UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE DIREITO

"A CRIMINALIDADE CIBERNÉTICA: UMA ANÁLISE JURÍDICA"

HUMBERTO DE OLIVEIRA PEDRA DOS SANTOS

RIO DE JANEIRO
2017/1

HUMBERTO DE OLIVEIRA PEDRA DOS SANTOS

“A CRIMINALIDADE CIBERNÉTICA: UMA ANÁLISE JURÍDICA”

Trabalho de conclusão de curso apresentado à Faculdade de Direito da Universidade Federal do Rio de Janeiro, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Carlos Eduardo Adriano Japiassú

Rio de Janeiro

2017/1º Semestre

CIP - Catalogação na Publicação

de Oliveira Pedra dos Santos, Humberto
d371c A criminalidade cibernética: Uma análise jurídica / Humberto de Oliveira Pedra dos Santos. -- Rio de Janeiro, 2017.
68 f.

Orientador: Carlos Eduardo Adriano Japiassú.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade de Direito, Bacharel em Direito, 2017.

1. Criminalidade Cibernética. 2. Direito Penal. 3. Direito Digital. 4. Computer Users. I. Eduardo Adriano Japiassú, Carlos, orient. II. Título.

341.559

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a).

“A CRIMINALIDADE CIBERNÉTICA: UMA ANÁLISE JURÍDICA”

Trabalho de conclusão de curso apresentado à

Faculdade de Direito da Universidade Federal do Rio de Janeiro, como requisito parcial para obtenção do título de Bacharel em Direito.

Data de aprovação: ____/_____/_____

Banca Examinadora:

_____

Prof. Guilherme Martins

_____

Membro da Banca

_____

Membro da Banca

RIO DE JANEIRO

2017/ 1º Semestre

Resumo

O presente trabalho tem, como objetivo primário, a análise do crimes cibernéticos em todas as suas peculiaridades, explicando a terminologia própria desde tipo de delito.

Ademais, o objetivo do presente trabalho monográfico também foi verificar a legislação penal e especial, realizado ampla pesquisa dos dispositivos penais pertinentes.

Por fim, foram examinadas as diversas formas de enfretamento destes delitos, sugerindo os meios mais eficazes de lidar com os delitos no âmbito digital.

Palavra-chave: Crimes Cibernéticos, Internet, usuários de computador, Ciberespaço.

Abstract

This work has as it's main objective the analysis of cybernetic crimes in any possible meanings, explaining it´s own terminologies.

Furthermore, the objective of this work was also verify the criminal law and special legislation, doing a ample research of all relevant legal devices.

Lastly, it was explored various ways of coping this particular crimes, being suggested the most effective tactics to deal with the transgressions made on the digital sphere.

Keywords: Cybernetics Crimes, Internet, computer users, cyberspace.

SUMÁRIO

1. INTRODUÇÃO

O presente trabalho é motivado pela ascensão contemporânea dos meios informáticos, que vêm modificando de forma considerável as relações sociais. É notório o fato que tais alterações impactam diretamente no ordenamento jurídico, uma vez que este não é estático e é obrigado a se ajustar de acordo com o desenvolvimento da sociedade.

Assim sendo, nos chama a atenção que o meio informático – que aqui chamarei de cibernético, ou virtual – é altamente fluido, e se desenvolve em uma velocidade considerável, de forma silenciosa. Dessa forma, é um ambiente que propiciou o cometimento de diversos crimes que foram se tornando cada vez mais complexos, e que exigiram da comunidade internacional uma solução jurídica para tratar tais injustos penais.

Em razão disso, surge a presente pesquisa, que busca analisar qual o tratamento jurídico atual dado aos crimes cibernéticos. Não só internacionalmente a Convenção de Budapeste surgiu dessa necessidade de se tratarem esses novos crimes sob a ótica do Direito, mas também se busca pesquisar como é o tratamento jurídico dispensado pelo Brasil, e se a legislação pátria tem dado conta de resolver todos os casos concretos acerca das infrações penais no meio cibernético.

Outrossim, os profissionais do Direito enfrentam não só as dificuldades acerca do tratamento jurídico per si, como também há o problema de o meio informático ser extremamente técnico e de alta fluidez, em que os próprios profissionais encontram dificuldade em se manter atualizados acerca dos avanços tecnológicos.

Em adição a isso, temos que o cometimento de crimes cibernéticos não se restringe ao território de um único país, que cria diversas dificuldades sobre a competência e a aplicação do Direito Penal de cada Estado.

Portanto, são muitas as razões que motivam este trabalho. A análise jurídica será feita à luz do Direito Penal Brasileiro; tal análise não pretende ser exaustiva, uma vez que se pautará meramente em descrever como o fenômeno atinge o ordenamento jurídico brasileiro, e como o aplicador do Direito no Brasil terá de enfrentar os desafios acerca dos crimes cibernéticos

2. CRIMES CIBERNÉTICOS

2.1. Introdução – Do conceito de crime

Antes de conceituar crimes cibernéticos, precisamos primeiramente caracterizar "crime" na sua acepção mais clássica. Tendo em vista que o atual Código Penal não fornece um conceito de crime, necessita-se esposar-se da doutrina penalista para definição deste.

Crime, segundo construção doutrinária moderna, é fato típico, antijurídico e culpável. Alguns autores como Basileu Garcia e Mezger sustentam que crime também que a punibilidade integra tal conceito.[1] Para Rogério Greco, o conceito de crime, numa visão analítica, é fato típico, ilícito e culpável somente.[2]

O fato típico se dividiria em tais elementos: conduta dolosa ou culposa, comissiva ou omissiva; resultado; nexo de causalidade entre conduta e o resultado e tipicidade. Greco define ilicitude como: "expressão sinônima de antijuricidade, é aquela relação de contrariedade, de antagonismo, que se estabelece entre a conduta do agente e o ordenamento jurídico."[3] E, por último, a culpabilidade é definida por ele como: "o juízo de reprovação pessoal que se faz sobre a conduta ilícita do agente."[4] Esta última, adotando a posição finalista de Greco, é dividida ainda em: imputabilidade; potencial consciência da ilicitude do fato e exigibilidade de conduta diversa.[5]

Conforme leciona Juarez Cirino dos Santos, o crime é definido pela descrição das condutas proibidas, e a cominação de penas e a previsão de medidas de segurança se realiza pela delimitação de escalas punitivas ou assecuratórias aplicáveis, respectivamente, aos autores imputáveis ou inimputáveis de fatos puníveis.[6]

Desta forma, temos que no Brasil a visão doutrinária mais aceita é de que crime é o fato típico, ilícito e culpável, sendo estes três os elementos do tipo. Temos o que a doutrina chama de "visões estratificadas", assim chamadas por causa do número de elementos do tipo que

[1] GRECO, Rogério. Curso de Direito Penal – Parte Geral - Vol 1 - 17ª Ed. 2015, p 196.
[2] Idem. p.197.
[3] Idem. p.197.
[4] Idem. p.198.
[5] Idem. p.198.
[6] DOS SANTOS, Juarez Cirino. Direito Penal – Parte Geral. Editora ICPC, Curitiba, 2014.

integram cada uma delas. Assim, é importante não olvidar que o ordenamento brasileiro adota de forma majoritária a visão estratificada tripartite do tipo. Ainda que seja a teoria mais aceita, temos diversas outras que tentam explicar qual o conceito de crime e quais seriam os elementos do tipo, discussão essa que não interessa ao presente trabalho.

Sendo o conceito de crime definido, passaremos agora ao estudo dos crimes cibernéticos, verificando se tal nomenclatura é apropriada e definiremos a modalidade deste delito em todos os seus elementos.

2.2. Crimes Cibernéticos

Existem várias terminologias para os chamados crimes informáticos, entre elas: crime cibernético, crime virtual e *cybercrime*. Todos estes são sinônimos, mas a terminologia mais adequada para tal seria "crimes cibernéticos", termo mais abrangente e também adotado pela Convenção de Budapeste, o instrumento internacional mais elaborado e completo referente à legislação destes.

Tendo em mente que todos os termos possuem o mesmo sentido, emprestamo-nos a definição do Irineu Francisco Barreto Junior[7]:

> Com o advento da Internet e da Sociedade da Informação, surgiu uma nova modalidade de crimes cometidos no espaço virtual da rede através de *e-mails* (correio eletrônico), *web sites* (sítios pessoais, institucionais ou apócrifo) ou mesmo ocorridos em comunidades de relacionamento na *Internet*, entre as quais a mais conhecida e o Orkut, propriedade do provedor de conteúdo americano Google. As transações comerciais eletrônicas, envolvendo compras que exigem a identificação do numero de cartão de credito, as transações bancarias, que solicitam registro de dados referentes as contas correntes bancarias, além do uso de senhas e demais mecanismos de segurança, assim como a profusão de novas modalidades relacionais mantidas em sociedade, através da *Internet*, propiciaram o surgimento de novas modalidades de crimes na *web*, batizados de *crimes virtuais.*

Frisa-se que o termo "crimes virtuais" está em perfeita consonância com "crimes cibernéticos", sendo este último o que será utilizado por todo trabalho. Cada autor conceitua o que acha mais apropriado, mas todos reconhecem a sinonímia entre os termos, conforme demonstra a definição do Moisés de Oliveira Cassanti para este tipo de delito:

---

[7] BARRETO Júnior, Irineu. Atualidade do Conceito de Sociedade da Informação para a Pesquisa Jurídica. In: PAESANI, Liliana Minardi (Coord.). O direito na sociedade da informação. São Paulo: Atlas, 2007, p. 71.

> Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido cibercrime. Outros termos que se referem a atividade são: **crime informático, crimes eletrônicos, crime virtual** ou **crime digital**.[8]

Já para Paulo Quintiliano, os chamados crimes cibernéticos são quaisquer tipos de delitos que utilizam aparatos de alta tecnologia para sua perpetração.[9] Segundo as lições de Luciana Boiteux, crimes cibernéticos são: "condutas antissociais alçadas à condição de fatos típicos por decisão de política criminal, diante da constatação da sua gravidade e necessidade de interferência do direto penal."[10]

Uma característica intrínseca dos crimes digitais é a ausência física do sujeito ativo do crime, o perpetrador. Desta forma qualquer crime praticado através da rede mundial de computadores é denominado crime cibernético, pois não há a presença física nem do autor do delito nem dos seus comparsas.[11]

Outro elemento dos crimes cibernéticos é sua correlação com as características da própria rede de computadores. A infraestrutura da internet permite uma troca de dados em escala global que facilita disseminação de ataques maliciosos pela via digital. Um simples ato de envio de *e-mail* de spam pode afetar milhares de pessoas em qualquer parte do globo.[12]

Vale frisar que nem toda conduta prejudicial a outrem pode ser caracterizada como crime cibernético. Se uma conduta for atípica, simplesmente o autor não poderá ser indiciado. Um exemplo clássico seria uma pessoa invadir o computador de alguém sem alterar,

---

[8] CASSANTI, Moisés de Oliveira. Crimes Virtuais: Vítimas Reais - Rio de Janeiro: Brasport, 2014, p. 3.

[9] SILVA, Paulo Quintiliano da. dos Crimes Cibernéticos e seus efeitos internacionais. Procedings of the Firts International Conference on Forensic Computer Science Investigation (ICoFCS´2006)/ Departamento de Polícia Federal
(ed.) Brasília, Brazil, 2006,124 pp.- ISSN 19180-1114

[10] BOITEUX, Luciana, Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual, RBCCRIM 47, 2004

[11] RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. Revista Jus Navigandi, Teresina, ano 7, n. 58, 1 ago. 2002. Disponível em:<https://jus.com.br/artigos/3186>. Acesso em: 18 out. 2016.

[12] SIEBER, Ulrich. *Greek National Section of the International Association of Penal Law. SPINELLIS, Dionysios (org.) Computer Crimes, Cyber-Terrorism, Child Pornography and Financial Crimes*, Atenas, 2003, p. 16.

modificar, obter ou deletar dados do computador deste sem burlar *firewalls*, antivírus, *antispyware* ou qualquer outro de sistema segurança da máquina.[13]

Tal conduta pode ensejar uma ação de danos morais, mas não um indiciamento na esfera penal.[14] Isto porque não poderá ser enquadrado no art. 154-A do Código Penal, *in verbis*:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Portanto, crimes cibernéticos são condutas típicas, ilícitas e culpáveis que ocorrem no ambiente virtual, o chamado ciberespaço. Resta agora definir o conceito de ciberespaço e indicar os sujeitos que participam delitos virtuais.

2.3. Ciberespaço

O ciberespaço nada mais é que um ambiente transfronteiriço que conecta todas os computadores ao redor do mundo. Frisa-se que o termo "computadores" refere-se a qualquer dispositivo interconectado passível de receber ataques maliciosos de diferentes tipos (*spyware, adware, malware, ransomware*, vírus entre outros). Ou seja, englobam-se aqui os *smartphones*¸ *tablets, personal computer* e quaisquer outros dispositivos informáticos.

Segundo Douglas Kellner, o prefixo "ciber" deriva de uma palavra de origem grega, cujo a qual o significado é "controle".[15] O físico Norbert Wiener usou o termo "cibernético" na década de 40 com o significado de "ciência do controle e da comunicação entre os seres vivos e as máquinas". Desde então, esse prefixo tem disso amplamente utilizado em termos relacionados ao domínio da computação e do que Fernando Cascais chama de "máquinas inteligentes".[16]

---

[13] WENDT, Emerson. Crimes Cibernéticos: Ameaças e procedimentos de investigação, 2ª Edição. Rio de Janeiro: Brasport, 2013, p. 19.
[14] Ibidem.
[15] KELLNER, Douglas. Como mapear o presente a partir do futuro: de Baudrillard ao *cyberpunk*. In: A cultura da mídia. Bauru: EDUSC, 2001. p.377-419.
[16] CASCAIS, Fernando. Dicionário de Jornalismo: as palavras dos media. São Paulo: Verba, 2001.

O termo foi utilizado pela primeira vez pelo aclamado escritor de ficção científica Willian Gibson em uma história curta chamada "Burning Chrome". Entretanto ele foi popularizado com o lançamento da obra considerada um dos pilares do movimento *cyberpunk*, a trilogia de livros chamada "Neuromancer".

Ibson se refere ao ciberespaço como: "(...) um espaço não-material, sem configurações geográficas, composto por redes de computadores, telecomunicações, programas, interfaces e banco de dados em que as experiências se desmaterializam e passam a concretizar-se em bits".[17]

Segundo a Professora Luciana Boiteux entende-se por ciberespaço: [18]

> O conceito de ciberespaço (*cyberspace)*, ou espaço virtual alcançado pela rede mundial de computadores, a Internet, que reduziu as distâncias e aproximou as pessoas, foi concebido como uma nova dimensão espacial que transcende fronteiras, e permite a todos aquelas conectados à rede imediato contato com qualquer lugar do mundo em segundos, independentemente de fronteiras ou meios de transporte.

O ciberespaço, assim como os crimes cibernéticos, tem inúmeras nomenclaturas, sem prejuízo de sentido. Ele pode ser chamado de *cyberspace*, mundo virtual ou até mesmo espaço cibernético e é nele onde são perpetrados os delitos virtuais.[19]

Este é um lugar imaterial, onde ocorrem inúmeras interações interpessoais, sendo a extensão do espaço físico em que vivemos. Exatamente por este motivo, deve-se atentar à segurança na rede, garantindo a proteção contra ataques cibernéticos.[20]

A problemática do ciberespaço é exatamente a sua internacionalidade. Um indivíduo na Colômbia invade um sistema de um estabelecimento na Alemanha, através de um provedor

---

[17] MAIAS, André, BRAVO, Rogério. "Geopolítica, geoestratégia e ciberespaço." (2010), p 3.
[18] BOITEUX, Luciana: Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual, RBCCRIM n. 47, 2004, p. 147.
[19] SOUZA, H.. DA AUSÊNCIA DE LEGISLAÇÃO ESPECÍFICA PARA OS CRIMES VIRTUAIS. JUDICARE. Disponível em: <http://fadaf.com.br/revistas/index.php/judicare/article/view/148>. Acesso em: 18 Out. 2016.
[20] SOARES, C. Guedes, TEIXEIRA, A. P., JACINTO, C.Riscos, Segurança e Sustentabilidade. Edições Salamandra, Lisboa, 2012, (ISBN 978-972-689-247-2), p. 175

russo, sendo que os efeitos de tal ataque cibernético ocorrerão em território brasileiro.[21] Onde estará configurado o lugar do crime? Tal impasse será estudado melhor no capítulo três da presente monografia. Passemos agora ao estudo dos sujeitos envolvidos nos crimes cibernéticos.

2.4. Classificação dos crimes cibernéticos

Assim com a definição de ciberespaço e a nomenclatura usada para designar crimes cibernéticos, os delitos virtuais são divididos de diversas maneiras dependendo do autor que os classifica.

A grosso modo, crimes cibernéticos são divididos em crimes cibernéticos impróprios e próprios. Estes podem ser chamados de crimes cibernéticos comuns e crimes cibernéticos autênticos, respectivamente. Nos primeiros, o canal utilizado é a internet, mas o alvo está fora dela. Alguns exemplos seriam as ameaças, o estelionato e o *cyberbullying*.

A internet é utilizada, portanto, como o meio. Já nos crimes cibernéticos próprios, o canal e o alvo estão em rede. Nesta categoria, incluir-se-iam a violação de dados de outrem, a invasão de perfis em redes sociais e o envio de vírus.

Além dessa classificação, Robson Ferreira[22] define os crimes cibernéticos também em 4 (quatro) instâncias: primeiro, quando o computador é alvo, o que coincide com a definição de crime cibernético próprio. Segundo, quando o computador é instrumento para o crime. Nesse caso, seriam crimes que poderiam ser feitos por outro canal, sendo o dispositivo eletrônico apenas um deles. Terceiro, quando o computador é incidental para o crime; em que o computador é necessário para que haja o delito, mas pode vir a ser utilizado para sua consumação. E por último, quando o crime está associado com o computador.

Um exemplo de crime cibernético no qual o computador é alvo seria a contaminação por vírus assim como furto de propriedade intelectual. Já no segundo caso, no qual o

[21] CONTE, Christiany Pegorari, SANTOS, Coriolano Aurélio de Almeida Camargo. "Desafios do direito penal no mundo globalizado: a aplicação da lei penal no espaço e os crimes informáticos." Revista de Direito de Informática e Telecomunicações n. 3.4, 2008.
[22] FERREIRA, Robson. Textos Acadêmicos, dez. 2001. apud PINHEIRO, Patrícia Peck. Direito Digital. 4. ed. São Paulo: Saraiva. 2010. p. 296.

computador é instrumento para o crime, teria a divulgação de pornografia infantil como exemplo mais claro. Isso porque a pornografia poderia ser disseminada por outros meios, sendo a internet apenas um desses canais.

Já em casos em que o computador seria incidental para o crime, temos a lavagem de dinheiro e os crimes contra a honra como exemplos mais clássicos. Pirataria de *software* e falsificação de programas exemplificam a classificação de crimes associados com o computador.

Dessa classificação de Robson Ferreira, pode-se constatar que das quatro categorias, três poderiam ser inseridas na definição de crimes cibernéticos impróprios. Seriam subdivisões deste. As hipóteses de "computador como instrumento para crime", "computador como incidental para o crime" e "crime associado ao computador" são abarcados todos pelo conceito de crime cibernéticos impróprios, ou seja, crimes em que o computador é o meio, mas não o alvo do delito.[23]

Já a hipótese "crimes em que o computador é o alvo" encontro paralelismo semântico com a definição "crimes informáticos próprios", em que o computador é o meio e alvo para a consumação da conduta criminosa.

Como dito anteriormente, cada autor tem sua própria classificação. O professor Quintiliano, por exemplo, divide os crimes cibernéticos em crimes cibernéticos *strictu sensu* e crimes cibernéticos *lato sensu*. Os primeiros seriam aqueles que além do emprego da tecnologia necessitam do uso da *internet* para serem perpetrados. Seriam os crimes sobre os quais versamos a maior do presente trabalho, como utilização vírus de computador para obter dados eletrônicos do alvo.

Já os crimes os crimes cibernéticos *lato sensu* seriam aqueles que se utilizam de tecnologia, mas não necessitam do emprego da *internet*. Esse tipo de crime seria ilustrado pelo exemplo dos infames "chupa-cabras", que são dispositivos implantados em caixas

[23] RODRIGUES DA SILVA, Marcelo, Cibercrime (parte 2). Disponível em <http://marcelorodriguesdasilva56.jusbrasil.com.br/artigos/121942261/cibercrimes-parte-2> Acesso em 8 de novembro de 2016.

eletrônicos (ATMs) de bancos ou em quaisquer outros lugares que obtém as senhas dos indivíduos que tem a infelicidade de utilizar seus cartões nessas máquinas "premiadas".[24]

Além dessas, uma classificação que merece destaque neste trabalho seria a do professor Emerson Wendt. Para ele os crimes cibernéticos são divididos em "crimes cibernéticos abertos" e "crimes exclusivamente cibernéticos". Os "crimes cibernéticos abertos" seriam aqueles realizados através do computador, mas que também poderiam ser praticados por outros meios. Exemplos seriam pornografia infantil, racismo e crimes contra a honra.

Já os "crimes exclusivamente cibernéticos" são aqueles somente praticados por meio de dispositivos conectados à *internet*, ou seja, não seria possível praticá-los sem acesso a um computador. Como exemplo destes crimes estão aqueles contra a urna eletrônica, interceptação telemática ilegal e "invasão de computador mediante violação de mecanismo de segurança com a fim de obter, adulterar ou excluir dados e informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".[25]

Este último exemplo de "crime exclusivamente cibernético" é interessante, pois apesar da classificação mais indicada para os crimes cibernéticos seja a clássica divisão entre crimes cibernéticos impróprios ou comuns – em que o meio para praticar o crime é o computador, mas o alvo está fora dele –, e crimes cibernéticos próprios ou autênticos – em que tanto o meio quanto o alvo é o computador –, Wendt afirma que também há outras condutas prejudiciais, mas atípicas.

Um exemplo seria "invadir um computador sem o fim de obter, adulterar ou excluir dados e informações sem violar mecanismo de segurança". Isto porque tal conduta, apesar de poder ser considerada prejudicial para alguns que seus dados, imagens ou vídeos sejam

[24] SILVA, Paulo Quintiliano da. dos Crimes Cibernéticos e seus efeitos internacionais. Procedings of the Firts International Conference on Forensic Computer Science Investigation (ICoFCS´2006)/ Departamento de Polícia Federal(ed.) Brasília, Brazil, 2006,124 pp.- ISSN 19180-1114

[25] WENDT, Emerson. Crimes Cibernéticos: Ameaças e procedimentos de investigação, 2ª Edição. Rio de Janeiro: Brasport, 2013, p. 19.

expostos a um estranho sem seu consentimento, não podem ser enquadrados no artigo 154-A do Código Penal[26], como já exposto no subcapítulo 1.2 deste trabalho monográfico.

A última classificação relevante que será citada nesta obra será a divisão dos crimes cibernéticos em "crimes cibernéticos puros", "crimes cibernético mistos" e "crimes cibernéticos comuns". Estes também são chamados de crimes informáticos, sem prejuízo de sentido. Marco Aurélio Rodrigues Costa define crimes cibernéticos puros como "toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas".[27]

Ou seja, o atacante planeja sabotar o sistema de computador da vítima, objetivando ganhar controle da máquina, roubar dados relacionados ao usuário que estão salvos no computador como senhas bancárias ou ainda danificar hardware do sistema para que este pare de funcionar.

Os crimes cibernéticos mistos são conceituados por Reginaldo César Pinheiro como "aqueles em que o uso da internet é condição *sine qua non* para a efetivação da conduta, embora o bem jurídico visado seja diverso ao informático".[28] Nesta modalidade de crime o computador é essencial para sua perpetração, mas o alvo do atacante não está no sistema do computador da vítima. O exemplo mais claro seria transferência de valores pecuniários da vítima para uma conta à escolha do agente ativo da conduta delituosa, ou seja, se utilizar do chamado *home-banking* com intuitos criminosos.

Por último, os crimes cibernéticos comuns são aqueles que utilizam a *internet* apenas como um canal para efetivação de um delito que pode ser realizado por outros meios. Crimes como o estelionato e a pornografia infantil já tipificados tanto pelo Código Penal (artigo 171) como pelo Estatuto da Criança e do Adolescente, respectivamente; ambos podem ser praticados sem o advento da *internet*, configurando-se, desta forma, o crime cibernético comum.

---

[26] Ibidem, p. 19.
[27] COSTA, Marco Aurélio Rodrigues. Crimes de informática. Revista Eletrônica Jus Navigandi, abril 1997. Disponível em: < http://www.jus.com.br/doutrina/crinfo.html>. Acesso em 24 de outubro de 2016.
[28] PINHEIRO, Reginaldo César. Os cybercrimes na esfera jurídica brasileira. Revista Eletrônica Jus Navigandi, agosto 2000. Disponível em <http://jus.com.br/revista/texto/1830/os-cybercrimes-na-esfera-juridica-brasileira>. Acesso em 24 de outubro de 2016.

À primeira vista, a divisão dos crimes cibernéticos em puros, mistos e comuns é seria aparentemente como mais abrangente do que a divisão clássica entre crimes cibernéticos próprios e impróprios, entretanto, com uma análise mais minuciosa, chega-se a conclusão que a última pode ser utilizada sem quaisquer problemas. Isto porque os crimes cibernéticos puros encontram perfeita sintonia de significação com os crimes cibernéticos próprios.

Os puros são definidos como crimes objetivam invadir o sistema de informática da vítima. Já os crimes cibernéticos ditos como próprios são aqueles nos quais o sistema informático é alvo e o meio do delito. Ambos podem ser considerados sinônimos.

Quantos aos crimes cibernéticos mistos e comuns, facilmente constata-se como ambos são englobados pela definição de crime cibernético impróprio. Este ocorre quando o meio para a realização da conduta ilícita é o sistema informacional, mas o alvo não está nos dados contidos naquele. Os crimes cibernéticos comuns são aqueles que se utilizam da *internet* como meio para um crime já pode ser realizado por outros canais, crimes estes que não objetivam roubo ou modificação de dados da vítima, seja como o exemplo estelionato ou pornografia infantil.

Já nos crimes cibernéticos mistos é necessário o uso do sistema informacional para praticá-los, mas o bem jurídico que o atacante procura atingir não está no sistema informático da vítima. Como pode-se ver, tanto os crimes cibernéticos mistos como os comuns podem ser abarcados pelos crimes cibernéticos impróprios.

Portanto, para fins de melhor compreensão, apesar de haver várias classificações para os crimes cibernéticos, a melhor a ser utilizada seria a divisão entre crimes cibernéticos impróprios ou comuns e crimes cibernéticos próprios ou autênticos. Nos crimes cibernéticos impróprios ou comuns, o meio para perpetrá-los seria através de um computador mas o alvo de tal crime não está nele.

Ou seja, mesmo que o atacante se utilize do computador para praticar o delito, o objetivo dele não é invadir nem adulterar ou furtar dados do computador da vítima. Seu objetivo está além disso, como por exemplo, difamar ou caluniar a vítima do ataques ou mesmo praticar *cyberbullying* com a mesma. O sujeito ativo do crime estaria se utilizando do

meio conhecido como *internet* mas seu alvo estaria no ciberespaço, atingindo, neste exemplo, a honra do sujeito passivo do crime.

Já os crimes cibernéticos próprios ou autênticos são aqueles que só podem ser praticados através do computador e seus semelhantes, e o alvo seria *software* ou *hardware* da vítima, violando suas informações.

2.5. As principais ameaças no ciberespaço

2.5.1. Os *crackers*

Definidas então as classificações mais relevantes no que concerne aos crimes cibernéticos, é preciso abrir um subcapitulo para demonstrar as principais maneiras que um usuário mal-intencionado se utiliza para praticar a conduta delituosa em face da vítima.

Primeiramente, faz-se necessário definir quem é o sujeito ativo dos crimes cibernéticos. Comumente na mídia, quando um ataque cibernético de larga escala ocorre, os criminosos que o praticam geralmente são referidos como "*hackers*". Entretanto, seria tal vocabulário o mais correto para definir "cibercriminosos"?

O termo "*hacker*" na verdade é o que possui o significado mais extenso. *Hacker* serve para designar qualquer pessoa que tenha amplo conhecimento de informática e programação. Basicamente, eles são *experts* da computação. Contudo, assim como um indivíduo habilidoso nas artes marciais, altamente treinado e com conhecimento gigantesco no manejo de armas de fogo pode usar seus atributos para proteção de uma carga ou de uma pessoa, ou grupo de pessoas, esse mesmo indivíduo pode utilizar todo o seu conhecimento para roubo de bancos ou até mesmo assassinato por aluguel.

Na mesma linha da analogia seguem os *hackers*. Indivíduos com alto conhecimento técnico-informático podem usar suas habilidades para achar falhas no sistema, seja a fim de modificá-los ou melhorá-los, seja até mesmo notificar a empresa ou grupo a qual o sistema pertence para que este não fique vulnerável a um ataque virtual.

Tais personalidades que promovem esses benefícios no ambiente cibernético são chamados mais especificamente de "*white-hat hackers".* Os "*white-hat hackers"* também são chamados de *hackers* éticos.[29] As próprias empresas os contratam para verificar falhas na segurança de seus sistemas. Algumas fazem ainda mais, pois além de contratar diversos profissionais para resguardar seus dados, simplesmente oferecem prêmios à qualquer um que consiga encontrar brechas nos seus códigos, como é o caso *Facebook* e *Google*.[30]

Mas então quem são os sujeitos que promovem os ataques delituosos no ambiente virtual? Esses seriam chamados de "*crackers*", também denominados de "*black-hat hackers*", ou *hackers* antiéticos. A palavra *crackers* é um termo em inglês que deriva do verbo "*to crack"*, que significa quebrar. *Cracking,* então, pode ser definido com o ato de "quebrar" os dispositivos de defesa do sistema de segurança de forma antiética e ilegal.

Os *crackers* sempre estão procurando os *xploits,* que são recursos que permitem explorar as vulnerabilidades de um código podendo inclusive modificá-lo em proveito próprio.

Há também o termo "*gray-hat hackers"* que se refere aos *hackers* que penetram num sistema sem, no entanto, modificá-lo ou praticar quaisquer ato que prejudiquem o(s) usuário(s) do supracitado sistema invadido.[31] Apesar de o fato de somente invadirem um sistema sem autorização já se configurar como uma infração, estes *hackers* nada fazem além de "quebrar", invadir o sistema de segurança que atacam. Este tipo de *hacker* não é relevante para o objeto de estudo do presente trabalho monográfico, sendo apenas necessário sua citação para fins referenciais.

Os *hackers*, portanto, que devem ser extensamente estudados, são *crackers* ou *black-hat hackers.* Estes podem tentar decifrar a criptografia, que nada mais é que o embaralhamento de informações de uma mensagem para que esta fique ininteligível. Ou eles

---

[29] FRAGA, Ewelyn Schots. As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo jurídico, p. 31 – 2. ed. – São Paulo: Ordem dos Advogados do Brasil, 2010.
[30] GUSMÃO, Gustavo. Brasileiro recebe maior prêmio do Facebook após encontrar bug. Exame.com, 26 jan 2014. Disponível em: <http://exame.abril.com.br/tecnologia/brasileiro-recebe-maior-premio-do-facebook-apos-encontar-bug-2/>. Acesso em 23 out 2016.
[31] FRAGA, Ewelyn Schots. As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo jurídico, p. 31 – 2. ed. – São Paulo: Ordem dos Advogados do Brasil, 2010.

podem tentar "crackear" *softwares*, ou seja, entender como um determinado programa funciona para então fazê-lo funcionar de forma incorreta, ou simplesmente emparelhar suas funcionalidades. Além disso, os *crackers* podem se especializar na criação de *malwares*, que são *softwares* maliciosos que prejudicam os usuários na rede, como *trojans*, *ramsonwares* ou vírus, que serão estudados logo a seguir.

Para Moisés de Oliveira Cassanti há algumas subdivisões para as espécies de *crackers*, sendo as mais relevantes a seguintes[32]:

> ***Carder*:** especialista em roubar informações bancárias como números de cartões de crédito, cartões de conta corrente ou poupança, ou contas em sites de movimentações bancárias, para comprar on-line, saques em caixas eletrônicos, transferência para contas de laranjas entre outro atos ilícitos.
> ***Defacer***: especialista em pichar sites normalmente deixando mensagens de protesto contra o próprio site.
> ***Spammer***: dissemina e-mails com correntes e vírus que podem danificar e roubar informações dos usuários, como senhas bancárias.
> ***Phisher***: especialista em aplicar golpes diversos. Eles são profundos conhecedores das falhas de um sistema.
> ***Phreaker***: especialista que utiliza técnicas para burlar os sistemas de segurança das companhias telefônicas, normalmente para fazer ligações de graça ou conseguir créditos.

Passa-se agora ao estudo das principais formas que os *crackers* se utilizam para atacar o sistema do usuário, que neste caso, é a vítima ou sujeito passivo do delito virtual.

2.5.2 Os *malwares*

Malwares nada mais são que *softwares* maliciosos. O nome é exatamente a contração das palavras em inglês "*malicious software*". Ou seja, são programas que o atacante se utiliza para roubar, danificar ou modificar dados do sistema informacional da vítima. Ao contrário do que se imagina, os *malwares* não invadem um computador por si só, como às vezes é alardeado em filmes hollywoodianos ou séries televisivas.

Para que eles invadam o computador do usuário, é necessário que este dê a permissão para o *malware* ser executado em sua máquina. Obviamente, os cibercriminosos não deixam os *malwares* aparentes, camuflando-os em mensagens de *e-mails*, afirmando que o usuário ganhou algum prêmio ou se passando por um amigo mandando fotos de uma viagem que

[32] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro, p. 2/3 Brasport, 2014.

supostamente teriam feito no passado. Tudo para que a vítima caia no golpe e venha a acessar o anexo, e assim infecte a sua máquina. Os *crackers* também escondem esses *softwares* nocivos em programas aparentemente inofensivos, nos quais o usuário é levado a instalar o *malware* juntamente com o *software* que deseja obter.

As maneiras para se infiltrar no sistema do usuário são apenas limitadas pela criatividade dos seus atacantes, que encontram hodiernamente novos meios de incitar a curiosidade ou de se aproveitar do descuido das vítimas para infectar o máximo de máquinas com seus *softwares* maliciosos. Alguns tipos de ataque já são conhecidos pelo grande público, como o exemplo anterior que o usuário recebe um *e-mail* em que é dito que ele ganhou uma quantia enorme de dinheiro. As recentes pesquisas comprovam que o número de golpes virtuais ou *malwares* só aumentam a cada ano, a se ver pelas estatísticas alarmantes: 76% dos usuários brasileiros já caíram em golpes virtuais[33]. Isso demonstra que ainda existe um enorme caminho de conscientização para que as pessoas sejam mais precavidas na *internet*, pois a maior parte dos crimes virtuais ocorrem por descuido da vítima.

Os *malwares* são apenas um termo genérico para quaisquer *softwares* hostis que prejudicam os usuários que têm suas máquinas infectadas. A seguir será listada os mais conhecidas espécies de *malwares*.

2.5.2.1 Vírus de computador

Talvez os mais conhecidos dos *malwares*, os vírus de computador são programas capazes de copiar a si mesmos. É necessário que algo o ative, portanto ele por si só não se executa.[34]

O Professor e pesquisador de Postura de Segurança da Universidade de New Haven em Connecticut, Frederick Cohen, foi quem programou e utilizou pela primeira vez este *software* nocivo. Segundo ele, a idealização foi apenas com o propósito científico, não tendo o professor sequer ideia da sua proliferação nos dias atuais.[35]

---

[33] Informações retiradas da pesquisa do *Ponemon Institute*, dos E.U.A., de 2012 reproduzida nos sítios virtuais: <http://mashable.com/2012/11/05/cybersecurity-infographic/#5QSRXQ_vKsqJ>, e < https://www.tecmundo.com.br/seguranca/32327-76-dos-usuarios-brasileiros-ja-cairam-em-golpes-virtuais.htm>. Acessado em 16 de junho de 2017.
[34] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro, p.8: Brasport, 2014.
[35] Idem, p. 9.

Para que o vírus aja, não basta que o programa esteja infectado por ele, pois deve haver ativação do evento pelo o usuário. Desta forma, o vírus pode ficar dormente horas ou até mesmo dias na máquina do usuário sem ser acionado, apenas esperando que o evento seja disparado pela vítima para poder agir.

Vale frisar que vírus são *softwares*¸ portanto não são capazes de danificar o *hardware* de sua máquina, ou seja, a parte concreta como o gabinete, teclado, disco rígido ou impressora. Um exemplo do que pode ocorrer gerando tal desentendimento seria um vírus infectando o BIOS[36] da placa-mãe tornando a máquina incapaz de ser inicializada, deduzindo-se erroneamente que o computador está quebrado. Entretanto, é possível levar a máquina numa assistência técnica capaz que remova o vírus fazendo o computador ligar novamente.[37]

O vírus de computador, além de ser uns dos *malwares* mais conhecidos, também é bem abrangente, pois tem várias modalidades. O professor cita algumas delas na sua obra, como é transcrito a seguir:

> **Vírus de arquivo:** anexa ou associa seu código a um arquivo de programa normal, costuma infectar arquivos executáveis, principalmente arquivos .*COM* e .*EXE*, e só tem efeito se os arquivos contaminados forem executados
> **Vírus de macro:** são pequenos programas escritos na linguagem de macro de um aplicativo (por exemplo, o *Word* e o *Excel* do *Microsoft Office*) que, em geral, só se propagam em documentos desse aplicativo. Por causa disso, eles também são chamados de vírus de documentos. Para se tornarem ativos, eles precisam que aplicativos correspondentes sejam ativados e que uma das macros infectadas seja executada. Diferentemente dos vírus "normais", os vírus de macro não atacam arquivos executáveis, mas comprometem as configurações dos componentes do programa. A macro modifica o modelo global, fazendo operações inesperadas ou se recusando a realizar outras, causando infecção a todos os arquivos subsequentemente editados no mesmo programa.
> **Vírus polimorfos** (palavra que provém do grego e que significa "que pode assumir várias formas"): são verdadeiros mestres do disfarce. Como um camaleão, ele se transforma a cada infecção, modificando sua assinatura e por isso é muito difícil ser detectado por programas antivírus.
> **Vírus de *e-mails*:** enviam-se a si mesmos para todos na lista de correspondência do programa de *e-mail* do usuário, espalhando-se rapidamente. O vírus se propaga assim que ativado, bastando a exibição do texto da mensagem no painel de visualização (não precisa abrir o anexo) para ocorrer a contaminação. Como resultado, enquanto o vírus costumavam meses ou anos para se propagar, estes agora

[36] A palavra BIOS é um acrônimo para *Basic Input/Output System* ou Sistema Básico de Entrada e Saída. Trata-se de um mecanismo responsável por algumas atividades consideradas corriqueiras em um computador, mas que são de suma importância para o correto funcionamento de uma máquina. Se a BIOS para de funcionar, o PC também para. Disponível em: <https://www.tecmundo.com.br/o-que-e/244-o-que-e-bios-.htm>. Acesso em 23 de outubro de 2016.
[37] Ibidem, p 9.

> fazem isso em horas. Isso torna muito difícil para os antivírus responder antes de um grande dano seja causado.[38]

Além desses, é forçoso citar ainda mais dois tipos de vírus elencados pelo Emérito Professor Emerson Wendt em seu livro "Crimes Cibernéticos: Ameaças e procedimentos de investigação": [39]

> **Vírus de boot:** Esta modalidade de vírus é considerada a precursora de todos os outros tipos de vírus, tendo surgido no final da década de 80 e causado muito transtorno para os usuários de computadores.
> Cabe esclarecer que todo disco possui um setor destinado à inicialização do sistema, e a principal característica do vírus de *boot* é que eles se fixam na partição de inicialização do sistema.
> Dentre as formas de infecção podemos citar o caso da pessoa que esquece um disquete contaminado no diretório A: do computador e no momento em que o sistema operacional do computador é inicializado ocorre sua infecção. Em seguida, casos outros disquetes sejam inseridos, são também contaminado espalham estes arquivos maliciosos em inúmeros computadores.
> CDs, DVDs ou *pen drives* podem ser utilizados para espalhar esses vírus.
> São exemplos desses tipos de vírus o *ping-pong*, o *jerusalem* etc.
> **Vírus *time bomb:*** Este tipo de vírus se caracteriza pelo fato da sua ativação ser deflagrada em determinada data. O programador que elabora esse tipo de código malicioso escolher determinada ocasião para que o vírus seja acionado. Quando chega essa data a vítima sofre seus efeitos.
> Essa modalidade de ameaça também é bomba-relógio ou gatilho.
> São exemplos desses vírus o *sexta-feira 13*, o *michenlangelo*, o *eros* e o *1º de abril.*

2.5.2.2 *Worms*

Worms, também chamados de vermes, são *softwares* maliciosos parecidos com os vírus, com a diferença de que não precisam de uma ação do usuário para se autorreplicar. Eles são programas completos, não necessitando de outro *software* hospedeiro para se expandir, gerando cópias de si mesmo.

O jeito mais comum de um *worm* infectar uma computador é através de anexos hostis em *e-mails*. O *worm* se autorreplica e envia mais *e-mails* para todos na lista de contatos do usuário atacado, expandindo-se indefinidamente e assim por diante. Geralmente os *worms* exploram as vulnerabilidades de computadores que estão com seus programas desatualizados. *Worms* são de difícil identificação, sendo notados apenas quando o computador está lento devido a enorme quantidade de cópias que o *worm* gerou de si mesmo. Como descrito

---

[38] Ibidem, p. 9-10.
[39] WENDT, Emerson. Crimes Cibernéticos: Ameaças e procedimentos de investigação – 2. ed. – Rio de Janeiro: Brasport, 2013, p. 24.

anteriormente, *worms* diminuem o desempenho da máquina, podendo lotar o HD[40] ou até mesmo impedir a execução de alguns programas.[41][42]

2.5.2.3 *Botnets*

Botnets se refere a uma rede de computadores infectados por um *malwares* que permite que o cibercriminoso, remotamente, os controle em conjunto para realizar um determinada tarefa. Muita das vezes os usuários dos computadores infectados nem tem ideia que sua máquina virou uma espécie de "zumbi" que age de acordo com as instruções do atacante.[43]

Estes PCs (*personal computers*, ou computadores pessoais) "zumbis", podem, por exemplo, serem comandados para todos acessarem ao mesmo tempo um *site* (sítio eletrônico). Com uma enorme carga de máquinas tentando acessar o *site* há uma sobrecarga no servidor, tornando incapaz de realizar as requisições de acesso dos usuários.[44]

Este tipo de ataque é conhecido como **DDoS**, acrônimo em inglês para *Distributed Denial of Service* ou Ataque Distribuído de Negação de Serviço. Este tipo de ataque é usado para derrubar grandes sites. Um dos exemplos seria o ataque realizado pelos grupos que na época se denominavam *Anonymous* e *LulzSec*, que derrubaram *sites* do governo brasileiro, deixando indisponíveis os sítios eletrônicos da Receita Federal, da Presidência da República e da Agência Brasileira de Inteligência.[45]

Podemos citar ainda outro ataque do *Anonymous*, desta vez em retaliação à operação do FBI (*Federal Bureau of Investigation*) em janeiro de 2012 onde o *site* Megaupload foi tirado do ar e muitos dos seus mantenedores levados em custódia, resultando em ataques DDoS que derrubaram o *site* do próprio FBI, assim como do MPAA (*Motion Picture Association of America*) e do RIAA (*Recording Industry Association of America*), organizações que também

---

[40] Disco duro ou disco rígido, também chamado de HD (derivação de HDD do inglês *hard disk drive*).
[41] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro, p.14: Brasport, 2014.
[42] WENDT, Emerson. Crimes Cibernéticos: Ameaças e procedimentos de investigação, p. 25 – 2. ed. – Rio de Janeiro: Brasport, 2013.
[43] Idem, p. 25.
[44] WENDT, Emerson. Crimes Cibernéticos: Ameaças e procedimentos de investigação – 2. ed. – Rio de Janeiro: Brasport, 2013, p. 20.
[45] PASSARINHO, Nathalia. *Site* da Presidência foi sobrecarregado "intencionalmente", diz Serpro. **Portal G1**. Disponível em: <http://g1.globo.com/política/noticia/2011/01/site-da-presedencia-foi-sobrecarregado-intencionalmente-diz-serpro.html>. Acesso em: 24 out 2016

fizeram *lobby* para derrubada do *Megaupload*.[46] Vale citar ainda o mais recente ataque DDoS que ocorreu nos Estados Unidos da América em outubro de 2016. Nesta ocasião milhares de dispositivos *IoT* infectados por um *malware* abalaram os servidores da *Dyn*, maior provedora de infraestrutura de internet dos EUA. [47]

IoT é acrônimo em inglês para *Internet of Things* ou Internet das Coisas. Seriam dispositivos eletrônicos que usamos hodiernamente como eletrodomésticos, câmeras de vigilância e até mesmo carros sendo conectados a internet. Especialistas apontam que a Internet das Coisas será a revolução que ocorrerá nas próximas décadas, onde, num futuro não tão distante, todos os aparelhos das lares domésticos estarão conectados à internet. Entretanto, com o exemplo deste ataque DDoS mais recente, é notório ver como tais dispositivos estão sendo vendidos sem os devidos *softwares* de segurança, deixando-o vulneráveis para serem usados como *bots* para intuitos maliciosos dos cibercriminosos.

Como último exemplo vale citar um golpe que se utilizou dos *botnets,* ou seja, como já explicitado é uma rede de computadores infectadas por um *malware* que pode ser utilizada para uma ação específica e simultânea, entretanto tal golpe não se utilizou de ataques DDoS. Em março de 2013, *crackers* comandaram mais de 100 mil PCs a clicarem simultaneamente em anúncios que pagam ao usuário por acesso, semelhante aos anúncios que são dispostos na maior plataforma de vídeos da internet, o Youtube, onde a cada milhares de cliques em um vídeo geram alguns centavos de dólar para o dono do canal. Resultado foi o seguinte: 9 bilhões de cliques geraram um prejuízo de 6 milhões de dólares por mês.[48]

2.5.2.4 *Trojans*

Trojan, também conhecido como cavalo de troia, é um *malware* que se passa por um programa comum que executa normalmente suas tarefas mas que contém códigos maliciosos que visam prejudicar a vítima de inúmeras formas. Moises de Oliveira Cassanti enumera algumas delas:[49]

---

[46] <http://www.crimespelainternet.com.br/a-nova-arma-do-anonymous-contra-sites-e-voce/>. Acesso em: 24 out 2016.

[47] <https://www.tecmundo.com.br/ataque-hacker/110871-entenda-internet-eua-massacrada-sexta-feira.html>. Acesso em: 25 out 2016

[48] <http: //www.bbc.co.uk/portuguese/vídeos_e_fotos/2013/03/130321_click_golpe_dg.shtml>. Acesso em: 27 out 2016

[49] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro, p.12: Brasport, 2014.

> **Instalação de *Keyloggers* *(histórico de teclas)***: esta ferramenta é muito usada por atacantes cuja finalidade é capturar tudo que a vítima digita, também capturando os cliques do *mouse*, *printscreen* da tela e vídeo da *webcam* (podendo ver tudo que o usuário está fazendo). Assim, é possível descobrir suas senhas do *Facebook*, *Skype*, *Twitter*, chats e, lógico, capturar números de contas, senhas e outras informações antes delas serem criptografadas por dispositivos de segurança do sistema financeiro. Depois de tudo capturado, é enviado (geralmente por *e-mail*) para alguém em algum lugar, que analisa o que foi digitado e levanta as informações necessárias(...)
> **Instalação de *Trojan-Downloader***: faz download de outros vírus para seu computador.
> **Instalação de *Trojan-Banker:*** seu objetivo PRINCIPAL é obter dados de autenticação de usuário e validação de transações em sistema de *internet banking*.
> **Inclusão de *Backdoors* (porta dos fundos):** é um utilitário de administração remota que, uma vez instalado, permite acesso de usuário e controla-lo através de uma rede ou da *internet*(...)

2.5.2.5 *Ransonware*

Uma modalidade sofisticada de *malware* criptografar o sistema da vítima, bloqueando seu acesso. Após, será deixado uma mensagem de "resgate", geralmente exigindo quantias vultuosas de dinheiro para que o atacante descriptografe o computador do usuário. Entretanto, assim como num sequestro de pessoas nada garante que o criminoso cumpra o que propôs após se entregue o dinheiro de resgate.[50]

3. LEGISLAÇÃO SOBRE O TEMA

3.1 Convenção de Budapeste

Este capítulo discorrerá sobre os diversos dispositivos legais que permeiam o ordenamento brasileiro referente ao tema "crimes cibernéticos". Entretanto, antes disso faz-se necessário um subcapítulo analisando a Convenção sobre o Cibercrime, também conhecida como Convenção de Budapeste. Começou a ser assinada em 23 de novembro de 2001, entrando em vigor em primeiro de julho de 2004.

Embora o Brasil não tenha ratificado o tratado, pode-se afirmar que este influenciou de alguma forma o legislativo brasileiro, sendo um dos seus objetivos da Convenção exatamente a uniformização da legislação penal acerca dos cibercrimes. Analisar a Convenção de

[50] Ibidem, p. 13

Budapeste é imprescindível para análise jurídica sobre os crimes cibernéticos, já que, como afirma Auriney Brito, a Convenção Europeia sobre Crimes Cibernéticos é "*o único instrumento internacional multilateral referente à legislação sobre cibercrimes*"[51].

A Convenção, como dito anteriormente, lida com a segurança da rede de computadores, fraude nos meios digitais, transgressão aos direitos autorais bem como a disseminação de pornografia infantil na *internet*. Além disso, "*contém (..) uma série de poderes e procedimentos que permitirão a adoção de medidas investigatórias dirigidas a sistemas informáticos, inclusive interceptação de dados*".[52] Esta, por exemplo, traz a hipótese da responsabilidade **penal** do provedor, algo não é incluso pela Carta Magna de 88 nem por todas a leis esparsas pelo ordenamento brasileiro, com exceção talvez apenas ao art. 241 do Estatuto da Criança e do Adolescente, que *in verbis*:[53]

> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008)
> Pena - reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008)

Alguns consideram que tal dispositivo pode ser interpretado responsabilizando os provedores, entretanto isto corre numa divergência doutrinária, podendo afirmar que a Convenção de Budapeste tem uma hipótese interessante ainda não aplicada no ordenamento jurídico brasileiro vigente.

Outro ponto que vale ser citado da Convenção é que esta preceitua que os provedores de acesso colaborem com a Justiça, tendo em vista que sem este auxílio não será possível combater a cibercriminalidade pragmaticamente.[54]

A Convenção é dividida em quatro capítulos, basicamente: o primeiro seria o uso dos termos, o segundo sobre medidas que devem ser tomadas internacionalmente, o terceiro sobre a cooperação internacional e o quarto seriam as disposições finais. Os capítulos ainda são divididos em seções e as seções ainda podem ser divididas em títulos.

---

[51] BRITO, Auriney, Direito Penal Informático, p. 48. Rio de Janeiro: Saraiva 2013.
[52] BOITEUX, Luciana. Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual, p. 169. Revista Brasileira de Ciências Criminais nº 47, 2004.
[53] Lei n° 8.069/90. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8069.htm>. Acessado em 19 de maio de 2017.
[54] BRITO, Auriney, Direito Penal Informático, p. 50. Rio de Janeiro: Saraiva 2013

O capítulo II, por exemplo, possui 3 seções, sendo primeira seção referente ao direito penal material, contendo 5 títulos; a segunda seção se refere ao direito processual, contendo também 5 títulos; e a terceira seção é referente à competência.

O capítulo III possui 2 seções, sendo a primeira relacionada ao princípios gerais, segmentado em 4 títulos e a segunda seção seria sobre as disposições específicas, fracionada em 3 títulos. Por fim, o quarto capítulo versa sobre "*os atos concatenados de execução do documento, identificando situações rotineiras estudadas na teoria gera dos tratados".*[55]

No capítulo *Uso de Termos*, a Convenção acertadamente apresenta definições de palavras e expressões, procurando assim evitar discrepâncias de interpretação que cada país-signatário poderia fazer caso não fosse esclarecido no texto do próprio tratado. Pela Convenção de Budapeste, seriam disposta da seguinte forma os termos:[56]

> a) "sistema de computador" significa qualquer equipamento ou um grupo de equipamentos conectados ou relacionados, um ou mais, os quais, viabilizados por um programa, realizam processamento automático de dados;
> b) "dados de computador" significa qualquer representação de fatos, informações ou conceitos em uma forma adequada para o processamento em um sistema de computador, incluindo um programa apropriado que possibilite ao sistema de computador realizar uma função
> c) "provedor de serviços" significa:
> i. qualquer entidade pública ou privada que proporciona para os usuários de seus serviços a possiblidade de se comunicarem por meio de um sistema de computador, e
> ii. qualquer outra entidade que processa ou armazena dados de computador em benefício de tal serviço de comunicação ou usuários desse serviço.
> iii. "tráfego de dados" significa qualquer dado de computador relacionado a uma comunicação por meio de um sistema de computador, gerado por um sistema de computador que forma uma parte de uma cadeia de comunicação, indicando a origem da comunicação, destino, rota, tempo, data, tamanho, duração, ou tipo de base desse serviço.

A Convenção ainda atenta ao Princípio da Proporcionalidade, pois persecução penal não pode ferir direitos humanos fundamentais. Desta forma, a integridade dos dados de computador, ou seja, os dados pessoais de cada indivíduo, não serão violados em prol de combate desmedido aos crimes cibernéticos. A plenitude dos dados pessoais virou um bem jurídico que deve ser protegido pelo chamado Direito Penal Informático.[57]

---

[55] Ibidem, p. 58.
[56] Ibidem, p. 55.
[57] Ibidem, p. 52.

Ciberespaço, aludido amplamente no capitulo anterior, também ganha sua definição na Convenção Europeia sobre Crimes Cibernéticos. Ele seria um "*espaço comum, utilizado pelos usuários da rede mundial de computadores (Internet) ao se conectarem aos serviços de comunicação e informação, para propósitos legítimos, mas que também podem estar sujeitos a abusos".*[58]

Por fim, a Convenção de Budapeste consolida que segurança informática é composta por disponibilidade, confidencialidade e integridade das informações dos usuários. Se estes três quesitos não forem satisfeitos, não se pode dizer que foi feita uma correta atividade estatal para punir os cibercrimes praticados.[59] Outro ponto que importante que merece ser destacado é que a Convenção não admite a modalidade tentada de delito, sendo **todos** os crimes dispostos nela dolosos.

Agora vamos discorrer sobre os crimes previstos em seus capítulos. Os idiomas oficiais do tratado são o inglês e o francês, sendo feita a tradução livre dos crimes para o português. O primeiro título versa sobre os crimes contra a segurança informática (confidencialidade, integridade e disponibilidade): *illegal access*, ou acesso ilegal à integralidade ou a parte de sistema de computadores, disposto em seu artigo 2º, é cometido quando há uma violação das medidas de segurança, com a intenção de obter dados de computadores ou outro intenção ilícita, independente do computador estar conectado ou não à *internet*; *illegal interception,* ou interceptação ilegal, disposto em seu artigo 3º, ocorre, como o próprio nome sugere, quando há uma interceptação sem autorização através de meio técnicos envolvendo sistemas de computação; *data interference*, ou interferência ou dano em dados de computador, disposto em seu artigo 4º, conduta tipificada por avariar, deletar ou alterar dados de PCs sem autorização, necessitando muitas vezes que ocorra um grave lesão para ser enquadrado neste tipo penal.[60]

---

[58] BOITEUX, Luciana. Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual, p. 169-170. Revista Brasileira de Ciências Criminais nº 47, 2004.
[59] BRITO, Auriney, Direito Penal Informático, p. 62. Rio de Janeiro: Saraiva 2013
[60] BOITEUX, Luciana. Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual, p. 171-172. Revista Brasileira de Ciências Criminais nº 47, 2004.

No Título 2 do Capítulo 2 são previstos dois delitos que estariam classificados, segundo definição exposta no capítulo 1 do presente trabalho monográfico, como crimes cibernéticos comuns, ou seja, condutas criminosas praticadas no meio virtual mas que poderia ser perpetradas em outras vias. São eles: *computer-related forgery*, ou falsificação eletrônica ou praticada por meio de computadores, disposto no artigo 7º, que seria modificação de dados com a intenção fazê-los passarem como autênticos e *computer-related fraud*, ou fraude eletrônica, disposto no artigo 8º, que seria lesar bens de um terceiro através de modificação de dados assim como interferência no funcionando da máquina informática sem autorização com fins de obter vantagem pecuniária para si.[61]

No artigo 9º da Convenção dispõe sobre um tema de crucial importância para o Direito Penal Informático, tendo em vista a facilitação que a *internet* trouxe para o compartilhamento de quaisquer arquivos sendo eles inofensivos ou deletérios a convivência em sociedade: *offenses related to child pornography*, ou crimes relacionados à pornografia infantil.

Vários tipos penais foram definidos no parágrafo primeiro deste artigo, como: produzir pornografia infantil com propósito de distribuição; oferecer ou tornar disponível a pornografia infantil; distribuir ou transmitir pornografia infantil e adquirir pornografia infantil, sendo que há uma reserva a esta hipótese, pois os Estados-signatários podem se reservar a não criminalizar a mera posse de material pornográfico envolvendo menor.

O parágrafo segundo do mesmo artigo define as hipóteses do que seria encarado como material pornográfico infantil, tendo também uma ressalva que apesar da Convenção definir que o limite para ser considerado menor é a idade de 18 anos, os Estados-parte podem reduzir em seus ordenamentos internos a maioridade para 16 anos.[62]

Frisa-se que os crimes relacionados à pornografia infantil já foram tipificados no nosso ordenamento jurídico interno, nos artigos 240 e 240-A do Estatuto da Criança e do Adolescente, sendo tal legislação brasileira abordada nos próximos subcapítulos.

Por fim, ainda pode-se citar a opção da Convenção de não criminalizar o *spam*, ou seja, os *e-mails* enviados não solicitados pelo usuário, que normalmente são enviados para um

[61] Ibidem, p. 172.
[62] Ibidem. p. 172-173.

enorme número de pessoas. A não criminalização foi intencionalmente escolhida, pois concluiu-se que medidas não-penais seriam mais adequadas para lidas com estas mensagens inoportunas.[63]

Exaurida a Convenção de Budapeste, veremos agora como o Legislativo brasileiro tem prestado atenção a esta temática, passando pelas legislações penais aprovadas assim como os projetos que tramitam ainda no Congresso.

3.2 O Marco Civil da Internet

Mesmo que o presente trabalho monográfico tenha como base um caráter penalista, mister se faz analisar a lei 12.965/2014, popularmente conhecido como o Marco Civil da Internet.

Este começou a ser esboçado em 2009, através de uma consulta pública feita na internet, tramitando no Congresso Nacional entre os anos de 2011 e 2014. Pode-se dizer que o Marco Civil foi debatido de forma multissetorial, pois diversos setores da sociedade participaram do sua confecção, entre eles empresas, organizações da sociedade civil, ativistas e comunidade técnica.[64]

Por fim, a lei federal 12.965 foi aprovada em 22 de abril de 2014 e sancionada no dia seguinte pela então presidente da República Dilma Rousseff, trazendo ao ordenamento jurídico brasileiro "direitos, deveres e garantias para todos que utilizam a *internet* em nosso país".[65]

O texto final do Marco Civil conta com 32 artigos. Dentre estes, podemos destacar os seguintes:[66]

> Art. 5º Para os efeitos desta Lei, considera-se: I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e

[63] Ibidem, p. 174.
[64] LEMOS, Ronaldo; SOUZA, Carlos Affonso. Marco civil da internet: construção e aplicação, Juiz de Fora; Editora Associada, 2016, p. 13.
[65] DE MATTOS, Alexandre Magalhães. Crimes na Internet (Locais do Kindle 2167-2170). Alexandre Mattos. Edição do Kindle.
[66] Lei n° 12.965 de 2014. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acessado em 19 de maio de 2017.

> irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes; II - terminal: o computador ou qualquer dispositivo que se conecte à internet; III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais; IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País; V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
> VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados; VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

O artigo 5º define as principais nomenclaturas do Marco Civil, para que estas possam ser aplicadas no mundo jurídico.

Já o artigo 7º contém treze incisos e, de um modo geral, aponta os direitos dos internautas no Brasil. Dentre eles, é garantido a inviolabilidade da vida privada, e caso esta não seja cumprida poderá ensejar indenização material e moral. Além disso, não poderá ser suspensa a conexão de internet pelo provedor, excetuando-se em casos de falta de pagamento ou para garantir qualidade de conexão do contratante. Por fim, exaurindo-se tal dispositivo legal, temos também a inviolabilidade e sigilo dos dados do fluxo de dados dos usuários. Ou seja, só poderão ser disponibilizados para uma investigação os dados armazenados pelos provedores ou empresas mediante ordem judicial. Em casos de fornecimento para terceiros tais dados apenas podem ser compartilhados com expressa permissão do usuário.[67]

O artigo 9º do Marco Civil, provavelmente um dos mais importantes do diploma legal em estudo, trata sobre a chamada "neutralidade da rede":[68]

> Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

Desta forma, não poderão os provedores de acesso à *internet* oferecerem pacotes diferenciados para usuários que utilizem mais os serviços que geralmente exigem mais da infraestrutura da rede, como serviços de *streaming* (tendo como melhor exemplo a empresa

[67] Ibidem Locais do Kindle 2189.
[68] Lei n° 12.965 de 2014. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acessado em 19 de maio de 2017.

Netflix), dos internautas que acessam páginas com arquivos menos "pesados" como *sites* de notícias, que contém predominantemente imagens e textos.

Os artigos 13º e 15º prelecionam, respectivamente a guarda dos *logs* de conexão pelo administrador autônomo pelo prazo de 1 (um) ano e dos *logs* de acesso pela empresa provedora de *internet* pelo prazo de 6 (seis) meses.[69] A legislação diferencia provedores de acesso à internet de provedores de aplicações: os primeiros são empresas que viabilizam a infraestrutura de acesso à rede mundial de computadores, como *GVT*, *Tim Live*, *Predianet*, *NET Virtua*; os segundos oferecem funcionalidades e serviços, como redes sociais, aplicativos de celular e demais empresas que têm serviços fundamentados na comunicação mediada por computadores.

Tal ferramenta é poderoso meio de combate aos crimes cibernéticos, talvez a maior de todas já criada para tal finalidade no âmbito jurídico brasileiro. Entretanto tem caráter demasiado invasivo, podendo comprometer a privacidade dos usuários. Só a título de comparação, a Corte de Justiça Europeia julgou inconstitucional este modelo de guarda e retenção de dados dos usuários, devido à sua ameaça aos direitos fundamentais dos mesmos.[70]

Já os artigos 18º e 19º do Marco Civil discorrem sobre a responsabilidade civil dos provedores de conexão e de aplicação. Vale frisar que os dois tipos de provedores são definidos, respectivamente, pelos incisos V e VII do artigo 5º do mesmo diploma legal, artigo este que já foi trabalhado na página anterior. Os artigos 18º e 19º, *in verbis*:[71]

> Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.
> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

O artigo 18º acertadamente isenta a responsabilidade dos provedores de conexão visto que tecnicamente impossível os impedir que todos os seus usuários pratiquem

[69] Ibidem, Locais do Kindle 2215.
[70] LEMOS, Ronaldo; SOUZA, Carlos Affonso. Marco civil da internet: construção e aplicação, Juiz de Fora; Editora Associada, 2016, p. 144.
[71] Lei n° 12.965 de 2014. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acessado em 19 de maio de 2017.

comportamentos lesivos a outrem. Além disso, não há nexo causal entre um dano causado a terceiro e a disponibilização de acesso à *internet* a um indivíduo.

Seria o mesmo que culpar os fornecedores de cartolina e tinta por qualquer cartaz ofensivo que alguém faça e exponha em uma praça pública, por exemplo. Vale ressaltar que em casos onde há danos decorrentes de **atos próprios dos provedores de conexão**, como a não disponibilização de serviços nas condições contratadas e em desacordo com a regulação setorial haverá responsabilidade civil dos mesmos.[72]

Já o artigo 19º, por uma opção do legislador, decidiu que um provedor de aplicações só será responsabilizado caso não tire o conteúdo ofensivo **após uma ordem judicial**. Logo, não se deve interpretar o dispositivo de maneira que só seria possível tirar do ar um material ofensivo após e somente com uma ordem judicial. Os servidores podem, por si próprios, determinarem requisitos para remoção de conteúdo em seus termos de uso e assim atender notificações extrajudiciais enviadas pelas supostas vítimas do dano decorrente de alguma publicação específica.[73]

Entretanto, caso entendam que o conteúdo especificado não viola os seus termos de uso podem mantê-lo sem quaisquer problemas, devendo o indivíduo que se sentiu ofendido procurar a via judicial para que haja remoção do material lesivo. Só após a ordem judicial **não atendida** que se poderá discutir a responsabilidade do provedor de aplicações.

Demonstrado em linhas gerais como funciona a lei 12.965/14, frisando-se que se trata de uma norma de caráter predominantemente principiológico, visto, desta forma, a edição do Decreto 8.711/2016 que discorre justamente sobre a implementação de vários conceitos estabelecidos no Marco Civil; iremos agora ao estudo das normas penais em nosso ordenamento jurídico referentes à temática da criminalidade cibernética, avaliando como o Legislativo brasileiro tem se portado diante desta problemática que hodiernamente assola a vida de todos.

3.3 Legislação Penal Brasileira acerca do assunto

[72] LEMOS, Ronaldo; SOUZA, Carlos Affonso. Marco civil da internet: construção e aplicação, Juiz de Fora; Editora Associada, 2016, p. 99.
[73] Idem, p. 101

Agora passemos aos estudos da legislação penal brasileira e como ela lida com a temática da criminalidade cibernética. Vale frisar que muitos estudiosos da área afirmam que a legislação atual já abrange por volta de 90% das condutas delituosas orquestradas na *internet*, sendo necessário apenas a edição de algumas leis para tipificar delitos onde o bem jurídico a ser protegido é o próprio sistema de computadores, logo a transgressão é apenas virtual, como seria o caso dos ataques DDoS (ataque de negação de serviço) e a distribuição de vírus.[74][75]

Iremos agora analisar algumas condutas transgressivas praticadas no ambiente virtual que já são tipificadas pela legislação vigente.

3.3.1 Calúnia

A calúnia é um crime contra a honra consistente em atribuir falsamente a alguém fato definido como crime podendo ser enquadrado pelo artigo 138 do Código Penal, tendo como pena de detenção de 6 (seis) meses a 2 (dois) anos e multa.[76][77]

Um exemplo claro deste tipo de delito no ambiente virtual seria alegar nas redes sociais como *Facebook*, *Twitter* ou *Whatsapp* que determinado pessoa subtraiu pertences nas Lojas Americanas, ou postar afirmando que foi agredido(a) por tal indivíduo apenas com o intuito de manchar sua reputação.

3.3.2 Difamação

Difamação seria outro crime contra a honra e consiste em atribuir a alguém fato ofensivo à sua reputação. Ela está tipificada pelo artigo 139 do Código Penal, com pena de detenção de 3 (três) meses a 1 (um) ano e multa.

Podemos citar como exemplos de difamação praticados no meio virtual:[78]

---

[74] BOITEUX, Luciana, Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual, RBCCRIM 47, 2004, p. 186
[75] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro, p. 24: Brasport, 2014.
[76] Idem, p, 24
[77]DE MATTOS, Alexandre Magalhães. Crimes na Internet (Kindle Location 1768). Alexandre Mattos. Kindle Edition.
[78] Idem, (Kindle Location 1777-1781).

> a) Encaminhar (*forward*) *e-mail* para várias pessoas com um boato eletrônico sobre uma pessoa ou um colega de trabalho.
> b) Postar (escrever) em comunidade eletrônica uma ofensa a algum membro dela.
> c) A prática do *cyberbullying* também é um exemplo quando se busca humilhar e ridicularizar demais pessoas através de comunidades

3.3.3 Injúria

O terceiro crime contra a honra consiste insultar ou ofender verbalmente, fisicamente ou por escrito ofendendo a dignidade ou o decoro de alguém. Esta conduta é capitulada pelo artigo 140 do Código Penal e a pena prevista é de detenção por um período de 1 (um) a 6 (seis) meses ou pagamento de multa. Exemplos deste crime sendo praticado na rede mundial de computadores seriam: [79]

> a) Enviar e-mail para uma pessoa degradando sua imagem, chamando-a de gorda, feia, burra e etc.
> b) Escrever nas páginas de recado ou em blogs pessoais textos que degradem a imagem dessa pessoa.

3.3.4 Divulgação de segredo

Tal crime consiste em divulgar documentos ou dados confidenciais ou protegidos a terceiros. Esta conduta delituosa é capitulada pelo artigo 153 do Código Penal, tendo pena prevista de detenção de 1 (um) a 6 (seis) meses ou pagamento de multa. Podemos citar como exemplo de divulgação de segredo na *internet*:[80]

> a) Enviar *e-mail* para terceiros com informação (pessoal, comercial e etc) considerada confidencial.
> b) Escrever em *chats* ou sites dados ou informações de pessoas, dados de empresas, segredos industriais, fórmulas, procedimentos de franquias e etc.
> c) Divulgar em comunidade eletrônica informações sigilosas de empresas.

3.3.5 Dano

Este delito se caracteriza pela destruição, inutilização ou deterioração de coisa alheia. Ele está capitulado no artigo 163 do Código Penal, tendo como pena prevista detenção de 1 (um) a 6 (seis) meses ou multa. Como exemplo deste tipo de crime na *internet*, poderíamos

[79] Ibidem, (Kindle Locations 1787-1792).
[80] Ibidem, (Kindle Locations 1797-1805).

citar o envio de vírus, ataques DoS ou DDoS (ataques de negação de serviço) ou qualquer outro que **destrua equipamentos ou seu conteúdo**.[81]

É importante citar isto a o envio de vírus ou ataque DoS ou DDoS em si não podem ser enquadrados neste artigo, como dito anteriormente esta é uma lacuna da legislação brasileira atual.

3.3.6 Estelionato

O crime de estelionato pode ser definido como induzir alguém ao erro com artifícios ou ardis surpreendendo a boa-fé da pessoa enganada. Tal crime é tipificado pelo artigo 171 do Código Penal com pena de reclusão de 1 (um) a 5 (cinco) anos e multa. Principais exemplos de estelionato no ambiente digital são:[82]

> a) Uma página na internet simulando uma operação bancária na qual o cliente acha que está acessando o site do seu banco.
> b) Um e-mail informando que alguém precisa de dinheiro/doações e informa contas bancárias para esse fim.
> c) Um e-mail ou uma página falsa na internet se fazendo passar por uma empresa idônea.
> d) A suposta venda de produtos em sites de vendas ou leilões onde, após receber o valor por determinado produto a pessoa que o anunciou não o entrega.

Este é, provavelmente, um dos crimes mais praticados na rede de computadores.[83] Vale frisar que as fraudes na *internet* que impactem o sistema financeiro, como a fraude em venda e investimentos e as transferências fraudulentas de fundos eletrônicos [84] podem ser enquadrados como estelionato.

Tais fraudes, genericamente chamadas de crimes financeiros na *internet* também são enquadradas em outros dispositivos na legislação especial, como a quebra de sigilo bancário (regulamentada pela Lei Complementar n. 105/2001); crimes de lavagem de dinheiro (Lei n.

---

[81] CASSANTI, Moisés de Oliveira. Crimes Virtuais: Vítimas Reais - Rio de Janeiro: Brasport, 2014, p. 25.
[82] DE MATTOS, Alexandre Magalhães. Crimes na Internet (Kindle Locations 1816-1828). Alexandre Mattos. Kindle Edition.
[83] Segundo o Perio da Polícia Federal, Dr. Paulo Quintiliano, "os crimes de internet mais comuns hoje em dia no Brasil estão relacionados aos golpes financeiros. Os ladrões estão migrando sua atividade para o espaço virtual, pois o risco é menor. Eles não vão trocar tiros com a Polícia". Cf.: Brasil organiza conferência sobre crimes virtuais. Jornal *O Estado de S. Paulo*, Caderno Link, p. L10, 20 ago. 2007.
[84] BRITO, Auriney, Direito Penal Informático, p. 109. Rio de Janeiro: Saraiva 2013.

9613/98) ou crimes contra o sistema financeiro nacional (tipificados na Lei n. 7492/86).[85] Este último será abordado em um tópico futuro neste capítulo.

3.3.7 Violação de direito autoral

O direito da propriedade artística, científica e literária nasce no momento da criação da obra pelo autor, sendo este o titular do direito. Tal direito subsiste por toda sua vida e é gozado até mesmo pelos seus herdeiros pelo prazo de 60 (sessenta) anos a contar do dia do falecimento do autor. Só a título de ilustração, os descendentes da obra de Machado de Assis, por exemplo, já não poderiam pleitear nenhuma ação alegando a violação de direito autoral tendo em vista que a morte do emérito escritor brasileiro ocorreu há mais de um século (1908 para ser mais exato).

O crime de violação de direito autoral é tipificado pelo artigo 184 do Código Penal, tendo pena prevista de detenção de 3 (três) meses a 1 (um) ano ou multa caso a violação consistir em reprodução por qualquer mesmo com o intuito de lucro ou reclusão de 1 (um) a 4 (quatro) anos e multa se intenção do agente perpetrador for a venda. Os exemplos mais clássicos deste delito na sua modalidade virtual são:[86]

> a) A venda de CD ou DVD pirata.
> b) A prática de baixar música ou vídeo da internet e vender.
> c) Copiar textos na *internet*, não mencionar a fonte, e divulgar que tais textos são de propriedade de quem os baixou.

3.3.8 Crime contra o sentimento religioso

Tal delito é caracterizado pelo escárnio às pessoas e à religião alheia. Tipificado pelo artigo 208 do Código Penal, a pena prevista é de detenção de 1 (um) mês a 1 (um) ano ou multa. Um exemplo deste tipo de transgressão no meio virtual seria o ato de criar comunidades *online* visando o deboche de indivíduos ou determinado(s) credo(s) religioso(s).[87]

---

[85] Idem, p. 112.
[86] DE MATTOS, Alexandre Magalhães. Crimes na Internet (Kindle Locations 1835-1845). Alexandre Mattos. Kindle Edition.
[87] Idem, (Kindle Locations 1849-1852).

3.3.9 Favorecimento da prostituição

O artigo 228 do Código Penal, *in verbis*:[88]

> Induzir ou atrair alguém à prostituição ou outra forma de exploração sexual, facilitá-la, impedir ou dificultar que alguém a abandone:
> Pena - reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (Redação dada pela Lei n 12.2015 de 2009)

Tal crime é cometido no âmbito virtual quando páginas com conteúdo adulto/erótico são acessadas através de *links*, chamadas e *pop-ups* de outras páginas.[89]

3.3.10 Apologia de crime ou criminoso

Capitulado pelo artigo 287 do Código Penal, o ato de fazer apologia de crime ou perpetrador do crime publicamente tem pena prevista de detenção de 3 (três) a 6 (seis) meses ou multa. Este tipo de crime na *internet* pode ser exemplificado das seguintes maneiras:[90]

> a) Criar comunidade, *site* ou *blog* para vangloriar criminosos.
> b) Criar comunidade, *site* ou *blog* para vangloriar ou enaltecer organizações criminosas.
> c) Criar comunidade, *site* ou *blog* onde são ensinadas técnicas para burlar contas de água, luz, TV por assinatura e etc.
> d) Fazer comentários através de *e-mail* ou em comunidade, *sites* ou *blogs* vangloriando criminosos, organizações criminosas ou ensinando técnicas para fraudar ou burlar serviços públicos.

3.3.11 Falsa identidade

Consuma-se este crime quando se apropria da identidade de outra pessoa a fim de obter vantagem indevida. É um tipo de delito que vem aumentando exponencialmente, visto sua facilidade de aplicação: apenas alguns cliques podem ser o suficiente para criar um invólucro de autenticidade, como, por exemplo, a criação de perfis falsos em redes sociais.

Tal delito consuma-se ao se atribuir a terceiros falsa identidade para obter vantagem, em proveito próprios ou alheio, ou para causar dano a outrem. Tipificado no art. 307 do CP tendo

---

[88] Decreto-lei n° 2.848/40. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 19 de maio de 2017.
[89] Ibidem, (Kindle Locations 1854-1855).
[90] Ibidem, (Kindle Locations 1868-1883).

a pena prevista de detenção de 3 (três) meses a 1 (um) ano, ou multa, se o fato não constituir elemento de crime mais grave.

Exemplos de falsa identidade no meio virtual:[91]

> a) Enviar e-mail com remetente falso (fazendo-se passar por empresa ou por terceiros).
> b) Criar identidade em comunidades de relacionamento fazendo-se passar por outra pessoa.

3.3.12 Peculato eletrônico

Com o advento da Lei nº 9.983 de 2000 foram criados novos tipos penais para o Código Penal brasileiro. Dentre eles, no capítulo dos crimes praticados por funcionário público contra a administração em geral foi adicionado o artigo 313-A, que tem a conduta descrita como inserção de dados falsos em sistema de informações, caracterizado pela inserção de dados falsos, adulteração ou exclusão de dados corretos dos sistemas da administração pública, sejam eles informatizados ou não, procurando obter vantagem para si ou para terceiros ou com intuito de causar danos. A pena prevista é de reclusão, de 2 (dois) a 12 (doze) anos e multa.

Além disso foi adicionado o artigo 313-B, que consiste na modificação ou alteração não autorizada de sistema de informações por funcionário público sem autorização da autoridade competente, tendo pena prevista de detenção, de 3 (três) meses a 2 (dois) anos e multa.

3.3.13 Exercício arbitrário das próprias razões

Tal crime, tipificado pelo artigo 345 do Código Penal, visa impedir que particulares tentem satisfazer suas pretensões, mesmo que legítimas, sem apreciação do Poder Judiciário, já que é deste a prerrogativa de dirimir conflitos de interesses entre os indivíduos. Logo, no âmbito virtual, caso receba *spams* na caixa de mensagens ou quaisquer tipos de *malwares* por um agente malicioso, não deve o indivíduo, em represália, reenviá-los para o seu emissor, caso contrário será enquadrado pelo artigo 345 do Código Penal. Esta conduta tem pena prevista de detenção de 15 (quinze) dias a 1 (um) mês ou multa, além da pena correspondente à violência.

---

[91] Ibidem, (Kindle Locations 1885-1894).

3.3.14 Práticas de jogos de azar

Há diversos sites na internet que simulam cassinos, oferecendo uma gama de jogos de azar, como máquinas caça-níqueis e baralhos. Tratam-se de páginas nacionais e estrangeiras, que atraem usuários através de publicidade como links e *pop-ups*, capazes de serem enquadradas no artigo 50 da LCP (Lei das Contravenções Penais), que pune com prisão simples seus praticantes, de três meses a um ano e multa.

Exemplos mais comuns da prática de jogo de azar pela internet:[92]

> a) Participar de cassino on-line.
> b) Fazer apostas em casas de apostas nacionais ou estrangeiras como a *Paddypower*, *skybet*, *ladbrokes* e etc.

3.3.15 Preconceito ou discriminação raça-cor-etnia

Neste subcapítulo vale destacar que apesar da redação da lei 7.716/89 ser estrita, configurando crime de racismo apenas a discriminação de raça, cor, etnia, religião ou procedência nacional, tal entendimento é bastante criticado. Muitos estudiosos apontam que deve haver a inclusão de todas as formas de discriminação nesta legislação, ou seja, mesmo atitudes discriminatórias por orientação sexual, idade, estado civil, enfermidade, deficiência física, condição social, filiação sindical ou partidária, ideias religiosas o políticas ou procedência nacional[93].

Tal interpretação foi feita no *Habeas Corpus* 82. 424-2/RS, que abordava a publicação de livros considerados antissemitas, no qual o Supremo Tribunal Federal entendeu que "não existem distinções entre os homens, seja pela segmentação da pele, formato dos olhos, altura, pêlos, ou por quaisquer outras características físicas, visto que todos se qualificam como espécie humana"[94]. O Supremo Tribunal Federal incluiu os judeus no conceito de raça,

---

[92] Ibidem, (Kindle Locations 1912-1924).
[93] ELUF, Luiza Nagib. A legislação brasileira face às convenções e aos pactos internacionais: questões especiais. *Revistas dos Tribunais*, vol. 699, p. 439. São Paulo: Revista dos Tribunais, 1994.
[94] HC 82424, Relator: Min. MOREIRA ALVES, Relator p/ Acórdão: Min. MAURÍCIO CORRÊA, Tribunal Pleno, julgado em 17/09/2003, DJ 19-03-2004, p. 17 EMENT VOL-02144-03, p. 524.

tornando tal delito imprescritível resultando na condenação do autor das publicações editoriais.

Concluindo, esta interpretação teleológica constitucional do artigo terceiro, inciso IV da Constituição de 1988 que visa a promoção do bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer formas de discriminação é ainda **minoritária**, prevalecendo a posição doutrinária estrita que o crime de racismo é configurado apenas pela discriminação de raça, cor, etnia, religião ou procedência nacional, nos termos da redação atual da Lei 7.716/89.

3.3.16 Pornografia infanto-juvenil

Primeiramente deve-se destacar que não existe crime de pedofilia como comumente acreditado. A pedofilia está incluída no conjunto dos transtornos parafílicos, sendo caracterizados por "qualquer interesse sexual intenso e persistente que não aquele voltado para a estimulação genital ou para carícias preliminares com parceiros humanos que consentem e apresentam fenótipo normal e maturidade física". Sintetizando, a pedofilia é a preferência sexual por crianças, sendo que o portador do transtorno pedofílico deve ter pelo menos dezesseis anos e ter, no mínimo, cinco anos a mais do que a criança.[95]

Pornografia infantil é definido pela Unesco[96] como qualquer meio de retratar ou promover abuso sexual de uma criança, incluindo materiais impressos ou de áudio, centrados nos atos sexuais ou órgãos genitais de crianças.

Entretanto, a predileção é pela expressão pornografia infantojuvenil, visto que esta é mais abrangente, em acordo com o artigo terceiro do Estatuto da Criança e do Adolescente (Lei n 8.069/90), que preceitua, *in verbis*: "A criança e o **adolescente** gozam de todos os direitos inerentes à pessoa humana, sem prejuízo da proteção integral de que trata esta Lei (...)".

---

[95] FRANCES, Allen. *Fundamentos do Diagnóstico Psiquiátrico.* (trad. de Marcelo de Abreu Almeida). Porto Alegre: Artmed, 2015 p. 170.

[96] Consultado em: <http://unescodoc.unesco.org/images/0011/001147/114734eo.pdf>. Acesso em 02/ de maio de 2017.

Salienta-se ainda que o crime de pornografia infantojuvenil não é de todo praticado por pedófilos, pois apesar de haver indivíduos que pratiquem tal conduta delituosa consumindo tal conteúdo (seja trocando, adquirindo ou posssuindo) por ter tal preferência sexual, há também diversas pessoas ou grupos criminosos que praticam o crime visando o lucro, existindo organizações inteiras voltadas para à produção e venda de material pornográfico infantojuvenil.[97]

Ressalta-se ainda que o bem jurídico tutelado nos tipos penais previstos no Estatuto da Criança e do Adolescente (arts. 241 a 241-D) é fruto de diversas controvérsias. Ao ver de Ângelo Roberto Ilha da Silva, o bem jurídico a ser resguardado nesses crimes tutelam a dignidade da criança e do adolescente, compreendendo sua formação moral, além de buscar resguardar a criança de outros males, já que tais dispositivos por vezes contemplam hipóteses de delitos pluriofensivos, como é o caso do artigo 241-D, que visa à proteção da criança de abuso sexual.[98]

Quaisquer indivíduos podem ser enquadrados como sujeito ativo destes crimes, visto que não há especificidade nos dispositivos penais destacados (art. 241 a 241-D do ECA) quanto ao autor do fato punível, tratando-se de crime comum. O sujeito passivo, entretanto, é tanto a criança (pessoa de até doze anos incompletos) como também o adolescente (pessoa entre doze e dezoito anos de idade) nas hipóteses dos artigos 241 ao 241-C. Já no dispositivo do artigo 241-D o sujeito passivo é somente a criança.[99]

Concluindo, a venda, o envio, a posse ou a simples exposição de fotos ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente imputará ao criminoso as seguintes penas previstas no ECA: reclusão, de 4 (quatro) a 8 (oito) anos e multa, na hipótese do art. 241; reclusão, de 3 (três) a 6 (seis) anos e multa, na hipótese do art. 241-A; reclusão de 1 (um) a 4 (quatro) anos e multa, na hipótese do art. 241-B; reclusão, de 1 (um) a 3 (três) anos e multa, nas hipóteses do art. 241-C; e reclusão, de 1 (um) a 3 (três) anos e multa, na hipótese do artigo 241-D.

---

[97] DA SILVA, Ângelo Roberto Ilha (organizador). *Crimes Cibernéticos.* Porto Alegre, 2017, p. 87.
[98] Ibidem, p. 93.
[99] Ibidem, p. 94.

São exemplos de crimes de pornografia infantojuvenil:[100]

> a) Disponibilizar fotos ou vídeos pornográficos na internet de crianças ou adolescentes.
> b) Armazenar tais fotos ou imagens em sites ou comunidades na internet.
> c) Enviar tais fotos por e-mail para outras pessoas.

3.3.17 Concorrência desleal

Um delito que frequentemente passa despercebido na rede mundial de computadores é o crime de concorrência desleal. Estando tipificado no artigo 195, em seus incisos III e VII da Lei 9279/98 a concorrência desleal pode ser definida com o emprego de meio fraudulento para desviar, em proveito próprio ou alheio clientela de outrem. A pena prescrita é de a detenção de 3 (três) meses a 1 (um) ano ou ser punido com aplicação de uma multa. Exemplos dessa prática são:[101]

> a) Desviar a clientela do concorrente usando a marca deste como palavra-chave ou como um link patrocinado em sites de busca.
> b) Utilizar selos ou marcas de institutos de pesquisa, verificação e etc atribuindo-se prêmios ou certificados que não possui.

3.3.18 Crime contra a propriedade industrial

Novamente mais um delito pouco notificado é o crime contra a propriedade industrial, tipificado também no artigo 195, IV e V da lei 9.279/96, também conhecida como lei da propriedade industrial. Tão conduta delituosa tem pena prevista de detenção de 3 (três) meses a 1 (um) ano ou aplicação de multa. São exemplos deste delito na *internet*:[102]

> a) Usar logomarca ou chamada de empresa não autorizada pelo titular desta em sua página da internet ou comunidade.
> b) Enviar e-mail usando logomarca ou chamada de empresa não autorizada pelo titular desta.

3.3.19 Pirataria de *Software*

Um dos delitos mais reincidentes na área da informática, a pirataria de *software*, ao contrário do que se acredita, não é restrito apenas à reprodução, ou a cópia, do *softwares*

[100] DE MATTOS, Alexandre Magalhães. Crimes na Internet (Kindle Locations 1935-1947). Alexandre Mattos. Kindle Edition.
[101] Idem, Kindle Locations 1948-1958.
[102] Idem, Kindle Locations 1960-1966.

popularmente conhecidos como ”piratas”, podendo ser enquadrado neste tipo penal o agente que venda, importe, adquira, oculte ou tenha em depósito tais programas piratas.

Tais condutas violam o artigo 12, § § 1º e 2º da Lei 9.609/ 98, também conhecida como Lei de Proteção da Propriedade Intelectual de Programa de Computador. A pena prevista para esse crime é de detenção, de 6 (seis) meses a 4 (quatro) anos ou multa. Exemplos mais comuns deste crime[103]:

a) Fazer ou usar cópia de software sem licença.
b) Anunciar em site a venda de programas piratas.

3.3.20 Crimes contra o sistema financeiro nacional

Após o caso ocorrido com Guilherme Amorim de Oliveira Alves (Processo 001.03.101766 TJMS), líder de uma quadrilha que aplicava golpes em correntistas de bancos com auxílio da *internet*[104], fraudes contra bancos e instituições financeiras passaram a ser enquadrados pelo artigo 18 da lei 7.492/86, popularmente conhecida como lei do colarinho branco.

Assim, quem fizer transferências fraudulentas de valores entre contas correntes serão punidas por este artigo, tendo pena prevista de reclusão de 1 (um) a 4 (quatro) anos e multa. São exemplos dessa conduta delituosa:[105]

a) Criar página falsa na internet simulando página de instituição bancária com o objetivo de obter, através de fraude, os dados bancários dos clientes da instituição.
b) Utilizar programas do tipo *keylogger* ou *spyware* para obter os dados de clientes de instituições bancárias.

3.4 Demais legislações

[103] Ibidem, Kindle Locations 1971-1983.
[104] RODRIGUES, Giordani. “Presa quadrilha que fraudava contas bancárias pela Internet” Disponível em: <http://www.conjur.com.br/2003-fev-24/presa_quadrilha_fraudava_contas_bancarias_web>, acessado em 4 de junho de 2017.
[105] DE MATTOS, Alexandre Magalhães. Crimes na Internet (Kindle Locations 1989-1995). Alexandre Mattos. Kindle Edition.

Ainda há legislações que merecem serem comentadas aqui, devido à mudança que geraram no nosso ordenamento jurídico, como a "Lei Azeredo" e a "Lei Carolina Dieckmann".

3.4.1 Lei Azeredo

Conhecida assim por ter como relator o então senador mineiro Eduardo Azeredo, a proposta de lei original (PL84/99) além do projeto de censura estava a obrigatoriedade de guardar todos os registros de navegação de todos os brasileiros por três anos.

Tal proposta foi muito criticada a ponto ser apelidada de "AI-5 digital", em alusão aos atos institucionais editados durante o governo militar, sendo Ato Institucional nº 5 o mais duro entre eles, pois concedia ao Presidente da República, entre outras prerrogativas, o poder de cassar mandatos, suspender os direitos políticos de quaisquer pessoas e decretar recesso no Congresso.

Esta PL 84/99 foi de iniciativa da Câmara dos Deputados, para depois ser renomeada para PLC 89/2003 no Senado, sancionada somente em abril de 2013 sob o formato de Lei nº 12.735/12. Boa parte do projeto original não foi incluída no texto final, entretanto veremos suas alterações no Código Penal brasileiro.[106]

Ao artigo 298 do nosso Código Penal foi adicionado o parágrafo único que equipara o cartão de crédito ou débito como documento particular. Antes disso era complicado punir indivíduos que praticavam fraudes com cartões de crédito ou débito na rede digital de computadores, pois era alegada a atipicidade. Isto era uma lacuna enorme na legislação visto que é forma de pagamento mais utilizada na *e-commerce*.

Ao artigo 356 do Código Penal Militar foi incluída a expressão "dado eletrônico". Desta forma, o artigo que tipifica o crime de traição (crime próprio de militar) também inclui quaisquer informações contidas em bases de dados militares. Logo, quem compartilhar ou divulgar dados eletrônicos de bases militares também será punido.

[106]DE MATTOS, Alexandre Magalhães. Crimes na Internet (Kindle Locations 2028-2035). Alexandre Mattos. Kindle Edition.

Além de mudanças do Código Penal e no Código Penal militar, a lei Azeredo, no seu artigo quarto, criou a obrigatoriedade dos estados criarem dentro da estrutura de suas respectivas Polícias Civis delegacias especializados no combate à ação delituosa na *internet* ou sistema informatizado. Entretanto, mesmo já se fazendo alguns anos desde que a lei 12.735 12 tenha entrado em vigor, nem todos os estados brasileiros criaram seus departamentos/delegacias especializados.[107]

Por último, foi incluído no inciso II do artigo 20 da Lei de Crimes Raciais (Lei nº 7.716/ 1989) as expressões "eletrônicas" e "publicação por qualquer meio". Tal alteração permite ao juiz determinar o bloqueio ou a retirada de quaisquer conteúdos que induzam ou incitem a discriminação ou preconceito de raça, etnia, religião ou procedência nacional do provedor de hospedagem na *internet*.

3.4.2 Lei Carolina Dieckmann

Outra legislação que deve ser citada é a lei 12.737 de 2012, popularmente conhecida como Lei Carolina Dickmann. A famosa atriz teve seu computador pessoal invadido em maio de 2012, onde supostamente foram copiadas fotos íntimas da mesma, sendo ela extorquida para que não revelassem tais imagens.

O projeto de lei que resultou na lei 12.737 de 2012 tratava exatamente dos problemas enfrentados pela artista sendo a lei apelidada exatamente em referência ao seu caso. Diferente da Lei Azeredo, que ficou em discussão por anos a fio, a aprovação da Lei Carolina Dickmann foi feita em tempo recorde, já que a PL foi apresentada em 29 de novembro de 2011 (PL 2793/2011) sendo sancionada em 30 de novembro de 2012, como lei ordinária 12.737/2012.

Vamos verificar agora as mudanças ocorridas no Código Penal com a aprovação de Lei Carolina Dickmann. Foi adicionado o artigo 154-A que segue *in verbis*:[108]

---

[107] SAFERNET BRASIL. Delegacias cibercrimes. Disponível em: <http://www.safernet.org.br/site/prevencao/orientacao/delegacias>. Acessado em 06 de maio de 2017.

[108] Decreto-lei n° 2.848/40. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 19 de maio de 2017.

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Frisa-se o *caput* desse artigo foi acertadamente formulado, punindo um tipo de crime onde o bem jurídico a ser protegido é o sistema de computadores em si. Depreende-se da leitura deste artigo também que o delito só ocorre quando o indivíduo tem o **dolo** de cometer a ação, como está expresso ao dizer "(...) com **o fim** de obter, adulterar ou destruir dados ou informações (...)" (GRIFO NOSSO), não sendo cabível neste tipo penal a modalidade culposa de conduta. Logo, o usuário que inadvertidamente compartilha ou encaminha *malwares* não está cometendo crime algum.

No entanto, os criadores de *malwares*, *worms*, ou quaisquer programas prejudiciais não sairão impunes, conforme demonstrado no parágrafo primeiro do deste mesmo artigo:[109]

> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

O parágrafo terceiro do artigo supracitado trata de uma questão já estudada neste trabalho monográfico: "§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o **controle remoto não autorizado do dispositivo invadido**(...)" (grifo meu).

Esta parte grifada claramente se refere aos *botnets*, *malwares* que infectam computadores sem os próprios usuários perceberem, transformando seus dispositivos em "zumbis" que realizam determinada ação orquestrada pelo cibercriminoso muitas vezes sem o conhecimento ou consentimento dos proprietários dos computadores infectados.

Esta determinada ação, por exemplo, pode ser um ataque DDoS, também já estudada num tópico anterior, onde o cibercriminoso atenta derrubar um sistema ou tirar do ar determinado *site* ou *serviço online*, sendo isto uma invalidação do sistema por sobrecarga de

---

[109] Decreto-lei n° 2.848/40. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 19 de maio de 2017.

acesso, não uma invasão.[110] Tal conduta felizmente também foi contemplada pelas alterações da Lei 12.737/2012 no nosso Código Penal, ao adicionar o seguinte artigo:[111]

> "Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

Apesar da Lei Carolina Dieckmann sofrer algumas críticas afirmando que seus dispositivos não são específicos o suficiente, muitos pesquisadores a aprovam, como é o caso de Souza e Lemos, do Instituto de Tecnologia e Sociedade:[112]

> Desde já adiantamos que, na visão do ITS, essa lei foi muito feliz em alcançar o devido equilíbrio entre o combate aos crimes digitais, ao mesmo tempo em que conseguiu reduzir eventuais efeitos colaterais relativos as condutas tipificadas, devendo ser preservada sua redação.

3.4.3 PL 215 de 2015 e seus apensos

Contemplemos agora projetos que ainda estão em tramitação. O projeto de lei 215 de 2015, que tem como autor o deputado Hildo Rocha, visava apenas o acréscimo do inciso V no artigo 141 do Código Penal. Neste artigo são tratadas as hipóteses de aumento de pena nos chamados crimes contra a honra. A proposta seria incluir este quinto inciso com o seguinte texto no dispositivo: "com utilização das redes sociais".[113] Logo, quaisquer casos de crimes contra a honra perpetrados em ambiente virtual seriam punidos com mais rigor.

Entretanto, neste projeto foram apensados mais quatro PLs, todos intentando um maior rigor às punições dados ao crimes contra honra no *internet*. Ocorre que um desses PLs apensados, mais precisamente o PL 1589 de 2015 da deputada Soraya Santos tem proposições que vêm gerando controvérsias.

---

[110] DE MATTOS, Alexandre Magalhães. Crimes na Internet (Kindle Locations 2154-2155). Alexandre Mattos. Kindle Edition.

[111] Decreto-lei n° 2.848/40. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 19 de maio de 2017.

[112] LEMOS, Ronaldo; SOUZA, CARLOS AFFONSO. Marco civil da internet: construção e aplicação. Juiz de Fora, Editora Associada, 2016, p. 143.

[113] CÂMARA DOS DEPUTADOS. Projeto de lei 215/14. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1298301&filename=PL+215/2015>. Acessado em 29 de maio de 2016.

A PL 1.589/2015 **altera** dispositivos do Marco Civil da Internet, retirando a necessidade de ordem judicial para requisição de dados pessoais dos usuários na *internet*, sendo muito criticado, posto que ensejaria facilmente violações da privacidade dos usuários. A título de exemplo, hoje, a polícia e o Ministério Público devem requerer a quebra de sigilo de registros e dados telefônicos pela via judicial, devendo o juiz avaliar a necessidade da medida ao caso concreto.

Com essa alteração do Marco Civil da Internet, não haveria um crivo judicial prévio para que as autoridades policiais e o MP requisitassem diretamente do servidor de conexão os seguintes dados: [114]

> a) registros de conexão à internet de qualquer pessoa (quando e onde se conectou);
> b) registros de acesso a aplicações de internet de qualquer usuário (quais sites, *APPs* ou programas ele acessou na rede);
> c) dados pessoais de qualquer pessoa;

Até o término da realização deste trabalho monográfico, a PL 215 de 2015 juntamente com seus apensos se encontram prontos para a apreciação do Plenário.[115]

3.4.4 Comissão Parlamentar de Inquérito de Crimes Cibernéticos – CPICIBER

Esta CPI foi instaurada em julho de 2015 pelo então presidente da Câmara dos Deputados, Eduardo Cunha. Os relatórios desta CPI foram bastante criticados por grupos da sociedade civil, como ITS Rio e o Artigo 19, afirmando que este seria um retrocesso na legislação acerca dos delitos informáticos. Inclusive o criador da WWW, Tim Berners-Lee, publicou uma "Carta-Aberta ao Legisladores Brasileiros", onde se mostrava contrário ao relatório final desta CPI, apontando que os projetos sugeridos neste iriam minar as conquistas obtidas com o Marco Civil da *Internet*.[116]

---

[114] SANTARÉM, Paulo Renã da Silva; ASSUNÇÃO, Guilherme Sena de. Honra, esquecimento, vigilância e punição na Internet: histórico de tramitação do "PL Espião" (Projetos de Lei 215, 1.547 e 1.589 de 2015) Disponível em: <http://direitoeti.com.br/artigos/honra-esquecimento-vigilancia-e-punicao-na-internet/>. Acessado em 1 de junho de 2017.

[115] CÂMARA DOS DEPUTADOS. Projeto de lei 215/14. Disponível em: <http:// http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=946034>. Acessado em 16 de julho de 2017.

[116] LEMOS, Ronaldo; SOUZA, CARLOS AFFONSO. Marco civil da internet: construção e aplicação. Juiz de Fora, Editora Associada, 2016, p. 40.

Oito PLs são propostos nesta CPI, que são estes:[117]

> 1) Projeto de Lei que estabelece a perda dos instrumentos do crime doloso, em qualquer hipótese, como efeito da condenação;
> 2) Projeto de Lei que altera a redação do art. 154-A do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, para ampliar a abrangência do crime de invasão de dispositivo informático;
> 3) Projeto de Lei que altera a Lei no 5.070, de 7 de julho de 1966, autorizando o uso dos recursos do Fistel por órgãos da polícia judiciária;
> 4) Projeto de Lei que inclui os crimes praticados contra ou mediante computador, conectado ou não a rede, dispositivo de comunicação ou sistema informatizado ou de telecomunicação no rol das infrações de repercussão interestadual ou internacional que exigem repressão uniforme;
> **5**) Projeto de Lei que altera o Marco Civil da Internet, Lei no 12.965, de 23 de abril de 2014, determinando procedimento específico para a retirada de conteúdos que atentem contra a honra e outras providências; (GRIFO NOSSO
> 6) Projeto de Lei que altera a Lei das Organizações Criminosas, a Lei da Lavagem de Dinheiro e o Marco Civil da Internet para incluir no rol das informações cadastrais de usuários o endereço de IP;
> 7) Projeto de Lei que altera o Marco Civil da Internet para possibilitar o bloqueio de aplicações de internet por ordem judicial;
> 8) Projeto de Lei que adiciona a Educação Digital entre as Diretrizes do Plano Nacional de Educação – PNE

Como dito anteriormente, tais projetos foram amplamente criticados, principalmente no que diz respeito às alterações propostas no Marco Civil, sendo lançados vários pareceres técnicos apontando suas problemáticas.

Mas a pergunta que deve ser feita é a seguinte: tais legislações são efetivas ao combates dos crimes cibernéticos ou serão usados apenas como aparatos de repressão e vigilância massiva? Estas e outras indagações seriam respondidas no próximo capítulo, que visa dirimir as dúvidas acerca do Direito Penal para conter o avanço da criminalidade cibernética.

4. OS DESAFIOS DO DIREITO PENAL DIGITAL

4.1 Dificuldades para o operador do direito

As dificuldades dos profissionais do Direito para lidar com os crimes cibernéticos são inúmeras. Primeiramente muitos operadores do Direito não possuem conhecimento dos termos próprios da tecnologia para saber lidar com estes casos. Além disso as provas de um

[117] VARON, Joana; TEIXEIRA, Lucas; AMARELA. 8 PLs são propostos pelo relatório final da CPI de Crimes Cibernéticos. Disponível em: <https://antivigilancia.org/pt/2016/03/8-pls-sao-propostos-pelo-relatorio-final-da-cpi-de-crimes-ciberneticos/>. Acessado em 15 de junho de 2017.

delito cibernético estão todas no computador, o que demanda um artefato pericial mais especializado.

Dentre tantas outras problemáticas e peculiaridades deste tipo de crime, a competência para julgar tais casos é uma questões a serem levantadas. Afinal, os perpetradores dos crimes cibernéticos os podem praticá-los literalmente em qualquer lugar do planeta, podendo o delito gerar efeitos num país ou até mesmo num continente diametralmente oposto. Como são dirimidos estes conflitos de competência no direito brasileiro? É o que veremos a seguir.

4.1.1 O espaço/tempo e a questão processual penal

Entre os inúmeros obstáculos que encontramos ao nos depararmos com os crimes cibernéticos no mundo jurídico, temos a questão do tempo e espaço, questão esta que dificulta a compreensão de como o intérprete virá a aplicar o Direito ao caso concreto.

Primeiramente, como o espaço territorial de cometimento dos ilícitos penais foi relativizado dados os avanços das tecnologias da informação, isso nos leva a perguntar: em qual território que são cometidos os crimes cibernéticos, e quais seriam os limites em que um Estado pode exercer a sua soberania e aplicar o seu Direito? O local de cometimento do injusto penal no meio cibernético não seria fixo, muito menos físico, e também poderia ser dito como atemporal. Nesse diapasão, surge à tona o termo *ciberespaço*, suposto local em que devemos considerar como o tal meio cibernético em que a conduta penal típica, ilícita e culpável teria sido perpetrada.

Como evidenciam Gontijo, Mendes-Silva, Viggiano e Paixão, o termo *ciberespaço* muitas vezes é acompanhado de expressões como *realidade virtual, redes telemáticas*, entre outros neologismos, e usados como sinônimos. Outrossim, apesar de certas dissidências de nomenclatura ou de definição, o importante é que eles chamam a atenção para o fato de que tal "espaço" deve ser atentamente analisado e considerado acerca do impacto que causa na sociedade. [118]

[118] GONTIJO, Cynthia Rúbia Braga; MENDES-SILVA, Ivone Maria; VIGGIANO, Adalci Righi; PAIXÃO, Edmilson Leite. *CIBERESPAÇO: QUE TERRITÓRIO É ESSE?*

Outrossim, ainda que exista toda uma discussão teórica acerca do que seria o *ciberespaço*, até mesmo de cunho sociológico e filosófico, o Judiciário brasileiro tem tentado dar soluções mais palpáveis nos processos que chegam aos nossos tribunais. Processualmente, ainda assim é difícil definir qual o local de cometimento do crime – se foi na casa do indivíduo, em um *cyber* café, ou em qualquer local público que permita o acesso à Internet. As possibilidades são inúmeras, e a utilização de dados falsos, ou o uso de computadores que não pertencem aos verdadeiros criminosos dificulta o trabalho das autoridades na investigação dos delitos.

Esse é um dos motivos pelos quais há doutrinadores que defendem que é necessária legislação específica sobre o assunto, de forma a assentar a procedimentabilidade dos crimes cibernéticos. Diante do narrado, surge uma sensação de insegurança jurídica dentro do nosso próprio ordenamento para determinar o local do crime. Mas os Tribunais Superiores têm tentado, em meio ao aparente caos, uniformizar o entendimento para fixação de competência dos crimes cibernéticos.

Ademais, não há ainda uma jurisprudência consolidada. Não é coincidência, portanto, que muitos tribunais pátrios ainda têm dificuldade de definir a própria competência, o que originou alguns conflitos de competência julgados pelo STJ. A seguir, apenas a título de exemplo, são alguns casos enfrentados pelo E. Superior Tribunal de Justiça:

> *DIREITO PROCESSUAL CIVIL. RECURSO ESPECIAL. AÇÃO DE INDENIZAÇÃO POR UTILIZAÇÃO INDEVIDA DE IMAGEM EM SÍTIO ELETRÔNICO. PRESTAÇÃO DE SERVIÇO PARA EMPRESA ESPANHOLA. CONTRATO COM CLÁUSULA DE ELEIÇÃO DE FORO NO EXTERIOR.*
> *(...)*
> *14. Quando a alegada atividade ilícita tiver sido praticada pela internet, independentemente de foro previsto no contrato de prestação de serviço, ainda que no exterior, é competente a autoridade judiciária brasileira caso acionada para dirimir o conflito, pois aqui tem domicílio a autora e é o local onde houve acesso ao sítio eletrônico onde a informação foi veiculada, interpretando-se como ato praticado no Brasil, aplicando-se à hipótese o disposto no artigo 88, III, do CPC. 15. Recurso especial a que se nega provimento.*
> *(STJ - REsp: 1168547 RJ 2007/0252908-3, Relator: Ministro LUIS FELIPE SALOMÃO, Data de Julgamento: 11/05/2010, T4 - QUARTA TURMA, Data de Publicação: DJe 07/02/2011).*
>
> *PROCESSUAL PENAL. CONFLITO NEGATIVO DE COMPETÊNCIA. NOTÍCIA-CRIME PELA SUPOSTA PRÁTICA DOS DELITOS PREVISTOS NOS ARTS. 20 E 21 DA LEI 5.250/97 (LEI DE IMPRENSA). LEI NÃO RECEPCIONADA PELA CONSTITUIÇÃO FEDERAL. ADPF 130/DF. APLICAÇÃO DOS ARTS. 138 E 139 DO CP E ART. 70 DO CPP. DUAS SEQUÊNCIAS DE FATOS DISTINTOS. PUBLICAÇÃO DE REPORTAGENS VEICULADAS NA REVISTA ISTOÉ. COMPETÊNCIA DO JUÍZO DO LOCAL DA IMPRESSÃO DA REVISTA.*

> *MATÉRIAS DISPONIBILIZADAS NO BLOG "CONVERSA AFIADA". COMPETÊNCIA DO LOCAL EM QUE PRATICADOS OS ATOS DE PUBLICAÇÃO. CONFLITO CONHECIDO. COMPETÊNCIA DA JUSTIÇA FEDERAL PAULISTA.*
> *1. Não recepcionada a Lei de Imprensa pela nova ordem Constitucional (ADPF 130/DF), quanto aos crimes contra a honra, aplicam-se, em princípio, as normas da legislação comum, quais sejam, art. 138 e seguintes do Código Penal e art. 69 e seguintes do Código de Processo Penal.*
> *2. Na hipótese de crime contra a honra praticado por meio de publicação impressa de periódico, deve-se fixar a competência do Juízo onde ocorreu a impressão, tendo em vista ser o primeiro local onde as matérias produzidas chegaram ao conhecimento de outrem, nos moldes do art. 70 do Código de Processo Penal. Remanesce, na prática, o resultado processual obtido pela antiga aplicação da regra de competência prevista na não recepcionada Lei de Imprensa.*
> *3. Crimes contra a honra praticados por meio de reportagens veiculadas pela internet ensejam a competência do Juízo do local onde foi concluída a ação delituosa, ou seja, onde se encontrava o responsável pela veiculação e divulgação de tais notícias.*
> *4. Conheço do conflito para declarar competente o Juízo Federal da 4ª Vara Criminal da Seção Judiciária do Estado de São Paulo.*
> *(STJ - CC 106625/DF 2009/0136422-1. Relator Ministro ARNALDO ESTEVES LIMA. Data de julgamento: 12 de Maio de 2010. S3 - TERCEIRA SEÇÃO. Data de Publicação: DJe 25/05/2010)*

4.1.2 Combate ao cibercrimes vs proteção da privacidade do usuários na rede

Com o crescimento exponencial dos delitos virtuais, muitas autoridades policiais, visando um célere resolução do problema, buscam saber o IP do usuário na rede. Mas o que seria o IP? O IP é uma sigla para *Internet Protocol* ou protocolo de *internet.* Este é um número único que cada computador que se conecta a *tnternet* recebe. Portanto, não existem dois dispositivos com o mesmo IP. Basta um usuário usar um serviço *online*, como acessar um *site* ou baixar um aplicativo na rede para ter seu número IP registrado.[119]

Vale frisar entretanto que existem várias maneiras de proteger seu IP, seja utilizando navegadores que os mascaram como o TOR ou usando redes privadas virtuais (VPNs) que deixam registrados o IP do **servidor** da VPN, não do seu dispositivo.

Ainda existem os *proxys,* que redirecionam sua conexão através de outro endereço IP, sendo este a ser registrado na rede e não o IP da sua máquina.[120] Enfim, todas essas observações são para demonstrar que o IP nem sempre não pode ser usado como identificação

[119]LEMOS, Ronaldo; SOUZA, Carlos Affonso. Marco civil da internet: construção e aplicação, Juiz de Fora, Editora Associada, 2016, p. 138.
[120]<https://www.segurisoft.com.br/vpn/esconder-ip-com-vpn-ou-proxy/>. Acessado em 16 de maio de 2017.

pessoal dos perpetradores de crimes cibernéticos, visto as inúmeras maneiras que o usuário tem burlar tal registro.

Como já citado anteriormente neste trabalho, para as autoridades policiais terem acesso ao IP e quaisquer outros dados dos usuários estas demandam de **autorização judicial**. Ocorre que há várias propostas legislativas para alterar o Marco Civil da *Internet*, **revogando** a necessidade de um crivo judicial prévio para obtenção desses dados. Um desses projetos já foi exposto no capítulo anterior, que seria o PL 215 e seus quatro apensos. Além desse, há o PLS 730 de 2015 de autoria do Senador Otto Alencar (PSD-BA).

Como também exposto anteriormente, grupos da sociedade civil e organizações acadêmicas se mostram contrários a tais PLs. Como é o caso do ITS Rio, que se manifesta da seguinte forma:[121]

> Esta proposta de que o delegado e os membros do Ministério Público possam requerer o endereço de IP de usuários sem ordem judicial prévia, transforma o delegado e os membros do Ministério Público em em juízes. Serão eles, e não os magistrados, que irão decidir que houve "indício de prática de crime por intermédio de conexão ou uso de *internet"*. Em outras palavras, essas autoridades passam a ter a função de julgadores, decidindo elas mesmas questões que somente um juiz poderia decidir para fins de investigação criminal ou instrução processual penal.
> Trata-se de medida claramente atentatória ao próprio Estado Democrático de Direito. É justamente a distinção entre juízes de um lado, e delegados e membros do Ministério Público de outro, que assegura o Estado Democrático de Direito. Quando delegados e membros do Ministério Público se confundem com juízes, caem por terra as garantias constitucionais mais basilares. O investigador vira juiz, subvertendo a ordem tal como países pré-modernos ou em países autoritários.

A questão de obter o IP sem autorização judicial é problemática por vários motivos. Caso o usuário não mascare seu IP, é possível saber exatamente de qual computador partiu a comunicação, seja ela um *post* no *Facebook*, um vídeo postado no *Youtube* ou até mesmo um simples comentário num *blog*.

Sabendo a localização da máquina, é possível chegar ao usuário, sabendo seu endereço, filiação e outros dados cadastrais. Tudo isso poderia ser obtido com apenas uma requisição de um delegado ou Membro do MP.[122]

---

[121] LEMOS, Ronaldo; SOUZA, Carlos Affonso. Marco civil da internet: construção e aplicação, Juiz de Fora, Editora Associada, 2016, p. 138-139.
[122] Idem, p. 138.

O Comitê Gestor da *Internet* no Brasil (CGI.br) também é contra a obtenção de dados de usuários pelas autoridades policiais sem ordem judicial bem como a utilização do IP como forma de identificação pessoal[123], visto que além de ser uma afronta à privacidade também pode ocasionar imputações de delitos a pessoas que não os cometeram, caso o infrator mascare seu IP e desta forma fique registrado na rede o protocolo de *internet* de um outro usuário.

4.1.3 Projetos legislativos recentes e bloqueio de aplicações pelos magistrados

Pelas últimas manifestações do Legislativo, as respostas para o enfrentamento da criminalidade cibernética seriam punições mais rigorosas aos crimes contra a honra cometidos na *internet* (PL 215/2015) e alterações no Marco Civil retirando a necessidade de ordem judicial para obtenção de dados de usuários pelas autoridades policiais e membros do MP (PL 1589/2015 e PLS 730/2015).

Além disso, alguns magistrados acreditam que o bloqueio de aplicativos seja a decisão judicial correta caso entendam que as empresas responsáveis por estes aplicativos não estejam cooperando nas investigações que envolvam crime organizado, tráfico de drogas ou até mesmo pornografia infantojuvenil.[124]

Estas duas não seriam as melhores formas de lidar com tal problemática. Primeiramente, não há necessidade de novas legislações, visto já ter ocorrido intensa reforma no nosso ordenamento jurídico. Tais modificações já começaram, mesmo que timidamente, desde a década de 80: a lei 7 646 87 tratava de proteção da propriedade intelectual de programas de computador. Esta foi revogada pela já citada lei 9 609 98.

Na década de 90 temos a edição da Lei 8 137 90 que passou a punir a utilização de programas de informática para sonegação fiscal (artigo 2, inciso V). Já a lei n 9 100 95 prevê em seu artigo 67, incisos VII, VIII e XI os chamados crimes eleitorais informáticos. Por

---

123 <http://www.cgi.br/esclarecimentos/ver/nota-de-esclarecimento-em-razao-do-relatorio-da-cpi-crimes-ciberneticos.pdf>. Acessado em 16 de maio de 2017.

124 <https://tecnoblog.net/174326/juiz-bloqueio-whatsapp-brasil/>; <https://tecnoblog.net/189494/justica-bloqueio-whatsapp-brasil-48-horas/>; e <https://tecnoblog.net/195057/justica-bloqueio-whatsapp-brasil-72-horas/>. Acessados em 17 de maio de 2017.

último, o artigo 10 da Lei 9 296 96 pune a interceptação de comunicações telefônicas, de informática ou telemática sem a autorização judicial[125].

Nos anos 2000 o Código Penal foi modificado (Lei nº 9.983 de 2000), incluindo os artigos 313-A (inserção de dados falsos em sistema de informações); 313-B (modificação ou alteração não autorizada de sistema de informações); e o artigo 153, § 1º-A, que tipifica a divulgação de informações sigilosas contidas nos sistemas de informação ou banco de dados da Administração pública[126].

Ainda com a aprovação da Lei 10 695 de 2003, resultante da CPI da Pirataria, o Código Penal foi alterado no que tange aos crimes relativos à propriedade intelectual e ao direitos autorais, adequando-se a nova realidade virtual. Em 2008 houve a aprovação da Lei 11 829, resultado da CPI da Pedofilia, alterando o ECA, tipificando a aquisição e posse de material de pornografia infantojuvenil dentre outras condutas delituosas já citadas no capítulo anterior[127].

Nesta última década foram aprovadas a "Lei Azeredo" (Lei nº 12.735/12) e a "Lei Carolina Dieckmann" (Lei 12 737 de 2012), ambas também já comentadas no capítulo 2. Por último, a mais celebrada lei ao combate dos cibercrimes no ordenamento brasileiro foi aprovada em 2014: o Marco Civil da *Internet* (Lei N° 12.965/14).

Amplamente analisada neste trabalho monográfico, vale citar ainda que há um mecanismo de investigação poderosíssimo nesta lei, talvez o mais expressivo no combate aos cibercrimes na legislação brasileira: "a obrigação da guarda de *logs* de conexão e *logs* de acesso de todos os usuários da *internet* brasileiros, pelo prazo de 1 (um) ano e 6 (seis) meses respectivamente"[128].Vale ressaltar que várias países europeus bem como Corte de Justiça Europeia não aprovaram esse modelo de guarda e retenção de dados dos usuários, julgando-o inconstitucional, por seu potencial invasivo e ameaçador à privacidade[129].

---

[125] BOITEUX, Luciana. Delitos Informáticos e Direito Penal Simbólico. In: Cezar Roberto Biterncourt (Org.) Direito Penal no 3º: estudos em homenagem ao Prof. Francisco Munoz Conde: 1 ed. Rio de Janeiro: Lumen Juris. 2007 v., p. 474
[126] Idem, p. 474.
[127] LEMOS, Ronaldo; SOUZA, Carlos Affonso. Marco civil da internet: construção e aplicação, Juiz de Fora, Editora Associada, 2016, p. 142.
[128] Idem, p. 143.
[129] Idem, p. 144.

Pelo exposto, a proposição de tipificação de mais condutas criminosas e aumento de penas nos mais recentes PLs propostos pelo nosso Legislativo se mostra desnecessário, visto o farto aparato jurídico presente na nossa legislação. Ademais, deve-se observar que o combate aos crimes cibernéticos não pode olvidar as garantias constitucionais e os direitos fundamentais, como a liberdade de expressão, direito à privacidade e o sigilo das comunicações.

Quanto às decisões dos magistrados de bloqueio de aplicativos, tal entendimento é extremamente prejudicial e pouco eficaz. Hoje a *internet* é um serviço essencial não só ao exercício da cidadania, mas também está integrado ao desenvolvimento econômico do país, como é o caso das *startups* que atuam em diversos segmentos como mensagens eletrônicas, mídias sociais, *e-commerce* entre outros[130].

4.1.4. Melhores proposições de enfrentamento aos crimes cibernéticos

Como já apontado anteriormente não basta apenas aumentar o aparato repressivo do Estado. A prevenção é o melhor caminho para boa parte do crimes que ocorrem na *internet*. Medidas técnicas de segurança voluntária devem adotados pelos usuários dos computadores[131]. Essa foi a conclusão do Núcleo Técnico de Crimes Cibernéticos da Procuradoria da República de São Paulo.

Tal Núcleo, juntamente com o grupo especializado da Procuradoria da República do Rio de Janeiro foi criado pelo Ministério Público Federal diante da modernização da criminalidade pelo meios digitais[132]. Ambas as Procuradorias, ao notarem que muitos casos dos delitos informáticos ocorrerem pela simples falta de precaução dos usuários da *internet*, firmaram convênios com a ONG SaferNet Brasil[133], atuando conjuntamente na prevenção deste tipo de delito.

---

[130] Ibidem, p. 146.
[131] BOITEUX, Luciana, Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual, RBCCRIM 47, 2004, p. 162.
[132] DA SILVA, Ângelo Roberto Ilha (organizador). *Crimes Cibernéticos.* Porto Alegre, 2017, p. 12.
[133] A ONG SaferNet Brasil é uma associação civil sem fins econômicos e lucrativos, sem vinculação religiosa, racial ou político partidária, fundada em 20 de dezembro de 2005, por um grupo formado por professores universitários, pesquisadores, cientistas da computação e bacharéis em Direito. Oferece um serviço de recebimento de denúncias anônimas de crimes e violações de direitos humanos na *internet* assim como oferece um *help desk* com apoio psicológico para vítimas de delitos cibernéticos.

Foi dessa ação conjunta que foram promovidas as Oficinas chamadas "*Promovendo o uso responsável e seguro da internet",* em 2009 na sede da Procuradoria da República de São Paulo e em 2010 na sede da Procuradoria da República do Rio de Janeiro. Tais oficinas se destinavam aos professores das redes pública e privada de ensino nos respectivos Estados[134].

Tal experiência foi muito bem recebida, tanto que após foram realizadas oficinas periodicamente tanto na sede da Procuradoria da República de São Paulo quanto da Procuradoria da República do Rio de Janeiro. Já em 2011, foram entregues pela ONG material pedagógico para 1.080 (um mil e oitenta) escolas da rede municipal do Rio de Janeiro.[135]

Diante do sucesso da empreitada, foi constatado que a informação, muito mais do que leis penais mais rígidas, seria uma importante ferramenta no combate aos cibercrimes. O usuário mais precavido não cai em golpes recorrentes do meio virtual, não instalando desatentamente *softwares* perniciosos tão pouco digitando senhas em *sites* sem antes checar sua autenticidade.

Outro método importante, já mencionado no presente trabalho monográfico, seria a capacitação dos operadores do direito para os enfrentamentos próprios da criminalidade cibernética. Tal prática já é adotada no Brasil, tendo como melhor exemplo o Grupo de Enfrentamento aos Crimes Cibernéticos da 2ª Câmara de Coordenação e Revisão do Ministério Público Federal (temática criminal). Tal grupo[136]:

> (...) é responsável por uma política institucional de atuação e capacitação para os membros do MPF voltado para a efetiva repressão dos crimes cibernéticos. Visa, entre outros objetivos, ao aprimoramento no que diz respeito ao enfrentamento dos crimes cibernéticos por meio de cursos de treinamento para novos procuradores (no Curso de Ingresso e Vitaliciamento); para os já integrantes na carreira e com ampliação também para abranger a magistratura federal.

5. CONCLUSÃO

[134] DA SILVA, Ângelo Roberto Ilha (organizador). *Crimes Cibernéticos.* Porto Alegre, 2017, p. 13.
[135] <http//rioeducaideias.blogspot.com.br/2011/09/safernet-entrega-1080-kits-para-as.html>. Acessado em 18 de maio de 2017.
[136] Idem, p. 15.

Diante de todo exposto, foi definido neste trabalho monográfico as diversas terminologias para se referir aos crimes cibernéticos, bem como as modalidades próprias que cada doutrinador faz destes delitos. Os demais termos peculiares a esses crimes, como ciberespaço, *malwares* e *hackers* também foram elucidados.

Após houve uma exposição das diversas legislações referentes a esse tema, mesmo que algumas não estejam no nosso ordenamento pátrio ou não sejam propriamente legislações penais, como é caso da Convenção de Budapeste e o do Marco Civil da *Internet*, respectivamente. As diversas modificações no Código Penal e nas diversas leis especiais foram também abordados extensamente ao longo do segundo capítulo, demonstrando que muitos, senão todos os crimes possíveis no rede mundial de computadores já estão tipificados na legislação brasileira.

No terceiro e último capítulo foi demonstrado a complexidade desses delitos, analisando as diversas maneiras de enfrentamento que tanto os membros do legislativo bem como os operadores do direito de uma forma geral vem sugerindo.

Foi visto que os mais recentes PLs apresentados são desnecessários, havendo um arcabouço jurídico abrangente para punição destes delitos. Como a evolução legislativa desse tema já alcançou certa maturidade, deve-se atentar a conscientização dos usuários na rede, como demonstrado na ótima experiência das Procuradoria da República de São Paulo e da Procuradoria da República do Rio de Janeiro relatada no no subcapítulo 3.1.4.

Estas medidas de segurança adotadas pelos usuários juntamente com a preparação dos professionais do direito para defrontamento dos cibercrimes se mostra o mais eficaz método de impedir a prática destes delitos.

A experiência mostra que o combate ao cibercrimes só é efetivo caso ele seja multissetorial, isto é, com a cooperação entre o setor público, o setor privado e a comunidade técnica e acadêmica demonstrando que política criminal vai muito além da criminalização e arbitramento de penas mais severas[137]

[137] LEMOS, Ronaldo; SOUZA, Carlos Affonso. Marco civil da internet: construção e aplicação, Juiz de Fora, Editora Associada, 2016, p. 144.

BIBLIOGRAFIA

BARRETO Júnior, Irineu. Atualidade do Conceito de Sociedade da Informação para a Pesquisa Jurídica. In: PAESANI, Liliana Minardi (Coord.). O direito na sociedade da informação. São Paulo: Atlas, 2007.

BOITEUX, Luciana. Delitos Informáticos e Direito Penal Simbólico. In: Cezar Roberto Biterncourt (Org.) Direito Penal no 3º: estudos em homenagem ao Prof. Francisco Munoz Conde: 1 ed. Rio de Janeiro: Lumen Juris. 2007 v.

_____,_____. Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual, p. 169. Revista Brasileira de Ciências Criminais nº 47, 2004.

BRITO, Auriney, Direito Penal Informático. Rio de Janeiro: Saraiva, 2013.

CÂMARA DOS DEPUTADOS. Projeto de lei 215/14. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1298301&filename=PL+215/2015>. Acessado em 29 de maio de 2016.

CASCAIS, Fernando. Dicionário de Jornalismo: as palavras dos media. São Paulo: Verba, 2001.

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

CONCEIÇÃO M. MARINS, Imaculada. SaferNet entrega 1.080 kits para as escolas da rede municipal de ensino do Rio de Janeiro, 6 de setembro de 2011. Disponível em <http//rioeducaideias.blogspot.com.br/2011/09/safernet-entrega-1080-kits-para-as.html>. Acessado em 18 de maio de 2017.

CONTE, Christiany Pegorari, SANTOS, Coriolano Aurélio de Almeida Camargo. "Desafios do direito penal no mundo globalizado: a aplicação da lei penal no espaço e os crimes informáticos." Revista de Direito de Informática e Telecomunicações n. 3.4, 2008.

COSTA, Marco Aurélio Rodrigues. Crimes de informática. Revista Eletrônica Jus Navigandi, abril 1997. Disponível em: < http://www.jus.com.br/doutrina/crinfo.html>. Acesso em 24 de outubro de 2016.

DA SILVA, Ângelo Roberto Ilha (organizador). Crimes Cibernéticos. Porto Alegre, 2017.

DECRETO-LEI N° 2.848/40. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 19 de maio de 2017.

DE MATTOS, Alexandre Magalhães. Crimes na Internet (Kindle Location 1768). Alexandre Mattos. Kindle Edition.

DIAS, Rafael. "O que usar para esconder a IP: VPN ou Proxy?", 27 de dezembro de 2016 Disponível em: <https://www.segurisoft.com.br/vpn/esconder-ip-com-vpn-ou-proxy/>. Acessado em 16 de maio de 2017.

DOS SANTOS, Juarez Cirino. Direito Penal – Parte Geral. Editora ICPC, Curitiba, 2014.

ELUF, Luiza Nagib. A legislação brasileira face às convenções e aos pactos internacionais: questões especiais. Revistas dos Tribunais, vol. 699, p. 439. São Paulo: Revista dos Tribunais, 1994.

FERREIRA, Robson. Textos Acadêmicos, dez. 2001. apud PINHEIRO, Patrícia Peck. Direito Digital. 4. ed. São Paulo: Saraiva. 2010.

FRAGA, Ewelyn Schots. As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo jurídico– 2. ed. – São Paulo: Ordem dos Advogados do Brasil, 2010.

FRANCES, Allen. Fundamentos do Diagnóstico Psiquiátrico. (trad. de Marcelo de Abreu Almeida). Porto Alegre: Artmed, 2015.

GRECO, Rogério. Curso de Direito Penal – Parte Geral - Vol 1 - 17ª Ed. 2015

GONTIJO, Cynthia Rúbia Braga; MENDES-SILVA, Ivone Maria; VIGGIANO, Adalci Righi; PAIXÃO, Edmilson Leite. *CIBERESPAÇO: QUE TERRITÓRIO É ESSE?*

GUSMÃO, Gustavo. Brasileiro recebe maior prêmio do Facebook após encontar bug. Exame.com, 26 jan 2014,. Disponível em: <http://exame.abril.com.br/tecnologia/brasileiro-recebe-maior-premio-do-facebook-apos-encontar-bug-2/>. Acesso em 23 out 2016.

HC 82424, Relator: Min. MOREIRA ALVES, Relator p/ Acórdão: Min. MAURÍCIO CORRÊA, Tribunal Pleno, julgado em 17/09/2003, DJ 19-03-2004, p. 17 EMENT VOL-02144-03, p. 524.

HIGA, PAULO. Juiz manda tirar WhatsApp do ar no Brasil. Disponível em <https://tecnoblog.net/174326/juiz-bloqueio-whatsapp-brasil/>. Acessado em 19 de junho de 2017.

_____,_____. Justiça manda operadoras bloquearem WhatsApp no Brasil por 72 horas <https://tecnoblog.net/195057/justica-bloqueio-whatsapp-brasil-72-horas/>. Acessado em 17 de maio de 2017.

KELLNER, Douglas. Como mapear o presente a partir do futuro: de Baudrillard ao cyberpunk. In: A cultura da mídia. Bauru: EDUSC, 2001. p. 377-419.

LEMOS, Ronaldo; SOUZA, Carlos Affonso. Marco civil da internet: construção e aplicação, Juiz de Fora, Editora Associada, 2016.

LEI N° 8.069/90. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8069.htm>. Acessado em 19 de maio de 2017.

LEI N° 12.965 de 2014. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acessado em 19 de maio de 2017.

NOTA DE ESCLARECIMENTO EM RAZÃO DO RELATÓRIO DA CPI – CRIMES CIBERNÉTICOS, DIVULGADO NO DIA 30 DE MARÇO DE 2016. Disponível em: <http://www.cgi.br/esclarecimentos/ver/nota-de-esclarecimento-em-razao-do-relatorio-da-cpi-crimes-ciberneticos.pdf>. Acessado em 16 de maio de 2017.

PASSARINHO, Nathalia. Site da Presidência foi sobrecarregado "intencionalmente", diz Serpro. Portal G1. Disponível em: <http://g1.globo.com/política/noticia/2011/01/site-da-presedencia-foi-sobrecarregado-intencionalmente-diz-serpro.html>. Acesso em: 24 out 2016.

PINHEIRO, Reginaldo César. Os cybercrimes na esfera jurídica brasileira. Revista Eletrônica Jus Navigandi, agosto 2000. Disponível em http://jus.com.br/revista/texto/1830/os-cybercrimes-na-esfera-juridica-brasileira. Acesso em 24 de outubro de 2016.

PONEMON INSTITUTE. Disponível em: <http://mashable.com/2012/11/05/cybersecurity-infographic/#5QSRXQ_vKsqJ>, e < https://www.tecmundo.com.br/seguranca/32327-76-dos-usuarios-brasileiros-ja-cairam-em-golpes-virtuais.htm>. Acesso em 16 de junho de 2017.

PRADO, JEAN Justiça manda operadoras bloquearem WhatsApp no Brasil por 48 horas. Disponível em <https://tecnoblog.net/189494/justica-bloqueio-whatsapp-brasil-48-horas/>. Acessador em 17 de maio de 2017.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. Revista Jus Navigandi, Teresina, ano 7, n. 58, 1 ago. 2002. Disponível em:<https://jus.com.br/artigos/3186>. Acesso em: 18 out. 2016.

RODRIGUES DA SILVA, Marcelo, Cibercrime (parte 2). Disponível em < http://marcelorodriguesdasilva56.jusbrasil.com.br/artigos/121942261/cibercrimes-parte-2> Acesso em 8 de novembro de 2016.

RODRIGUES, Giordani. “Presa quadrilha que fraudava contas bancárias pela Internet” Disponível em: <http://www.conjur.com.br/2003-fev-24/presa_quadrilha_fraudava_contas_bancarias_web>, acessado em 4 de junho de 2017.

SAFERNET BRASIL. Delegacias cibercrimes. Disponível em: <http://www.safernet.org.br/site/prevencao/orientacao/delegacias>. Acessado em 06 de maio de 2017.

SANTARÉM, Paulo Renã da Silva; ASSUNÇÃO, Guilherme Sena de. Honra, esquecimento, vigilância e punição na Internet: histórico de tramitação do "PL Espião" (Projetos de Lei 215, 1.547 e 1.589 de 2015) Disponível em: <http://direitoeti.com.br/artigos/honra-esquecimento-vigilancia-e-punicao-na-internet/>. Acessado em 1 de junho de 2017.

SIEBER, Ulrich. Greek National Section of the International Association of Penal Law. SPINELLIS, Dionysios (org.) Computer Crimes, Cyber-Terrorism, Child Pornography and Financial Crimes, Atenas, 2003.

SILVA, Paulo Quintiliano da. dos Crimes Cibernéticos e seus efeitos internacionais. Procedings of the Firts International Conference on Forensic Computer Science Investigation (ICoFCS´2006)/ Departamento de Polícia Federal (ed.) Brasília, Brasil, 2006. ISSN 19180-1114.

SOARES, C. Guedes, TEIXEIRA, A. P., JACINTO, C.Riscos, Segurança e Sustentabilidade. Edições Salamandra, Lisboa, 2012, (ISBN 978-972-689-247-2).

SOUZA, H.. DA AUSÊNCIA DE LEGISLAÇÃO ESPECÍFICA PARA OS CRIMES VIRTUAIS. JUDICARE. Disponível em: <http://fadaf.com.br/revistas/index.php/judicare/article/view/148>. Acesso em: 18 Out. 2016.

VARON, Joana; TEIXEIRA, Lucas; AMARELA. 8 PLs são propostos pelo relatório final da CPI de Crimes Cibernéticos. Disponível em: <https://antivigilancia.org/pt/2016/03/8-pls-sao-propostos-pelo-relatorio-final-da-cpi-de-crimes-ciberneticos/>. Acessado em 15 de junho de 2017.

WENDT, Emerson. Crimes Cibernéticos: Ameaças e procedimentos de investigação, 2ª Edição. Rio de Janeiro: Brasport, 20