UNIVERSIDADE CATÓLICA DO SALVADOR

CURSO DE DIREITO

FELIPE SOUSA ANDRADE DE ALMEIDA

A VULNERABILIDADE NO CIBERESPAÇO: ESTUDO SOBRE A PRÁTICA DE INFRAÇÃO DOS CRIMES CIBERNÉTICOS

SALVADOR

2020

FELIPE SOUSA ANDRADE DE ALMEIDA

A VULNERABILIDADE NO CIBERESPAÇO: ESTUDO SOBRE A PRÁTICA DE INFRAÇÃO DOS CRIMES CIBERNÉTICOS

Trabalho de Conclusão de Curso apresentado ao Instituto de Direito da Universidade Católica do Salvador, como parte dos requisitos para a obtenção do título de Bacharel em Direito.

Orientador: Prof. Ms. Carlos Alberto José Barbosa Coutinho

SALVADOR

2020

FELIPE SOUSA ANDRADE DE ALMEIDA

A VULNERABILIDADE NO CIBERESPAÇO: ESTUDO SOBRE A PRÁTICA DE INFRAÇÃO DOS CRIMES CIBERNÉTICOS

Trabalho de Conclusão de Curso apresentado ao Instituto de Direito da Universidade Católica do Salvador, como parte dos requisitos para a obtenção do título de Bacharel em Direito.

Orientador: Prof. Ms. Carlos Alberto José Barbosa Coutinho

Salvador,___de_____de _____.

BANCA EXAMINADORA

_____

Prof. Ms. Carlos Alberto José Barbosa Coutinho, UFBA, UCSAL
Orientador

_____

Prof. Ms. Jader Veloso Costa, UFBA, UCSAL
Examinador

A VULNERABILIDADE NO CIBERESPAÇO: ESTUDO SOBRE A PRÁTICA DE INFRAÇÃO DOS CRIMES CIBERNÉTICOS

Felipe Sousa Andrade de Almeida[1]

Prof. Ms. Carlos Alberto José Barbosa Coutinho[2]

RESUMO

Este artigo pretende trazer uma descrição abrangente posto que, o cibercrime continua a ser um perigo latente para mostrar os desafios enfrentados pela humanidade à medida que surgem problemas em torno da segurança da informação. Trata-se de um estudo científico realizado através de pesquisa de revisão bibliográfica tendo por referência Nutti, Martins, Vianna, Morimoto, Inellas, Pinheiro, dentre outros fundamentados na abordagem da ciência jurídica e da computação para assegurar um democrático espaço virtual.

Palavras-chave: Crimes Cibernético. Internet. Globalização. Segurança da Informação.

ABSTRAT

This article aims to provide a comprehensive description as cybercrime remains a latent danger in order to show the challenges faced by humanity as problems around information security arise. This is a scientific study carried out through bibliographic review research with reference to Nutti, Martins, Vianna, Morimoto, Inellas, Pinheiro, among others based on the approach of legal science and computing to ensure a democratic virtual space.

Keywords: Cybercrimes. Internet. Globalization. Cybersecurity.

SUMÁRIO

[1] Graduando do Curso de Direito da Universidade Católica do Salvador. E-mail: felipesousa.almeida@ucsal.edu.br

[2] Graduação em Direito pela Universidade Católica do Salvador (UCSAL), pós-graduado em Direito Processual Civil pelo Juspodivm e Mestre em Estudos Interdisciplinares sobre a Universidade - PPGEISU/ IHAC/ UFBA. Professor e Orientador da Universidade Católica do Salvador. E-mail: carlos.coutinho@pro.ucsal.br

1 INTRODUÇÃO

Com o avanço da tecnologia da informação, a Internet tornou-se um fenômeno na vida da humanidade. É uma rede internacional de computadores interconectados, que apresenta facilidade para que todos possam se comunicar ou realizar transações comerciais a qualquer hora e em qualquer lugar.

"A internet é mais que um simples meio de comunicação eletrônica, formada não apenas por uma rede mundial de computadores, mas por uma rede mundial de Indivíduos. Indivíduos com letra maiúscula, porque estão inseridos em um conceito mais amplo, que abrange uma individualização não só de pessoas físicas, como também de empresas, instituições e governo." (PINHEIRO, 2010, p.44).

Tem sido desenvolvida muitas maneiras de interação no ciberespaço. Um exemplo é o nascimento da tecnologia de aplicação sem fio que permite que os telefones celulares acessem a Internet, paguem uma conta bancária, reservem passagens aéreas, entre outros. Por outro lado, o avanço da internet e do mundo digital não levou somente a um progresso positivo. Uma das coisas negativas que muitas vezes acontece no mundo virtual é o crime cibernético.

A perda dos limites do espaço e do tempo na Internet pode contribuir para propagação dos crimes. Com a sua expansão multiplicou-se as chances de ações de comportamento antissocial e criminoso que foram consideradas improváveis. A maioria das ameaças cibernéticas são indiscriminadas. Eles não se importam se seu alvo for um médico ou um transportador de petróleo, enquanto esse indivíduo tiver dinheiro e tiver dispositivos conectados à Internet, este pode tornar-se um alvo.

Este artigo foi desenvolvido com o proposto de identificar os principais antagonismos que os órgãos da persecução penal lidam no enfrentamento do crime cibernético na perspectiva da doutrina penalista e da Tecnologia da Informação e Comunicação. Trata-se de esclarecer através de uma pesquisa de revisão bibliográfica, constituído de livros, artigos em sítios na internet. Utilizando o método dedutivo tendo por referências autores que discorreram sobre a relação do Direito Penal com os crimes em ambientes virtuais, embora perceba-se uma escassez na literatura jurídica a nível de suporte nacional que aprofunde o tema.

A cibercriminalidade apresenta novos desafios para a aplicação da lei. Devido à sua natureza transnacional, uma resposta real e sólida a tal ameaça exige uma cooperação internacional envolvendo a participação de todas as partes envolvidas na comunidade internacional. No entanto, a vulnerabilidade surge da crescente dependência da tecnologia, da

falta de medidas legais e da falta de cooperação a nível nacional e internacional, representando obstáculo real para a resposta efetiva a essas ameaças.

Um hacker pode entrar em um sistema sem uma autorização oficial. Alguns deles ao se infiltrarem no sistema notificam seus pontos fracos e encaminham essas falhas para o administrador do servidor, mas alguns deles usam essa vulnerabilidade descoberta para lucrar. Normalmente, o perpetrador sabota ou rouba a informação valiosa e confidencial. No entanto, alguns estão fazendo apenas porque eles se sentiram desafiados a tentar suas habilidades para penetrar em um sistema que possui alto grau de proteção.

A ordem jurídica tem a obrigação de responder com a máxima urgência aos novos desafios tecnológicos, impedindo que os Estados e suas respectivas legislações, permaneçam vulneráveis quanto a segurança da informação, privacidade dos cidadãos, além do sigilo e proteção dos dados. O ramo do direito na área da segurança digital tem como obrigação acompanhar as mudanças tecnológicas na ânsia de responder aos novos desafios, sendo objeto de estudo fundamental e relevante a compreensão dos problemas apresentados pela nova sociedade da informação que se expande a uma velocidade assustadora.

Esta é uma pesquisa pura, pois através desta procura-se atualizar conhecimento mais do que produzir resultados concretos e tem como propósito contribuir para um conhecimento existente. Ainda que o conhecimento que esta pesquisa produza possa posteriormente ser utilizado como base para a criação de alguma solução ou mitigação dos riscos e danos causados pelo crime cibernético.

No aspecto metodológico, buscou-se guiar a pesquisa de forma qualitativa, utilizando o método dedutivo, focando-se na temática, em primeiro lugar, com uma análise geral do assunto e em seguida realizar sua delimitação correspondente com a análise dos aspectos da persecução penal e os desafios encontrados na aplicabilidade de leis contra os crimes cibernéticos. Ainda com base em caráter transdisciplinar, conditas entre searas distintas do direito penal cibernético, direito internacional, direito processual penal, direito constitucional, direitos e princípios fundamentais, direito digital e segurança da informação, buscando verificar a aplicabilidade do direito à tecnologia e segurança da informação para sua efetivação

2 CRIMES CIBERNÉTICOS

2.1 CONCEITOS

Um ambiente digital seguro é um assunto de grande importância na realidade atual da sociedade da informação e da nova economia que marca o curso da cultura e do progresso do mundo de hoje. O tráfego diário na Internet aumenta consideravelmente, milhares de usuários acessam vários sites para consumir algum produto ou serviço dos muitos que as empresas digitais oferecem atualmente, porém, o ecossistema digital é altamente vulnerável a ataques de criminosos digitais que colocam em risco a segurança dos usuários, que podem ser danificados em sua propriedade ou em sua pessoa. Portanto, é vital para cada nação ter um sistema jurídico atualizado, capaz de proteger efetivamente os usuários contra qualquer comportamento criminoso típico deste ambiente tecnológico. Nessa mesma esteira, Guilherme de Souza Nucci (2010, p. 34) esclarece que:

> Estamos em um momento de transição em que as relações humanas se tornam cada vez mais interativas através dos dispositivos moveis de comunicação, porém, estamos nos tornando cada vez mais vulneráveis aos ataques a nossa esfera de privacidade. (NUCCI, 2010, p. 34)

Para a ciência jurídica, o crime é um objeto de estudo de extrema importância no seu objetivo de gerar conhecimento para sua aplicação em prol do bem-estar social. A segurança de cada pessoa (pessoa no sentido amplo dos direitos humanos e também das empresas que possuem reconhecimento jurídico sujeitas a direitos e obrigações) é fundamental para preservar a paz e a ordem que favoreçam o desenvolvimento da humanidade.

Em primeiro lugar, deve-se fazer uma separação entre as condutas ilícitas realizadas no espaço físico e as do mundo virtual, ou seja, as condutas típicas, sejam ações ou omissões, que tenham consequências jurídico-penais sob a teoria clássica dos crimes, são percebidos pelos nossos sentidos de forma imediata e natural, pelo contrário, os comportamentos ilegais perpetrados no ambiente virtual são aqueles que exclusivamente os nossos sentidos podem perceber através da utilização de um dispositivo eletrônico e cuja plataforma de comunicação é essencialmente a Internet.

Nesse sentido, Gabriel Cesar Zaccaria Inellas esclarece que:

> A internet é uma rede de computadores, integrada por outras redes menores, comunicando entre si, os computadores se comunicam através de um endereço lógico, chamado de endereço IP, onde uma gama de informações são trocadas, surgindo ai o problema, existe uma quantidade enorme de informações pessoais disponíveis na rede, ficando a disposição de milhares de pessoas que possuem acesso à internet, e quando não disponíveis pelo próprio usuário, são procuradas por outros usuários que

> buscam na rede o cometimento de crimes, os denominados Crimes Virtuais. (INELLAS, 2004, p.3)

No espaço dos crimes, há os crimes cibernéticos cuja manifestação é realizada no ambiente virtual. Normalmente o nome deste tipo de crimes vem acompanhado do prefixo “cibernético” e “virtual”. De forma que se pode definir os crimes cibernéticos como aquelas condutas criminosas, que são perpetradas através do uso das diversas Tecnologias da Informação e Comunicação como computadores, celulares e da Internet, consideradas prejudiciais, que violam os demais usuários dentro do ciberespaço. Neste ponto, cumpre frisar as lições do autor Augusto Rossini:

> O conceito de delito informático poderia ser descrito como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade. (ROSSINI, 2004, p.110).

Como ressalta Marco Aurélio Rodrigues da Costa, a maioria da doutrina define o crime de informática pelo bem jurídico protegido, conferindo uma definição incompleta. Então, segundo ele o crime digital é “todo aquele procedimento que atenta contra dados, que faz na forma em que estejam armazenados, compilados, transmitidos ou em transmissão”. Em busca de uma definição para os crimes virtuais, Joao Marcelo de Araújo Júnior destaca como "uma conduta lesiva, dolosa, a qual não precisa, necessariamente, corresponder a obtenção de uma vantagem ilícita, porém praticada, sempre, com a utilização de dispositivos habitualmente empregados nas atividades de informática". Na visão de Ivette Senise Ferreira, crime de informática é "toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão".

O crime cibernético é uma realidade indesejável em todos os países do mundo onde a tecnologia está presente, em maior ou menor grau. Segundo Guimarães e Furlaneto Neto, crime Informático é "qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados". A principal diferença entre a delinquência tradicional e o crime digital reside na natureza do computador, estrutura de rede e alcance global. Espera-se que o crime cibernético continue aumentando devido ao aumento maciço de celulares, carros elétricos, eletrodomésticos e sistemas industriais.

2.2 AS PARTES ENVOLVIDAS

Se entende como vítima do crime cibernético qualquer usuário no ciberespaço que sofre um ataque criminoso. portanto, se as medidas básicas de segurança não forem adotadas pelo usuário, este estará em um risco latente. Deve-se ressaltar que ser apenas um usuário conectado na Internet já pode ser considerado uma vítima em potencial, e só adquire essa categoria quando o dano for perpetrado. Para Patrícia Peck Pinheiro, "o maior estimulo aos crimes virtuais é dado pela crença de que o meio digital é um ambiente marginal, um submundo em que a ilegalidade impera" (2013, p.311).

A categoria de delinquentes cibernéticos é composta por aqueles indivíduos que, utilizando dispositivos digitais como instrumento, cometem uma infração classificada como crime. Túlio Lima Vianna enquadrou os cibercriminosos em cinco classes:

> 1 – CRACKERS DE SISTEMAS – piratas que invadem computadores ligados em rede. 2- CRACKERS DE PROGRAMAS – piratas que quebram proteções de software cedidos a título de demonstração para usá-los por tempo indeterminado, como se fossem cópias legítimas. 3- PHREAKERS – piratas especialistas em telefonia móvel ou fixa. 4- DESENVOLVEDORES DE VÍRUS, WORMS e TROJANS – programadores que criam pequenos softwares que causam algum dano ao usuário. 5- PIRATAS DE PROGRAMAS– indivíduos que clonam programas, fraudando direitos autorais. 6- DISTRIBUIDORES DE WAREZ – webmasters que disponibilizam em suas páginas softwares sem autorização dos detentores dos direitos autorais. (VIANNA, 2001, Pg. 62,).

Os benefícios oferecidos pela Internet, como a interação automatizada e a interconexão global podem ser uma faca de dois gumes na segurança cibernética, dificultando a tarefa de persecução penal das agências governamentais. Além disso, a capacidade dos cibercriminosos pode ultrapassar o nível de conhecimento e experiência das autoridades, de modo que a prevenção e a educação em segurança eletrônica para usuários da Internet é a melhor arma. Para Martins (2011) "os criminosos cibernéticos são invasores de sistemas que atuam por espíritos de emulação, desafiando seus próprios conhecimentos técnicos e a segurança de sistemas informatizados de grandes e organizações governamentais".

Pode-se nomear como partes de acordo com Reis (2015) que fez uma classificação dos atores que intervêm nos vários crimes cibernéticos como usuário final de Internet; *spammers*; *defacers*; hackers (*white hats*) que descobrem brechas dos sistemas e consertam essa falha em

prol da segurança digital; crackers (*black hats*) que usam seu conhecimento técnico com intenções maliciosas em prol do crime virtual; terroristas; empresas que fornecem segurança cibernética e software de segurança, como programas antivirus.

Os hackers chapeis brancos são indivíduos éticos que trabalham em empresas de tecnologias e desenvolvem ferramentas em prol da segurança digital. Quando descobrem uma vulnerabilidade em um servidor, geralmente contatam o administrador desse sistema e expõem a falha encontrada para que este conserte essa brecha.

Os hackers chapeis pretos, também conhecidos como crackers e *black hats*, encontram e exploram brechas na segurança de servidores de agencias importantes e as vendem dentro do mercado negro para empresas ou grupos de hackers que estejam interessados em obter esta falha para ter acesso à alguma informação valiosa ou danificar seu sistema.

Conceitua o doutrinador Morimoto (2005) o que é um hacker e, em seguida, exemplifica a diferença entre hacker e cracker:

> Alguém que estuda sistemas ou qualquer tipo de conhecimento humano pelo simples desafio de dominá-los. No sentido original da palavra, o Hacker é alguém que usa seus conhecimentos para ajudar outros, direta ou indiretamente. Hackers foram os principais responsáveis pelo desenvolvimento da internet, criaram o Linux, o MP3 e a filosofia do software livre. Atualmente o termo vem sendo muito usado em relação aos Crackers que invadem sistemas e promovem outras modalidades de baderna virtual, criancices como desconfigurar páginas ou ficar invadido PCs de usuários leigos. Hackers usam sua inteligência de maneira positiva, constroem coisas, crackers só destroem.

Pode-se pensar que se trata de profissionais com conhecimentos aprofundados em telecomunicações ou software, mas nem sempre é esse o caso, afinal assim como a Internet tendeu a democratizar o acesso à informação, também tende a democratizar algumas atividades criminosas, tornando mais fáceis para mesmo os que não são especialistas em computação usarem a Internet para o crime, como fraude. Ademais, a desterritorialização que a Internet permite, favorece os criminosos experientes a atuarem de maneiras mais sofisticadas que tornam sua captura e verificação do crime mais complexas.

São as infrações favorecidas pela informática ou, como denominam outros autores, crimes informáticos impróprios (CHAGAS, 2012). Estes procedimentos podem ser feitos por pessoas comuns, sem exigência de alto conhecimento informático (CHAGAS, 2012)

Estão envolvidas também as agências governamentais especializadas no combate aos crimes cibernéticos que compõem a estrutura do Estado como FBI e NSA nos EUA; a Europol na Europa e; o Ministério Público Federal, o Departamento da Policia Federal e Delegacias

especializadas em crimes digitais no Brasil. Essas entidades possuem algumas funções que são a proteção dos usuários da Internet em seus trabalhos de prevenção da criminalidade, a reparação dos danos causados as vítimas e a persecução aos perpetradores.

2.3 O CRIME CIBERNÉTICO DENTRO DA INTERNET

Atualmente, vive-se momentos em que governos e corporações estão espionando usuários de internet e alguns países estão proibindo ou ameaçando enfraquecer as tecnologias de privacidade, tais como redes virtuais privadas (VPNs) e criptografias, e exigindo mais vigilância e retenção de dados. Os recursos de anonimato são projetados para serem resistentes aos ataques de hackers e adversários estatais, como a Agência de Segurança Nacional (NSA) e a Agência Central de Inteligência (CIA).

Fowler, Denis afirma que VPN usa a infraestrutura de uma rede pública para fazer as conexões entre *nodes* geograficamente dispersos, em vez de usar os próprios cabos exclusivamente para o uso de uma única rede. Porque uma VPN representa uma conexão temporária estabelecida em uma rede pública para proteger o ponto de onde partiu a conexão de origem.

Estratégias de roteamento garantem um bom nível de anonimato do usuário com este tipo de sistema. Além da rede aberta que já é amplamente conhecida, existe o que se convencionou denominar de rede obscura (Darknet), que através de alguns programas e protocolos é possível ter acesso a essas redes privadas, mantendo a identidade anônima do usuário para não revelar o endereço IP de onde parte a conexão, além de manter o sigilo das comunicações entre as partes. As principais delas se destacam a I2P, a FREENET e a Rede ONION conhecida por TOR (*The Onion Router*).

De acordo com um estudo realizado pela Universidade de *Portsmouth* em 2014, 80% do tráfego *darknet* foi gerado por uma visita a sites que oferecem materiais de abuso infantil. A *deep web* tem um forte anonimato para seus usuários, e muitos bens e serviços perigosos são comercializados lá sob seu refúgio. O crime de abuso infantil tem sido, sem dúvida, o crime mais perigoso cometido no *darknet*, que também tende a gerar tráfego para a maioria dos *sites*.

O navegador TOR garante o anonimato e é necessário para acessar a *darknet*, disponível para navegar pela rede *onion*. Este é um programa que deve estar instalado no computador para que possa ser utilizado, sendo então possível acessar as informações privadas que nele se tratam. De acordo com as notas deste software, qualquer pessoa pode ser usuário. Um uso nobre de tal

software, é a possibilidade de comunicação em países onde há um controle da Internet e das informações que circulam, ou seja, um método para contornar a censura estatal usado por muitos jornalistas e ativistas, especialmente nos casos em que o governo é considerado como um repressor. No entanto, a escuridão que oferece, também se torna um espaço de oportunidade para se envolver em comportamentos criminosos, como a transferência de pornografia infantil, ou comunicações para fins terroristas e motivos financeiros envolvendo criptomoedas ou de espionagem.

Segundo dados da Verizon (2019), 70% das violações, deve-se a motivos financeiros ou de espionagem. Um terço (32%) das violações envolveu *phishing*. Mais da metade (56%) das violações de dados levaram meses ou mais para serem descobertas. O *ransomware* continua sendo uma grande ameaça e é o segundo tipo mais comum de malware relatado.

Diane Barret, Kalani K. Hausman e Martin Weiss (2015) afirmam que os crimes eletrônicos mais comuns que ambos, empresas e indivíduos, podem sofrer são: *spam* que é o envio de e-mails indesejados; roubo de propriedade intelectual, *download* ilegal de direitos autorais como músicas ou filmes; *ransomware*, uma forma particular de *malware* que serve para extorção digital, desabilitando um computador ou uma conta de e-mail até que o resgate seja pago por sua remoção; vandalismo (*deface*), no qual trata-se de desfazer a estrutura de um site; *phishing*, onde ocorre o envio de e-mails ou outras mensagens eletrônicas para adquirir informações confidenciais, enganando uma pessoa para que esta envie dinheiro; ataques de negação de serviço distribuído, também conhecido como DDoS, é um tipo de ataque que deixa indisponível a rede de um sistema por um tempo indeterminado, através de diversos outros pontos de conexão de outras redes no ciberespaço que realizam o ataque de forma simultânea; ataques de *malwares* que consiste em instalar um vírus ou outro código malicioso em computadores ou dispositivos com acesso à Internet, prejudicando o sistema operacional da vítima; violação de dados, representando a perda ou roubo de computadores ou dispositivos armazenamento eletrônico; roubo de identidade, em que ocorre através de um sistema de computador ou e-mail, os criminosos obtêm dados pessoais, fazendo uso de uma identidade para acesso fraudulento a dados de cartão de crédito, conta bancária ou mesmo danos morais a uma pessoa; o uso indevido das mídias sociais de maneiras que podem prejudicar os usuários, o mesmo que se traduz em eventos como a perseguição cibernética ou o roubo de identidade; ameaças internas, como um funcionário insatisfeito ou outras informações privilegiadas destinadas a minar os protocolos de segurança da agencia; guerra cibernética é o ataque coordenado e simultâneo que afeta diversas redes, servidores e sites de Internet ao redor do

globo; espionagem cibernética, importa na espionagem feitas pelas agências de vigilância do governo (Agência de Segurança Nacional) ou empresas à informação que circula na rede, incluindo o correio eletrônico ou as informações de um servidor.

Alguns dos ataques bem sucedidos às empresas em 2019, de acordo com o Grupo Cyberedge são através de *malwares*, ou seja, virus, backdoor, cavalo de troia ransomware. Ataques de *phishing*, engenharia social, ataques de negação de serviço como DDoS, DoS, *booters* e *stressers*. Em seguida, ataques de aplicativos da Web, por exemplo, transbordamento de dados, injeções de SQL e *cross-site scripting*. E muitos deles também são cometidos por *downloads* de arquivos executáveis maliciosos através de *pop-ups*, javascript e *flash player* nos *sites*.

3 CRIMES CIBERNÉTICOS NO BRASIL

3.1 PANORAMA SOBRE A CRIMINALIDADE ONLINE BRASILEIRA

Retratar o Brasil no período de uma década, faria com que a maioria das pessoas elaborasse uma imagem mental associada de festividades coloridas em uma cidade onde o Cristo Redentor estende seus braços sobre as favelas e praias densamente povoadas, como também ver que é o segundo maior gerador de crimes cibernéticos do mundo, sendo o número 1 na América Latina como fonte e alvo de ataques online.

Os padrões de *malware* e fraude on-line no Brasil são desenvolvidos e usados por criminosos e gangues locais que se especializam em direcionar seus sistemas de pagamentos e serviços. De acordo com o Comitê Gestor da Internet no Brasil, com cerca de 54% dos 209 milhões de cidadãos do país que já utilizam a Internet, o cibercrime é um empreendimento lucrativo para pequenos criadores e novos mafiosos que diversificam seu portfólio.

Uma indicação para as taxas de sucesso dos crimes cibernéticos vem da Febraban, a Federação Brasileira de Bancos, que afirma que as fraudes bancárias eletrônicas causam 95% das perdas para os bancos brasileiros. O facilitador deste crime é o único mercado negro subterrâneo brasileiro, que é similar ao russo em tamanho e atividade. Lima (2005, p.60) definiu fraude virtual como invasão de sistemas computadorizados e posterior modificação de dados, com o intuito da obtenção de vantagem sobre bens, físicos ou não, por exemplo, a adulteração de depósitos bancários, aprovações em universidades, resultados de balanços financeiros, pesquisas eleitorais, entre outros.

Os brasileiros entraram no mundo do crime on-line pouco depois de seus análogos de língua russa e inglesa já terem fundado um vívido mercado negro para serviços e mercadorias. Isso reduziu as barreiras de entrada e aprimorou a curva de aprendizado para os cibercriminosos locais que usam o conhecimento para atacar bancos e serviços de pagamentos online locais. Quase todo o malware usado no Brasil é feito para ataques locais.

Os fatores que ajudam os hackers brasileiros a serem tão bem-sucedidos enquanto usam técnicas básicas do crime de informática são: vítimas leigas e desinformadas, necessidades especiais de segurança e fator de repressão fraca. Uma população online muito grande que recentemente começou a usar a Internet com níveis baixos ou inexistentes de consciência de segurança agregado ao fator do país ter leis de crimes digitais fracas e não condizentes com a realidade atual dos crimes digitais, no qual o criminoso tem acesso a infinitos mecanismos e artimanhas para dificultar a sua autoria do crime e, também, se assim quiserem podem dificultar a perícia dando fim no disco rígido ou o criptografando-o.

Em uma diferença bastante gritante do que se veria no típico submundo de língua inglesa ou russa, onde o sigilo e o anonimato são de suma importância, os criminosos cibernéticos no Brasil vivem abertamente, comunicando-se onde podem ser rastreados pelas autoridades policiais usando até sua localização exata, sem estarem preocupados em esconderem sua verdadeira identidade, devido à falta de dissuasão legal.

De muitas maneiras, o cibercrime no Brasil é tratado como grupos de redes sociais públicas, no qual, por muito tempo, os infratores usavam extensivamente o Orkut (um site de redes sociais operado pela Google) e os serviços do *Internet Relay Chat* (IRC) que serviram principalmente de mercado para troca de dinheiro e bens e serviços criminais e atualmente operam pelo Facebook, Whatsapp, Discord e VK (uma rede social de origem russa), em que um grande esquema de pirataria foi montado.

É importante notar que, embora esteja lidando com grandes volumes de cibercrime de pequeno porte, o Brasil ainda pode estar no meio de um período de carência. Enquanto os criminosos locais defraudam os pagamentos de boleto, um de cada vez, o cibercrime organizado da Europa Oriental pode facilmente mudar seu foco para o Real Brasileiro, ou se aliar com hackers brasileiros por meio das redes sociais e forums na internet usando o Google tradutor e o Yandex tradutor para planejar ataques contra instituições bancárias, o governo e armazenar números de cartões de crédito dos cidadãos brasileiros para uso futuro ou vendê-los para fraudadores na *deepweb*.

A arena do cibercrime brasileiro é líder em fraude na internet. O Brasil tem o segundo maior número de fraudes bancárias online e malware financeiro tendo como alvo qualquer país do mundo, não voltando-se somente ao sistema bancário brasileiro, mas expande-se até em fraude e roubo de criptomoedas. O seu submundo do crime cibernético continua a crescer devido a uma combinação do crescente número de infratores, bem como a uma pobre legislação criminal e ineficácia da aplicabilidade da lei perante a esses casos. Isto é provavelmente devido a uma série de fatores que incluem orçamentos limitados dedicados a combater o crime cibernético, falta de consciência de segurança digital e conscientização entre os setores público e privado e uma população de usuários geralmente desinformada.

A boa notícia é que combater os criminosos que nem sequer se escondem através do anonimato vai tornar a vida mais fácil para a aplicação da lei. Mas serão necessárias novas leis para levar os suspeitos à justiça e implicações mais sérias para os criminosos se afastarem do cibercrime. Dito isso, diminuirá drasticamente dos volumes os crimes, desligando os autores que não possuem conhecimentos técnicos profundos.

3.2 CENÁRIO DO SUBMUNDO DOS CRIMES CIBERNÉTICOS DO BRASIL

De acordo com o estudo *Ascending the Ranks: The Brazilian Cybercriminal Underground in* 2015, da Equipe de Pesquisa de Ameaças Futuras da *Trend Micro*, o submundo do cibercrime brasileiro continua amadurecendo, apesar do desenvolvimento de ferramentas ou táticas exclusivas ou sofisticadas. As evidências sugerem que o Brasil é o um dos cinco países de maior gerador de crimes cibernéticos do mundo, sendo o primeiro lugar na América Latina. Talvez o que torna este submundo mais distinto do que outros, seja como os cibercriminosos brasileiros aproveitam as oportunidades apresentadas por redes sociais como Facebook, YouTube, Twitter, Instagram e Skype.

Roubos de dados pessoais e fraudes de cartão de crédito são as principais violações virtuais praticadas pelo submundo brasileiro. Cavalos de troia bancários (*Trojan Banking*) são as principais ameaças, ao lado de *phishings*, neste cenário, cujas suas técnicas baseadas no cavalo de troia são populares e são usadas para roubar credenciais de usuários, incluindo envenenamento de DNS, janelas de navegador falsas, extensões maliciosas de navegador e *proxies* maliciosos.

Os cibercriminosos brasileiros usam há muito tempo fraudes de *phishing*, enviando aos usuários falsas páginas de bancos para roubar suas credenciais bancárias *on-line*. Em muitos

kits modernos de *phishing*, o código que gera a página falsa puxa muito do conteúdo HTML do site do banco genuíno. Esta ação pode ser detectada por soluções de segurança que, muitas vezes, ajudam os pesquisadores a encontrar novas páginas *fakes* e adicioná-las ao banco de dados para enviar vítimas a páginas de *phishing* quando tentam navegar para o seu banco ou site do provedor de cartão de crédito.

Quando se têm êxito no roubo de dados de pessoas, colocam à venda dados pessoais dos cidadãos brasileiros como número de celular e telefone residencial, endereço completo, nome completo, CPF, número da identidade em sites específicos. Apesar da tentativa de banimento do site pelo Ministério Público Federal, atualmente continua ativo um dos dois sites que divulgam dados pessoais de brasileiros, tanto de forma gratuita quanto paga, que é o www.tudosobretodos.se, no qual seu domínio está na Suécia e não no Brasil. Outro site que entrou no ar, mas foi bloqueado logo em seguida que tinha essa mesma finalidade era o www.telefone.ninja. Acredita-se que o site foi fechado rapidamente porque o servidor encontrava-se hospedado aqui mesmo no país. Porém, atualmente, o www.fenixconsultas.com.br continua ativo e realizando buscas.

Outro jeito de buscar dados pessoais brasileiros de forma legal e obter o endereço, CEP, CPF ou RG é através da pesquisa pelo nome do indivíduo no site www.telelistas.net e averiguar se consta às informações. O outro procedimento é através do CADSUS WEB, no qual busca-se os dados pessoais de determinada pessoa no site de Cadastro Nacional de Usuários do Sistema Único de Saúde. A busca também pode ser realizada no site do Serasa, mas os que detém conhecimentos avançados no assunto, conhecem sites com acesso restrito, ou pouco divulgados, que são criados no submundo da internet.

Doxxing é o nome técnico no meio informático no qual os crackers fazem uso desta prática virtual para pesquisar, descobrir a real identidade e coletar dados privados de indivíduos alvo, expondo as suas verdadeiras informações na rede. Também conhecida na comunidade digital como "*exposed*", geralmente são atreladas em desmascarar, intimidar ou ameaçar algum concorrente rival ou vítimas de *cyberbullying* e *cyberstalking*. Recentemente, a exposição de dados vem sendo amplamente requisitada no Youtube, onde alguns canais populares até pagam quantias absurdas em dinheiro para que algum hacker exponha todos os dados, inclusive nome completo dos pais, de algum canal anônimo ou pessoa que não esteja na condição de figura pública que esteja na mira da cultura do cancelamento.

Ademais, os perpetradores fazem uso das redes sociais utilizando a ingenuidade e a falta de conhecimento da maioria de seus usuários, tendo como enfoque a obtenção de dados

sensíveis, esta prática é denominada engenharia social. De acordo com Soeli Claudete Klein (Klein, 2004, p. 9), que define tal conceito:

> A engenharia social atua sobre a inclinação natural das pessoas de confiar umas nas outras e de querer ajudar. Nem sempre, a intenção precisa ser de ajuda ou de confiança. Pelo contrário, pode ser por senso de curiosidade, desafio, vingança, insatisfação, diversão, descuido, destruição, entre outros. A engenharia social também deve agir sobre as pessoas que não utilizam diretamente os recursos computacionais de uma corporação. São indivíduos que têm acesso físico a alguns departamentos da empresa por prestarem serviços temporários, porque fazem suporte e manutenção ou, simplesmente, por serem visitantes. Há ainda um grupo de pessoas ao qual é necessário dispensar uma atenção especial, porque não entra em contato físico com a empresa, mas por meio de telefone, fax ou correio eletrônico. (KLEIN, 2004, p. 9)

A continuação da profissionalização do mercado de cibercriminosos revela que, mesmo dentro do vasto subsolo global, os mercados regionais se diferenciam uns dos outros pelos tipos de bens e serviços que estão vendendo. À medida que as reputações se solidificam na Deep Web, criminosos mais experientes podem começar a patrocinar os mercados que sabem vender os tipos específicos de *malware*, ferramentas e serviços que eles estão buscando especificamente, formando uma imensa rede obscura de *botnets* com hierarquias. Consoante Emerson Wendt e Higor Vinicius Nogueira Jorge (2013) cada *botnet* pode lançar ataques de negação de serviço altamente prejudiciais em larga escala, sendo empregadas para fins de ciberterrorismo e guerra cibernética.

4 A BATALHA JURÍDICA CONTRA O CRIME VIRTUAL

Dados fornecidos pela *IBM Security X-Force Threat Intelligence Index*, o custo médio da violação de dados no mundo em 2019 foi de 3,86 milhões de dólares. Em um mundo em que mais de 40% da população mundial está usando atualmente a internet, de acordo com dados da União Internacional de Telecomunicações, os ataques cibernéticos representam uma ameaça para o progresso e à estabilidade mundial. Tamanha é a gravidade do crime cibernético que se estima que "crimes contra dados (os dados que fluem através da Internet) afetarão um quarto da população mundial no ano de 2020", portanto, é fundamental ter legislação e políticas públicas eficazes para prevenir, impedir, investigar, processar e julgar o comportamento criminoso no uso das tecnologias da informação, especialmente a Internet, bem como o fortalecimento de cooperação entre os setores público e privado.

O combate a esses comportamentos é prioritário, pois existe duas ferramentas: as normas legais e os sistemas de segurança tecnológica. No ciberespaço, se as autoridades tentassem seguir a mesma linha de "defesa", os esforços desenvolvidos seriam então inúteis, em uma plataforma virtual, que, é um paraíso para os cibercriminosos pela facilidade com que um crime pode ser cometido.

A implementação de mecanismos de defesa reduziria muito os ataques cibernéticos bem-sucedidos, no entanto, os invasores desenvolvem continuamente softwares mais poderosos que não podem ser identificados pelos sistemas de segurança ou mesmo quebram os códigos de segurança existentes, diminuindo assim a possibilidade de prevenção dos crimes virtuais, e torna necessária a aparência de fiscalização para punir as ações criminosas perpetradas.

Um dos primeiros documentos sobre o assunto, que é significativo para se tentar regular uma categoria tão sensível quanto as questões criminais no ambiente eletrônico, é a Declaração Multissetorial do NETmundial que foi o resultado da conferência NetMundial, como um conjunto de discussões e propostas globais que apresentam um esquema das regulamentações necessários para a evolução rumo a uma governança no ecossistema da Internet, que não tem força vinculante. Como um dos pilares em que se baseou a discussão das questões no NetMundial, foram os princípios de governança da Internet em que foi acordado que os direitos protegidos no ambiente físico também devem ser protegidos no ambiente digital.

Os acordos e convenções internacionais incentivam a harmonização das leis e regulamentos cibernéticos e procuram criar cooperação entre as nações para responder ao cibercrime. O Conselho da Convenção da Europa sobre Cibercriminalidade é um referencial normativo de caráter internacional, que obriga os países que possuem tratados a cooperar uns com os outros para combater o cibercrime. Este tratado tem por finalidade: "prevenir ações direcionadas contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, redes e dados informáticos, bem como o uso indevido de tais sistemas, redes e dados facilitando a sua detecção, investigação e repressão a nível nacional e internacional e fornecer acordos que permitam uma cooperação internacional rápida e confiável"

A partir de 2001, as Nações Unidas (ONU) adotaram resoluções que encorajam os Estados membros a tomarem medidas adequadas contra o cibercrime. Solicitou aos seus membros que tomem nota da Convenção sobre Cibercriminalidade (Convenção de Budapeste) redigida pelo Conselho da Europa.

A Convenção de Budapeste é a primeira e única convenção internacional para encorajar a harmonização das leis e regulamentos cibernéticos e para construir a cooperação entre as

nações no controle do cibercrime. Está aberto aos Estados membros do Conselho da Europa e a Estados não membros. Atualmente é a convenção mais aceita sobre cibercrime, com 51 estados ratificados aderidos em dezembro de 2016. Os principais membros incluem países europeus e os Estados Unidos.

No entanto, o Brasil, a China e a Rússia, não são signatários da Convenção de Budapeste, porque não estavam envolvidos na elaboração, deixando-os atrasados no desenvolvimento das leis contra os crimes cibernéticos para os padrões necessários. Todavia, como a presente Convenção se baseia nos tipos de cibercrimes originados no final da década de 1990, uma série de novos métodos de ataque não são explicitamente cobertos pela Convenção.

5 DESAFIOS À APLICABILIDADE DE LEIS CONTRA OS CRIMES CIBERNÉTICOS

Além da questão de anonimato discutida anteriormente, outro aspecto a ser abordado é a questão da competência dos tribunais que procuram exercer seu poder e proteger os usuários, ou seja, um outro grande desafio à aplicação das leis de crimes cibernéticos é a jurisdição. Levando em conhecimento os princípios de independência do Estado, soberania e integridade territorial, cada estado-nação do mundo, têm autoridade para tornar as leis vinculativas para as coisas e para todas as pessoas dentro da sua entidade geográfica, chamada de país.

Pela razão acima mencionada de estados-nação que fazem leis sobre o mesmo assunto de diferentes jurisdições, o conflito de leis é inevitável. A jurisdição pode ser definida como o poder de um tribunal ou juiz para tratar de uma ação, petição ou processo. Dada a natureza peculiar do crime virtual, os crimes cibernéticos transcendem estados e jurisdições. São crimes transfronteiriços e, assim, um cibercriminoso pode sentar-se no conforto de sua casa, escritório, cibercafé ou onde ele escolher, com um laptop ou celular conectado à Internet e realizar suas atividades ilegais que seriam sentidas a milhares de quilômetros de distância, de onde ocorreu o ato.

A questão da jurisdição na Internet não é uma questão simples precisamente por causa de sua natureza global, descentralizada e anônima, no entanto, alguns autores, como o caso de Fabrício Bertini Pasquot Polido e Lucas Costa dos Anjos (2018) simplesmente apontaram que a transmissão de protocolos da Internet TCP/IP foram projetados para ser geograficamente independente, mas existem tecnologias sofisticadas e ferramentas eletrônicas dentro dos limites físicos e também em decorrência de obrigações estabelecidas pela lei do foro (*lex fori*) legais

locais, é possível determinar a localização de um computador ou servidor, e, muitas vezes, até do próprio responsável pela conexão com a internet. Esses pontos fornecem a justificativa e a capacidade de os Estados soberanos fazerem valer sua autoridade.

De modo que os Protocolos de Internet (IP) são as ferramentas que servem às autoridades para determinar com precisão se são competentes para investigar e, quando apropriado, punir as questões trazidas em consideração, sem infringir a soberania de outra nação ou mesmo a jurisdição de um Estado em um determinado país. Assim, mesmo na Internet, que carece de limites geográficos, a questão da jurisdição é tratada de forma tradicional, ou seja, a delimitação de endereços IP, reduz o tratamento dado à Internet para confiná-la para fins jurisdicionais a ter um limite geográfico.

A legislação brasileira somente prevê a quebra do sigilo de dados mediante autorização judicial, ou seja, a autoridade policial ou judiciária poderá requerer, a qualquer provedor de aplicações de internet, acesso aos registros de conexão, no qual somente assim poderá saber a localização do cliente contratante do provedor de internet, que concedeu a ele a utilização daquele determinado endereço IP.

Os metadados a serem guardados são geralmente relacionados a serviços de telefonia, números de telefones, duração da chamada e sobre serviços de Internet, os endereços eletrônicos (e-mail) do remetente e do destinatário e os endereços IP. Qualquer outra forma de obter esses dados poderá acarretar a ilegalidade da prova, e as informações restarão inidôneas.

A maior barreira enfrentada pelas autoridades estatais é a proteção trazida pela criptografia presente em aplicativos de comunicação, como WhatsApp e Telegram, e principalmente na Deep Web, fazendo-se necessária uma auditoria minuciosa em busca de identificar logs, cookies, fingerprints, número de série da placa de rede do dispositivo eletrônico (endereço MAC) deixados no local do crime e monitorar atividades e problemas dentro do sistema. Nesse sentindo, lecionam Fernandes e Caldi (2017):

> O problema se agrava com a criação e distribuição gratuita de programas como o TOR (The Onion Router), que possibilita a participação das pessoas em uma ‘rede paralela’ conhecida como ‘Deep Web’. Além disso, o desenvolvimento das tecnologias 3G e 4G para smartphones, que estão se tornando o principal meio de comunicação, possibilita mobilidade tanto ao acesso quanto à distribuição de material ilícito. Acrescente-se a essa realidade o fato de a computação em nuvem possibilitar verdadeiros ‘paraísos de armazenamento e compartilhamento. (FERNANDES e CALDI, 2017, p.105)

Para resumir o desafio jurisdicional para a aplicação das leis de crimes cibernéticos, significa que se o obstáculo do anonimato é escalado e um cibercriminoso é claramente

identificado, mas ele está situado em outro país, além de onde a vítima está domiciliada, o tribunal não tem jurisdição geograficamente e também remissão. Então salta imediatamente para a extradição do criminoso como uma solução, mas este processo, isto é, a extradição é repleta de seus próprios desafios, além do requisito de dupla incriminação, especialmente quando não existe tratado de extradição ou tratado de assistência jurídica mútua entre o estado requerente e o estado que tem a custódia do criminoso.

A configuração institucional adequada para a segurança cibernética variará ao longo do tempo e do local, dependendo da configuração de segurança em questão e das capacidades prevalecentes dos participantes individuais. O setor privado pode, em algumas situações, compensar as deficiências da parte do governo. Alguns estados podem estar em posição de aumentar a consciência de segurança de seus cidadãos, enquanto outros não. Mas não há dúvida de que a cooperação entre os setores é a direção geral em que se deve ir.

O princípio da dupla incriminação deve ser cumprido, o que significa que, antes que um criminoso possa ser extraditado validamente, a alegada ofensa deve ser um crime punível na jurisdição que procura a extradição, e também deve ser punível quando o criminoso está domiciliado. Sem cumprir este critério, o criminoso não pode ser extraditado. O medo do tratamento desumano é uma barreira para a extradição e isso basicamente inclui tortura e castigo degradante que provavelmente será levado ao criminoso.

5.1 CUSTO, TEMPO E ESFORÇOS INCORRIDOS EM INVESTIGAÇÃO E PROCESSO

Dada a natureza da evidência, isto é, forense, necessária no processo da cibercriminalidade, em oposição à coleta de provas em crimes terrestres, não é particularmente barata por causa do equipamento de alta tecnologia, materiais e conhecimentos envolvidos para realizar essas investigações.

Com referência específica à interação empresarial e social, o advento da tecnologia tem dois resultados, um lado representa as inúmeras vantagens que são a velocidade e precisão da informação e das comunicações ao homem onde quer que este esteja situado e cujo desenvolvimento descreveu o mundo como uma aldeia global, o outro marcou notoriamente o lado negro, que é o aumento desagradável dos crimes virtuais.

No tocante a flexibilidade e com relação às falhas de segurança, tem-se uma grande preocupação por parte das empresas e instituições financeiras com sua credibilidade no mercado que pode ser afetada com a divulgação de deficiências de

seus sistemas de informática. Em decorrência disso, muitos dos representantes das empresas optam por ressarcir a vítima ou mesmo arcar com seu próprio prejuízo, ao invés de comunicar os crimes às autoridades para que sejam investigados. Assim como as empresas mais atingidas pelo problema evitam oficializar os crimes de que foram vítimas, com receio de expor a vulnerabilidade de seus sistemas, as empresas fabricantes de sistemas informáticos também são vítimas das ações danosas.

Quando o lado obscuro se aproxima, apresenta uma dura tarefa para que os investigadores e outras autoridades responsáveis pela aplicação da lei desvendem o caso, dada a massa de informações que precisam de perícia técnica e exame cientifico, como percorrer inúmeros arquivos e romper códigos criptografados, antes de pistas que foram intencionalmente escondidas ou destruídas, levando, muitas vezes, a perseguição de criminosos cibernéticos a custos exorbitantes, além de tempo e esforços de especialistas que deveriam estar sendo usados de forma útil em outros empreendimentos.

Neste momento, é necessário ressaltar que o primeiro e principal desafio na aplicação das leis contra os cibercriminosos, é a identificação dos criminosos. Seja como for, é relativamente mais fácil quando o criminoso está localizado dentro da jurisdição e uma tarefa muito mais árdua, se um cibercriminoso estiver em outro país diferente de onde esse criminoso é desejado para fins de prisão e acusação.

Nos casos em que um criminoso é procurado extraterritorialmente, surgem muitas questões que representam custos adicionais na investigação do cibercrime e incluem as viagens aéreas onde é conveniente que os investigadores tenham que estar fisicamente presentes noutra jurisdição e, quando não, telefones e teleconferências, não são evitáveis porque os pesquisadores precisam interagir em outras jurisdições, de modo a efetivamente reunir os esforços para desvendar o cibercrime. E tais interações entre os investigadores, deve notar, não é fácil devido às diferenças horárias, por exemplo, pode ser que, quando alguns americanos estão na cama, os ugandeses podem estar no trabalho. Os custos adicionais associados às viagens incluem alojamento, alimentação, transporte, entretenimentos e outros custos diversos.

Além disso, no que diz respeito a diferentes jurisdições é a questão da barreira linguística, portanto, onde os investigadores chineses devem trabalhar com homólogos ingleses, as diferenças linguísticas ocasionam problemas que devem ser resolvidos pelos tradutores com custo adicional, onde há necessidade de troca de documentos para serem traduzidos, garantindo custos adicionais.

Além de tudo o que precede, existem outros intangíveis ainda, questões muito importantes, tais como diferenças de cultura, atitude e percepção dos países em relação aos crimes digitais e deve-se tomar conhecimento do princípio da dupla incriminação; a cooperação de testemunhas e outras partes interessadas também não é garantida e não pode ser tomada como certa. Deve-se acrescentar que, além do custo da investigação, outra variante do custo do crime virtual é o custo associado à ação penal, para isso, os advogados devem ser contratados a um custo muito elevado, além de taxas de arquivamento e outras despesas acessórias de litígios. De tudo o que foi afirmado, é manifestamente claro que o custo da investigação e a acusação dos crimes cibernéticos é proibitiva, o que, por vezes, leva muitos casos a serem descartados, com efeito, os cibercriminosos continuam a florescer.

5.2 ESCASSEZ DE ESPECIALISTAS NA PROSSECUÇÃO DOS CIBERCRIMES

Os cibercriminosos são oportunistas sempre procurando caminhos para fazer riquezas ilegais ou em casos raros causar sérios estragos em sistemas informáticos, foram descritos como ladrões profissionais, criminosos especialistas em computadores e problemas envolvendo o espaço virtual, portanto, a esperteza desses criminosos não pode ser justaposta com as agências de aplicação da lei que são meros funcionários do governo que estão mal treinados, mal remunerados, desmotivados e que oferecem seus serviços sem a devida proteção e segurança.

Além dos relatados fatores acima mencionados de formação precária, remuneração e segurança e proteção inadequadas no trabalho para os funcionários da agência de aplicação da lei, outro óbice é a escassez de especialistas na perseguição de crimes digitais. No Brasil no período de implantação da rede mundial de computadores não houve investimentos necessários de combate aos cibercrimes e muito menos capacitação dos agentes, sabendo-se que em outros países já aconteciam, de modo que ficou mais fácil a pratica de crimes na rede.

O volume de crimes cibernéticos que ocorrem no país, supera a quantidade de agentes capacitados para realizar as persecuções, em concordância afirmou Carlos Eduardo Sobral, chefe da unidade de Repressão a Crimes Cibernéticos da Policia Federal na CPI dos Crimes Cibernéticos, realizada no dia 20/08/2014 "O volume de investigação vem crescendo, e o efetivo tem que crescer na mesma proporção. Hoje o nosso efetivo acaba sendo menor do que o volume que necessita para que seja dado um rápido andamento às investigações" (apud. Canuto, Luiz Cláudio, 2015).

No que tange ao combate das práticas de crimes virtuais, o Brasil ainda se encontra em um nível de preparação a desejar, seja porque existem poucas delegacias especializadas como também um número insuficiente de profissionais capacitados para apurar as ocorrências de tais crimes.

É um fato bem conhecido que, se, mesmo que as agências de aplicação da lei tenham feito um bom trabalho na investigação da cibercriminalidade, na fase de litígio, a experiência dos promotores ainda é muito importante para garantir a condenação do cibercriminoso, cabe à ação penal provar seu caso além de qualquer dúvida. Infelizmente, este não é o caso, uma vez que existe uma escassez de promotores habilidosos nos departamentos de justiça do governo, no entanto, os cibercriminosos têm acesso irrestrito a advogados particulares renomados que cobram taxas legais muito elevadas, o que não é um problema para os cibercriminosos, pois eles poderiam pagar facilmente altos honorários profissionais para os melhores advogados especializados em práticas de crimes digitais.

Além disso, a questão do anonimato dos cibercriminosos e a natureza de evidências que muitas das vezes são tênues, no que se refere ao fato de que os investigadores só podem contar com vestígios e rastros deixados nos computadores e na Internet, tudo vai agravar o caso dos promotores que não estão tão familiarizados no tratamento de litígios de crimes virtuais em comparação com suas contrapartes na prática privada. Essas lacunas identificadas, são uma vantagem para o criminoso virtual, que, além de conhecimentos técnicos em casos de crime virtual, têm fundos mais do que suficientes para contratar advogados de primeira linha.

5.3 FALTA DE LEGISLAÇÃO ADEQUADA

A aplicação das leis de crimes cibernéticos tem sido largamente prejudicada devido a legislações inadequadas e a ineficácia da mesma, onde existem leis vigentes para o cibercrime. De acordo com as Nações Unidas, existem 193 membros da ONU, 2 Estados observadores e 6 Estados com reconhecimento parcial, totalizando 201 países no mundo. Uma inferência simples que poderia ser extraída de dados acima é que menos de 40% dos países do mundo possuem leis que proíbem o cibercrime.

Dado o cenário acima da falta de legislações relevantes especificamente estabelecidas para o crime informático, é evidente que o desenvolvimento equivale a dar aos cibercriminosos uma licença para operar livremente sem medo, mas sim com impunidade. A ausência de leis necessárias é ainda mais prevalente em África, onde 54 países que constituem o continente,

apenas 4, Camarões, Quênia, África do Sul e Zâmbia possuem leis que criminalizam os crimes cibernéticos. Espera-se que, quando a Nova Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais entre em vigor, a lacuna na lei e política em relação aos crimes cibernéticos e outros atos incidentais, devem ser dirigidos frontalmente.

É instrutivo notar que, mesmo quando existem legislações sobre os crimes virtuais, as disposições das referidas leis existentes não são suficientemente graves para dissuadir os cibercriminosos de seus atos ilegais. Alguns exemplos bastariam para reforçar a afirmação sobre o efeito de leis não dissuasivas; Na Austrália, existe a Lei de Cibercriminalidade de 2001, Lei do Código Penal de 1995: infrações de serviços informáticos e de telecomunicações e Lei de Telecomunicações (Intercepção e Acesso) de 1979, todas essas leis prescrevem sentenças leves entre um a três anos de prisão, exceto pornografia infantil.

De tudo o que precede, é evidente que o estado da lei não é punitivo o suficiente e, mesmo que as leis existentes sejam aplicadas, isso causará pouco ou nenhum impacto sobre os cibercriminosos, uma vez que as leis não podem impedir os criminosos de seus atos ilegais.

5.4 CARÊNCIA DE UMA LEI UNIVERSAL QUE REGE OS CRIMES CIBERNÉTICOS

A carência de uma lei universal que rege os crimes cibernéticos é o desfecho sobre o qual este artigo ancora esta discussão, e afirma, como em outro lugar antes, agora enfatizado, que os crimes cibernéticos não respeitam nenhuma jurisdição porque é possível que um criminoso possa estar em São Paulo e perpetrar seu ato que teria efeitos na Alemanha, Estados Unidos ou em qualquer lugar do mundo.

Argumenta Roberto Chacon de Albuquerque, que olhando de uma forma prática, uma pessoa que vive no Brasil pode alterar dados que estejam guardados na Itália, deslocando-os para a Alemanha, visando obter vantagem ilícita. Do mesmo modo que um vírus pode ser criado por um país e espalhado para milhares de computadores por toda a terra. A transmissão de dados pode incluir vários países, de tal forma que o lugar do crime seja definido de forma quase fortuita. (ALBUQUERQUE apud CRESPO, 2011, p. 117)

Dito, por outras palavras, é que, os crimes cibernéticos são crimes sem fronteiras, transnacionais e internacionais e que, tais crimes, são cometidos no ciberespaço, mas a maioria das leis e políticas que lidam com os crimes digitais até a presente data, são nacionais ou regionais. A única lei que lida especificamente com cibercriminosos em caráter internacional,

é a Convenção de Budapeste que, para todos os efeitos, é dificultada por dificuldades associadas ao Direito Internacional, questão já amplamente discutida.

Os crimes cibernéticos têm apenas uma jurisdição, isto é, o mundo inteiro. Ao fazê-lo, as leis e políticas existentes que são fragmentadas, nacionais, regionais ou quase internacionais não podem lidar com os problemas gerados pelos crimes virtuais. As leis de crimes cibernéticos continuarão a sofrer desafios de execução. A única lei que pode abordar frontalmente a ameaça dos crimes cibernéticos é aquela lei que teria apenas uma jurisdição, aplicável globalmente, e não até que a vontade política seja reunida para promulgar essa lei universal, a humanidade continuará a ser atormentada pelos desafios de aplicação das leis de crimes digitais.

6 CONSIDERAÇÕES FINAIS

Crime cibernético geralmente pode ser definido como um crime cometido ou facilitado através da Internet. É qualquer atividade criminosa envolvendo computadores e redes. Pode variar da fraude aos emails não solicitados (Spam). Pode incluir o roubo distante de segredos governamentais ou corporativos por transgressão criminal em sistemas remotos ao redor do globo. Cibercrime incorpora qualquer coisa, desde transferir arquivos de música, filme, vídeo e jogo eletrônico ilegalmente a roubar milhões de dólares de contas bancárias online. Também inclui infrações não monetárias, como a criação de vírus para serem instalados em outros computadores ou a publicação de informações comerciais confidenciais na Internet.

Conhecer os fatos e as tendências é crítico para os esforços de prevenção do crime e proteção de dados pessoais nos setores público e privado. Isso também ajuda na criação de ferramentas e estratégias para combater os cibercriminosos. Em virtude das ferramentas utilizadas hoje para cometer/perpetrar crimes cibernéticos, os criminosos são agora mais anônimos e, portanto, difíceis de identificar.

O Brasil está passando por uma revolução digital com poucos paralelos no mundo em desenvolvimento. A taxa de penetração digital e a adoção de redes sociais aumentaram exponencialmente na última década. Durante esse período, o Brasil testemunhou um aumento de dez vezes no acesso à Internet e nas assinaturas de telefones celulares, com mais da metade de sua população de 200 milhões de pessoas atualmente online.

O primeiro passo é concentrar-se no preenchimento de lacunas de conhecimento. Há uma conversa animada no Brasil sobre os muitos desenvolvimentos positivos relacionados a governança eletrônica, cidades inteligentes, soberania digital e novas tecnologias.

Curiosamente, há um silêncio sobre questões relacionadas à segurança cibernética. Quando discutidos, as conversas tendem a ser reservadas aos mais altos níveis de governo, forças armadas, órgãos responsáveis pela aplicação da lei. Os estudiosos brasileiros precisam começar a entender melhor a dinâmica dos hackers e dos grupos de cibercriminosos, as formas em que o crime tradicional está migrando para a internet, as maneiras em que as forças de segurança estão adaptando novas tecnologias de vigilância. Mas isso também significa que o governo deve incentivar um debate mais amplo com uma clara estratégia de comunicação sobre a necessidade da segurança digital.

Uma expansão tanto no número de cibercriminosos quanto nas oportunidades de se envolver em atividades ilegais altamente lucrativas tem alimentado parcialmente essa tendência, assim como o desenvolvimento de novas ferramentas de crime virtual em áreas como malware móvel. No entanto, uma grande parte do problema está relacionado a padrões e práticas de segurança digitais de empresas e indivíduos. Uma proporção significativa da atividade do cibercrime envolve ainda a reciclagem contínua de técnicas relativamente antigas, soluções de segurança para as quais estão disponíveis, mas não amplamente adotadas.

Em 2017 se viu a evolução das tendências estabelecidas no cibercrime. A ameaça do Ransomware continuou a crescer e agora se expandiu para setores como a saúde. O abuso sexual de crianças em linha continua a ser uma prioridade muito alta para todos os países, com a cooperação internacional estabelecida como uma parte significativa da estratégia para proteger as crianças e identificar as vítimas e o pedófilo.

A comunidade de cibercriminosos em expansão conseguiu explorar ainda mais a crescente dependência da tecnologia e da Internet. Além dos crimes expostos nesse trabalho, também houve uma mudança marcada nas atividades relacionadas ao tráfico de seres humanos, terrorismo e outras ameaças na internet. Em resposta, as autoridades responsáveis pela aplicação da lei aumentaram os seus conjuntos de habilidades e a sua capacidade de trabalhar em conjunto, havendo uma significativa melhora na parceria entre a indústria e os órgãos de persecução penal, levando à interrupção e prisão de muitas associações de cibercriminosos e indivíduos de alto perfil associados a abuso infantil, proprietários de serviços de DDoS, booters e botnets, e fraudes em cartões de pagamento.

Os instrumentos jurídicos e os mecanismos tecnológicos são instrumentos fundamentais para alcançar este objetivo. O fortalecimento das leis nacionais e a cooperação internacional são armas na luta contra a criminalidade no ambiente digital. Porém o crescente

uso indevido de anonimato legítimo e serviços de encriptação para fins ilegais continua a ser um sério desafio para a detecção, investigação e acusação de criminosos.

Um risco é que o excesso de regulamentação possa sufocar o desenvolvimento comercial e tecnológico nos países em desenvolvimento e aqueles céticos de uma abordagem intervencionista também argumentam que o mercado poderá fornecer medidas de prevenção da criminalidade mais efetivas e soluções eficientes para os problemas do crime cibernético do que o próprio estado.

Com efeito o presente trabalho não buscou esgotar o tema proposto, vez que, diante da complexidade deste não seria possível. Em verdade, tem mais a pretensão de promover a reflexão do que propriamente dar uma resposta, realizando uma crítica aos critérios dos fundamentos doutrinários com os quais vem se procurando equacionar a questão.

RELATÓRIO ANTIPLÁGIO

Relatório gerado por: felipesousa.almeida@ucsal.edu.br
Arquivos Termos comuns Similaridade
FELIPE TCC 12.20.docx X
https://ambitojuridico.com.br/cadernos/direito-constitucional/ajudicializacao-da-saude-e-o-papel-das-camaras-de-conciliacaono-estado-da-bahia
146 0,76
FELIPE TCC 12.20.docx X
https://repositorio.ufba.br/ri/bitstream/ri/16979/1/Dissertação
EISU Carlos Alberto Coutinho.pdf
380 0,62
FELIPE TCC 12.20.docx X
https://www.escavador.com/sobre/7582083/carlos-alberto-josebarbosa-coutinho
50 0,41
FELIPE TCC 12.20.docx X
https://oglobo.globo.com/economia/cursinhos-para-criminososvirtuais-sao-vendidos-livremente-na-internet-18468229
27 0,25
FELIPE TCC 12.20.docx X
https://aofirs.org/articles/over-80-percent-of-dark-web-visitsrelate-to-pedophilia-study-finds
16 0,13
FELIPE TCC 12.20.docx X
https://www.trendmicro.com/vinfo/br/security/news/cybercrimeand-digital-threats/brazilian-cybercriminal-underground-2015
12 0,1
FELIPE TCC 12.20.docx X
https://www.trendmicro.com/vinfo/us/security/news/cybercrimeand-digital-threats/brazilian-cybercriminal-underground-2015
8 0,07
FELIPE TCC 12.20.docx X
https://www.wired.com/2014/12/80-percent-dark-web-visitsrelate-pedophilia-study-finds
8 0,03
FELIPE TCC 12.20.docx X
http://noosfero.ucsal.br/carlos.coutinho
2 0,01
FELIPE TCC 12.20.docx X
https://noticiasquentes.net/tag/sites-de-pedofilia-da-deep-web
- Download falhou. HTTP response code:
- Remote host terminated the handshake

REFERÊNCIAS

Ascending the Ranks: **The Brazilian Cybercriminal Underground in 2015**," Trend Micro. Disponível em: http://bit.ly/1o5txbh. Acesso em: 12 outubro de 2020

BARRETT, Diane; WEISS, Martin; HAUSMAN, Kirk. **CompTIA Security+ SYO-401 Exam Cram**. Pearson IT Certification, 2015.

BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diario Oficial Rio de Janeiro.

BUDAPESTE, CONVENÇÃO. **Convenção sobre o Cibercrime**. Budapeste, 2001. Disponível em: <http://www.coe.int/t/dghl/cooperation/economic crime/Source/Cybercrime/TCY/ETS_ Acessado em: 21 nov 2020.

CENTRO UNIVERSITÁRIO "ANTONIO EUFRÁSIO DE TOLEDO" de Presidente Prudente. **Normalização de apresentação de monografias e trabalhos de conclusão de curso.** 2007 – Presidente Prudente, 2007, 110p

CGI. **TIC Kids online Brasil 2015**: Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil. São Paulo: Comitê Gestor de Internet no Brasil, 2016.

CHAGAS, Fernando Vinicius de Souza. **Estelionato eletrônico: necessidade de tipificação?** Disponível em: http://www.meuadvogado.com.br/entenda/estelionatoeletronico-necessidade-de-tipificacao.html

COLLI, Maciel. Cibercrimes. **Limites e perspectivas à investigação policial de crimes cibernéticos.**Curitiba: Juruá Editora. 2010.

COSTA, Marcos Aurélio Rodrigues. Crimes de informática. Disponível em: **Revista eletrônica Jus Navigandi.** Site: http://www.jus.com.br/doutrina/crinfo.html

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

Cyberedge. 2019 **Cyberthreat Defense Report**. USA, p. 19. Disponivel em: https://cyber-edge.com/cdr/. Acesso: 20 out 2020.

DAOUN, Alexandre Jean. **Crimes informáticos:** direito eletrônico: a internet e os tribunais. Bauru: Edipro, 2001, p. 206.

DE SOUSA, Danilo Dimas. **Crimes Virtuais Contra Honra**. Clube de Autores, 2016.

Fernandes, Simone dos Santos Lemos; CALDI, Valéria. **Do Reflexo do Desenvolvimento das Novas Tecnologias de Informação na Prática de Crimes contra Crianças e Adolescentes**. Conforme SILVA, Ângelo Roberto Ilha da (Org.) Crimes Cibernéticos. Porto Alegre: Livraria do Advogado, 2017

GOMZIN, Slava. **Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions**. John Wiley & Sons, 2014.

GREENBERG, Andy. **Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds**. Disponível em: https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/. Acesso em: 23 out. 2020

GUPTA, Sandeep. **Hacking in the Computer World**. Mittal Publications, 2004.

IBM X-Force Exchange: **Cost of Data Breach Study: Global Analysis**, 2019. Disponível em: https://www.ibm.com/br-pt/marketplace/ibm-xforce-exchange. Acessado em: 15 nov 2020

INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. 2º ed., atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009

KLEIN, Soeli Claudete. **Engenharia social na Área da Tecnologia da Informação**. 2004. 63p., Monografia (trabalho de Ciências Exatas e Tecnológicas, Centro Universitário Feevale. Novo Hamburgo, RS. 2004

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** Campinas, SP: Ed. Millennium, 2005.

LISKA, Allan; GALLO, Timothy. **Ransomware: Defendendo-se da extorsão digital. Editora** Novatec, 2017.

M294 Manual para apresentação de trabalhos acadêmicos. [e-book] / coordenação, Linda Carla Vidal Bulhosa Gomes. 2. ed. Universidade Católica do Salvador, Sistema de Bibliotecas. – Salvador: UCSal, 2020.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coords). **Direito digital: direito privado e internet**. 3. Ed. Indaiatuba: Foco, 2020.

MARTÍN, Ricardo M. Mata y. **Delincuencia informática y derecho penal**. Madrid: Edisofer S.L., 2001, p.37

MORIMOTO, Carlos E. **Dicionario Tecnico de Informatica**. 3ª Ed., 2005. Disponível em: www.guiadohardware.net. Acessado em: 23 nov 2020.

NETO, Mário Furlaneto; GUIMARÃES, José Augusto Chaves. **Crimes na internet:** elementos para uma reflexão sobre a ética informacional. Disponível em: <http://www.cjf.jus.br/revista/numero20/artigo9.pdf

NUCCI, Guilherme de Souza. **Manual de Direito Penal**- v. 1. 10. ed. Rio de Janeiro: Forense, 2017

PINHEIRO, Patricia Peck. **Direito Digital.** 4.ed.rev.,atual.e ampli. São Paulo: Saraiva, 2010.

POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos, BRANDÃO, Luiza Couto Chaves. **Governança global da internet, conflitos de leis e jurisdição [recurso eletrônico]**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2018. Disponível em: http://irisbh.com.br/wp-content/uploads/2018/06/Governanca_global_da_internet_IRIS.pdf. Acesso: 15 nov 2020

RECUERO, Raquel. **Redes Sociais na Internet**. Porto Alegre: Editora Sulina, 2009.

REIS, Wellington José dos. **Internet 11: navegação prática e segura**. 1.ed. Santa Cruz do Rio Pardo - SP: Editora Viena, 2015.

Reunião Global Multissetorial sobre o Futuro da Governança da Internet (2014) ***NETmundial Multistakeholder Statement.***

ROQUE, Sergio Marcos. **Crimes de informática e investigação policial**. São Paulo: Justiça penal,2000.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A Convenção de Budapeste e as Leis Brasileiras.** Disponível em: <http:// www.mp.am.gov.br/index.php/centros-de-apoio/combate-ao-crimeorganizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras> Acesso em: 15 out. 2020

TRIVINOS, Augusto N. S. **Introdução à pesquisa em ciências sociais**. São Paulo: Ed Atlas 1997

Verizon (2019) Verizon 2019 Data Breach Investigations Report.

VIANNA, Túlio Lima**. Fundamentos de Direito Penal Informático**. Rio de Janeiro: Forense, 2003. ISBN 85-309-1619-0.

WENDT, Emerson e NOGUEIRA JORGE, Higor Vinicius. **Crimes Cibernéticos, Ameaças e procedimentos de investigação.** São Paulo, Editora Brasport, 2013. 2° Edição.