terceiro sistema é conhecido como persuasão racional, ou livre convencimento motivado. Poderia ser entendido como a junção dos dois primeiros, haja vista se tratarem de dois extremos. A verdade é que nesse sistema o juiz realiza uma análise lógica das provas acostadas aos autos, de maneira que ao valorá-la deverá fundamentar sua decisão, explicando as razões pelas quais formou determinado juízo de valor. Assim, sem a rigidez do primeiro sistema, nem a

libertinagem do segundo, é possível dar liberdade ao magistrado para que encontre a verdade acerca dos fatos tratados na demanda, sem que se anule a fiscalização estatal, realizada na fundamentação das decisões, que não pode ser arbitrária, seguindo critérios legais.

Ressalva-se, entretanto, que não apenas as partes poderão produzir provas durante a instrução processual, como também o juízo poderá determiná-las, de maneira que ao final da ação se conheça a verdade real dos fatos, e não apenas uma verdade formal, sem que, para tanto, fira o princípio da imparcialidade e se torne um inquisidor.

A esse respeito Humberto Theodoro Junior *Apud* Adeneele Garcia[79], ensina que a convicção do magistrado estará condicionada a:

> a) aos fatos nos quais se funda a relação jurídica controvertida;
> b) às provas desses fatos, colhidas no processo;
> c) às regras legais e máximas de experiências;
> d) e o julgamento deverá ser motivado.

Baseado no princípio da busca da verdade processual, seguindo esta corrente ideológica à qual se filia Luigi Ferrajoli, o juiz poderá determinar a produção de prova que será obtida, por intermédio da execução de laudos periciais, exames de corpo de delito, oitiva das testemunhas, dos acusados, dos ofendidos, inclusive efetuando acareações e reconhecimento de pessoas ou coisas, além de confissões ou documentos e objetos coletados por meio de mandados de busca e apreensão[80].

No ordenamento jurídico pátrio, não há qualquer empecilho para a utilização de provas eletrônicas, conforme versa o art. 225 do Código Civil[81]:

> As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos

[79] CARNEIRO, Adeneele Garcia. **Crimes Virtuais:** elementos para uma reflexão sobre o problema na tipificação. Disponível em: http://www.ambito-juridico.com.br/. Acesso em: 02 ago.2014.
[80] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.55.
[81] BRASIL.Lei nº 10.406/2002: Código Civil. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em 10 out. 2014.

> ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão.

Ademais, o art. 332 do Código de Processo Civil[82] versa que:

> Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa.

O Código de processo pena[83]l também aceita as provas eletrônicas, conforme versa o art. 231:

> salvo os casos expressos em lei, as partes poderão apresentar documentos em qualquer fase do processo.

Ademais, o art. 232 do mesmo diploma legal também versa que

> consideram-se documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares.

A justa causa,construção doutrinária, consiste num suporte mínimo probatório necessário ao início da ação penal. Este lastro de prova também é imprescindível nos crimes de informática. A preocupação inicial, na fase investigatória, deve ser apurar a existência do crime e descobrir quem foi o seu autor[84].

Em se tratando de crime perpetrado através da internet, é necessário identificar a máquina utilizada. Mas não é só. Em muitos casos, um único computador é utilizado por diversas pessoas, sejam membros de uma família, sejam estudantes de uma escola ou universidade ou funcionários de uma empresa. Em tais casos, a investigação deve identificar quem efetivamente utilizou o computador para a prática delituosa. Sem esta apuração não será possível o oferecimento da denúncia[85].

---

[82] BRASIL.Lei nº 5.869/73: Código de Processo Civil. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l5869compilada.htm>. Acesso em 10 out. 2014.
[83]BRASIL.Decreto - Lei nº 3.589/73: Código de Processo Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em 10 out. 2014.
[84] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 80.
[85] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 80.

Particularmente sobre a investigação policial e a posterior confecção de laudo pericial, o sucesso ou insucesso de tais provas depende inicialmente da capacitação do investigador e do perito, tornando-os aptos ao manuseio de moderníssima tecnologia para se buscar os indícios que possibilitarão o ato de flagrante de delito virtual ou a coleta de provas por intermédio do cumprimento de mandados de busca e apreensão, preservação do loca, dos instrumentos e objetos do crime[86].

Sobre o local do crime, tanto a autoridade policial quanto a judiciária deverão determinar que os peritos recriem o ambiente virtual no qual ocorreu o delito, utilizando-se dos vestígios deixados pelo "cracker" ou "hacher", quando da consumação do crime cibernético, além de efetuar a apreensão de computadores, periféricos, aplicativos e principalmente, descrever minúcias o "*inter criminis*", o que possibilitará ao membro do Ministério Público (MP) uma denúncia alicerçada em provas idôneas e irrefutáveis para que o magistrado forme seu convencimento inequívoco sobre a culpabilidade do acusado e a posterior condenação do criminoso cibernético[87].

Com efeito, é fácil concluir que a investigação nos crimes praticados através da Internet deverá ser especializada, sustentada em meios tecnológicos precisos.

6.1 MEIOS DE PROVA

Os chamados meios de prova são os meios pelos quais a provas serão produzidas. Em especial no ramo do direito penal, onde vige o princípio da verdade real, não existe limitação aos meios de prova, reduzindo ao máximo os requisitos legais exigidos para a produção da prova processual, haja vista entender-se que as limitações prejudicam a descoberta real, e resulta na descoberta da verdade formal.

A produção da prova na instrução processual clássica pode ser feita por intermédio de documentos, vistorias, perícias, inspeções judiciais, declarações das

[86] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.55.
[87] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.56.

partes e testemunhas. O título VII do Código de Processo Penal[88] foi reservado à temática da prova, sendo que, no capítulo III está preceituado o interrogatório do acusado, no capítulo IV coube abordar a confissão, no capítulo V tratou-se dos preceitos referentes ao ofendido, no capítulo VI a abordagem sobre as testemunhas, no capítulo VII fez-se o reconhecimento de pessoas ou coisas, no capítulo VIII tratou-se da acareação, no capítulo IX o espaço foi reservado aos documentos, no capítulo X foram tratados sobre os indícios e no capítulo XI a atividade de busca e apreensão. [89]

A única limitação determinada é a licitude das provas. Ainda que não estejam previstas em lei as provas serão admitidas, desde que sejam consideradas licitas.

Especificamente, podemos citar algumas das provas pelas quais se podem demonstrar a ocorrência de um fato típico, como a realização de exame de corpo de delito e perícias em geral, capazes de determinar as marcas deixadas pela execução do delito nas maquinas utilizadas como meio para o cometimento do ilícito; interrogatório do acusado, onde a busca pela verdade real dos fatos pode ser solucionada com as palavras do executor; confissão, prova segura acerca da autoria delitiva; perguntas ao ofendido, pois a vítima pode fornecer indícios capazes de apontar o autor do fato, bem como comprovar a materialidade do crime; testemunhas, meio de prova mais difícil, haja vista ser o meio virtual utilizado em razão do facilidade em se manter anônimo; reconhecimento de pessoas ou coisas, acareação, quando os depoimentos das testemunhas se contradizem; documentos, acostados aos autos para demonstrar a veracidade das alegações; e, por fim, os indícios e busca e apreensão, para ampliar o conjunto probatório dos autos.

A prova no crime cibernético deve se submeter às mesmas disposições dos processos tradicionais, adequando-se a investigação criminal e a instrução processual no sentido da busca por efetividade e legitimidade.

---

[88] BRASIL.Decreto - Lei nº 3.589/73: Código de Processo Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em 10 out. 2014.
[89] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.83.

A escassez doutrinária sobre o assunto direciona para a utilização do direito comparado ou preceitos de lei que se aproximem da realidade demonstrada no caso concreto. Equivocadamente se recorre ao uso da analogia e da hermenêutica jurídica para preencher as lacunas legais que são diversas, diante da omissão e apatia legislativa[90].

Assim, o exame pericial, as inspeções judiciais e a busca e apreensão transformam-se em ferramentas eficientes na produção da prova no crime cibernético, diante de uma realidade em que impera a escassez de técnicas e recursos humanos para investigar, processar, punir o criminoso cibernético.

6.1.1 Prova Pericial

Perícia é um meio de prova que consiste num exame feito por alguém com conhecimento técnico científico. O juiz, como ser humano que é, não tem obrigação de saber de tudo. Muitas vezes necessita do auxílio de outras pessoas para esclarecer fatos e fornecer informações. Assim ocorre em assuntos relativos à Medicina, Engenharia, e Informática. Desta forma, para julgar o réu pela prática de um crime de informática, o juiz não precisa conhecer o sistema de funcionamento de um computador. Mesmo que o juiz seja da época da antiga máquina de escrever, ele terá auxílio de uma pessoa que conhece profundamente a informática, a Internet e seus mecanismos - o Perito. Assim, este é um auxiliar do magistrado[91].

A investigação criminal e a instrução processual demandam procedimentos técnicos para dar legitimidade à prova produzida mediante o crime cibernético que será executada por intermédio do exame de corpo de delito e dos exames e dos exames periciais, a fim de apontar a veracidade do fato, sendo elaborado por profissionais especializado em *hardware*, *software*, tráfego e segurança de rede[92].

---

[90] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.83.
[91] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 113.
[92] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.80.

A perícia poderá ser determinada pela autoridade policial (art. 6º, VII, CPP) ou pelo juiz. As partes, no entanto, podem requerer sua produção, a acusação deverá fazê-lo quando do oferecimento da denúncia ou na fase das diligências e a defesa na defesa prévia ou também na fase das diligências[93].

Esses mencionados profissionais poderão definir sobre a existência de vestígios da atividade criminosa desenvolvida e efetivada no ambiente cibernético, por exemplo, indicando a origem de um email, sua autoria, integralidade, adulteração, destinatário, itinerário utilizado para chegar ao destino final, endereços virtuais envolvidos, protocolo de comunicação (*Internet Protocol - IP*) que identificará sua tramitação e propriedades físicas[94].

Desta forma, o exame pericial identificará o email, objeto de investigação criminal e da produção probatória judicial que, caso seja necessário, poderá ser estendida à máquina que originou tal mensagem que servirá de prova documental[95].

A prova pericial é necessária nos crimes que deixam vestígios (art. 158, CPP). Os crimes de informática, em regra, são infrações não transeuntes. Desta forma o corpo de delito tem que ser submetido à análise. A perícia deverá ser feita por pessoa que possua conhecimento técnico sobre informática, programação e internet. O perito deverá informar ao juiz o tipo de equipamento, os programas instalados, os arquivos e outras considerações que considerar importantes. O laudo deverá ser elaborado com minuciosa descrição do material, além de conter as respostas aos quesitos que forem formulados (art. 160, CPP)[96].

Para realização da perícia, será preciso buscar e apreender o computador, na forma do artigo 240 do CPP. A busca poderá ser determinada de ofício pela autoridade ou mediante requerimento das partes (art. 242, CPP). O mandado de busca deverá conter o local da diligência, o nome do proprietário, o motivo, os fins da diligência e a assinatura da autoridade (art. 243, CPP). Realizada a busca e apreendido o material, este será encaminhado aos peritos. Nossa lei determina que

[93] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 113.
[94] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.80.
[95] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.80.
[96] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 114.

sejam dois peritos oficiais; nos locais onde não houver, duas pessoas idôneas (art. 159, CPP)[97].

6.1.2 Busca e Apreensão

A perícia judicial também pode ser efetuada na estação de trabalho, no computador pessoal ou qualquer outro equipamento que seja objeto de investigação, sendo necessária uma ordem judicial de busca e apreensão com natureza cautelar, a fim de que se verifique a procedência ou improcedência de email, arquivo, registro ou programa que tenha sido objeto do crime, por intermédio daquele *IP adress* (IP ADDRESS = endereço de protocolo de comunicação para a internet - Internet Protocol - IP)[98].

O citado autor aduz que as tecnologias de recuperação de dados apagados em computador estão cada vez mais modernas e têm permitido, inclusive, refazer toda a estrutura de um HDD(hard disk drive) mesmo depois de duas operações de formatação de dados. E acrescenta que com essa medida cautelar, o magistrado poderá certificar-se da materialidade e autoria do delito pela análise do objeto e do lugar do crime, ressalvada a atividade com equipamentos móveis (notebooks, ipod, telefone celular).

Caso os vestígios sejam insuficientes ou inexistentes por terem sido apagados de forma irrecuperável, poderá ainda o juiz dirigir-se, mediante ofício, ao administrador de determinado provedor de internet, ordenando que a mencionada empresa apresente os dados armazenados e registros de tráfego de rede sobre o usuário investigado[99].

---

[97] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 115.
[98] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.82.
[99] DARÓS MALAQUIAS, Roberto Antonio. Op. Cit., p.82.

7 O PROBLEMA DA AUTORIA

A identificação dos autores nos crimes cibernéticos é um dos grandes desafios para as autoridades na *persecutio criminini*s. Tal realidade não é restrita ao Brasil, mas a todos os países em que a internet está presente.

Um indivíduo que se encontra na cidade de São Paulo, por exemplo, pode enviar um email com vírus para um computador localizado na cidade de Belém. Caso o vírus cause danos significativos no referido computador, presume-se que o proprietário se dirigirá a uma Delegacia de Polícia para noticiar o fato e a partir daí inicia-se a dificuldade, pois sem meios tecnológicos, não há a possibilidade de saber sequer de onde partiu o email portador do vírus.

Nos crimes praticados através da Internet, não é difícil a identificação da máquina utilizada, o problema é saber quem utilizou o computador para cometer a infração. A identificação da autoria deve ser precisa, não pode a autoridade policial indiciar o proprietário do computador, ou o Ministério Público denunciá-lo, sem possuir outros elementos de prova, além do fato de ser ele o dono do equipamento. Na imensa maioria das vezes, o computador não é privativo de uma só pessoa, ao contrário, várias podem utilizá-lo(...). Necessária uma precisa investigação para tentar identificar a autoria[100].

Quando um usuário navega na internet, lhe é atribuído um numero de IP – Internet Protocol. É esse numero que propicia a identificação do usuário na rede, ou a investigação de algum crime que tenha ocorrido, a questão é que este número só é atribuído ao usuário no momento em que ele esta conectado, após este período, quando o mesmo desligar o modem, o endereço de IP será atribuído a outro usuário, caso o mesmo não tenha optado por um IP Fixo.

O IP quando solicitado ao provedor de acesso à internet, deve vir acompanhado de data, hora da conexão, e o fuso horário do sistema, sendo que esses dados são imprescindíveis, tendo em vista que sem os mesmos fica

[100] CASTRO, Carla Rodrigues Araujo de. Op. Cit., p. 95.

impossível fazer a quebra de sigilo dos dados. Após a localização do provedor, deve-se requerer ao juiz o pedido de quebra do sigilo de dados telemáticos, para que o provedor de acesso informe quem estava vinculado ao endereço de IP naquele momento em que ocorreu o crime, ou seja, seu endereço físico.

A começar pela característica dos agentes que praticam os crimes desse gênero. Geralmente, esses indivíduos possuem elevado conhecimento a respeito da informática e, por tal motivo, procuram agir sem levantar suspeitas.

Somente a título de exemplo, os hackers costumam utilizar celulares clonados para ter acesso à Internet, inviabilizando a identificação do local da chamada e de seu autor, mediante rastreamento de sinal[101].

Esses agentes comumente praticam crimes em lugares públicos, isto é, lugares onde o acesso ao computador é destinado a um grande número de pessoas. Não adiantaria identificar o computador nestes casos, pois inúmeros são os seus usuários. É o que ocorre, por exemplo, nos denominados “Cyber Café’s”.

Com efeito, não se dúvida que a identificação dos autores dos crimes cibernéticos é um grande desafio para as autoridades responsáveis pela investigação. Contudo, tudo indica que esses problemas serão minimizados ou até mesmo solucionados futuramente. No Brasil, já é possível verificar alguns avanços, no sentido de existirem Delegacias e Promotorias especializadas nesta seara de crimes.

Não raramente surgem notícias de casos envolvendo crimes praticados através da Internet, onde os componentes das quadrilhas especializadas nesses crimes são identificados. Uma atitude que vem sendo utilizada é a quebra de sigilo bancário dos suspeitos, prática eficaz nos crimes que envolvem questão patrimonial.

[101] ARAS, Vladimir.Crimes de Informática.Uma nova criminalidade. **Jus Navigandi**, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/artigos/2250>. Acesso em: 8 jul. 2014.

A tendência é que surjam instrumentos tecnológicos capazes de identificar os usuários, mesmo se estiverem em lugares públicos. Técnicas biológicas, como a impressão digital, a análise de pupila, ou até mesmo o uso de assinaturas digitais, criptografia por chaves assimétricas, etc., poderão ser utilizadas no combate à impunidade. De acordo com Vladimir Aras[102]:

> [...] O único método realmente seguro de atribuição de autoria em crimes informáticos é o que se funda no exame da atuação do responsável penal, quando este se tenha valido de elementos corporais para obter acesso a redes ou computadores. Há mecanismos que somente validam acesso mediante a verificação de dados biométricos do indivíduo. Sem isso a entrada no sistema é vedada. As formas mais comuns são a análise do fundo do olho do usuário ou a leitura eletrônica de impressão digital, ou, ainda, a análise da voz do usuário.

O citado autor complementa dizendo:

> [...] Como dito, somente os mecanismos de assinatura eletrônica e certificação digital e de análise biométrica podem conferir algum grau de certeza quanto à autoria da mensagem, da informação, ou da transmissão, se considerado o problema no prisma penal.

Apesar de todos os problemas, a sociedade é esperançosa no sentido de surgirem novos mecanismos para o combate dos crimes informáticos. Mesmo sem os precisos mecanismos, os operadores do direito continuarão lutando em busca da solução dos inúmeros problemas, apesar das incontáveis dificuldades.

[102] ARAS, Vladimir.Crimes de Informática.Uma nova criminalidade. **Jus Navigandi**, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/artigos/2250>. Acesso em: 8 jul. 2014.

8 NECESSIDADE DE ORDEM JUDICIAL PARA OBTENÇÃO DE DADOS SOBRE O USUÁRIO DA INTERNET

Importa ressaltar que não podemos confundir “interceptação de dados telemáticos” com “quebra de sigilo dos dados de conexão e de usuário”.

A primeira diz respeito ao recebimento por parte da Autoridade Policial de todos os acessos e conexões realizados pelo investigado em ambiente de Internet. Se equipara, em todas as questões legais, à interceptação telefônica, devendo, portanto, ser realizada em sede de Inquérito Policial, sendo necessária, portanto, a provocação do Poder Judiciário e Ministério Público, por meio de Representação, a fim de obtermos a autorização judicial, nos moldes da legislação vigente.

A segunda, a quebra do sigilo dos dados de conexão e de usuário, trata-se “somente” da disponibilização por parte das empresas, em um primeiro momento, qual teria sido o IP utilizado e o horário (incluindo informações de fuso horário) de determinada ação criminosa realizada em um serviço de Internet, como redes sociais, contas de e-mail, programas de mensagens instantâneas, dentre outros e em um segundo momento das informações do usuário que efetivamente utilizou aquele IP de determinado provedor, ou seja, qual teria sido, supostamente, o endereço físico no “mundo real” em que o computador ou outro equipamento informático com acesso à Internet estaria instalado no momento da conduta criminosa[103].

O requisito de ordem judicial para obtenção de ordem de toda e qualquer informação relativa a um crime cibernético é outra questão que atravanca a investigação e representa uma das facetas do excesso de burocracia, que apenas prejudica e/ou retarda o esclarecimento desse tipo de delito. A solução ficaria na necessária diferenciação entre os acessos aos dados cadastrais e aos *logs* de conexão e/ou de acesso[104].

---

[103] CORRÊA, Rafael. **Quebra de sigilo de IP necessita de autorização judicial?** Disponível em <http://rafaelcorrea.com.br/quebra-ip/>. Acesso em 29 Jan 2015.
[104] WENDT, Emerson; Jorge, Higor Vinícius Nogueira.Op. Cit., p. 236.

A exemplificação prática dos dias atuais está na obtenção de dados cadastrais sem ordem judicial, por exemplo, junto à Microsoft do Brasil (nos casos de dados cadastrais do Outlook (Hotmail), Live etc.) e Mercado Livre(www.mercadolivre.com.br).

A prática adotada pelos administradores de tais sites, relaciona-se com seu aspecto contratual, ou seja, todos os que se cadastram e usam dos serviços aceitam os "Termos de Uso" e as "Políticas de Privacidade" e, no contexto, esses sites podem fornecer as informações aos órgãos públicos da lei, independentemente de ordem judicial. Infelizmente poucos administradores de sites e serviços perfilam entendimento semelhante, de modo que prevalece o posicionamento sobre a necessidade de determinação judicial para que forneçam essas informações[105].

[105] WENDT, Emerson; Jorge, Higor Vinícius Nogueira.Op. Cit., p. 236.

9 DELEGACIAS ESPECIALIZADAS

A falta de capacitação dos policiais e também de outros atores da persecução penal, como o Ministério Público e o Judiciário, representa um grande desafio, na medida em que pode impedir a punição dos cibercriminosos e, por consequência causar impunidade.

O Brasil tem avançado significativamente quanto à criação de núcleos de investigações especializados no combate e prevenção de delitos cometidos por meios eletrônicos, como a criação das Delegacias Especializadas de Repressão a Crimes contra Informática e Fraudes eletrônicas.

No âmbito Federal é possível contar com a Unidade de Perícia Informática da Polícia Federal, criada desde de 1996 e denominada como SEPFIN (Serviço de Perícia em Informática). Ademais, devido à crescente criminalidade eletrônica e a necessidade de criar meios preventivos para reduzir tal criminalidade, foram desenvolvidas no Brasil iniciativas privadas especializadas no recebimento de denúncias de crimes que violem os direitos humanos praticados pelo meio virtual.

Este é o caso da organização não governamental SaferNet Brasil, que é uma associação civil de direito privado, entidade com referência nacional no enfrentamento aos crimes e violações aos Direitos Humanos na Internet através de acordos de cooperação firmados com instituições governamentais, a exemplo do Ministério Público Federal, e as denuncias são feitas pelo link: http://www.safernet.org.br/site/denunciar[106].

Alguns estados brasileiros já contam com delegacias especializadas, são eles: São Paulo, Rio de Janeiro, Espírito Santo, Paraná, Rio Grande do Sul, Goiás, Pará, Mato Grosso, Sergipe e Distrito Federal, no entanto, estão localizados apenas em suas capitais[107].

.

---

[106] **Crimes virtuais: Como proceder? Disponível em** www.cyber**crimes**.com.br/p/**delegacias-especializadas**.html. Acesso em: 25 out 2014.

[107] **Delegacias especializadas em crimes virtuais.** Disponível em <www.safernet.org.br/site/prevencao/orientacao/delegacias>. Acesso em: 30 out 2014.

10 CONCLUSÃO

No presente trabalho foi abordado a utilização da internet e da tecnologia por criminosos para a prática delituosa: os denominados crimes cibernéticos. Foram apontadas as dificuldades encontradas para a resolução de tais crimes.

Demonstrou-se que, sendo o Direito regulador da ordem na sociedade cabe, a este acompanhar os avanços e atualizar o ordenamento jurídico para a tipificação de tais condutas.

As considerações demonstradas ensejam o melhor entendimento do tema que apesar de complexo vem tomando grande espaço em nossas vidas. Demonstrou a premente necessidade da regulamentação das condutas delituosas praticadas por meios eletrônicos, analisou-se a dificuldade de obtenção de provas nesse tipo de delito, bem como a dificuldade para identificar a autoria do crime.

A legislação já existente mostra-se insuficiente frente aos crimes praticados por meio da internet, verificando-se assim, a necessidade da tipificação de determinadas condutas delituosas no nosso ordenamento jurídico, adequando-o à essa nova modalidade.

É fácil vislumbrar que a tecnologia não só potencializou as ações criminosas como passou a exigir do Estado uma nova postura institucional. São necessários avanços legislativos, hermenêuticos e investigatórios para exercer um efetivo papel regulador no mundo virtual.

É possível concluir que as normas penais existentes no Brasil não são suficientes para punir as condutas delituosas ocorridas na Internet, pois tais leis devem ser mais específicas, acrescentando, por exemplo, circunstâncias agravantes ou de aumento de pena. Ou ainda a melhor medida aplicável ao combate à criminalidade informática é a assinatura do Brasil à Convenção de Budapeste, vez que possui em seu corpo textual medidas revestidas de proporcionalidade e razoabilidade além da liberdade conferida aos seus signatários de tomar as medidas

legislativas que acharem necessárias sem estar em desacordo com a convenção e sem perder o seu poder soberano, para que a partir de uma legislação específica seja possível buscar procedimentos eficazes e concretos ao tratamento desses delitos.

Em linhas de conclusão, percebe-se que os crimes cibernéticos provocam enormes prejuízos financeiros, patrimoniais e pessoais à sociedade, e até o presente momento a ampla maioria das condutas ilícitas no ambiente cibernético permanecem sem previsão legal e, portanto sendo condutas atípicas.

Esse novíssimo fenômeno criminoso campeia sem obstáculos pelo sistema jurídico, enquanto não cessam de surgir novos "tipos penais cibernéticos" que surpreendem os operadores do direito, deixando a sociedade assustada e perplexa, diante dos legisladores que se mostram vagarosos e silentes. É de fundamental importância uma análise criteriosa, responsável e ética a respeito do tema cibercriminalidade, posicionando-se urgentemente pela reestruturação do sistema normativo.

11 REFERÊNCIAS

ARAS, Vladimir.Crimes de Informática.Uma nova criminalidade. **Jus Navigandi**, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/artigos/2250>. Acesso em: 8 jul. 2014.

BLUM, Renato Opice. **Crimes Eletrônicos**: A nova lei é suficiente? Disponível em <http://www.opiceblum.com.br/lang-pt/02_artigos_a001.html?ID_ARTIGO=119#>. Acesso em 11. nov. 2014.

BOGO, Kellen Cristina. **A história da Internet: como tudo começou.** 2000. Disponível em < http://www.portalguia.com.br >. Acesso em 09 jun. 2014.

BRASIL. Constituição Federal de 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em 10 out. 2014.

BRASIL. Decreto-Lei nº 2.848/40: Código Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 10 out. 2014.

BRASIL. Lei 12.737/2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 10 out. 2014.

BRASIL. Lei 12.965/2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 out. 2014.

BRASIL. Projeto de Lei da Câmara nº 3.891/2000. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=20405> . Acesso: em 11 nov. 2014.

BRASIL. Projeto de Lei do Senado nº 385/2005. Disponível em: < http://www.senado.gov.br/atividade/materia/Consulta>. Acesso em: 11 nov. 2014.

BRASIL. Projeto de Lei do Senado nº 463/2003. Disponível em: < http://www.senado.gov.br/atividade/materia/Consulta>. Acesso em: 11 nov. 2014.

BRASIL. Projeto de Lei do Senado nº 6.024/2005. Disponível em: < http://www.senado.gov.br/atividade/materia/Consulta>. Acesso em: 11 nov. 2014.

BRASIL. Projeto de Lei do Senado nº 76/2000. Disponível em: < http://www.senado.gov.br/atividade/materia/Consulta>. Acesso em: 11 nov. 2014.

BRASIL. Decreto - Lei nº 3.589/73: Código de Processo Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em 10 out. 2014.

BRASIL.Lei nº 5.869/73: Código de Processo Civil. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l5869compilada.htm>. Acesso em: 10 out. 2014.

CARNEIRO, Adeneele Garcia. **Crimes Virtuais:** elementos para uma reflexão sobre o problema na tipificação. Disponível em: http://www.ambito-juridico.com.br/. Acesso em: 02 ago.2014.

CASTRO, Carla Rodrigues Araujo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003.

CERT.br. **Cartilha de Segurança para Internet**. Disponível em: <http://cartilha.cert.br>. Acesso em: 15 set.2014.

CORRÊA, Rafael. **Quebra de sigilo de IP necessita de autorização judicial?** Disponível em <http://rafaelcorrea.com.br/quebra-ip/>. Acesso em 29 Jan 2015.
Crimes virtuais: Como proceder? Disponível em www.cyber**crimes**.com.br/p/**delegacias**-**especializadas**.html. Acesso em: 25 out 2014.

DAOUN, Alexandre Jean. **Os novos crimes de informática**. Disponível em: <http://www.advogado.com/internet/zip/novocrim. Acesso em 05. nov.2014.

DARÓS MALAQUIAS, Roberto Antonio. **Crime cibernético e prova:** A investigação criminal em busca da verdade.Curitiba: Juruá, 2012, p. 64.

Delegacias especializadas em crimes virtuais. Disponível em <www.safernet.org.br/site/prevencao/orientacao/delegacias>. Acesso em: 30 out 2014.

FERNANDES, David Augusto. **Crimes Cibernéticos: O descompasso do Estado e a realidade.** Disponível em: http://www.direito.ufmg.br/revista/index.php/revista/ . Acesso em 17. Set. 2014.

FERREIRA, Ivette Senise. **Direito e Internet**: Aspectos jurídicos relevantes. 2 ed. São Paulo: Quartier Latin, 2005, p.26.

GOUVEIA, Sandra Medeiros Proença. **O direito na era digital**: Crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997. Disponível em: <http://books.google.com.br/books>. Acesso em: 16 jul. 2014.

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. **Boletim do IBCCrim**. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

HISTÓRIA. **História da internet**. Disponível em: <http://www.slideshare.net/guest06f3c/historia-da-internet-1162354>. Acesso em: 16 jul. 2014.

INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**.São Paulo: Editora Juarez de Oliveira, 2009.

MENDES, Eugenia Gonçalves Mendes; VIEIRA, Natalia Borges. **Os Crimes cibernéticos no ordenamento jurídico brasileiro e a necessidade de legislação específica**. Disponível em: http://www.gcpadvogados.com.br/artigos/ . Acesso em: 31 Out. 2014.

MINISTÉRIO PÚBLICO FEDERAL - PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO - GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. **Crimes Cibernéticos:** Manual Prático de Investigação. São Paulo, 2006. Disponível em: < http://www.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1ticaversaofinal.pdf >. Acesso em: 15 out. 2014.

MIRABETE, Júlio Fabbrini. **Manual de Direito Penal**: Parte Geral. 19 ed. São Paulo: Atlas, 2003, p. 122.

WENDT, Emerson; Jorge, Higor Vinícius Nogueira. Crimes ciberneticos: Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2013.