FACULDADE DE DIREITO DE CACHOEIRO DE ITAPEMIRIM - FDCI

BRUNO DE PAULA MAGANHI

CRIMES INFORMÁTICOS: ASPECTOS RELEVANTES SOB A ÓTICA DA LEGISLAÇÃO BRASILEIRA PENAL

CACHOEIRO DE ITAPEMIRIM-ES
2017

BRUNO DE PAULA MAGANHI

CRIMES INFORMÁTICOS: ASPECTOS RELEVANTES SOB A ÓTICA DA LEGISLAÇÃO BRASILEIRA PENAL

Monografia Jurídica apresentada ao curso de Direito da Faculdade de Direito de Cachoeiro de Itapemirim como requisito parcial para obtenção do título de bacharel em Direito.
Orientador: Prof. Izaias Corrêa Barboza Junior

CACHOEIRO DE ITAPEMIRIM-ES
2017

BRUNO DE PAULA MAGANHI

CRIMES INFORMÁTICOS: ASPECTOS RELEVANTES SOB A ÓTICA DA LEGISLAÇÃO BRASILEIRA PENAL

Monografia apresentada à Faculdade de Direito de Cachoeiro de Itapemirim como requisito parcial para obtenção do título de Bacharel em Direito

Aprovada em 04 de outubro de 2017.
Nota: 10,0

BANCA EXAMINADORA

_____
Professor orientador Izaias Corrêa Barboza Junior

_____
Professor Cristiano Hehr Garcia

_____
Professora Márcia Pruccoli Gazoni Paiva

A todos da minha família e amigos que sempre torceram, incentivaram e acompanharam não somente pelo meu sucesso profissional como todos os meus objetivos.

AGRADECIMENTO

Agradeço primeiramente a Deus, pois me sustentou e supriu até aqui, permitindo que eu o louvasse ao vencer mais essa etapa de minha vida.

Agradeço também aos meus pais, Antonio e Angela, pelo apoio demonstrado. A minha família, que sempre esteve presente e apoiaram mais esta geração, por mim representada, que adentra no ramo jurídico. Agradeço, ainda, a Daniele que me acompanhou nessa jornada, suportando e orando pelo meu sucesso. Ele também é seu.

Graças dou aos amigos que ganhei nessa faculdade e que me acompanharam e viveram boa parte das dificuldades comigo, sempre me incentivando e ajudando a vencer os contratempos do curso.

Agradeço pela vida da Sônia e do Pablo, da biblioteca. Este projeto não seria possível se não fosse a assistência de vocês.

Por último, porém um dos mais importantes, agradeço ao meu professor Marcus Vinícius, não só pela supervisão como Coordenador do Núcleo de TCC, mas principalmente pela ajuda como amigo, me acalmando diante das dificuldades, e pela orientação dada. Este trabalho só existe graças a intervenção e orientação do senhor.

“Não importa o que aconteça, continue a nadar.”
(WALTERS, Graham: Procurando Nemo, 2003)

MAGANHI, Bruno de Paula. **Crimes Informáticos: Aspectos Relevantes Sob a Ótica da Legislação Brasileira Penal**. 49 f. Monografia (Bacharelado em Direito). Faculdade de Direito de Cachoeiro de Itapemirim-FDCI: Cachoeiro de Itapemirim, 2017.

RESUMO

O presente trabalho busca analisar, de maneira sintética, os aspectos mais importantes e relevantes dos delitos informáticos e do Direito Penal Informático brasileiro. Para tanto, fez-se necessário compreender, inicialmente, o processo de criação da Internet e toda a trajetória traçada para que esta evoluísse e se tornasse essa rede que une todo o planeta. Posteriormente, foram elencados os principais artefatos, métodos e técnicas utilizados no cotidiano virtual e que, por isso, se tornam instrumentos para a prática de crimes. Em seguida foram expostas algumas condutas que podem vir a ser consideradas delitos informáticos, uma vez que, de certa forma, atingem bens informáticos juridicamente protegidos pelo nosso ordenamento jurídico, finalizando, então, com uma análise acerca dos delitos, conceituando-os, expondo características tanto dos delitos quanto dos delinquentes e propondo uma sistematização para a produção de um legislação específica que seja capaz de inibir e punir condutas criminosas virtuais, não se atendo simplesmente às técnicas veiculadas. Este estudo foi realizado através de pesquisas em livros e sites da Internet, em sua grande maioria dada a escassez de doutrinas específicas confiáveis. Por fim, conclui-se que, com o advento da Internet, houve um grande aumento a qualidade de vida das pessoas, entretanto este novo mundo, com infinitas possibilidades, também gerou um campo obscuro, onde a prática de crimes de espalha exponencialmente, principalmente no Brasil onde não há uma legislação específica eficaz. Com o que é tratado neste trabalho, percebe-se a necessidade de uma legislação capaz de inibir e punir delitos virtuais.

Palavras-chaves: Crimes informáticos. Crimes. Informática. Internet. Legislação.

MAGANHI, Bruno de Paula. Computer **Crimes: Relevant Aspects from the Perspective of Brazilian Criminal Law**. 49 p. Monograph (Bachelor of Law). College of Law Cachoeiro de Itapemirim: Cachoeiro de Itapemirim, 2017.

ABSTRACT

This paper aims to analyze, in a synthetic way, the most important and relevant aspects of computer crimes and, the Brazilian Computer Criminal Law. In order to do so, it was necessary to understand, initially, the process of creating the Internet and the entire trajectory traced to evolve and become the network that unites the entire planet. Subsequently, it was listed the main artifacts, methods and techniques used in the virtual daily life and, therefore, they become instruments for the practice of crimes. Thus, some experts consider this conduct as computer crimes, since, to a certain extent; they affect computer assets legally protected by our legal system. Concluding with an analysis of crimes, conceptualizing them, exposing characteristics of both crimes and delinquents and proposing a systematization for the production of a specific legislation that is capable of inhibiting and punishing virtual criminal conduct, not simply following the techniques. Concluding with an analysis of crimes, conceptualizing them, exposing characteristics of both crimes and delinquents and proposing a systematization for the production of a specific legislation that is capable of inhibiting and punishing virtual criminal conduct, not simply following the techniques. This study demanded a research based on books and internet sites, mostly because of the scarcity of specific doctrines. Finally, it is concluded that, with the advent of the Internet, it has been a great increase in people's quality of life, but this new world, with infinite possibilities, has also generated an obscure field, where the practice of crimes spreads exponentially, mainly in Brazil where there is no specific legislation. As this paper shows, it is needed a capable legislation of inhibiting and punishing virtual crimes.

Key-words: Computer crimes. Crimes. Computing. Internet. Legislation.

SUMÁRIO

INTRODUÇÃO

O presente trabalho busca realizar uma análise acerca dos delitos informáticos e seus aspectos mais importantes e relevantes, compreendendo como ocorreu o processo de criação da própria internet que se tornou um meio propício ao crescimento intelectual, diminuição das barreiras geográficas, mas também um meio obscuro onde não se sabe o quão seguro se está, tampouco se já não há vulnerabilidade ou quebra de segurança que possa permitir um terceiro acessar, alterar, modificar ou excluir dados e informações particulares. É imprescindível, também, entender como a legislação brasileira tem se portado diante destes casos, uma vez que constituem uma prática criminosa muito nova e dinâmica onde o Brasil se faz muito prematuro no legislar sobre tal temática.

Como parte inicial deste trabalho, nesta breve introdução, a intenção é apresentar o tema principal já delimitado que motivou a síntese deste trabalho, da mesma maneira que o problema, a justificativa e os objetivos, gerais e específicos, a serem alcançados.

A disposição deste trabalho está dividida em 04 (quatro) capítulos de desenvolvimento. O primeiro buscou, de maneira sucinta, explorar o passado da internet, seu objetivo de criação e no que essa se tornou, visto que é a responsável por permitir interações interpessoais a distância, como também que criminosos virtuais cometam crimes por todo mundo.

O segundo capítulo foi desmembrado em várias seções, buscando expor e explicar as principais técnicas utilizadas para se cometer um *cibercrime*, abordando artefatos físicos (*hardwares*) como também artefatos eletrônicos (*softwares*) que são utilizados por agentes criminosos a fim de acessar um sistema ou uma máquina, e destes manusear banco de dados, informações sigilosas, monitoramento ilegal, e até mesmo o controle total da máquina.

O terceiro capítulo também se divide em alguns capítulos, onde são abordadas algumas condutas que podem vir a ser consideradas crimes informáticos, tais como o acesso ilegítimo à sistemas e computadores alheios, a interceptação ilegítima com o intuito de se colocar no meio entre uma comunicação eletrônica, o dano informático ao alterar ou modificar dados alheios sem permissão, a fraude informática, o

scamming que consiste em esquemas de negócios fraudulentos e, por último, a perturbação de serviços abordando uma ótica mais voltada aos crimes telemáticos.

Por sua vez, o quarto capítulo trouxe alguns aspectos acerca do Direito Penal Informático, tais como, conceito, características, análise do perfil do sujeito ativo nesses crimes, finalizando com uma breve sistemática para futuras, e necessárias, legislações penais específicas.

A fim de produzir este trabalho, foram utilizadas em larga escala pesquisas e artigos de estudiosos do tema. Por ser muito escassa a doutrina específica sobre tal temática, utilizou-se, de maneira muito concentrada duas doutrinas em especial, a saber, o *Manual de Crimes Informáticos*, escrito por Damásio de Jesus e José Antonio Milagre, bem como a obra *Crimes Informáticos e suas Vítimas*, do autor Spencer Toth Sydow.

É valido, ainda, salientar que durante a realização das pesquisas para a elaboração deste trabalho monográfico, algumas dificuldades foram encontradas, como escassez de obras confiáveis, informações desconexas. Entretanto uma se destacou, que foi a impossibilidade de êxito nas buscas realizados nos computadores da faculdade da maioria das técnicas deste trabalho, umas que, por motivos de segurança da rede, boa parte foi bloqueada, dificultando, assim, a elaboração desta monografia.

Com o advento da internet, as relações das pessoas entre si e/ou entre instituições se tornou extremamente veloz, não havendo fronteiras. Desta forma, é fundamental compreendermos como se porta o Direito Penal, em especial o brasileiro, diante deste novo mundo, onde a cada instante milhões se conectam por meio de computadores, celulares, *tablets*, realizando compras, vendas, se comunicando, tudo em tempo real.

1. HISTÓRICO E CONCEITO DA INTERNET

A comunicação interpessoal é o princípio básico para a vivência em sociedade. Expor opiniões, discutir assuntos, expressar vontades, absorver conhecimento são atitudes que nos colocam e compõem a comunidade humana formando, assim, civilizações e históricos.

Diante disso, o homem desperta em si o desejo de sempre ir além de sua zona de conforto, buscando mais informações e conhecimento sobre pessoas e suas comunidades sociais.

1.1. Histórico da Internet

A internet, desde sua criação, proporciona uma facilidade aos que procuram estar em contato com várias partes do mundo, afinal, está presente em cada canto do planeta, sempre em expansão e atualização, sendo o caminho que muitos tomam para obter notícias, trabalhar, se comunicar bem como se divertir.

> [...] No atual modelo social, a informação, poder e o motor para o desenvolvimento e bem-estar social. Tal sociedade da informação é caracterizada por diversos meios e ferramentas comunicativas de modo a aprimorar seu padrão de vida. (JESUS; MILAGRE, 2016, p. 17, *apud* LEVY, 1999)

Porém, de seus inúmeros usuários, poucos são os que possuem conhecimento sobre sua origem e os caminhos que passou até se tornar essa massa mundial.

Tudo começou em 1969, em meio à guerra fria, onde foi criada pela ARPA (*Advanced Research Projects Agency*), uma subdivisão do Departamento de Defesa dos Estados Unidos, a ARPANET (*Advanced Research Projects Agency Network*). O intuito de sua criação foi para garantir a segurança dos dados sigilosos do governo americano que ficavam, assim, espalhados por vários servidores em diferentes locais. Desta forma, evitava-se a perda desses dados valiosos no caso de um possível ataque inimigo.

Além de toda a segurança estabelecida por essa rede evitando que se perdessem dados sigilosos, possibilitava-se, ainda, a não interrupção da comunicação entre as bases, como expõe Gustavo Teixeira Caetano (2010, p.10), em seu trabalho

monográfico de conclusão de direito, ao citar Fabrízio Rosa, Mario Furlaneto e José Augusto Chaves:

> [...] O Departamento de Defesa dos EUA apoiou uma pesquisa sobre comunicações e redes que poderiam sobreviver a uma destruição parcial, em caso de guerra nuclear. A intenção era difundi-la de tal forma que, se os EUA viessem a sofrer bombardeiros, tal rede permaneceria ativa, pois não existiria um sistema central e as informações poderiam trafegar por caminhos alternativos até chegar ao seu destinatário. Assim, em 1962, a ARPA encarregou a Rand Corporatino (um conselho formado em 1948) de tal mister, que foi apresentar seu primeiro plano em 1967. Em 1969, a rede de comunicações militares foi batizada de ARPANET (rede da agência de projetos avançados de pesquisa).
> [...] Fazendo uma digressão histórica sobre o surgimento da internet, Paesani menciona que o projeto Arpanet da Agência de Projetos Avançados (Arpa) do Departamento de Defesa norte-americano confiou, em 1969, à Rand Corporation a elaboração de um sistema de telecomunicações que garantisse que um ataque nuclear russo não interrompesse a corrente de comandos do Estados Unidos. Desse modo, a solução aventada foi a ciração de pequenas redes locais (LAN), posicionadas nos lugares estratégicos do país e coligadas por meio de redes de telecomunicações geográficas (WAN). Na eventualidade de uma cidade vir a ser destruída por um ataque nuclear, esse conjunto de redes conexas – internet, isto é, internetworking, literalmente, coligação entre redes locais distantes, garantiria a comunicação entre as remanescentes cidades coligadas.

Posteriormente esse sistema foi utilizado pelas universidades, possibilitando que estudantes pudessem compartilhar, de forma ágil à época, os resultados de suas pesquisas e estudos através do envio de mensagens eletrônicas, aperfeiçoado por Ray Tomlinson (2017):

> Em 1971, Tomlinson começou a enviar mensagens para si mesmo e para seus colegas como brincadeira. Ele somou as funcionalidades dos aplicativos SNDMSG (uma contração da expressão em inglês "send message", ou seja, "enviar mensagem") e o Readmail, para leitura de correio. Mas esse sistema permitia apenas o compartilhamento de textos. O engenheiro também trabalhava em um protocolo chamado CPYNET, para transferência de arquivos entre computadores conectados em rede. Ao juntar os dois programas, ele conseguiu enviar uma mensagem para seus colaboradores, anunciando sua criação.
> O conceito de correio eletrônico já existia e estava implementado em sistemas como o AUTODIN. Entretanto, esse foi o primeiro sistema capaz de enviar mensagens entre diferentes nós conectados à ARPANET. Tomlinson também inovou na medida em que escolheu o símbolo @ para distinguir as mensagens destinadas às caixas de correio na máquina local das que se dirigiam à rede, por ser o símbolo que significa "at", ou seja, estar em algum lugar.
> [...] Em março de 1972, Ray Tomlinson escreveu o software básico de e-mail com as funções de enviar e ler, motivado pela necessidade dos desenvolvedores da ARPANET de ter um fácil mecanismo de coordenação.

Já no final da década de 80 a rede foi aberta às empresas, iniciando, assim, a transição da ARPANET para a Internet como a conhecemos hoje, através da criação do “www” (*World Wide Web*), um banco de dados com *hiperligações* que permitia a apresentação de informações entre cientistas do mundo inteiro mesmo utilizando máquinas e sistemas operacionais distintos:

> A Organização Europeia para a Investigação Nuclear (CERN) foi a responsável pela invenção da World Wide Web, ou simplesmente a Web, como hoje a conhecemos. Corria o ano de 1990, e o que, numa primeira fase, permitia apenas aos cientistas trocar dados, acabou por se tornar a complexa e essencial Web.
> O responsável pela invenção chama-se Tim Berners-Lee, que construiu o seu primeiro computador na Universidade de Oxford, onde se formou em 1976. Quatro anos depois, tornava-se consultor de engenharia de software no CERN e escrevia o seu primeiro programa para armazenamento de informação – chamava-se Enquire e, embora nunca tenha sido publicada, foi a base para o desenvolvimento da Web.
> Em 1989, propôs um projeto de hipertexto que permitia às pessoas trabalhar em conjunto, combinando o seu conhecimento numa rede de documentos. Foi esse projeto que ficou conhecido como a World Wide Web. A Web funcionou primeiro dentro do CERN, e no Verão de 1991 foi disponibilizada mundialmente.

Posteriormente, com a rede interligando computadores do mundo todo, o Departamento de Defesa desativou a ARPANET, sendo substituído pela NSFNET (*Nacional Science Foundation*) onde foi criado o padrão TCP/IP (*Tranmission Control Protocol* / *Internet Protocol*), um conjunto de camadas responsáveis por determinadas tarefas, a exemplo da comunicação entre o servidor de internet e computador local, utilizado até hoje.

Em relação ao Brasil, a internet nasceu no âmbito acadêmico ao fim da década de 80, sendo disponível apenas aos professores e funcionários de universidades e instituições de pesquisa. Foi privatizada em 1995, tonando-se de acesso público através de provedores independentes.

Desta forma, é possível atualmente o acesso à internet por diversos meios – *notebooks, netbooks, desktops*, celulares. Com o advento da banda larga e o aumento na velocidade de transmissão de dados a navegação mais célere se tornou uma realidade com a realização de um número muito maior de tarefas, sejam elas referente a lazer, estudo, comunicação, segurança, compras e muito mais, simultâneos e num curto espaço temporal.

2. MEIOS PARA A PRÁTICA DE CONDUTAS QUE PODEM SER CONSIDERADAS CRIMES INFORMÁTICOS

Atualmente os usuários de computadores, em especial os que possuem acesso à internet, ouvem de maneira constante os termos *vírus,* cavalo de troia*, spyware, adware*, como sendo os responsáveis por todo e qualquer dano causado em suas máquinas, e vez ou outra a palavra *malware*. De fato, todos buscam, de forma genérica, nos causar algum dano.

Os crimes informáticos podem ser praticados de inúmeras formas, afinal, a internet é um meio livre que permite que inúmeras condutas sejam praticadas em seu bojo.

Desta forma, é imprescindível a compreensão das principais técnicas, artefatos e métodos utilizados para a prática de tais crimes que podem ou não ser associados à inúmeros comportamentos ou ataques relevantes ao Direito Penal. Damásio de Jesus e José Antonio Milagre (2016) trazem os principais artefatos utilizados:

2.1. *Malware*

O termo *malware* deriva da expressão inglesa *malicious software*, ou seja, “programa malicioso” e consiste em um *software* clandestino que se aloja, de forma ilícita, em um computador alheio. São programas e comandos idealizados com diversos fins, podendo apenas infiltrar-se num computador ou sistema, bem como causar danos, apagar dados, roubar informações, divulgar serviços, etc.

O termo *malware* engloba todo tipo de programas perigosos, invasivos e mal-intencionados que podem vir a afetar um computador ou sistema alheio, sendo gênero de inúmeras espécies - *vírus, trojan, spyware, adware, worms*, e outras.

2.2. Vírus

É uma espécie de *malware*. É o mais utilizado para fins de causar algum dano a um computador. Ele é capaz de alterar dados ou sistemas, destruir, alterar arquivos e programas, até mesmo executar funções inesperadas em um sistema computacional ou dispositivos informáticos.

Sua principal distinção de outras espécies de *malwares* deriva de sua semelhança com o vírus biológico, uma vez que consegue infectar um sistema, fazer cópias de si mesmo e tentar se espalhar para outros computadores. Neste caso, dá-se o nome de *worm*.

É comumente utilizado em anexo de e-mails, uma vez que quase sempre é necessária uma ação do usuário para que o vírus seja acionado.

2.3. *Trojan*

É uma espécie de *malware*. Consiste num conjunto de ações desenvolvidas a fim de executar funções ocultas e indesejadas, muitas vezes instalando, de maneira forçada, diversos componentes dos quais o usuário não tem conhecimento.

Ele é uma instrução ou código malicioso comumente ocultado em outro *software*, que, após sua instalação, torna um computador ou sistema vulnerável ou explora vulnerabilidades pré-existentes, sendo possível, além de acessar um sistema, tornar-se administrador deste, copiar informações confidenciais. Um *trojan* pode ser compactado e inserido a um programa comum inofensivo, como um jogo e até mesmo uma apresentação de *slides.*

2.4. *Sniffing*

É a pratica de capturar pacotes de dados transmitidos por uma rede TCP/IP, sendo possível a interceptação e decodificação dos conteúdos que trafegam em uma rede entre computadores a ela conectados.

Muitas vezes esse artefato é utilizado de maneira inofensiva pelo administrador de rede a fim de verificar se uma *network* está operando de maneira eficiente através do monitoramento do fluxo de informações. Entretanto, sua utilização pode advir da intenção criminosa de obter cópias de arquivos confidenciais ou senhas pessoais ou ainda informações bancárias através da captura do tráfego de dados não criptografados. Também pode ser combinado com outras técnicas como o *arp poisoning* (item 2.21).

Esse *software* pode ser facilmente programado para registrar fluxos específicos como sessões de telefonia por internet ou de e-mail, e uma vez capturados os dados,

os *crackers* conseguem extrair facilmente *logins*, senhas, textos de mensagens, dentre outras informações.

2.5. *Backdoor*

É um código malicioso que permite o escalonamento de privilégio, a invasão, a tomada do sistema ou desligamento dos mecanismos de segurança, bem como o acesso facilitado a um sistema ou máquina previamente invadido, ou seja, “é um meio não documentado de acessar um sistema, burlando os mecanismos de autenticação” (JESUS; MILAGRE, 2016).

Esse tipo de *software* pode ser inserido de forma proposital por alguns programadores, bem como por atacantes durante o comprometimento de um sistema, ou ainda através do ataque de vírus, *trojans* e *worms*. Comumente, o *backdoor* é utilizado de maneira a facilitar o acesso futuro a um sistema previamente comprometido.

2.6. *Spyware*

É um código ou programa malicioso instalado ou injetado normalmente em aplicativos baixados de fontes duvidosas, que possui caráter espião, ou seja, sua função é coletar informações das atividades realizadas pelo usuário num determinado computador e envia-las ao destinatário.

Comumente são coletadas informações relativas aos hábitos de consumo dos usuários – técnica muito utilizada por diversas empresas, de maneira legal, para coletar informações de seus assinantes, com o objetivo de lhes apresentar conteúdos de anúncio mais personalizadas de acordo com seus hábitos e/ou interesses. Entretanto, alguns permitem o controle da máquina pelo atacante.

2.7. *Keylogging* e *Screenlogging*

A técnica do *Keylogger* consiste num programa que é capaz de monitorar, capturar e armazenar tudo que é digitado pela vítima no teclado de seu computador. Essa captura gera um arquivo que posteriormente é acessado pelo atacante. Há ainda adaptadores inseridos entre o teclado e o computador, o chamado *Keylogger* físico,

que podem vir a possuir, inclusive, o mecanismo de envio dos arquivos via *wireless*, dispensando, assim, a necessidade da retirada posterior do mesmo para a leitura dos dados armazenados

De maneira independente, porém similar, o *screenlogger* consiste na captura do espelho da tela do computador – *screenshots* – ao clicar do *mouse*, a fim de monitorar dados e informações de teclados virtuais, contornando, assim, os mecanismos de segurança de *sites* bancários.

2.8. *Defacement*

Consiste no ato de modificar ou danificar um *site*, ou seja, uma “pichação de *sites*”, através da remoção de uma página principal, inserção de mensagens ou alteração do conteúdo visual de um sítio na rede mundial de computadores.

Normalmente é praticado em protestos por *hackers* ou *crackers* se valendo de uma técnica usada para aplicar o d*efacement*.

2.9. *Rootkits*

É uma espécie de *software* que possui a função de corromper a atividade convencional de um sistema operacional, utilitários, bibliotecas, ou arquivos de sistema, gerando atividades subsidiárias diversas das esperadas de outros *softwares* do computador infectado. Damásio de Jesus e José Antonio Milagre (2016, p. 37) trazem de maneira didática o que vem a ser os *rootkits* e outras funções desse programa:

> Tipo de *software* normalmente utilizado por atacantes que têm como objetivo manter um atacante com acesso no alvo. Normalmente ele é composto de um conjunto de *trojans* e *backdoors* para permitir acesso futuro ao atacante e ocultar os processos criados por ele, tais como ocultar a existência de uma *backdoor* ou a execução de um *keylogger* deixado em execução por um atacante no alvo.

Este *software* possui como função, ainda, a camuflagem de programas e processos ante aos métodos convencionais de detecção, bem como garantia de acesso exclusivo a um computador e as informações nele contidas.

2.10. DoS e DDoS

A sigla DoS significa *Denial of Service* (ou ataque de negação de serviços). Consiste num meio que busca tornar indisponível os recursos de um sistema para seus utilizadores através da sobrecarga, voltado principalmente para ataques à servidores *web*, tornando as páginas indisponíveis no *WWW*.

Este tipo de ataque pode ser realizado através de inúmeras técnicas, destas existes as mais antigas, e não mais usadas, são *pingflood*, *floodsmtp*, *floddicmp_echo*, dentre outras. Atualmente, são utilizadas outras técnicas, tais como:

a) inundação de pacotes – é o envio de diversos pacotes de rede com o intuito de congestionar o *link* de conexão da máquina-alvo, tonando, assim, a usuários legítimos o acesso ao sistema devido ao alto tráfego;
b) problemas de protocolo – seu funcionamento consiste na exploração de alguma falha do protocolo ou da implementação do protocolo de comunicação com seus clientes utilizado pelo serviço;
c) problemas de codificação – técnica utilizada com o intuito de varrer o sistema de um *software* a fim de detectar algum vulnerabilidade que é capaz de fazê-lo parar de funcionar de forma abrupta;
d) ataque de disco – consiste em esgotar todo o espaço disponível para armazenamento de um dispositivo até que o mesmo não suporte mais informações e consequentemente pare de funcionar;
e) DDoS (*Distributed Denial of Service*) – neste caso utiliza-se várias máquinas para se fazer um ataque de negação de serviço. Corriqueiramente utiliza-se a técnica de inundação de pacotes, uma vez que inúmeras máquinas possuem o poder de gerar muito mais tráfego do que somente uma.

É válido destacar que esta técnica não se equipara à prática do crime de invasão de sistemas ou dispositivos informáticos (art. 154-A do Código Penal), sendo tão somente uma invalidação advinda de um sobrecarga.

2.11. DNS *Poisoning*

Trata-se da quebra da segurança ou integridade de dados do DNS (*Domain Name System* – Sistema de Nomes e Domínio) de um serviço, isto é, ao acessar determinado *site* a *cache* salva com o intuito de otimização do processo pode não vir

no endereço DNS real, o que pode direcionar um acesso para um *site* falso ou serviço criado pelo atacante.

2.12. *Brute Force*

O método do *brute force*, como o próprio nome diz, utiliza-se de “força bruta” para conseguir quebrar senhas bem como acesso a sistemas. Consiste em tentar todas as combinações possíveis, tendo como principais alvos servidores de *email*, ou que possuam Telnet ativo, FTP, HTTP com autenticação, dentre outros. Essa técnica pode ser realizada de maneira manual, o que tornaria este ataque extremamente moroso e ineficaz, como também através de *softwares* que o automatizam.

2.13. Ataque de Dicionário

É uma outra técnica com o intuito de quebra de senhas, onde o atacante utiliza palavras do dicionário que eventualmente façam parte da composição de uma senha. Esta técnica pode ser utilizada de forma conjunta com a técnica do *brute force* para a geração de palavras não existentes, ao que se dá o nome, então, de *Syllabe*.

2.14. *Rainbow Table*

Ataque destinado à quebra de senhas criptografadas, consiste em submeter os *hashs* (senhas digeridas) a uma tabela de *hashs* já calculados para realização de comparações.

2.15. *Scanning*

Esta técnica consiste, basicamente, no escaneamento de portas varrendo diversos *hosts*, identificando portas abertas, vulnerabilidades e informações, como, por exemplo, o tipo de sistema operacional de um servidor.

Diante das principais modalidades de *scanning*, destacam-se o *Host Scan* (descoberta de máquinas ativas na rede), o *Port Scan* (varredura de portas abertas

de um *host*) e o *Vulnerability Scan* (busca por vulnerabilidades em um servidor de acordo com os serviços em execução).

2.16. *Connection Back*

Atualmente em desuso, esta técnica ou aplicação consiste em fazer com que a vítima se conecte diretamente ao atacante, sendo que, a partir de tal conexão, o atacante passa a ter acesso à máquina da vítima.

Essa técnica é útil diante de algumas situações e empecilhos como o *firewall* ou o não conhecimento do IP do computador da vítima.

> Normalmente, o atacante é quem tenta se conectar em uma máquina. Porém, muitas vezes um *firewall* local ou de rede pode bloquear essas tentativas ou, mesmo, a máquina não está acessível diretamente à Internet ou o seu endereço IP é desconhecido. *Connection back* é uma técnica que consiste em fazer a máquina da vítima conectar-se ao computador do atacante, o que muitas vezes contorna os problemas descritos acima (JESUS, Damásio de; MILAGRE, José Antonio, 2016, p. 39).

2.17. SQL *Injection*

Consiste numa técnica de ataque que manipula o código do banco de dados de linguagem universal para a comunicação entre aplicativos e banco de dados relacionais, chamado código SQL (*Structured Query Language*).

O atacante insere comando maliciosos – *SQL querys* – no banco de dados com o intuído de extrair informações guardadas no banco de dados.

O agente altera os parâmetros ou instruções que são executadas sobre uma ou mais tabelas de banco de dados, o que permite um acesso indevido, alteração, inclusão ou destruição de informações

O grupo Lacking Faces, uma célula da Anonymous, explica que a SQL *injection* funciona como uma falha lógica, ou seja, é simplesmente uma falha que, devido a liberdade de interpretações, permite manipulações indesejáveis por terceiros que não os programadores (PAYÃO, 2017).

2.18. *Buffer Overflow*

É uma espécie de vulnerabilidade baseada no transbordamento de dados em *buffer*. Quando uma variável de um programa recebe mais informações do que ele foi programado para suportar e o programador, ao desenhar inicialmente o *software*, não criou nenhum tipo de checagem para evitar que isso ocorresse.

Os resultados diante desse estouro de *buffer* podem ir muito além de uma simples tela de erro e interrupção do programa que está sendo executado mas sim causar uma negação de serviço e até mesmo a execução de códigos arbitrários no computador que possui o programa vulnerável, através da modificação do fluxo de execução de um *software*.

2.19. *Botnets*

São conjuntos de *softwares* instalados que se mantem conectados à Internet uma vez que mantem comunicação constante com outros programas similares a fim de executar determinadas tarefas.

Comumente, a máquina infectada por este sistema obedece aos comandos enviados do criminoso digital (*handler*) que o instalou, transformando essa máquina em um “zumbi” que é utilizada para ataques e prática de diversos outros crimes digitais, dificultando, assim, a apuração de autoria. *Botnet* em si, consiste em uma rede de computadores compostas por vários *bots*, que estão prontos para receber comandos.

2.20. *Session Hijacking*

O denominado sequestro de sessão, ou sequestro de *cookie*, é uma técnica onde o invasor descobre uma conexão TCP ativa entre dois computadores, assumindo o controle para obter acesso não autorizado a informações ou serviços em um sistema. Atualmente, consta em desuso tal prática, ao passo que vem se destacando o chamado *session hijancking* de uma aplicação *web*, que nada mais é do que capturar o número/*token* de sessão e utiliza-lo para acessar a aplicação.

2.21. ARP *Poisoning*

O *ARP poisoning* (Envenenamento do protocolo de resolução de endereços) consiste no ato de responder a um pedido de informação de *MAC Address* (endereço físico de um computador) vinculado a determinado IP feito por uma máquina conectada a uma rede *Ethernet*, de maneira falsa, onde informa-se o *MAC* da máquina do atacante, e não do destinatário almejado.

Esta técnica é muito utilizada para viabilizar um tipo de ataque informático conhecido como *Man-in-the-midle,* permitindo que o criminoso digital intercepte e recolha informações confidenciais que são trocadas entre uma ou mais máquinas.

2.22. Exploração do Kernel

Kernel é o componente mais importante de um computador, logo, bastante desconhecido por leigos. Ele é responsável, de maneira muito simplória, por garantir que todos os programas de um computador tenham acesso aos recursos básicos ao seu pleno funcionamento, como por exemplo a memória RAM. Ele realiza a interação de *hardwares* e *softwares*.

Na obra de Damásio de Jesus e Jose Antonio Milagre (2016, p. 41), há uma explicação objetiva de como funciona este tipo de ataque informático:

> O Kernel é o núcleo de sistemas operacionais. Método muito sofisticado e de difícil detecção. Com a subversão do Kernel, o criminoso digital pode se tornar invisível a programas de segurança da informação, sistemas de detecção de intrusos e outros mecanismos.

Ao acessar o Kernel, o atacante, além de se tornar quase invisível aos métodos de detecção, possui acesso irrestrito a toda máquina, podendo manipular *softwares* e impedindo o pleno funcionamento destes.

2.23. *Watering Hole Attack*

Esta técnica é costumeiramente utilizada pelos atacantes que visam grandes empresas, que normalmente investem mais em segurança da informação. Neste caso, ao invés de um ataque direto ao sistema da empresa-alvo, busca-se sistemas

periféricos e menores, como o de parceiros desta empresa ou mesmo sistemas que funcionários da empresa-alvo acessam.

Faz-se uso de uma máquina pivô, usualmente mais vulnerável que as demais, a fim de se conseguir acessar o servidor ou máquina do alvo, que possuía algum tipo de interação com o pivô infectado.

3. PRÁTICAS INFORMÁTICAS QUE PODEM CARACTERIZAR CONDUTAS CRIMINOSAS

Como visto no capítulo anterior inúmeras técnicas e artefatos podem ser utilizados no meio informático. Estes possuem a capacidade, ou não, de caracterizar condutas criminosas, uma vez que são apenas meios que podem ser utilizados para diversos fins, não se enquadrando na concepção da teoria finalista da ação, que funde a vontade com a finalidade na conduta como condição *sine qua non* para a prática efetiva de um ato criminoso. É como diz Fernando Capez (2016, p.130) ao tratar desta teoria:

> Não se pode [...] desconhecer que a finalidade, o dolo e a culpa estão na própria conduta.
> [...] Descobriu-se, assim, a finalidade, como elemento inseparável da conduta. Sem o exame da vontade finalística não se sabe se o fato é típico ou não.
> Partindo desse pressuposto distinguiu-se a finalidade da causalidade para, em seguida, concluir-se que não existe conduta típica sem vontade e finalidade, e que não possível separar o dolo e a culpa da conduta típica, como se fossem fenômenos distintos.

Desta forma, não é certo que sejam objetos de legislação criminal as técnicas e artefatos no âmbito informático, mas sim os comportamentos e condutas que possuem em seu cerne tais técnicas.

Por muito tempo buscou-se, de maneira equivocada e errônea, tipificar e punir as técnicas e armas, uma vez que as técnicas, artefatos e armas cibernéticas se modificam. Passou-se, ainda, a tipificar dezenas de comportamentos, que muitas vezes coincidiam uns com os outros, causando, dessa forma, uma redundância criminal.

Entretanto, com o advento das Leis de Crimes Informáticos (Leis n. 12.735 e n. 12.737, ambas de 2012) o legislador entendeu a necessidade de dar relevância penal apenas a condutas intoleráveis e recorrente na sociedade onde estas são relacionadas a potenciais crimes próprios, onde a informática é o bem jurídico agredido.

Serão expostas, então, as principais condutas que são dignas de análise relevante do Direito Penal Informático. Outrossim, vale ressaltar que condutas

ofensivas a outros bens jurídicos e que são realizadas por meio da informática, não serão analisados, uma vez que o próprio Código Penal os trata com a devida vênia.

3.1. Acesso Ilegítimo

Considera-se acesso ilegítimo o ingresso sem a devida autorização de quem possa lhe conceder a um sistema, podendo este ser considerado isolado ou um grupo interligado.

É possível analisar que os objetos jurídicos tutelados por esse tipo penal é o direito à intimidade e a segurança da informação, uma vez que tais dados e informações são pertencentes a determinada pessoa. Em suma, se busca a proteção da liberdade individual, onde cada pessoa tem o direito de manter íntegros e seguros seus dados no âmbito informático, seus dispositivos que acessam e armazenam informações e que são protegidos por mecanismos de segurança, de acessos sem prévia autorização – expressa ou tacitamente.

Para tal prática, não se faz necessária a violação de nenhum meio de segurança – o que caracterizaria o crime de invasão de dispositivo informático, previsto no artigo 154-A, do Código Penal. Spencer Toth Sydow (2015, p.114-115), em sua obra acerca dos crimes informático explica tal prática:

> O tipo penal aqui denominado refere-se ao ingresso não autorizado de um usuário no sistema alheio, seja ou não para obter alguma vantagem, seja ou não por meios ardilosos, violentos, ou até mesmo por conta de um subterfúgio que venha a enganar o legítimo detentor dos direitos relativos ao sistema, levando-o a permitir o ingresso, sob erro.
> [...] Por vezes, o usuário sequer percebe que seu aparato sofreu uma violação de privacidade, pois que a instalação de um programa faz com que haja uma verdadeira entrada escondida (denominada “vulnerabilidade” pela Lei n. 12.737/12), de acesso livre e desimpedido, que é conhecida no jargão informático como porta dos fundos ou *backdoor*. Nenhuma violência terá havido, mas sim um ardil.

O artigo 6º, da lei complementar 109/2009 traz de forma bem clara e sucinta o conceito desse tipo para fins penais:

> 1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
> 2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas

> informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.
> 3 - A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança.
> 4 - A pena é de prisão de 1 a 5 anos quando:
> a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou
> b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.
> 5 - A tentativa é punível, salvo nos casos previstos no n.º 2.
> 6 - Nos casos previstos nos n. 1, 3 e 5 o procedimento penal depende de queixa.

Convenções internacionais entendem ainda que o acesso ilegítimo somente se caracteriza de maneira efetiva quando fica comprovada que tal acesso possuiu intenção ilegítima do agente invasor.

3.2. Interceptação Ilegítima

Essa prática está diretamente relacionada ao uso de técnicas para se ter acesso a transmissões não públicas, a fim de conseguir subtrair dados e informações. Acerca do conceito para aspectos jurídicos da interceptação, considera-se ser o ato de se intrometer em comunicações alheias, de maneira que possa vir a impedi-las ou ter acesso a conteúdo, não público, desta.

Diante da legislação brasileira, tal conduta possui tipicidade nos termos do artigo 10, da Lei n. 9.276/96: “Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa”.

3.3. Interferência De Dados (Dano Informático)

Consiste no ato consciente e ilegítimo com o intuito de danificar, apagar, deteriorar, alterar ou eliminar dados e informações de um sistema informático, podendo ser causado por um ou mais agentes. Especificamente, diz respeito ao dano informático.

Caso o dano seja decorrente de uma prévia invasão à um sistema ou máquina, tem-se caracterizado o tipo penal descrito no artigo 154-A do Código Penal,

entretanto, é necessário o enquadramento da conduta em determinadas características, quais sejam:

I. Deve estar explicito que houve uma invasão de determinado dispositivo móvel, ou ao menos a tentativa de fazê-lo;
II. Tal dispositivo burlado deve ser de outrem, ou seja, não pode pertencer ao agente invasor;
III. Não se faz exigida obrigatoriamente a conexão do dispositivo em pauta à Internet, podendo ele estar desconectado, e, assim, possibilita abarcar qualquer tipo de burla em dispositivo eletrônico;
IV. O mecanismo de segurança presente no dispositivo invadido deve ter sido violado de maneira indevida;
V. O titular do dispositivo não pode autorizar expressa ou tacitamente;
VI. O agente deve, necessariamente, ter como alvo a obtenção (acesso a informação ou cópias dos dados contidos no dispositivo), adulteração (alteração dos arquivos do dispositivo ou alteração de alguma informação arquivada) ou destruição (violar de maneira irrecuperável arquivos do dispositivo).

Para que tal conduta possa ser enquadrada nos termos do artigo 154-A, a lei determina que o dispositivo vítima do ataque deve ser protegido por *mecanismo de segurança*, não informando, porém, que tipo de mecanismos são considerados seguros para este fim, tampouco se a segurança a ser violada é lógica (advinda de *softwares*) ou física (através de travas).

Rogério Greco cita Marco Aurélio Rodrigues da Costa em sua obra ao tratar do artigo penal supracitado:

> [...] a Lei nº 12.737, de 30 de novembro de 2012, inserindo o art. 154-A ao Código Penal, criou o delito de *invasão de dispositivo informático*, prevendo, outrossim, o chamado *crime informático puro*, isto é, aquele, segundo definição de Marco Aurélio Rodrigues da Costa, cuja conduta ilícita "tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas." (GRECO, 2017, p.544, *apud*, RODRIGUES DA COSTA, 2009).

Desta forma, diferencia-se, diante de um mesmo tipo penal, duas maneiras peculiares de o fazê-lo e intenta-lo: os crimes informáticos praticados com o computador (crime informático de meio) – sendo caracterizados, basicamente, pela celeridade e distância no tempo e no espaço, a facilidade de encobrimento e a

dificuldade probatória – e os crimes praticados contra o computador (crime informático próprio), visando os dados e *softwares* nele contidos.

Entretanto, caso haja apenas o dano, não se valendo o agente criminoso de invasão, caracteriza-se o tipo do artigo 163 do Código Penal, que trata do crime de dano.

3.4. Falsidade ou Fraude Informática

Diante da legislação brasileira vigente, esta prática criminal está tipificada no capítulo I do título X do Código Penal que trata dos crimes praticados por funcionários públicos contra a Administração Pública em Geral, tipificada nos artigos 313-A e 313-B.

O primeiro traz em seu bojo a figura da inserção de dados falsos em sistemas de informações. Este artigo, bem como o 313-B, foi criado graças a Lei 9.983/00 e inserido no Código Penal como mais uma forma do crime de peculato, sendo-lhe dado a identidade de *peculato eletrônico* em virtude da maneira como o delito é praticado.

Observando o tipo penal, identifica-se dois comportamentos distintos. O primeiro diz respeito ao próprio funcionário, devidamente autorizado, que *introduz* dados falsos ou *facilita* a inserção destes por um terceiro nos sistemas informatizados ou bancos de dados pertencentes à Administração Pública.

Todavia, percebe-se a existência de uma segunda forma de conduta previsto pelo tipo que é a figura do funcionário que *modifica* ou *exclui*, indevidamente, dados verdadeiros da Administração Pública.

Rogério Greco (2017, p. 712) explica como deve ocorrer a ação do agente para que haja tipificação da conduta:

> Para que ocorra a infração penal em estudo, o agente deve atuar com uma finalidade especial, entendida, pela maioria da doutrina, como um elemento subjetivo que transcende ao dolo, vale dizer, a finalidade de obter vantagem indevida (de qualquer natureza, podendo, até mesmo, não ter conotação econômica) para si ou para outrem ou para causar dano.

Vale destacar, ainda, que é possível tal incurso penal ocorrer no âmbito eleitoral, na forma do artigo 72 da Lei 9.504/97, que é uma norma comparativa ao artigo 313-A do Código Penal:

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

Fernando Galvão (2013), em sua obra sobre *Crimes Contra a Administração Pública* ainda destaca:

> Se o funcionário público não está autorizado a intervir no sistema informatizado ou no banco de dados, ou se quem faz a intervenção não é funcionário público (art. 327 do CP), a inserção de dados falsos, a alteração ou exclusão de dados verdadeiros que estão inseridos em um documento pode caracterizar o crime de falsidade ideológica – art. 299 do CP.

O artigo 313-B se distingue de seu antecessor uma vez que se caracteriza como um tipo que não exige uma condição especial do funcionário público (que no art. 313-A precisa ser aquele autorizado a manipular os dados), bastando a ele apenas a condição de funcionário público.

É necessário, ainda, analisar as duas condutas inseridas neste artigo, *modificar* e *alterar*. Gramaticalmente são consideradas sinônimos, entretanto, diante do texto do artigo é possível identificar que o ato de *modificar* induz o entendimento de uma alteração brusca e radical em um programa ou sistema de informação. Já a ação de *alterar*, mesmo significando mudança, remete a uma mais suave, sem que haja total quebra dos parâmetros iniciais.

Outrossim, é possível a prática do delito em tela na forma omissiva, quando for o caso de o agente, de forma intencional, nada faz para impedir a prática do crime, devendo, assim, responder nos termos do artigo 13, §2º, do Código Penal.

3.5. *Scamming*

Termo em inglês que traduzido de maneira livre e literal significa “defraudar” e consiste, basicamente, em fazer uso do *ciberespaço*, valendo-se da boa intenção das vítimas, para captarem algum tipo de vantagem destas.

Tem como principais alvos pessoas que fazem uso da Internet, e de todo o campo que recursos que nela subsistem, porém não possuem preparo para lidarem com armadilhas bem elaboradas. Spencer Sydow (2015) fala como ocorre tal prática:

> Também conhecido como *confidence trick* ou truque e confiança, é delito de relacionamento em que o ofensor e o ofendido comunicam-se direta ou indiretamente, sendo que o primeiro tenta persuadir o segundo a alguma ação, geralmente cessão de informações sensíveis ou transferência de valores em pecúnia ou crédito. Tais ações, quando operadas no ciberespaço, receberam o nome de engenharia social (ou engenhosidade social), sendo tal meio verdadeiro laboratório para que os usuários com má intenção experimentem diferentes técnicas ardilosas para obtenção de valores.

Este tipo de delito costumeiramente é veiculado através de *emails*, muitas vezes não solicitadas (também conhecidos como *spam*), em anúncios atrativos onde haja a expressão “clique aqui”, ou ainda em *sites* que possibilitam interações interpessoais onde se estipula uma determinada mensalidade (*sites* de relacionamento) para que os usuários possam conhecer companheiros, ou que possam se escrever em listas de adoção, sem nunca alcançarem seus objetivos.

Estes delitos podem ser classificados da seguinte maneira, de acordo com Sydow (2015):

a) Sistemas de enriquecimento rápido/*get-rich-quick schemes*: através de diversas variáveis informáticas (envio de mensagens SMS; *banners* em *sites*) indicam que o usuário ganhou uma quantia grande de dinheiro, porém somente pode ter acesso a tal quantia mediante o pagamento de algum valor;
b) Sistemas que envolvem o relacionamento mais duradouro com pessoas distantes: são colhidas informações e dados pessoais, através da sedução dos interessados em encontrar alguma companhia por meio de cadastros feitos, muitas vezes em salas de bate-papo, sites de relacionamento, *sites* de busca de amantes, e assim possibilitam que recursos e valores sejam desviados;
c) Sistemas que possuem produtos pseudo-valiosos/*gold brick schemes*: prática que possui caráter lesivo duplo, uma vez que alguém faz a oferta de determinado produto por um valor muito abaixo do comercializado usualmente, e ao adquirir tal produto, o usuário percebe o negócio enganoso;
d) Sistemas de extorsão: situações onde o agente criminoso, em posse de alegações verdadeiras ou não, faz exigências pecuniárias para não levar a

público tais conteúdos “sigilosos”. Muito comum quando se trata de questões sexuais, relações extraconjugais ou ainda transações bancárias ilegais;

e) Sistemas de jogatina: práticas que envolvem jogos de azar, ou ainda jogos legalizados configurados de forma que impossibilitem que o jogador vença, se tornando, assim, armadilhas exploradoras do vício dos usuários.

3.6. Interrupção ou Perturbação De Serviços

A intenção da criação deste tipo penal foi tutelar a integridade regular de serviços telegráficos, radiográficos, telefônicos e, por meio da lei 12.737/12, que alterou o *caput* do artigo 266 do Código Penal inserindo o §1º, os serviços telemáticos ou de informação de utilidade pública, que passaram a possuir sanção isonômica do tipo penal constante no *caput*.

Dos Reis (2013) fala de tal tema:

> Trata-se de um tipo penal que visa proteger a incolumidade pública no que tange à regularidade dos serviços telegráficos, telefônicos, informáticos, telemáticos e de utilidade pública. É um delito comum que admite a tentativa, cuja pena possibilita a suspensão condicional do processo, desde que o delito não seja cometido por ocasião de calamidade pública (art. 266, §2º).

Rogério Greco se faz das palavras de Nélson Hungria que trata deste assunto trazendo alguns conceitos:

> O elemento material é tanto o emprego de violência contra as instalações ou aparelhos como contra o *pessoal* dos serviços mencionados no texto legal, de modo a resultar *interrupção* (paralisação) ou *perturbação* (desarranjo parcial, retardamento) de tais serviços, ou obstáculos ou embaraço ao seu restabelecimento. A enumeração dos serviços de telecomunicação é *taxativa*. Assim não poderia, por analogia ser incluído o *serviço postal.*
> *Telégrafo* é toda instalação que possibilita a comunicação do pensamento ou da palavra mediante transmissão à distância de sinais convencionais. Compreende o telégrafo elétrico (terrestre ou submarino) ou semafórico.
> *Radiotelegrafo* é o telégrafo sem fio, funcionando por meio de ondas eletromagnéticas ou “ondas dirigidas”
> *Telefone* é a instalação que permite reproduzir à distância a palavra falada ou outro som.

Damásio de Jesus e José Antonio Milagre (2016) trazem em seu estudo sobre os crimes informáticos o conceito das novas práticas adicionadas à redação do tipo legal pela lei 12.737/2012:

> A telemática pode ser entendida como o conjunto de tecnologias de transmissão de dados que resultam da união de recursos de telecomunicações e da informática, e que permitem o processamento, a compreensão, o armazenamento e a comunicação de dados. [...] por consequência, resultam da associação da informática com as telecomunicações para promover o uso da informação de maneira mais interativa e eficaz.

É importante destacar que o tipo penal previsto no §1º do artigo 266 do Código Penal é direcionado não somente ao fato de interromper, impedir ou dificultar o restabelecimento de um serviço de utilidade pública, mas sim a toda prestação de serviço que tem o objetivo de transmitir informações a população em geral.

A doutrina ainda destaca um aspecto especial desta norma:

> Destaca-se, também, que se a lei protege serviços de utilidade pública não essenciais, mas que proporcionam benefícios a determinados cidadãos, entendemos que serviços públicos informáticos também são objeto jurídico da legislação. Nesse contexto poderíamos inserir alguns aplicativos sociais oferecidos por prefeituras, hospitais, polícias, entre outros. (JESUS, MILAGRE, 2016)

O artigo 266 do Código Penal prevê uma proteção à incolumidade pública. Entretanto, em caso de haver um ataque criminoso que venha a interromper ou perturbar a comunicação de particulares, de maneira particularizada, é possível que tal conduta seja inserida e punida de acordo com o artigo 151, §1º, III, do Código Penal.

4. ASPECTOS DO DIREITO PENAL INFORMÁTICO BRASILEIRO

No que tange à legislação penal no Brasil, utiliza-se o sistema da reserva legal, previsto no artigo 1º do próprio Código Penal: “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal”. Desta forma, deve haver um cuidado muito grande ao legislar sobre tecnologia da informação, para que a legislação criada seja capaz de acompanhar a atualização constante e exponencial de tais sistemas.

Com a criação dos computadores, viu-se o nascimento deste novo ramo do Direito, uma vez que estes são utilizados em todo o cotidiano das pessoas e empresas privadas, inclusive o Estado.

Porém, diante deste vasto mundo criado pela Internet, que veio reduzindo distâncias, quebrando as barreiras geográficas e aproximando pessoas, o anonimato muitas vezes utilizado (e vedado pelo artigo 5º, inciso IV da Constituição Federal) possibilita a prática de crimes de alta complexidade, exigindo do Estado soluções rápidas e eficazes, uma vez que crescem ao passo que vão surgindo avanços tecnológicos.

Vladimir Aras (2001), ao falar sobre estes delitos, diz que:

> Muitos outros bens jurídicos estão em jogo, quando se cuida da criminalidade pela Internet (uma das formas de criminalidade informática), como os direitos de autor, que têm sido, desde a disseminação da WWW, quase que “desinventados”, por conta da facilidade de realizar cópias de textos, livros, músicas e filmes. Aliás, como prova o caso em que a indústria fonográfica americana contende com o provedor Napster, em razão da extrema facilitação de cópias de música digital no formato MP3.
> Não podem, contudo, ser olvidadas velhas práticas que, no ciberespaço, tomaram fôlego novo, a exemplo dos web sites de agenciamento de prostituição (fato enquadrável no art. 228 do Código Penal), a pedofilia virtual (art. 241 do Estatuto da Criança e do Adolescente); o controvertido “adultério virtual” e os crimes patrimoniais em geral, denominados genericamente de fraudes eletrônicas.

E continua dizendo que:

> [...] a vida online nada mais é do que, em alguns casos, uma reprodução da vida “real” somada a uma nova forma de interagir. Ou seja, representa diferente modo de vida ou de atuação social que está sujeito às mesmas restrições e limitações ético-jurídicas e morais aplicáveis à vida comum (não eletrônica), e que são imprescindíveis à convivência. [...] a incidência do Direito é uma necessidade inafastável para a harmonização das relações jurídicas ciberespaciais, é preciso rebater outra falsa ideia a respeito da Internet: a de que seriam necessárias muitas leis novas para a proteção dos

> bens jurídicos a serem tutelados pelo Direito Penal da Internet. [...] Os bens jurídicos ameaçados ou lesados por crimes informáticos merecerão proteção por meio de tutela reparatória e de tutela inibitória. Quando isso seja insuficiente, deve incidir a tutela penal, fundada em leis vigentes e em tratados internacionais, sempre tendo em mira o princípio da inafastabilidade da jurisdição, previsto no art. 5º, inciso XXXV, da Constituição Federal.
> A atuação do Direito Penal será imprescindível em alguns casos, por conta da natureza dos bens jurídicos em jogo. Pois, pela web e no ciberespaço circulam valores, informações sensíveis, dados confidenciais, elementos que são objeto de delitos ou que propiciam a prática de crimes de variadas espécies. Nas vias telemáticas, transitam nomes próprios, endereços e números de telefone, números de cartões de crédito, números de cédulas de identidade, informações bancárias, placas de veículos, fotografias, arquivos de voz, preferências sexuais e gostos pessoais, opiniões e ideias sensíveis, dados escolares, registros médicos e informes policiais, dados sobre o local de trabalho, os nomes dos amigos e familiares, o número do IP (Internet Protocol, o nome do provedor de acesso, a versão do navegador de Internet (browser), o tipo e versão do sistema operacional instalado no computador. [...]não há como negar a interação entre a Internet e o Direito Penal. Isto porque o ciberespaço e sua cultura própria não estão fora do mundo. E, estando neste mundo, invariavelmente acabarão por sujeitar-se ao Direito, para a regulação dos abusos que possam ser cometidos pelo Estado contra a comunidade cibernética e para a prevenção de ações ilícitas e ilegítimas de membros da sociedade informatizada contra bens jurídicos valiosos para toda pessoa ou organização humana.

Desta forma, é imprescindível que seja feita uma análise pormenorizada da criminalidade informática, a fim de que seja possível entender suas variações e peculiaridades, possibilitando, assim, a produção de uma legislação que a trate e tipifique suas condutas com a devida vênia.

4.1. Generalidades dos Crimes Informáticos

A legislação brasileira desde sempre foi falha diante dos crimes informáticos, uma vez que se buscava adequar condutas *cibernéticas* a uma lei da época do rádio. Não se tratava a informática como um bem de relevância jurídica, o que dificultou que fossem aprovadas legislações nesse sentido. O Decreto-Lei nº 2.848/40 (nosso Código Penal) traz em seu bojo diversos delitos informáticos, porém, se faz omisso em situações onde deveria agir de maneira incisiva.

Damásio de Jesus, em sua obra conjunta com José Antonio Milagre (2016, p.48), discorrem acerca da evolução tecnológica e de como esta influência à síntese de normas:

> Como salienta Ferreira Lima (2011, p.6), diante da evolução tecnológica existe uma predisposição social em reconhecer bens jurídicos informáticos e, dentre os que mais se sobressaem, temos o sigilo e a segurança de dados e

> informações eletrônicas. Para a autora, é tal juízo de reprovação (violação a dados e a informações privadas) que move o Direito Penal. De fato, tal juízo de reprovação existia, mas foi preciso que uma pessoa pública, atriz popular, fosse vítima de um suposto crime informático para que o legislativo finalizasse uma discussão de mais de 10 (dez) anos no Congresso Nacional, com a aprovação da Lei nº 12.737/2012, sancionada em 30 de novembro do mesmo ano.

A partir daí, foram considerados de valor jurídico fundamental das relações sociais os dispositivos e dados informáticos, que norteiam toda uma sociedade dependente da tecnologia da informação, e, assim, tutelando-os através do Direito Penal.

Uma vez que já se sabe quais os bens jurídicos tutelados no direito penal em sede de crimes informáticos, faz-se imprescindível uma conceituação deste delito. Segue, então, algumas definições segundo alguns estudiosos.

Segundo Ramalho Terceiro (2002):

> [...] os crimes perpetrados neste ambiente se caracterizam pala ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas.

Para Augusto Rossini (2004), é possível conceituar “delito informático” como:

> Conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa/culposa, praticado por pessoa física/jurídica, com uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.

Gustavo Caetano (2010), em sua monografia, cita o conceito dado pela advogada Patrícia Peck (2009):

> [...] o crime eletrônico é, em princípio, um crime de meio, isto é, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por hackers, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso quer dizer que o meio de materialização da conduta criminosa pode ser virtual, contudo, em certos casos, o crime não (CAETANO, 2010, p.54, *apud*, PECK, 2009).

Há, ainda, o conceito trazido por Vladimir Aras (2001):

> Delitos computacionais, crimes de informática, crimes de computador, crimes eletrônicos, crimes telemáticos, crimes informacionais, ciberdelitos, cibercrimes... Não há um consenso quanto ao *nomen juris* genérico dos delitos que ofendem interesses relativos ao uso, à propriedade, à segurança ou à funcionalidade de computadores e equipamentos periféricos (*hardwares*), redes de computadores e programas de computador (estes denominados *softwares*).

Desta forma, é possível concluir que o termo “delito informático” sustenta em si crimes e contravenções penais, envolvendo tanto condutas praticadas na Internet propriamente dita, quanto comportamentos ligados à sistemas informáticos, de meio ou de fim, sendo possível, ainda, incorporar a essa denominação transgressões onde o computador é tão somente utilizado como uma ferramenta, sem que haja, obrigatoriamente, uma conexão à rede mundial de computadores ou qualquer outro tipo de conexão telemática.

Ao chegar a um consenso quanto a definição desta infração, faz-se necessária uma análise acerca das características destas condutas. Analisando os delitos informáticos percebemos que há certos padrões de comportamento ilícito que se diferenciam dos demais ramos do Direito Penal, ou seja, estes delitos possuem determinadas regras-padrão que sustentam os pensamentos e estudos jurídicos penais.

Sendo assim, conclui-se que são traços da delinquência informática, segundo estudo de Spencer Sydow (2015), as seguintes características:

- Interatividade – Este elemento nos diz que toda e qualquer ação (informática, telemática, ou tão somente tecnológica) pressupõe um comando humano. Máquinas e sistemas são possuem autonomia para decidirem quando praticar ou não praticar determinadas atitudes. Toda e qualquer ação/técnica somente se dará mediante um comando de um usuário, podendo ser prévio (por meio de uma programação para responder atitudes de outros usuários) ou atual (onde alguém faz uso de uma máquina para atingir um objetivo);
- Mobilidade (ou portabilidade) – Tal característica faz menção aos avanços tecnológicos no que diz respeito a miniaturização dos componentes eletrônicos, isto é, a diminuição do espaço físico de dispositivos eletrônicos e seus componentes. Desta forma, antigos computadores que ocupavam o espaço de uma sala, hoje possuem muito mais funcionalidades e sendo permitido seu transporte de maneira mais prática para ser realocados em

outro endereço (*desktop*), ou ainda, dispositivos móveis, que precipuamente não possuem um local físico fixo. Assim, a identificação da localização através no número IP de uma máquina conectada à Internet (seja via *wi-fi* ou por acesso de uma rede telefônica) não se faz mais possível, uma vez que estas não se prendem mais a somente um endereço fixo;

- Conversabilidade – Diz respeito a capacidade de comunicabilidade entre diferentes *hardwares*, ou seja, independente do que seja transmitido, ou do formato de leitura do dados compartilhados entres dispositivos eletrônicos, os dispositivos, sendo eles computadores que se comunicam através do Protocolo TCP/IP (linguagem que faz possível o acesso, em escala mundial, a diversos *sites* e bancos de dados *online*) ou *hardwares* que transmitem arquivos por uma porta USB, a comunicação ocorre entre tais aparelhos de maneira intuitiva e automatizada, não sendo possível vincular tais comunicações à atitudes tipificadas pela lei como delitos;
- Conectividade – Este traço de identidade se refere à capacidade tecnológica que um dispositivo eletrônico possui de conectar à outro aparelho ou uma rede. Esta conexão depende, obrigatoriamente, que os aparelhos que se conectam “falem a mesma linguagem”. Em tese, pressupõe, ainda, um requerimento de um dispositivo, e a aceitação do requerido. Entretanto, existem formas de se conectar explorando falhas na segurança, ou requerendo uma autorização para uma pseudo-conexão segura, onde o requerido aceita, e assim, autoriza em erro o compartilhamento dos itens;
- Mundialização – Atualmente com advento da informática surgiu o novo conceito de “cidadão do mundo”, uma vez que por meio dela, barreiras geográficas, políticas e religiosas que separavam o planeta e impossibilitavam sua exploração, hoje são possíveis graças a esta rede mundial. Desta mesma forma que diversas dificuldades de relacionamento a distancia foram resolvidas por meio da Internet, a insegurança, proporcionalmente, aumentou. Não se conhece o usuário do outro lado da rede; não se sabe com quem está se relacionando ao certo;
- Fracionabilidade – neste caso trata-se do fato de que um delito informático consiste no fracionamento de dados, ou seja, os traços da delinquência

informática podem estar minimamente incluídos em pedaços de programações, não sendo necessária uma reorganização total dos códigos. A simples falta de uma parte de uma linha de comandos, ou ainda uma alteração nesta, pode inutilizar completamente os dados podendo, também, trazer brechas de segurança a serem exploradas.

- Divisibilidade – Se difere da característica anterior pelo fato desta fazer menção a forma como os dados são transmitidos, ao contrário da *fracionabilidade* que se refere à composição dos dados e sua segmentação no que tange à programação. A divisibilidade se torna penalmente relevante quando se observa pela ótica de que ao transmitir um dado pela Internet, seus pacotes podem ser interceptados, e tais interceptações podem ocorrem em locais onde não há uma restrição legal quanto a isso, podendo gerar captação de dados de maneira indiscriminada e incontrolável;
- Intangibilidade – diz respeito a não materialidade dos dados informáticos, isto é, pacotes, blocos de dados, linhas e programação formam, quando “lidos” por uma máquina capaz de juntar tais elementos logicamente, informações que podem vir a ter valor pecuniário. Entretanto, quando se observa segundo a ótica do Direito Penal, ocorre uma incongruência visto que delitos virtuais não burlam nem atingem bens materiais, e sim dados não materializados e, consequentemente, não tutelados com a devida cautela pelo Direito Penal. Eis aí a necessidade de uma legislação especial;
- Disponibilidade – consiste, basicamente, na possibilidade de acessar não só arquivos e dados contidos na própria máquina, mas também na possibilidade de acesso à programas e serviços contratados na rede por meio de um site, onde o usuário consegue armazenar dados, acessar e compartilhar arquivos. Esta *disponibilidade* subsiste ainda quando se fala em comunicação, uma vez que um usuário estabelece conexão com outra máquina ou uma rede (conexão ativa) se disponibiliza a ser conectado sem sua iniciativa (conexão passiva), sendo possível, assim, enviar arquivos e comandos, bem como recebe-los;
- Pluralidade – este aspecto diz respeito a composição dos dados informáticos. Tais conteúdos são constituídos por *bits* (também chamado de “digito binário” que é a unidade básica de constituição de sistemas

digitais). Esses valores não podem ser materializados ou resumidos a alguma forma física palpável uma vez que são constituídos por números (0 ou 1). Assim, ao replicar uma linha de programação de um sistema ou *software* a cópia criada é exatamente igual ao original, ou seja, é possível haver vários arquivos originais, idênticos com funcionalidades similares;

- Ubiquidade (ou simultaneidade) – esta característica pode ser considerada o traço de identidade mais marcante dos delitos informáticos. Também chamada de onipresença, ela se baseia no princípio da não territorialidade, ou seja, é possível estar em mais um lugar ao mesmo tempo, isso graças a conectividade dos dias atuais que permite um indivíduo estar em município, se conectando a um provedor em outro local, visitando, ainda, um site de um país distinto que exibe vídeos hospedados em outro continente. Isso, na ótica os delitos informáticos, se funde ao fato de um agente criminoso agir de maneira generalizada e simultânea em vários locais, podendo ocorrer, ainda, que em algum destes locais essas condutas delinquentes não sejam consideradas atentados ao Direito Informático e seus bens juridicamente tutelados;
- Velocidade – este aspecto tem relação direta com os demais, uma vez que graças a ele é possível transmissões e recebimentos de dados cada vez mais dinâmicos, abrindo assim, campo para ataques (contaminações por *malwares*, escravização de máquinas e outros), permitindo, assim, ao delinquente informático agir de maneira rápida e simultânea.

4.2. O Criminoso Digital

De acordo com Júlio Mirabete (2011, p. 106), sujeito ativo “é aquele que pratica a conduta descrita na lei, ou seja, o fato típico”.

Lindolfo Pires Neto (2009, p. 11-12), em seu trabalho monográfico, diz que que o sujeito ativo nos delitos informáticos poderia ser caracterizado como uma pessoa que se vale de seus conhecimentos acerca da informática a fim de praticar a conduta típica com o intuito de prejudicar outrem, atentar contra a liberdade individual, à privacidade, à honra, dentre outros, para proveito próprio ou de terceiros, utilizando a Internet.

Em pesquisa publicada na Internet, Marcelo Baeta Miranda (2001) indica como seria o perfil do criminoso virtual:

> [...] pessoas jovens, inteligentes acima da média, educados, com idade entre 15 e 32 anos, do sexo masculino, magros, caucasianos, audaciosos e aventureiros, movidos pelo desafio da superação do conhecimento, além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e que agiram, simplesmente, por "brincadeira". Ademais, tem preferência por ficção científica, música, xadrez, jogos de guerra e não gostam de esportes de impacto.

Dentro do âmbito do processamento da informação, que é a informática, muito já se foi dito acerca de perfis de criminosos virtuais. Segundo estudo realizado por Damásio de Jesus e José Antonio Milagre (2016), a definição de *cracker* já foi diretamente relacionada ao criminoso digital. Entretanto, atualmente esta vinculação conceitual foi alterada, pois verificou-se que grande parte dos crimes praticados se deu por fatores como a ignorância dos usuários, o despreparo das autoridades investigativas e, principalmente, à banalização e difusão das técnicas e ferramentas para a realização de práticas delitivas. Destacam, ainda, que há um número crescente de adolescentes que o fazem.

Continuando seu estudo, os autores acima falam da hipótese de tais crimes ocorrerem contra uma empresa, podendo então ser classificados como *insider* (quando praticado por um empregado, preposto ou pessoa interna desta empresa) e *outsider* (onde o criminoso não possui vinculo algum com a empresa fraudada).

E completam dizendo:

> [...] os criminosos digitais, em sua maioria, não praticariam crimes do mundo real, porém interessam-se pela prática delituosa virtual, amparados pela falsa sensação de anonimato e conhecedores do despreparo das autoridades em investigarem delitos desta natureza (JESUS, MILAGRE, 2016, p. 56).

Diante de tais perspectivas e conceitos é possível apenas destacar que o delinquente virtual não possui traços e padrões físicos, tampouco se apresenta desta maneira, afinal, pode agir de qualquer local do mundo, o que lhe traz uma sensação de segurança e imunidade às leis.

4.3. Competência e Lugar

Neto (2009) esclarece que a problemática da competência territorial dos delitos informáticos baseia-se na falta de fronteiras proporcionada pela Internet e na dificuldade da identificação do criminoso.

Essa escassez de limites territoriais se torna um fator tenso nesse âmbito visto que muitas vezes estão envolvidos nas ações criminosas mais de um país, onde cada possui sua própria legislação, ficando difícil precisar qual a competência para apurar a ação criminosa.

No que tange ao local do delito e competência para seu julgamento, foi adotada pelo Brasil, no artigo 6º do Código Penal, a teoria da Ubiquidade que considera lugar do crime aquele onde foi praticada a conduta típica, bem como onde ocorreram os resultados de tal conduta.

> Para a incidência da lei brasileira é suficiente que um único ato executório atinja o território nacional, ou então que o resultado ocorra no Brasil. A teoria não se importa, contudo, com os atos preparatórios, nem com os atos realizados pelo agente após a consumação (MASSON, 2008, p. 144).

O Código de Processo Penal, em seu artigo 69, também traz instruções sobre a competência jurisdicional

> Art. 69. Determinará a competência jurisdicional:
> I – o lugar da infração;
> II – o domicílio ou residência do réu;
> III – a natureza da infração;
> IV – a distribuição;
> V – a conexa ou continência;
> VI – a prevenção;
> VII – a prerrogativa de função.

Acerca da extraterritorialidade dos crimes, existem algumas jurisprudências que tratam sobre esse assunto:

> CONSTITUCIONAL. PROCESSUAL PENAL. PENAL. COMPETÊNCIA. ART. 109, V, DA CF. Art. 6º E ART. 7º, II, A, DO CP. ART. 241, "CAPUT" DO ECA. DEC. 5.007/04. "CRIME À DISTÂNCIA". EXTRATERRITORIALIDADE CONDICIONADA DA LEI PENAL BRASILEIRA. PUBLICAÇÃO DE FOTOS LASCIVAS DE MENORES NA INTERNET. SÍTIO DE ORIGEM ALEMÃ. PROVEDOR (INTERNET PROTOCOL) DE NACIONALIDADE BRASILEIRA. SUBSUNÇÃO AO ART. 241 DO ECA. COMPETÊNCIA DA JUSTIÇA FEDERAL. RECURSO MINISTERIAL PROVIDO. I - Extraterritorialidade condicionada da Lei Penal Brasileira (art. 7º, II, a , do CP) concernente ao Princípio da Justiça Universal ou Cosmopolita. Aplicação concomitante da Teoria da Ubiquidade em relação ao lugar do crime eis que delito de execução transnacional (art. 6º do CP). II - A execução e consumação ocorreu através

> da Internet, englobando, ao menos, dois países: Brasil e Alemanha. Fato que, aliado à existência de acordo internacional tratando do tema, conduz à competência da Justiça Federal para processamento e julgamento do feito. III - Crime instrumentalmente conexo à rede telemática, considerando-se a utilização da rede mundial de computadores para consecução da prática criminosa (delito informático impróprio). IV - A conduta ora sub examen amolda-se perfeitamente no preceito primário do art. 241 do ECA, eis que há subsunção integral da conduta ao preceito primário do tipo mencionado. V - A previsão de combate internacional à pornografia de menores, prevista em decreto, encontra, em seara legislativa interna, consonância e arrimo no delito previsto no art. 241 do ECA, antes e depois da redação dada pela lei 10.764/03. (lex certa).
> (TRF-3 - RCCR: 48936 SP 2004.03.00.048936-3, Relator: DESEMBARGADORA FEDERAL CECILIA MELLO, Data de Julgamento: 28/09/2004, SEGUNDA TURMA).

Em relação a identificação do usuário, também existem dilemas. Identificar a máquina utilizada para a realização da conduta é fácil, afinal, ao conectar-se em uma rede TCP/IP, que lhe permite acesso em escala global a diversos *sites* e banco de dados *online*, é registrado, a cada acesso, seu endereço IP, possibilitando assim, a individualização e posterior localização do computador utilizado. Todavia, dificilmente se sabe quem foi o usuário no momento do crime, porquanto se faz uso de máquinas compartilhadas em *lan houses* ou pertencentes a empresas onde diversos usuários se conectam.

4.4. Legislação Penal Informática no Brasil

4.4.1. Teoria TCC: Técnica, Comportamento e Crime

Ao compararmos o Brasil com demais soberanias, no quesito legislação penal informática, percebe-se uma nítida discrepância de desenvolvimento. Até recentemente, toda legislação acerca de crimes de informática que subsistia se concentrava na Lei 9.983/2000, que veio a acrescentar alguns artigos ao Código Penal, porém, focados tão somente nos funcionários públicos. Com a advento da Lei 12.737/2012, expandiu-se, de maneira tímida, a tutela legislativa à bens informáticos.

> A evolução da legislação brasileira contra os crimes virtuais ou cibernéticos implica a tipificação de outros crimes praticados na internet, constituindo-se esta uma necessidade social. É evidente que o mundo moderno exige do Direito que acompanhe as mudanças e evoluções da sociedade e impeça que os crimes cometidos fiquem sem punição (AMÂNCIO, 2013, p. 27, *apud*, OLIVEIRA JUNIOR, 2012, p. 1)

Durante bastante tempo cobrou-se uma legislação eficiente acerca dos crimes virtuais. Diante de tal clamor, o legislativo brasileiro diversas vezes, de maneira

errônea, buscou tipificar técnicas informáticas ao invés de condutas que se valiam de tais técnicas. Entretanto, buscar punir técnicas gera uma ineficácia tremenda da norma, uma vez que essas de modificam, nascem e morrem dia após dia, perdurando tão somente, as condutas criminosas, que vão se amoldando e aperfeiçoando.

Damásio de Jesus e José Antonio Milagre (2016) trazem em sua obra uma proposta diferenciada de compreensão do crime digital (TCC – Técnica, Comportamento e Crime), onde sistematizam aspectos a serem levados em consideração a fim de criar normas penais informáticas eficientes que não precisem ser complementadas com o tempo. Desta forma, trazem três pontos a serem analisados:

- Técnica: Vislumbra-se o método utilizado pelo agente para praticar tal ação típica. Esta pode ser utilizada de maneira manual ou por meio de subtécnicas, métodos automatizados ou ferramentas;
- Comportamento: Neste, analisa-se o que motivou o agente a utilizar determinada técnica, ou mais de uma técnica, se houve participação de mais agentes, se foi por ação ou omissão, se foi destinado à rede de computadores, dispositivos informáticos ou sistemas informatizados;
- Crime: Este aspecto une os dois anteriores (se houve um ou mais comportamentos e quantas técnicas foram utilizadas) e busca qual o bem jurídico tutelado foi violado através deste conjunto.

Expostos os três aspectos que devem ser considerados, faz-se algumas analises. Inicialmente é necessário frisar que não se legisla sobre técnica, visto que isto resulta numa legislação extremamente específica, porém, pouco eficaz e que se torna obsoleta de maneira muito veloz.

Assim sendo, deve-se identificar, primeiramente, um comportamento, que é mediado por uma ou mais técnicas, e que mereça tutela penal e desta forma tal comportamento, caso se enquadre numa atividade reprovável, ganha *status* de “crime”.

Desta maneira, é importante lembrar, segundo os autores supra, que não é recomendável que se atenha a detalhar extremamente quais técnicas compõem e possibilitam determinado comportamento, a sim de que mantenham o foco na reprovabilidade da ação típica cometida, e não nos meios empregados para que esta fosse consumada.

CONSIDERAÇÕES FINAIS

O intuito deste trabalho não é analisar e demonstrar de forma taxativa características e peculiaridades dos delitos informáticos, mas tão somente compreender como ocorreu o nascimento da internet, como esta se propagou por todo planeta alcançando proporções e extensões não pretendidas ao tempo de sua criação. Almejou-se, ainda, compreender como funcionam cada uma das principais técnicas utilizadas para que a pratica de crimes virtuais seja efetivada, bem como entender, de forma genérica, como se portam as os agentes criminosos.

A busca por uma legislação moderna, eficiente e dinâmica o suficiente para que não se torne inútil em si mesma também foi um dos objetivos deste trabalho, uma vez que se se analisou formas de legislar que gerasse leis eficientes e justas que não estejam focadas tão somente nos meios veiculados, mas sim nos comportamentos e, principalmente, no impacto que estes geram na sociedade e nos bens juridicamente afetados.

É imprescindível, também, dizer que a cooperação internacional possui papel fundamental em virtude da rede, visto que esta se espalha e interliga cantos geograficamente distantes, permitindo, assim, vítimas e agressores nem tão distantes uns dos outros, mesmo sendo de países e nacionalidades distintas. Essa cooperação implicará numa uniformização de leis, facilitando as comunicações entre polícia e judiciário e, consequentemente, uma padronização de *logs* que viria a gerar uma repressão eficaz a tais crimes.

REFERÊNCIAS

ALMEIDA, Carolina. **O conceito por detrás da Lei de Interceptação Telefônica (Lei nº 9.296/96)**. Disponível em: <https://carolinacaa.jusbrasil.com.br/artigos/112214757/o-conceito-por-detras-da-lei-de-interceptacao-telefonica-lei-n-9296-96>. Acesso em: 15 ago. 2017;

AMÂNCIO, Tania Maria Cardoso Silva. O IMPACTO DA INFORMÁTICA NA SOCIEDADE E O DIREITO NO BRASIL. **Revista Jurídica Consulex**, [S.l.], n. 405, p. 24-28, dez. 2013;

AMOROSO, Danilo. **Aprenda as diferenças entre vírus, trojans, spywares e outros.** Disponível em: <https://www.tecmundo.com.br/phishing/853-aprenda-as-diferencas-entre-virus-trojans-spywares-e-outros.htm>. Acesso em: 19 jul. 2017;

ARAS, Vladimir. **Crimes de informática. Uma nova criminalidade**. Disponível em: <http://www.informatica-juridica.com/trabajos/crimes-de-informatica-uma-nova-criminalidade/>. Acesso em: 29 ago. 2017;

_____, Vladimir. **Crimes de informática. Uma nova criminalidade**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <https://jus.com.br/artigos/2250>. Acesso em: 30 ago. 2017;

BRASIL. Constituição (1988). **Constituição [da] República Federativa do Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 16 jun. 2017;

_____. Decreto Lei nº 2848, de 7 de dezembro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 16 jun. 2017;

_____. Lei n. 12737, de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 16 jun. 2017;

_____. Lei n.º 9296, de 24 de julho de 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em: 26 ago. 2017;

_____. Tribunal Regional Federal (3 região). RCCR 48936. Apelante: Justiça Pública. Relatora: Desembargadora Federal Cecilia Mello. Data do acordão: 28 set. 2004. Disponível em: <https://trf-3.jusbrasil.com.br/jurisprudencia/19174044/recurso-criminal-rccr-48936-sp-20040300048936-3-trf3>. Acesso em: 07/09/2017;

CAETANO, Gustavo Teixeira. **CRIMES PRATICADOS PELO COMPUTADOR DA DIFICULDADE EM APURAÇÃO DOS FATOS**. 2010. 71 p. Monografia Jurídica (Bacharel em Curso de Direito) - Faculdade de Direito de Cachoeiro de Itapemirim, Cachoeiro de Itapemirim - ES, 2010;

CAPEZ, Fernando. Fato típico: Conduta. In: CAPEZ, Fernando. **Curso de direito penal – parte geral (arts. 1º a 120)**. 20ª. ed. São Paulo: Saraiva, 2016. p. 141-142. v.1;

DE OLIVEIRA, Jôline Cristina . **O cibercrime e as leis 12.735 e 12.737/12**. 2013. 60p. trabalho de conclusão de curso (Bacharelado em Direito) - Departamento de Direito da Universidade Federal de Sergipe, São Cristóvão, 2013. Disponível em: <https://www.conteudojuridico.com.br/pdf/cj045489.pdf>. Acesso em: 14 ago. 2017;

FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. **Revista da Faculdade de Direito**, Belo Horizonte, n. 62, p. 139-178, jan. 2013;

GRECO, Rogério. **Curso de Direito - parte especial (artigos 213 a 361)**. 13. ed. Niterói: Impetus, 2016. 1121 p. v. 3;

_____, Rogério. **Curso de Direito Penal - parte especial (artigos 121 a 212)**. 14. ed. Niterói: Impetus, 2017. 1090 p. v. 2;

INTERNET. Disponível em: <https://pt.wikipedia.org/wiki/Internet#Hist.C3.B3ria>. Acesso em: 16 jun. 2017;

INTRODUÇÃO a Computação: Conceito de bit e byte. Disponível em: <http://producao.virtual.ufpb.br/books/camyle/introducao-a-computacao-livro/livro/livro.chunked/ch02s01.html>. Acesso em: 04 set. 2017;

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016. 208 p.;

LEI do cibercrime. Disponível em: <http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis>. Acesso em: 14 ago. 2017;

LIMA, Simão Prado**. Crimes virtuais: Uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade**. Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=15260&revista_caderno=3>. Acesso em: 26 out. 2016;

MASSON, Cleber Rogério .**Direito penal esquematizado: Parte geral**. São Paulo: Método, 2008. 1035 p.;

MIRABETE, Julio Fabbrini. **Manual de Direito Penal**: parte geral. 27. ed. São Paulo: Atlas, 2011. 466 p. v. 1;

MIRANDA, Marcelo Baeta. **Abordagem dinâmica aos crimes via internet**. Disponível em: <https://jus.com.br/artigos/1828/abordagem-dinamica-aos-crimes-via-internet/1>. Acesso em: 06 set. 2017;

NETO, Lindolfo Pires. **CRIMES CIBERNÉTICOS: necessidade de uma legislação específica no Brasil**. 2009. 38 p. Monografia Jurídica (Bacharel no Curso de

Graduação em Direito) - Faculdade de Ensino Superior da Paraíba, João Pessoa, 2009;

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **O problema na tipificação penal dos crimes virtuais**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 7, n. 58, 1 ago. 2002. Disponível em: <https://jus.com.br/artigos/3186>. Acesso em: 29 ago. 2017;

RAY Tomlinson. Disponível em: <https://pt.wikipedia.org/wiki/Ray_Tomlinson>. Acesso em: 16 jun. 2017;

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal**. Disponível em: <http://www.dhnet.org.br/dados/cursos/anp/rossini_cibercrime.pdf>. Acesso em: 30 ago. 2017;

SEGURANÇA na Internet. Disponível em: <https://segnet.jimdo.com/malware/keyloggers-e-screenloggers/>. Acesso em: 25 jul. 2017;

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. 2. ed. São Paulo: Saraiva, 2015. 360 p.;

VIEIRA, Luiz. **ARP Poisoning**. Disponível em: <https://imasters.com.br/artigo/10117/seguranca/arp-poisoning?trace=1519021197&source=single>. Acesso em: 08 ago. 2017.