ADRIENNE DUARTE

CRIMES VIRTUAIS: conceito e formas de investigação

CURSO DE DIREITO – UNIEVANGÉLICA

2020

ADRIENNE DUARTE

CRIMES VIRTUAIS: conceito e formas de investigação

Monografia apresentada ao Núcleo de Trabalho de Curso da UniEVANGELICA, como exigência parcial para a obtenção do grau de bacharel em Direito, sob a orientação do Professor Me. Adriano Gouveia Lima.

ANÁPOLIS - 2020

ADRIENNE DUARTE

CRIMES VIRTUAIS: conceito e formas de investigação

Anápolis, _____ de _____ de 2020.

Banca Examinadora

_____

_____

RESUMO

A presente monografia tem por intuito, esclarecer dúvidas e requintar a compreensão no tocante ao universo dos crimes eletrônicos, os quais estão se tornando mais frequentes. Várias foram as obras estudadas para que as informações compartilhadas aqui, fossem ricas de detalhes para que não restassem dúvidas sobre como esses crimes ocorrem, como são investigados e qual o caminho um criminoso segue para que consiga consumar um crime virtual. No decorrer do artigo, são discorridas quais são as normas abrangentes aos crimes virtuais, e por fim, uma série de instruções, medidas assecuratórias para se proteger do mundo dos cibercrimes.

Palavras chave: Crimes Eletrônicos, Cibercrimes, Internet, Deep Web.

SUMÁRIO

INTRODUÇÃO

A presente monografia, objetiva a melhor compreensão do universo dos crimes eletrônicos, os quais podem e são praticados em todo território mundial pela simples conexão com um sistema de internet. Seja por smartphones ou computadores.

Com o grande avanço da tecnologia, esses tipos de crimes acontecem com mais frequência, e é de fundada e notória relevância estudar a fundo o assunto tratado, para que sejam solucionadas certas questões e ainda, elucidar os cidadãos a respeito de informações importantes envolvendo o mundo virtual.

Logo, não mais se pode analisar o direito apartado dos fenômenos tecnológicos. O trabalho engloba também o ordenamento jurídico moderno envolvendo o tema exposto, tendo em vista que a sociedade sofre com os crimes virtuais com cada vez mais frequência.

Com o avanço da internet e dos suportes digitais de acesso a ela, os criminosos modificaram a sua atuação e os crimes virtuais se destacaram do final da década passada até os dias atuais, não apenas pela simples prática dos delitos mais comuns como espionagem e sabotagem das máquinas, mas também, em procedimentos mais hábeis como racismo, pornografia infantil, abuso sexual, pirataria dos programas virtuais pagos, subtração de valores em contas bancárias, dentre outros. E são sobre esses e outros crimes que o presente trabalho se trata.

É notória a gravidade da situação, portanto segue a relevância estudar a fundo o assunto tratado, para que sejam solucionadas certas questões e, por fim

elucidar os cidadãos a respeito de informações importantes envolvendo o mundo virtual.

A pesquisa realizada, tem por objetivo principal, esclarecer e assegurar uma maior proteção aos usuários da internet, para que haja menos praticas delituosas e assim, a decadência de vítimas acerca do tipo penal.

CAPÍTULO I – CONCEITO DE CRIME ELETRÔNCO

Este capítulo aborda sobre o aspecto histórico do conteúdo do tema tratado, o conceito dos crimes eletrônicos, o desdobramento de suas ocorrências, e o que elas acarretam no mundo jurídico, com sua rápida propagação em todo o território mundial. Também discorre sobre as classificações, assim como suas modalidades e seus tipos, além de arrazoar as grandes redes utilizadas para a prática dos atos ilícitos, e como de fato ocorre um crime virtual.

1.1 A Evolução e o conceito dos crimes eletrônicos

A internet surgiu nos Estados Unidos, na década de 1970, quando o Departamento de Defesa Norte-Americano criou um sistema que interligava vários centros de pesquisas militares, permitindo a transmissão de informações e dados. Isso só foi possível devido ao acúmulo de estudos sobre a informática, e também ao desenvolvimento dos computadores (TEIXEIRA, 2007).

De início, o seu uso era restrito apenas aos Estados Unidos, para fins de pesquisas em universidades, logo mais se expandiu ao uso comercial e após, se ampliou ao continente Europeu. A rede foi ganhando espaço nas realidades sociais, e na década de 80, evolui para o termo internet. O tempo, e as pesquisas realizadas foram elementos cruciais para o que hoje é possível, por meios tão simples na palma da mão, com apenas um toque (TEIXEIRA, 2007).

Cientistas trabalhavam em prol da evolução tecnológica, estudando as transmissões de dados. Como exemplo, a criação do “www” que significa World Wide Web*,* (rede mundial de computadores), domínio criado pela Organização

Europeia Para a Investigação Nuclear, objetivando facilitar o uso de eletrônicos conectados a rede de dados informáticos, que possibilita o acesso conjunto entre várias pessoas, no mesmo site, ao mesmo tempo. Também o “https” Hyper Text Transfer Protocol Secure (protocolo de transferência de hipertexto seguro), divulgado pela empresa norte-americana Netscape, desenvolvido para o envio de mensagens criptografadas que permitiam a segurança dos usuários da internet. (WERNER, 2001, online).

Após estas criações, que foram as bases para o desempenho da internet, foram surgindo aos poucos, as plataformas que permitem o acesso a dados e informações mundiais pelo seu acesso, como o Google, Yahoo, Hotmail, entre outros, que são os responsáveis para pesquisas de modo rápido na internet, e que são aptos ao compartilhamento de dados em uma alta velocidade. (WERNER, 2001, online).

Os benefícios que essa invenção tecnologia possibilitou ao ser humano, engloba todas as áreas da vida de qualquer usuário, seja no ramo profissional, proporcionando o rápido tráfego de envio de dados, ou no lazer, contribuindo para a colheita de informações do mundo todo em segundos, com o acesso a jornais e revistas online, por exemplo.

Com toda essa magnificência, quem poderia delinear que algo feito com o intuito benevolente, fosse atingir proporções tão drásticas como as que hoje são percebidas? Como todas as coisas disponíveis ao ser humano se tornam objeto de crueldade em algum momento, com a internet não poderia ser diferente.

Não se sabe ao certo qual foi o primeiro relato de um vírus criado por meios eletrônicos, o que teria sido a iniciativa para que, logo mais começassem as práticas de atos ilícitos através desses vírus, que foram se aperfeiçoando com o tempo. Alguns estudiosos acreditam que tudo começou quando um grupo de programadores desenvolveu um jogo chamado Core Wars em 1984.Tal jogo era capaz de se reproduzir, cada vez que era executado sobrecarregando a memória da máquina do outro jogador. Os inventores desse jogo também criaram o que seria um

tipo de programa aproximado do que conhecemos hoje por antivírus, capaz de destruir cópias geradas pelo Core Wars (WENDT, 2012, online).

Já outros pesquisadores do tema, consideram que o primeiro a desenvolver um vírus teria sido Richard Skrenta, com apenas quinze anos de idade, em 1982, quando criou o Elk Cloner. Esse artefato contaminava o computador da marca Apple, e se difundia por cópias do disquete contaminado. É importante asseverar que esse código malicioso não causava grandes problemas, mas futuramente faria escola. O vírus era capaz de apresentar um pequeno ‘poema’ na tela do equipamento infectado, e gerava cópias de si mesmo quando um disquete era inserido no computador. Quando essa mídia era utilizada em outro sistema, o processo se propagava. (JORGE, 2012, online).

Há também um terceiro caso envolvendo dois irmãos paquistaneses, no ano de 1986, com a invenção de um vírus para computador chamado Brain. Ele atingia o setor de inicialização do disco rígido do computador, e tinha como finalidade detectar uso não autorizado de um software médico de monitoramento cardíaco que haviam desenvolvido. Porém o código sofreu modificações maliciosas as quais o transformaram em um vírus que se espalhava através de disquetes infectados. O Brain causava lentidão nas operações do sistema e ocupava demasiada memória operacional dos computadores. (QUINTO, 2011).

Não existe uma posição consensual sobre quais dos casos citados se sucederam, mas entende-se que foram estes, a base para o surgimento dos crimes eletrônicos. Há, portanto, informações as quais relatam que a denominação cibercrime (cybercrime, em inglês) surge pela primeira vez, no final dos anos 90, em reunião de um subgrupo envolvendo os sete países mais ricos do mundo e a Rússia. (D’URSO, 2019).

Doravante, surgiu o primeiro Cavalo de Tróia de que se tem notícia, em 1986, conhecido como PC Write, o qual se apresentava como um editor de textos, mas, quando executado, corrompia os arquivos do disco rígido do computador. O Cavalo de Tróia é um vírus responsável por invadir computadores, e acessar informações de todos os dados gravados na memória da máquina utilizada, além de

ter o poder de infectar outros dispositivos que estão conectados à ela por redes wi-fi, ou bluetooth. (MONTEIRO, 2008).

Com toda a modernidade cultural se expandindo diariamente, a evolução dos crimes eletrônicos é constante, não sendo mais uma matéria que se pode ficar avulsa, sem o conhecimento necessário para se precaver. Atualmente, com a amplificação tecnológica, já foram localizados milhares de vírus, dentre os quais, serão classificados, esmiuçando suas definições logo mais, no tópico 1.4 deste capítulo. O conhecimento de Vicente Greco Filho (2000, p.85), pode elucidar a respeito da introdução ao crime virtual, vejamos:

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

Vale ressaltar que, conforme estudo de Ivette Senise Ferreira (2011), sistemas ou computadores, como muitas outras ferramentas usadas por criminosos, como armas e explosivos, são ferramentas usadas por criminosos para promover o crime. Devido ao crescente grau de informatização das atividades individuais e coletivas desenvolvidas na sociedade, o Estado deve proteger novas formas e danos aos ativos e interesses diversificados. Esse tipo de informatização deu aos criminosos novas ferramentas e levou à formação de crimes informáticos específicos, cujo escopo não foi avaliado adequadamente.

Diversas são as definições para o tipo penal, alguns autores de forma mais sucinta, brevemente descrevem os crimes eletrônicos, como um mecanismo de praticar atos ilícitos por meio de computadores, outros mais amplos, trazem à definição celulares, tablets, até televisões que possuem conexão com dados de

internet. Dentre todas as citações, a que mais esclareceu, no entanto, foi a de Frabízio Rosa, (2006, p. 55), que conceitua os crimes virtuais da seguinte forma:

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; O 'Crime de Informática' é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; Assim, o 'Crime de Informática' pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável; Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública.

Profusas são as denominações para os crimes eletrônicos. São chamados cibercrimes ou, há quem prefira chamá-los de crimes virtuais, entretanto, não importa qual o nome se dê para esta pratica ilícita, pois seu conceito é bem simples de ser compreendido.

Levando-se em conta que atualmente, conforme dados disponibilizados pela Organização das Nações Unidas, 51,2% (cinquenta e um, vírgula dois porcento) da população mundial tem acesso à internet, é notável que as pessoas nascidas a partir do ano 2000, não estão acostumadas a se excluírem dos avanços tecnológicos, levando esse número a crescer ano após ano, logo, conclui-se que com o uso da internet, as informações chegam de forma mais célere e clara a todos, o que não permite a ignorância em massa sobre temas que englobam o mundo virtual. Como expressa o Juiz Federal, Doutor Emanuel Alberto Sperandio Garcia Gimenes (2013, online):

> Ao lado dos benefícios que surgiram com a disseminação dos computadores e do acesso à Internet, surgiram crimes e criminosos especializados na linguagem informática, proliferando-se por todo o mundo. Tais crimes são chamados de crimes virtuais, digitais,

> informáticos, telemáticos, de alta tecnologia, crimes por computador, fraude informática, delitos cibernéticos, crimes transnacionais, dentre outras nomenclaturas. À medida que o número de conexões entre computadores cresce, cresce também o da criminalidade neste meio, com criminosos incentivados pelo anonimato oferecido pela rede e pelas dificuldades de investigação no ambiente virtual.

Conforme demonstrado, não há uma definição específica sobre crimes eletrônicos, há divergência entre doutrinadores, porém seu núcleo permanece igual em todos os conceitos, sendo como um dano causado com ferramentas virtuais, para atingir um bem jurídico.

Todos os dados compartilhados por meios virtuais ficam salvos em dispositivos, redes de dados do sistema fornecido para navegação, ou seja, todas as informações que são trocadas diariamente por internautas, não desaparecem, mesmo excluídas da máquina utilizada para o feito. O autor Carlos Alberto Rohrmann (2005, p. 4), relata que:

> A comunicação de dados através da Internet não se dá pela mesma lógica da comunicação telefônica ordinária. Nesta, uma vez estabelecida a ligação entre duas pessoas, o circuito se fecha, pois a comunicação ocorre como se houvesse uma ligação dedicada, exclusiva, entre as duas pessoas. Já no caso da Internet, a comunicação não 'fecha' um circuito dedicado. As mensagens trocadas entre os usuários são transformadas em 'pacotes' que trafegam por rotas variadas ao longo da rede.

Existem milhares de servidores, como a Microsoft, que disponibilizam os chamados Data Centers, que de acordo com a empresa System IT Solutions (2017, online), são: "projetados com uma série de fatores em mente, como o espaço físico, a capacidade de investimento da empresa e até mesmo a oferta de energia e riscos locais". Basicamente, todos os dados que não se sabe para onde vai, fica armazenado nestes centros de processamentos de dados.

Eles funcionam como uma espécie de prateleira virtual infinita, com todos os dados, de todas as pessoas que alguma vez já utilizaram a internet na vida. Como se os dados estivessem em pastas separadas com todos os conjunto de informações que foram pesquisados, e adicionados em sites que foram acessados, pelos utilitários da internet. De acordo com a pesquisa disponibilizada pelo Locaweb (2014, online):

> Data Center é: um local destinado a concentrar os equipamentos que uma empresa ou organização utilizam para o processamento e armazenamento de dados, o que, dependendo do tamanho do empreendimento, pode acolher milhares de servidores, outros bancos de dados informatizadores e componentes auxiliares.

Os dados salvos nestes data centers são protegidos pelas empresas que prestam os serviços, ou seja, caso uma empresa precise de segurança para esconder seus dados, os serviços prestados pelo data center entram em ação para auxiliá-las (AQUIM, 2017).

1.2 A globalização dos crimes eletrônicos

Se a humanidade não progredisse em conjunto com a ciência e a tecnologia, é possível imaginar que, a raça humana já houvesse se extinguido. É um efeito natural do instinto de sobrevivência: caminhar rumo ao que facilita as tarefas diárias. Desde o período da globalização mundial, aproximando os povos e suas nações, se percebe a troca de mercadorias entre os países, objetivando o avanço global de todas as comunidades.

A internet foi o marco principal do desenvolvimento humano, pois através dela, é possível até mesmo entrar em contato com foguetes fora da atmosfera, com satélites que circulam pelo universo, enviando aos astrônomos e cientistas informações cruciais para a proteção do planeta e as descobertas de novos astros cósmicos, informações importantes para que se estude a vida em outros lugares no universo.

É impossível imaginar a vida hoje, sem um aparelho eletrônico, como o celular, que se tornou o objeto mais usado em todo o mundo, todas as pessoas necessitam dele. O mundo desde 1960 começou a se modernizar e acontecer no ambiente virtual, logo, todos também se veem obrigados a migrar para essa realidade, caso contrário, vão se atrasar em todos os âmbitos sociais.

A sociedade mundial moderna busca o novo. O insaciável desejo de sempre inovar traz à tona coisas grandiosas, que podem realmente auxiliar de alguma forma na destruição de barreiras impostas maleficamente, em algum

momento da história. Se a população pudesse ser definida em uma frase, hoje, seria: para onde caminha a tecnologia, iremos atrás. Como discorre a respeito a professora Patrícia Edí Ramos (s/d, online):

> Atualmente são outras as maneiras de compreender, de perceber, de sentir e de aprender, em que a afetividade, as relações, a imaginação e os valores não podem deixar de ser considerados. Na sociedade da informação aprende-se a reaprender, a conhecer, a comunicar-nos, a ensinar, a interagir, a integrar o humano e o tecnológico, a integrar o individual, o grupal e o social.

O que se vê, são ferramentas como sites de compras, aplicativos de filmes, séries, músicas, fotos e mensagens, destruírem os meios utilizados off-line para isto. Quem no ano de 2019, utiliza locadoras, CD's, máquinas fotográficas, ou cartas? Até mesmo para fazer refeições, não é mais preciso sair de casa para isso. Devidamente, empresas que não estão investindo seus capitais em sites para compras, estão falindo no mercado.

É um fato indiscutível que a melhor invenção humana até hoje foi a internet, e como já dito anteriormente, os povos caminham sempre em direção ao tecnológico, pelo fato de ser mais prático, e assim, evitar desperdício de tempo. O que antes, demoraria horas para cumprir, agora se faz com em poucos minutos.

Pelo fato de ser tão cômodo o uso dos dados, crianças e adultos se esquecem dos perigos que a internet oferece, e assim, fazem cadastros em sites com seus CPFs, utilizam seus dados bancários em aplicativos de compras, ou até mesmo deixam memorizados nas notas de seus celulares as senhas de seus cartões. É a partir desse descuido de utilitários, que os criminosos agem.

1.3 O desdobramento dos crimes eletrônicos, como ocorrem

No brasil, o número de pessoas afetadas pelos crimes em meios digitais, de acordo com dados disponibilizados pelo relatório de 2017 da Norton Cyber Security Insights, acarretou o prejuízo de aproximadamente 22 bilhões de reais. Incluindo os dados, cerca de 62 (sessenta e dois) milhões de brasileiros, foram vítimas desses crimes no ano de 2017. (REPORT, 2018).

Já são diversos os tipos de vírus, suas modalidades se estendem ao ponto de que cada um tem sua finalidade especifica, tais como, o Vírus de Boot: considerado precursor de todos os tipos de vírus, tendo surgido no final da década de 1980, agindo de forma a se fixar na partição de inicialização do sistema; Worm: conhecido também como verme, reside na memória ativa do computado e se replica automaticamente; Botnets: se caracterizam por computadores infectados por arquivos que possibilitam o controle remoto do computador da vítima; Deface: desfiguram sites ou perfis de redes sociais, entre outros, citados anteriormente como o Cavalo de Tróia. (BARROS, s/d).

Quanto a classificação dos vírus, têm-se o Hijacker: que sequestra o navegador de internet da vítima e a faz navegar por sites diferentes daqueles digitados; Rootkit: programas que permanecem ocultos no computador e podem ser instalados de forma local ou remota; Sniffer: monitoram todo o tráfego da rede, interceptando e possibilitando a análise de dados; Backdoor: deixa o computador vulnerável para ataques ou invasões; Hoax: chamados também de boatos cibernéticos, consistindo em falsas histórias divulgadas pelo meio digital, causando transtornos para a vítima e o Keylogger: monitora as informações digitadas pela vítima (BARROS, s/d).

Esclarecido as modalidades e as classificações, os crimes virtuais se entendem por três tipos, os puros que são a conduta cometida de forma geral, englobando tanto a parte física do computador, quando seus dados internos; Os crimes mistos, que tem por dolo lesionar algum bem jurídico da vítima, como o acesso a dados bancários para a transferência de valores, e por fim, os denominados crimes eletrônicos comuns, que não necessitam da informática para sua consumação, mas se realizam através dos meios digitais, exemplos que abrangem são a prática de injúria, calúnia e difamação, compreendendo também o racismo, a pedofilia, entre outras (VIANNA, 2003).

Os exemplos citados de crimes eletrônicos comuns, também se desdobram para a explicação do que é chamado pela doutrina de crime eletrônico impróprio, eles qualificam os delitos praticados por meio virtual, onde o praticante utiliza de um computador ou celular para consumar o ato, porém não reputa a

violação de algum dado eletrônico, que seriam os crimes dos artigos 138, 139 e 140 do Código Penal Brasileiro, ou seja, o bem jurídico danificado não seria eletrônico. (VIANNA, 2003).

Já para os crimes eletrônicos próprios, a quebra de sigilo de dados é obrigatória para se configurar, verbi gratia, o tipo penal de intercepção telemática ilegal, descrito na lei 9296/96, em seu art. 10 (Planalto, 1996): “realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei”.

Além das definições acima, também há a ramificação quanto aos autores que praticam o delito. A advogada Giovanna Sartório (online, 2018), explica:

> Os autores de tais crimes podem ser classificados como ativos e passivos. O exemplo, não apenas aquele que dissemina conteúdo pornográfico infantil é responsável pela prática do crime, mas o cidadão que simplesmente realiza o acesso, também está cometendo um crime.

Visto isto, já se tem uma clareza mais aprofundada sobre como surgiram, o que são e como ocorrem os crimes virtuais. Com a era digital é importante ter em mente, como é o funcionamento por trás das telas, no interior desta rede de dados. Importante salientar também, para os meios utilizados pelos criminosos cometerem os crimes virtuais, o que foi detalhado neste capítulo. Além de ter várias subdivisões, como demonstradas acima, são inúmeros os tipos penais que se enquadram nestes crimes, assunto este, que será discutido nos próximos capítulos.

CAPÍTULO II – INVESTIGAÇÃO, SEGURANÇA JURÍDICA E O MEIO PROBATÓRIO

Este capítulo aborda a forma a qual é realizada a investigação dos crimes eletrônicos, quais os meios utilizados para se chegar ao agente causador do ato ilícito que configura este tipo penal. Também exemplifica quais as formas de se assegurar que a jurisdição esteja de acordo com os usuários de internet, conforme a lei brasileira. No mais, também esclarece como as provas são produzidas e quais os meios utilizados para se comprovar a veracidade das mesmas.

2.1 As redes obscuras e a investigação nos crimes eletrônicos

A internet vem sendo cada vez mais utilizada para todos os tipos de serviços, com isso nossa forma de viver o dia-a-dia está se transformando, assuntos que antigamente eram tratados que demoravam mais de horas, hoje podem ser realizados em minutos. O computador, o celular, até mesmo em relógios digitais, as informações são transmitidas de forma codificada e enviadas em questão de segundos. (FRAGOMENI, 1987).

Para entender como os criminosos atuam nas redes, é necessário o entendimento sobre a base da internet, a história começa na guerra fria em 1960, com o medo da aniquilação numa guerra nuclear. O Departamento de Defesa Americano e a Agência de Desenvolvimentos de Projetos Avançados (ARPA) desenvolveram uma rede de computadores para a transmissão de informações imune a sabotagens. A ideia foi criar uma rede com vários computadores que pudessem trocar informações através de várias conexões independentes, de tal

forma que se uma conexão ou um computador fossem paralisados os outros poderiam continuar a trocar informações (FAGUNDES, online).

O primeiro crime eletrônico foi noticiado em 1973 com John T. Draper, que descobriu que o apito de plástico, produzia sons exatamente na mesma frequência que era usada para acessar o satélite para ligações de longa distância, com um tom de 2.600 Hz. Com isso, conseguia fazer ligações sem precisar pagar por elas. O que foi, e ainda é considerado por muitos como o primeiro cibercrime. (PAYÃO, 2017).

A partir daí surgiram cada vez mais os criminosos virtuais, que dia após dia evoluem. A mais famosa técnica para se cometer crimes eletrônicos mundialmente conhecida, é a chamada Deep Web, que é acessada por meio de navegadores especiais, como o TOR, que impede o rastreio das atividades dos usuários na rede, desenvolvido por Paul Syverson, Mike Reed e David Goldshlag, como discorre Felipe Villela (2018, online):

> O TOR foi originalmente projetado e implementado pelo Laboratório Central da Marinha para Segurança de Computadores, juntamente com a ajuda da DARPA, a agência criada no ápice da guerra fria com o intuito de converter os Estados Unidos em uma superpotência tecnológica. Anteriormente, a DARPA já havia comandado os estudos para a criação de uma rede descentralizada de computadores, capaz de resistir a qualquer ataque localizado, e foi assim que nasceu a Arpanet, o início do que hoje chamamos internet.

TOR significa "The Onion Router", em português à tradução: o roteador cebola, que se refere a como ele funciona, por meio de camadas, dentro de um mesmo sistema. A atividade da Internet através do TOR deve passar por diferentes redes de sobreposições, e cada rede ajuda a criptografar o tráfego do computador. Devido a essas camadas adicionais de segurança, o programada tende a ser mais sobrecarregado, caggerando de maneira mais lentamente que os navegadores comuns. (EMAG, 2017).

Basicamente, toda a internet que a maioria da população conhece e utiliza, engloba apenas 1% (um por cento) de todo o conteúdo que ela oferece, essa camada composta pela minoria é denominada surface web, ou a superfície da interenet, traduzido para o português. Já a Deep Web e a Dark Web, compoem os

outros 99% (noventa e nove por cento) de utilitários. Os estudiosos costumam usar a analogia do iceberg para explicar a internet, onde a parte que fica exposta (surface web) é ínfima, em relação a parte que fica escondida (deep/dark web). Pesquisas realizadas pela empresa Google, já apontaram que a rede obscura da internet possui mais de 14,5 bilhões de páginas para serem acessadas (BARROS, 2018).

A Deep Web e a Dark Web, são compostas por sites, páginas, que não podem ser localizados por qualquer meio de busca online, que necessitam de ferramentas especiais para serem acessadas, como o TOR, já descrito acima, ou seja, só é possível acessar essas cadeias online, se houver realmente o interesse pra isso. É como se houvesse uma lente, sob os olhos dos utilitários virtuais, e que ela impossibilitasse a visualização dessa parte obscura virtual, ela está lá, mas só é possível a ver se retirar essa lente. Essas redes não aparecem em mecanismos de pesquisa e, assim, as duas definições não são compatíveis com os programas comuns, gerando então um sistema de certa forma, irrastreável. (ROHR, 2016).

Dito isto, deve-se frisar que apesar de haverem mais redes como a Deep Web ela é a conhecida como a mais perigosa, por conter números volumosos de ocorrências de crimes, como venda de órgãos no mercado negro, pornografia infantil, grupos de ódio extremista, Hitman's que são assassinos contratados, videos Snuffs, conhecidos como filmagens de assassinatos, filmagens de estupro, aulas de fabricação de armas químicas, biológicas e bombas caseiras, tráfico de Drogas, fornecedores de serviços de hackers, experimentos científicos com humanos, os quais compartilham documentos e imagens, como trancar humanos com besouros-tigres para testar quantos dias eles sobrevivem ou até mesmo substituir as pernas dos humanos por patas de cabras (BBC, 2016 apud SILVA, 2015).

Além dos citados, também se encontram na Deep Web fóruns de canibalismo. Como exemplo, ficou conhecido o caso do "Canibal de Rotenburg", em 2003, que confessou ter comido a vítima a pedido da mesma. A investigação desse ato, levou a policia a descobrir vários fóruns como o "Cannibal Cafe" e "Guy Cannibals". Nesses fóruns, descobriu-se na epoca da investigação, de receitas sobre a melhor forma de ingerir a carne humana, até os voluntários, pessoas que se dispoem a serem obejto de tortura para a prática. (SILVA, 2015).

Outro crime bastante repugnante encontrado nas áreas obscuras da internet são os conhecidos por modificarem meninas entre 8 e 16 anos em Bonecas Sexuais Humanas. As garotas são compradas de suas famílias, ou até mesmo sequestradas, e a partir de então são transportadas a salas de cirurgia clandestinas ao redor do mundo, e são transformadas pelos denominados “Doll Makers”, que retiram alguns de seus membros, como as pernas, os braços e até mesmo os dentes, e no lugar, colocam proteses de silicone, elas são vendidas, com um manual de instruções para sua sobrevivência, tudo isso, para resistirem à perversão sexual de seus compradores que as obtem pelo preço de 40 mil até 700 mil dólares. (SILVA, 2015).

Também é bastante comum a tortura por encomenda, as quais, pessoas de todo o mundo, realizam compras de pessoas, principalmente crianças e adolescentes, com o intuito de fazerem torturas lastimáveis as mesmas, até elas sucumbirem à morte. Existem também, clubes, onde os sádicos colocam suas vítimas para lutarem entre si até que um morra. O pagamento é feito pela moeda virtual, conforme os padrões da Deep Web, tendo em vista, que a criptomoeda conhecida como BitCoin é irrastreável, não podendo localizar de onde e pra onde foram suas transferências (SILVA, 2017).

Como então é feito o trabalho investigativo para este tipo de crime o qual não se deixa rastro? A alçada para investigação, de início, compete a instauração do inquérito policial, que será feito após a denúncia do crime em alguma delegacia especializada em cibercrimes, portanto, doravante, começa a fase da apuração de provas.

O delegado deve procurar manter na íntegra a comprovação probatória adquirida, pois para este tipo penal, todo ato feito por algum aparelho eletrônico, deixa algum tipo de rastro codificado em alguma rede de dados, até mesmo na deep web, em mensaens criptografadas, ou nos IPs das máquinas utilizadas para cometer os crimes. Com isso, o Delegado de polícia procura investigar os vestígios deixados para buscar descobrir a sua autoria, para isso, é de suma importância, não deletar arquivos, ou não se desfazer de um aparelho que foi atacado/invadido, por algum vírus, justamente por essa razão. Para esse crime, qualquer dado é importante, para localizar o criminoso. (TEIXEIRA, 2013).

A investigação dos crimes virtuais é feita através de uma análise técnica, que permite verificar a autoria e materialidade dos crimes praticados por meio de uma rede que interliga os computadores, os principais delitos cibernéticos praticados no Brasil são: a pornografia infantil; as fraudes bancárias; os crimes contra a honra (calúnia, injúria e difamação); a apologia e incitação aos crimes contra a vida; e o tráfico de drogas. (WENDT, 2017).

Segundo TEIXEIRA (2013, p.49), conforme o pensamento de Wendt, ele traz um rol de delitos praticados no Brasil que são bastante comuns nos dias de hoje, com ele destaca-se, como ditto anteriormente as fraudes bancárias, os crimes contra honra como a calunia, a difamação e a injúria. Contudo, a polícia tem o dever de investigar e punir as condutas ilícitas praticadas no mundo virtual. A era da informática facilita o fenômeno conhecido como globalização, além de facilitar a informação, ela gerou novas formas de práticas ilícitas surgindo assim os crimes cibernéticos.

Conforme Camila Barreto dispõe, a era digital atinge tanto a questão do direito individual quanto o direito coletivo, pois a criminalidade afeta a todos visto que os crimes virtuais podem atingir uma só pessoa ou a coletividade (2014, p.15) “a criminalidade da informática passou a atingir também os bens jurídicos difusos em contrapartida aos bens jurídicos individuais atingidos pela criminalidade não informática”.

O que se busca na investigação desses crimes é identificar nos meios de comunicação o endereço do IP que é utilizado pelo criminoso durante a ação. Para Teixeira (2013, p.43) “O endereço IP, também conhecido como endereço lógico, é um sistema de identificação universal onde cada computador possa ser identificado exclusivamente, independente da rede em que esteja operando”.

Das evidências que podem ser obtidas a partir das investigações dos crimes virtuais, o endereço IP é, sem dúvidas, a de maior relevo para a solução do crime a ser investigado. (DORIGON, 2018).

2.2 A Proteção constitucional do sigilo de dados

No ano de 2009, surgiu no Brasil, a proposta do Marco Civil da Internet, pela Secretaria de Assuntos Legislativos do Ministério da Justiça, logo em seguida, em 2014, a Lei foi aprovada e entrou em vigor no território nacional. A lei traz os direitos e deveres de cada cidadão dentro do mundo virtual, enquanto estiver navegando por algum site. (MARTINS, 2015). Conforme prevê a Legislação Brasileira no artigo 5º, inciso XII da Constituição Federal de 1988:

> É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Basicamente, o que se entende é que para acessar as provas eletrônicas, é necessário a invasão de arquivos confidenciais de algum individuo, visto que funciona da seguinte forma, em que a conexão de rede acessada a um modem de rede de dados, que é ligado a um provedor de acesso. Para o usuário ter acesso a rede, o provedor que ele utiliza, lhe atribui um número de protocolo exclusivo pelo tempo em que se mantém conectado na rede, que seria o IP. Ele contém 4 séries numéricas de 0 a 255, por exemplo: IP 200.181.15,14 (SCHREINER, 2006).

A Lei do Marco Civil (13.853/19), frisando também sobre este aspecto estabeleceu em seu artigo 2º, inciso I, que um dos fundamentos da proteção de dados é o respeito à privacidade, porém, há uma discussão doutrinária referente ao foco dessa proteção constitucional, como transcreve Hugo Cesar Hoeschl:

> O dispositivo constitucional aludido (inciso XII do art. 5º.) trata de formas de comunicação. Tutela e protege meios, e não o conteúdo de mensagens. São as comunicações telefônicas, por carta, telegráfica e a transmissão de dados, a qual é uma forma de comunicação. Não teria o menor sentido o dispositivo tratar de forma e, atabalhoadamente, abordar o conteúdo no meio da disposição [...], e descabe a interpretação que acaba por eliminar um meio - quando o dispositivo fala de meios - para inserir um conteúdo. É claro, sabe-se, existe uma preocupação jurídica em torno da proteção das informações da vida privada das pessoas, na qual a expressão "dados" eventualmente aparece. Mas não é o caso. O texto constitucional está se referindo à "comunicação de dados", uma forma de comunicação, como já foi dito, ou de telecomunicação, tal como foi consagrada pelo Decreto 97.057/88.

Portanto, surge uma enorme dúvida jurídica de como assegurar a proteção do sigilo de dados, pois todos estão sujeitos ao envio de mensagens,

correspondências, compartilhamentos de fotos, vídeos e áudios. Atualmente o cellular, por exemplo, é o companheiro inseparável da maioria da população, até mesmo em bancos, já não se tem a necessidade de ir para fazer transações.

Visto essas informações, o Supremo Tribunal Federal, acatou o Recurso Extraordinário 1055941/2019, a respeito do compartilhamento de dados privados, que até o momento ainda não foi julgado. Conforme exposição do tema 990 da Repercussão Geral, onde diz que não há a necessidade de autorização pelo Poder Judiciário, para o compartilhamento de dados bancários e fiscais emitidos pela Receita Federal e pela Unidade de Inteligência Financeira (UIF), com os órgãos do Ministério Público e as autoridades policiais, para fins de investigação criminal. (STF, 2019).

Como se vê em deslinde, o tema proposto em Recurso Extraordinário, ainda não detêm de uma pacificação do Supremo, Com o julgamento do Recurso Extraordinário envolvendo o tema, houve então a suspensão envolvendo todos os procedimentos e investigações judiciais, iniciados pelo compartilhamento de dados detalhados pelas autoridades, sem a autorização prévia do judiciário (SAGMEISTER, 2020).

Portanto, resta impossível para se prosseguir alguma investigação criminal online, sem acessar dados particulares e proteger totalmente os dados da vítima, por exemplo. O marco civil da internet prevê que a quebra de sigilo de dados em poder do provedor de aplicações de internet é submetida ao controle jurisdictional, do art. 10, 1º, qual seja (PLANALTO, online):

> Art. 10. - § 1º. O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo.

Tecnicamente, o artigo se refere a guarda e a disponibilização dos dados eletrônicos, com segurança dos dados pessoais privados de cada utilitário do sistema. Todos estes, devem ser obrigatoriamente preservados, observando a proteção constitucional de sigilo de dados, mantendo fora de perigo que a

intimidade, a vida privada, a honra, e imagens das partes sejam divulgadas e expostas. Previsão legal disposta no artigo 13, da Lei do Marco Civil (PLANALTO, online) “cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento”.

Portanto, como mencionado, cabe a empresa provedora do sistema, do software, por exemplo, do site responsável pela origem de algum vírus que foi o causador do crime, manter todos os dados de qualquer aparelho, pelo prazo de 01 ano para fins de segurança. De suma importância é, ressaltar o artigo 10, § 3º neste artigo, (Planalto, online). Obsevar-se que é possível a autoridades administrativas, conforme determinado pelo parágrafo 3º, mediante a requisição direta, sem necessidade da ordem judicial. Vejamos o que diz Pamella Gabrielle Giacchetta (2015, online):

> A Conforme previsto de forma clara pelo artigo 10, § 3º, a exceção é aplicável estritamente a dados que informem “qualificação pessoal, filiação e endereço”. Requisições de autoridades administrativas visando o fornecimento de dados que não se enquadrem nos conceitos previstos extrapolam os limites da exceção e caracterizam abuso de poder. É o caso, por exemplo, de requisições que objetivem o fornecimento de telefone, e-mail e endereços de IP (Internet Protocol), ainda que sejam tais dados coletados no momento do cadastro no serviço.

Para realizar uma investigação de crimes eletrônicos, é inviável não acessar dados privados da vítima ou do acusado, pois para uma análise das provas, é necessário a identificação do IP do computador de onde foi acessado o aparelho para o ato criminoso, são feitas algumas analises para o próximo passo da investigação, ela irá depender de vários fatores e informações disponíveis, que só podem ser acessadas, se houver a infiltralção da polícia no aparelho da vítima. Segundo Melo (online, s/d):

> se o hospedeiro é um provedor conhecido, que hospeda, gratuita ou mediante remuneração, sites de terceiros (por exemplo, “HPG”, “Geocities”, “Terra”); b) se a página está registrada em nome de uma empresa não conhecida. Nessa última hipótese, seria preciso analisar o caso concreto, e verificar se é possível requerer a quebra do sigilo de dados telemáticos sem que o autor da página tome conhecimento disso. Se o provedor que hospeda a página for conhecido (e brasileiro), o investigador deverá requerer, judicialmente (ver modelo no anexo III), a quebra de sigilo de dados telemáticos,

> para que o hospedeiro forneça uma cópia, em mídia não-regravável (CD-R), das páginas investigadas e também os logs, isto é, os registros de criação e alteração da página. É no log que encontramos as três informações que nos são necessárias para prosseguir: a) o número IP; b) a data e a hora da comunicação; e c) a referência ao horário, incluído o fuso horário GMT ou UTC.

Visto e analisado estes quesitos, se consegue ter um certo limite, de até onde o sigilo de dados pode ser acessado, mediante as normas previstas no marco civil da internet, para que os parâmetros da privacidade estabelecidos na Constituição Federal não sejam violados.

2.3 Valor probatório das provas eletrônicas

Conforme artigo 332 do Código de Processo Civil Brasileiro, as provas são admitidas desde que observados todos os meios legais, bem como os moralmente legítimos, a provar a verdade dos fatos. Sendo de extrema importância, identificar a origem, conceito, finalidade, destinatário e o objeto utilizados para se conseguir a prova utilizada (SOUZA, 2012).

As provas processuais, tem por objetivo final o convencimento do juiz sobre determinado assunto julgado em questão, tratando de provas físicas, as mesmas, como regulamenta o Código Civil e o Código de Processo Penal, devem estar em grande maioria autenticadas, ou caso não necessite, devem estar devidamente assinadas. Discorre Nucci (2019, p.15) sobre o assunto:

> Convencendo-se disso, o magistrado, ainda que possa estar equivocado, alcança a certeza necessária para proferir a decisão. Quando forma sua convicção, ela pode ser verdadeira (correspondente à realidade – verdade objetiva) ou errônea (não correspondendo à realidade – verdade subjetiva), mas jamais falsa, que é um “juízo não verdadeiro”. Sustentar que o juiz atingiu uma convicção falsa seria o mesmo que dizer que o julgador atingiu uma “certeza incerta”, o que é um contrassenso

Como a internet vem sendo uma grande aliada em todos os âmbitos do judiciário na atualidade, utilizá-la como meio para se provar fatos, vem sendo cada vez mais frequente nos processos. “A prova digital, também conhecida como eletrônica, é um conjunto de informações dispostas em uma sequência de bits e consignada em uma base física eletrônica”. (ROMANO, 2011).

Porém com toda essa modernidade processual, a preocupação é que os documentos sejam alterados por vias eletrônicas. Visando proteger esse aspecto criou-se a Medida Provisória 2.200/2001, a qual determinou ser obrigatória a assinatura, conforme a autenticidade pela Chave de Segurança Brasileira, “para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica” (MP 2.200/01). Esta assinatura eletrônica confere uma codificação ao documento que pode ser verificada a sua autenticidade, conforme a Medida, caso o documento esteja alterado, ocorre sua invalidação.

Os documentos eletrônicos, foram regulamentados pelo Decreto de número 8.539/2015, o qual dispõe em seu artigo 2º, inciso II: “documento digital - informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional”. (PLANALTO, 2015).

Este Decreto sancionado, diferenciou em seu artigo 2º, alíneas a e b, do inciso II, os documentos nato-digitais, que seriam os que são originalmente criados através de programas eletrônicos, dos documentos digitalizados, que são definidos por aqueles que são convertidos de físicos para digitais, com o exato código digital representado. (PLANALTO, 2015).

CÁPITULO III – LEGISLAÇÃO CORRESPONDENTE E SEUS TIPOS PENAIS

Neste capitulo, prevalece a legislação, em como a jurisdição preocupa-se em tipificar os crimes virtuais em suas ramificações, quais as leis expressas no Código Penal Brasileiro envolvendo o tema, com suas explicitações. Ainda, alude quais os tipos de crimes eletrônicos mais recorrentes, e como se assegurar para não ser mais uma vítima.

3.1 Legislação nacional, internacional e tratados aplicáveis

Utilizando os ensinamentos de NUCCI (2015), o bem jurídico é o que justifica a existência de uma norma, um crime, tipificado no Código Penal. Para tanto, quando se tem várias denúncias, reclamações acerca de um determinado tema, que esteja trazendo algum mal a sociedade, é discutido qual o bem jurídico em questão está sendo ameaçado. Para o doutrinador:

> A tipicidade, a ilicitude e a culpabilidade, gravitam em torno do bem jurídico (...) conforme o grau de lesão provocado ao bem jurídico, ingressa-se na avaliação da culpabilidade, tanto na parte concernente à formação do delito, como também no âmbito da aplicação da pena, afinal, bens jurídicos fundamentais demandam penas mais severas.

O bem jurídico tutelado nos crimes eletrônicos se qualifica de acordo com sua tipificação. Há duas ramificações, como visto no capítulo I deste artigo, os crimes virtuais próprios, (VIANA, 2003, P. 13-26) “São aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados).”, e os crimes virtuais impróprios, (Damásio, 2014) “o agente

se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço real, ameaçando ou lesando outros bens.”, um exemplo são os crimes contra a honra.

Há várias leis e tratados envolvendo crimes eletrônicos ao redor do mundo. Algumas antigas normas, são ainda utilizadas atualmente, porém, em outros casos, novas regulamentações são estritamente necessárias para o bom uso, e segurança das ferramentas eletrônicas e maior credibilidade em relação a realização de tarefas, e até mesmo entretenimento, por meio eletrônico. (BASSO, 2007).

Além da falta de legislação específica, há um problema maior no rastreamento, porque a transmissão de dados é rápida e imediata, e isso prejudica a evidência de comportamento ilegal. Portanto, é necessário treinamento especial e são necessários meios técnicos que possam determinar a localização do crime e a pessoa responsável. No mesmo estudo, ele complementou acerca das leis brasileiras (PINHEIRO, 2013, p. 26 e 27):

> O primeiro decreto condenatório por crime eletrônico no Brasil foi proferido pela juíza da 3ª Vara da Justiça Federal de Campo Grande (MS), Janete Lima Miguel. Isso apenas vem confirmar que nossa legislação vigente pode ser aplicada aos crimes cibernéticos. Porém, para alguns autores deveria ser formulada uma lei prevendo todas as ações danosas na Internet, mesmo que o bem jurídico tutelado seja o mesmo já tutelado pela lei previamente existente. Para isso é preciso avaliar os bens. Devemos nos preocupar em achar um meio termo entre liberdade de informação e proteção de dados pessoais, para que os bens jurídicos tutelados por leis aplicadas no mundo físico tenham valia também para o mundo virtual, e vice-versa. Ainda assim, não podemos nos enganar e desejar que o Direito Penal tutele todos os bens relevantes para a sociedade, sob pena de levarmos o sistema à falência.

Quando ainda não existiam leis sobre crimes eletrônicos, eram eles tipificados por analogia, como por exemplo, o furto de dados se enquadrava no furto do código penal. Crimes como estelionato, extorsão, ameaça, entre outros, possuem bens jurídicos já tutelados no Código Penal e por isto o que diferencia é apenas quanto ao meio utilizado, o que aqui, seria o eletrônico. Para Diniz (2006, p.45), “[…] sendo exigência de lei anterior para definir a conduta delituosa e cominar a pena atinente, não é cabível o emprego da analogia ou ampliações da

lei penal, através da interpretação, para incriminar determinada conduta e trazer prejuízos ao sujeito ativo". Acerca da tipificação dos cybercrimes, aduz Pinheiro (2013, p. 28):

> […] as condutas chamadas de crimes virtuais (embora inexista legislação específica) encontra-se tipificada em textos legislativos existentes (Código Penal e legislação esparsa) e, ao contrário do que alguns autores afirmam, a aplicação da lei já existente a essas condutas não é caso de analogia, pois não são crimes novos, não são novos bens jurídicos necessitando de tutela penal, a novidade fica por conta do modus operandi, de como o criminoso tem feito uso das novas tecnologias, com foco na Internet, fazendo com que os estudiosos e os aplicadores do Direito tenham que renovar o seu pensamento.

A Lei nº 9.609/98, também conhecida como Lei do Software, foi uma das primeiras a entrar para a legislação brasileira a respeito do assunto. Ela estabeleceu definição para o programa de computador, como conjunto de instruções de linguagem natural ou codificada para fazê-los funcionar de modo e para fins determinados. (PLANALTO, 1998).

Com o avanço da internet no Brasil, houve uma preocupação em relação aos direitos autorais, em vias eletrônicas. Como iriam proteger os direitos de criações pessoais, quando ficou tão fácil copiar e colar a ideia de alguém? Todo conteúdo disponível na internet, decorre do esforço, criatividade, e do intelecto pessoal de um indivíduo, porém, esse direito deve ser resguardado. Para isso, criou-se, no mesmo ano de 1998, a Lei n° 9.610, que abrange os Direitos Autorais, logo em seu artigo 7°, lê-se que há o resguardo de obras intelectuais, tangíveis ou intangíveis, ou seja, todas as obras criadas eletronicamente, são resguardadas pela lei. No próprio artigo, são definidas em 13 parágrafos, quais são essas obras, explicitamente. (PLANALTO, 1998).

A primeira Lei a respeito desse tipo penal, se deu nos Estados Unidos, no ano de 1980, foi nomeada como Lei de Privacidade de Comunicação Eletrônica. Logo após, foi aprovada, no mesmo país, a Lei de Fraude e Abuso de Computadores, a CFAA, que ainda está e vigor. Nos anos 2000, foi criado, o Centro de Denúncias de Crimes na Internet, e de acordo com pesquisadores, foram até o ano de 2015, reportadas 3.463.620 (três milhões, quatrocentos e sessenta e três mil e seiscentos e vinte) denúncias. (FBI, 2015).

O tratado internacional que abrange o tema aqui exposto, foi firmado em 2001, a chamada Convenção de Budapeste, que conta hoje, com mais de 20 países membros. O Brasil, só concluiu a sua adesão em dezembro de 2019. O tratado tem como objetivo definir os crimes mais comuns ocorridos na internet, como fraudes, pornografia infantil, invasão de redes, violações do direito autoral, entre outros. Além de definir os crimes, o tratado também, possibilita a cooperação para a investigação e evolução penal mundial, tendo em vista que, todos os países do mundo sofrem com esse problema (PGR, 2018).

Os países membros do tratado, podem se juntar, na investigação de criminosos mundiais, que atacam e roubam informações importantes via internet, como investigações sigilosas, pesquisas governamentais, dados bancários de empresas mundialmente influentes. Um dos casos mais conhecidos, foi o vírus orquestrado por David L. Smith, conhecido como ‘O Vírus Melissa’, no ano de 1999, onde causou o prejuízo de mais de US$80.000.000, (oitenta milhões de dólares) (COSTA, 2011).

Outros hackers famosos, são conhecidos por burlar o sistema do Departamento Federal de Investigação (FBI), de sites como Yahoo, e até mesmo da Administração Nacional da Aeronáutica e Espaço (NASA). Muitos deles, são recrutados, para auxiliar em investigações policiais, como ocorreu com o hacker mais famoso da história, Kevin Mitnick, que foi um dos criminosos mais procurados pela polícia americana nos anos 90, porém atualmente, é dono de uma empresa de proteção à informações pessoas (VELASCO, 2019).

No cotidiano atual, ao que diz respeito a legislação brasileira, a Lei mais conhecida é a Lei 12.737/12, conhecida com “Lei Carolina Dieckmann”, que foi intitulada com essa nomenclatura, pelo fato da atriz ter sido alvo de ataques cibernéticos, onde hackers invadiram seu celular. A Lei abrange invasão de dispositivo telemático e ataque de denegação de serviços de informações (PLANALTO, 2012).

A Lei, alterou os artigos 154, 266 e 298 do Código Penal. assim veremos respectivamente. Adicionando o dispositivo 154-A, o crime de invasão de dispositivo informático, que prevê a pena de 03 (três) meses a 01 (um) ano, para

quem (PLANALTO, 2012):

> 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.

Caso dessa invasão, resulte prejuízo econômico, a pena é aumentada de um sexto a um terço, e ainda, se houver, como demonstrado no dispositivo da Lei (Planalto, 2012) “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”, a pena é aumentada, de 03 meses como pena mínima, passa agora a ser de 06 (seis) meses a mínima e 02 (anos) a máxima, com o acréscimo de multa.

Podendo ser agravada, como dispõe a Lei (Planalto, 2012) “se houver a divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos”, e também se for cometido o delito, contra figuras políticas do Estado, como o Presidente da República.

O artigo 266, do Código Penal, trata da interferência em redes de tráfego na internet, como um meio para bloquear, por exemplo, algum sinal telefônico, ou de rádio. Vejamos o que diz Rogério Tadeu Romano (2014), a respeito do assunto:

> Duas são as modalidades contidas no artigo 266, referentes ao serviço telegráfico, radioelétrico ou telefônico, em enumeração taxativa. A primeira modalidade é interromper, paralisar, fazer cessar, perturbar. A segunda, envolve serviço interrompido e a conduta do agente é impedir, dificultar. Assim a norma do artigo 266 do Código Penal visa ao serviço de forma que se o comportamento é interromper ou perturbar o aparelho telegráfico ou telefônico determinado, ou a comunicação de duas pessoas, não haverá enquadramento no artigo 266. Consuma-se o crime com a interrupção ou perturbação do serviço ou quando o agente logra impedir ou dificultar o seu restabelecimento.

Por fim, a última alteração feita, foi no artigo 298, que prevê o crime de falsificação de documento particular. A Lei 12.737, incorporou com o parágrafo 4º, o crime de falsificação de cartão de crédito, ou cartão de débito, com pena de reclusão

de 01 (um), a 5 (cinco) anos e multa. Há bastante discussão a respeito do crime envolvendo a falsificação de cartões, visto que, ele abrange, vários crimes previstos na legislação brasileira, como Murilo Cezar Antonini Pereira (2013), discorre brilhantemente a respeito de quais são eles:

> Por óbvio que o problema decorre principalmente do bem jurídico tutelado (patrimônio) e do elemento “fraude”, comum nos indigitados tipos penais. Uma coisa é certa, os referidos crimes não podem ser confundidos. Debruçando sobre a nossa legislação penal, pode-se notar que o furto mediante fraude está previsto no inciso II do §2º do art.155 do Código Penal. O furtador engana a vítima, buscando diminuir sua vigilância sobre a coisa, a qual é subtraída. Percebam que o agente nada mais faz do que aplicar “golpe patrimonial imperceptível” que recai sobre coisa alheia móvel da vítima. Analisando ainda o nosso Código Penal, o estelionato pode ser observado no art.171, caput, do referido estatuto penal repressivo. O estelionatário também engana a vítima, porém no sentido de mantê-la ou induzi-la em erro, com o fito de obter vantagem patrimonial ilícita.

Para o escritor, e muitos outros doutrinadores, é importante frisar a importância de equipara cartões bancários à documentos pessoais, tanto que no parágrafo único, do artigo 298, da Lei nº que compara cartões de crédito a certificados privados. (PLANALTO, 2012).

Seguindo para mais norma jurídica brasileira, no mesmo ano em que a Lei dos Cibercrimes foi publicada, também surgiu a Lei do Marco Civil, criada com o designío de complementar as Leis brasileiras que abrange os crimes virtuais. Inicialmente lida com conhecimentos e conceitos básicos, listando os direitos dos usuários. Além de determinar as garantias, direitos e obrigações no ambiente virtual, também representa os princípios de liberdade, neutralidade e privacidade. A ênfase é colocada nos direitos para garantir a privacidade e a inviolabilidade da vida privada que se localiza por trás das telas digitais. (PLANALTO, 2014).

O Marco Civil, trouxe a luz, o que os doutrinadores chamam de princípio da privacidade na internet, que estabelece e garante aos usuários a inviolabilidade das suas comunicações, colocando assim a confidencialidade de suas informações no provedor de recursos da Internet. As violações de tais garantias só podem ser executadas por ordens judiciais, essenciais para esclarecer atos ilegais e tentar determinar os autores. (NORTHFLEET, 2020).

Outro assunto bastante discutido é o disposto no artigo 18, da Lei do Marco Civil, onde diz que “O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros”, assunto complementado com o artigo 19 da mesma lei, vejamos:

> 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.
> § 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.
> § 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.
> § 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

Como pode ser visto na leitura do artigo 19, o Marco Civil da Internet estipula que o provedor de conexão não será responsável pelo conteúdo gerado por terceiros. Por outro lado, se ele não tomar medidas para tornar o conteúdo infrator indisponível sob uma ordem judicial específica, o provedor de aplicativos da Internet será responsável apenas pelos danos causados pelo conteúdo gerado pelo terceiro. (PLANALTO, 2014).

No entanto, sabemos que ao punir atos que violam esses princípios, a punição é pacífica e nenhum resultado satisfatório foi alcançado. Além disso, a solicitação de informações privadas exige uma ordem judicial, e o provedor da Internet não pode fornecer dados como IP, senha e login do criminoso, o que torna a investigação demorada. Independentemente da manifestação efetiva de garantias e direitos, essas cláusulas não podem abranger totalmente o campo de atividades dos cibercriminosos. Em outros regulamentos (como casos de compras on-line), existem lacunas no fornecimento. Sujeito à Lei de Defesa do Consumidor, que é a responsável por abranger esses casos em específico. (TEFFÉ, 2017).

Além disso, o Direito Penal também lista alguns crimes cometidos pela Internet, como crimes contra reputação. No entanto, o atual Código Penal foi formulado nos anos 90. Portanto, em alguns casos, ao lidar com crimes modernos que ocorreram ao longo dos anos, está desatualizado e a punição pelas consequências sofridas pela vítima não é grande. Portanto, o Brasil carece de legislação especial para o crime cibernético. Em muitos casos, os criminosos não são punidos, porque certos comportamentos não têm representantes típicos, mas existe uma lacuna entre atos. (MPF, 2018).

Percebe-se, pelo discorrido nos parágrafos acima, como a Lei acerca da internet, é vaga. Ainda atualmente, o Brasil não conta com um dispositivo legislativo que abrange totalmente os crimes por si só. Para a investigação em vias de cibercrimes, é necessária uma análise de vários dispositivos legais, para que o sujeito praticante do crime tenha uma pena justa. Como foi explicado, no caso de fraude, com cartões bancários, em que há a discussão, sobre fraude, furto e estelionato. Conforme Filho (2016), demonstra em seu artigo:

> Embora o Marco Civil da Internet tenha sido bastante festejado por ser a primeira lei do mundo a disciplinar os direitos e deveres dos usuários da rede, não se perceberão mudanças substanciais, uma vez que esta não acrescentou praticamente nada à legislação vigente. A expectativa criada com a discussão dessa lei deu-se pela crença errônea de que as normas contidas na Constituição Federal, no Código Civil, no Código Penal, nos Códigos de Processo Civil e Penal, no Código de Defesa do Consumidor, no Estatuto da Criança e do Adolescente e na lei sobre interceptação de comunicações (Lei n.9.296/96) não teriam aplicação nas relações jurídicas estabelecidas na internet.

Com o avanço da tecnologia e o aumento do número de usuários, é essencial formular uma lei para definir os atos criminosos cometidos no ambiente virtual e punir os autores dos resultados prejudiciais, levando em conta os dilemas atuais, e como as vítimas de fato são prejudicadas por determinados atos, que podem ter seu caráter diminuído.

Na questão do crime cibernético, ainda existem muitas mudanças no sistema legal, analisá-los é um ato comum e causa prejuízos ao país. É necessário restaurar a proteção legal e buscar eficácia na prática. Na última pesquisa divulgada pelo

Instituto Ipsos, o Brasil conquistou o segundo lugar de países com o maior número de casos de cyberbullying no mundo. (MARQUES, 2018).

3.2 Os tipos de crimes virtuais mais comuns.

Os crimes descritos no Código Penal Brasileiro são: Pornografia infantil online (art. 241 - ECA); Fraude bancária eletrônica (art. 155 - CP); Violação a direitos autorais (art. 164 – CP); Divulgação indevida de dados sigilosos (art. 153 – CP); Atribuição de falsa identidade (art. 307 - CP); Estelionato eletrônico (art. 171 – CP); Violação da imagem e da honra (arts. 139/141 - CP); Interceptação clandestina de dados (art. 10 – lei 9296/96); Alteração indevida de sistemas de informação do Governo (art. 313-A - CP); (PLANALTO, 1940).

Os Crimes contra a honra, dentre tantos crimes cibernéticos, são os mais denunciados, dentre eles os de calúnia, difamação e injúria, previstos no código penal do art. 138 a 145 do CP. Por meio da Internet, é muito comum, especialmente em sites de entretenimento, como as redes sociais, encontrar ofensas envolvendo preconceito sexual, racial, religioso, entre outros. Esses crimes são tão recorrentes, pelo fato de o criminoso, estar acobertado, muitas vezes pelo anonimato.

Esses crimes caracterizados contra a honra, deram o encadeamento ao que é chamado de cyberbullying, um dos maiores males que afeta a saúde mental de pessoas em todo mundo. De acordo com uma pesquisa realizada pela Unicef (online, 2019), um terço de jovens em cerca de 30 países sofrem com isso. De acordo com as informações do órgão “quase três quartos dos jovens também disseram que as redes sociais, incluindo Facebook, Instagram, Snapchat e Twitter, são os locais mais comuns para o bullying online.” O site de notícias BBC News, postou em 2014, a seguinte reportagem, a respeito do que ocorreu com uma jovem estadunidense a respeito do cyberbullying:

> O caso da jovem Rehtaeh Parsons, de 17 anos, que se enforcou em abril do ano passado após meses de assédio e ofensas pela internet, causou comoção nacional e motivou a aprovação de uma

> lei na província canadense de Nova Scotia para punir este tipo de crime. (...) Dois anos antes de tirar a própria vida, Rehtaeh havia sido abusada sexualmente por quatro jovens que fotografaram o episódio e postaram imagens nas redes socais. O assunto rapidamente ganhou os corredores da escola da jovem, que começou a ser xingada e a receber ameaças por meio de torpedos e de seus perfis nas redes sociais.

Essa terrível situação, é só uma entre milhares que acontecem todos os anos, não apenas com jovens, mas com adultos e crianças. Outro crime bastante comum, é a prática da pornografia infantil, A consumação dos crimes ocorre quando o criminoso divulga fotos ou vídeos obscenos de crianças na internet. Tal conduta está prevista no Estatuto da criança e do adolescente a partir do art. 240. O autor Lúcia Martinelli (2000) fez uma interessante colocação a cerca desse crime:

> A pornografia infantil talvez seja o crime que mais provoque a repulsa da sociedade. Não há qualquer forma de se aceitar as situações constrangedores a que crianças são subordinadas, para saciar as fantasias de pessoas desequilibradas. A pedofilia é um fenômeno fora dos padrões comuns toleráveis pela sociedade, encontrando na Internet um veículo para satisfazer virtualmente os seguidores dessa prática. Esta modalidade aparece na Internet de duas maneiras: pelas "home pages" e por correio eletrônico. Na primeira opção, os gerenciadores das páginas 34 recebem uma quantia dos usuários (através de depósito ou cartão de crédito), que dispõem de um acervo de fotos e vídeos. Na segunda opção, o material é distribuído de um usuário a outro, diretamente.

Os praticantes, muitas vezes utilizam a Deep Web, rede de internet vista no capitulo anterior, para propagar fotos e vídeos de crianças. Esse crime, é considerado pela Organização Mundial da Saúde (OMS), como um distúrbio mental, e aqui completo com as palavras de Croce, é um “desvio sexual caracterizado pela atração por criança ou adolescentes sexualmente imaturos, com quais os portadores dão vazão ao erotismo pela prática de obscenidades e atos libidinosos”. (CROCE, 2004).

O crime de violação dos direitos autorais, também tem prática constante, ele consiste em, (art. 184. CP) “violar direitos de autor e os que lhe são conexos”, o doutrinador Cléber Masson (2014, p 775) explica que os direitos de propriedade intelectual têm proteção legal, considerando que até mercadorias intangíveis têm valor econômico a partir do momento em que têm o significado de ciência, literatura, obra de arte e qualquer tipo de invenção.

De acordo com o artigo 184 do Código Penal, para se caracterizar o crime a respeito de direitos autorais, é necessário auferir o dolo de lucro. O lucro pode ser direto, quando por exemplo, ocorre a venda não autorizada de obras de arte e, o indireto quando, um estabelecimento para atrair clientes, organiza um evento com músicas de determinado artista. (SCOFIELD, 2015). A respeito do tema, também preconiza Guilherme Tomé de Melo e João Pedro Rosa de Souza (2019):

> O lucro direto é facilmente reconhecível, trata-se, verbi gratia, da circunstância em que um website disponibiliza para download e-books mediante o pagamento de uma quantia em dinheiro, sem anuência do detentor dos direitos de autor daquelas obras. Já o lucro indireto, por sua vez, é mais imperceptível, seria o caso no qual o administrador de um website, novamente desautorizado a fazê-lo, publique no mesmo diversas obras cujo acesso integral é gratuito aos usuários, mas possui anúncios publicitários de terceiros nas páginas em que se encontram obras. Assim, lucram percebendo mais ganhos pelo tráfego de usuários alavancado pela disponibilização das obras que, por vezes, é o único conteúdo atrativo do website.

Outro crime virtual, bastante popular são os de falsa identidade, é muito comum encontrar nas redes sociais perfis falsos, onde pessoas criam identidades falsas usando fotos de outras pessoas, seja por divertimento ou para prejudicar alguém, configurando assim os crimes prescritos no artigo 307 do Código Penal. (BRAMBILLA, 2020).

Atualmente, no cenário de guerras políticas invisíveis, se tem visto a prática frequente das propagações de fake news pelas redes sociais, que é definido como propagar informações falsas, como se fossem verdadeiras. Muitos não sabem, mas a prática de criar e propagar fake news, é considerada crime, com previsão legal nos artigos 339 e 340 do Código Penal, nos artigos 297, 323 ao 326-A, 350 do Código Eleitoral Brasileiro (Lei Federal nº 4.737/1965) e nos artigos 33, § 4º, 34, 35, e 37 da Lei de Pesquisas Eleitorais Fraudulentas (Lei nº 9.504/1997). (Vade Mecum, 2020).

3.3 Como se proteger de crimes cibernéticos.

Por fim, após expor detalhadamente os crimes eletrônicos, como eles ocorrem e quais são, percebe-se que é de grande relevância, que a população

saiba como se resguardar, para não se ter mais vítimas desses delitos. Empresas que trabalham com programas de proteção informática, como as de criações de antivírus, são as pioneiras para dar uma orientação de qualidade acerca do assunto. A Avast (online), por exemplo, instrui da seguinte forma:

> Aqui estão alguns hábitos de navegação sensatos que ajudarão você a se defender: Desconfie de e-mails inesperados com links ou anexos suspeitos; Não baixe nada de fontes desconhecidas; Verifique se você está em um site legítimo antes de digitar qualquer informação pessoal; Sempre aplique atualizações de software imediatamente (elas corrigem vulnerabilidades de segurança); Não use Wi-Fi público não criptografado (em cafeterias, aeroportos, etc.) sem uma VPN; Use senhas fortes e exclusivas e não reutilize a mesma senha em várias contas; Use a autenticação de dois fatores sempre que possível.

Até mesmo departamentos altamente protegidos, podem ter seus sistemas invadidos, informações sigilosas furtadas, como aconteceu recentemente em maio de 2020, por consequência da morte do jovem George Floyd nos EUA, um grupo de hackers famosos na internet por expor crimes políticos, conhecidos popularmente como Anonymous, invadiram o canal de rádio das policias de Chicago, também inativaram o site, para que ficassem impossibilitadas de se comunicarem referentes as manifestações antirracistas ocorridas em Minneapolis, pela morte do rapaz. dados privados publicados sem autorização. Portanto, toda a segurança é necessária quando se envolve está rede de fios que liga todo o planeta com apenas um toque (ALEX, 2020).

Para complementar, as informações acima, a também empresa de segurança informática Norton (online), publicou um artigo online com algumas recomendações adicionais para se precaver:

> Proteja sua rede doméstica com uma senha de criptografia forte e com uma VPN. Uma VPN criptografará todo o tráfego que sai dos dispositivos, até que chegue ao destino desejado. Mesmo que um hacker consiga acessar a sua linha de comunicação, nada será interceptado a não ser o tráfego criptografado; mantenha-se atualizado sobre as grandes violações de segurança. Se você tiver uma conta em um site que tenha sido afetado por uma violação de segurança, procure saber o que os hackers conseguiram obter e altere sua senha imediatamente; gerencie as suas configurações de mídias sociais para manter a maior parte das suas informações

> pessoais e privadas bloqueadas. Os criminosos cibernéticos de engenharia social podem obter suas informações pessoais com apenas alguns pontos de dados, portanto quanto menos você compartilhar com o resto do mundo, melhor.

O Brasil possui algumas delegacias especializadas em crimes cibernéticos. No entanto, se sua cidade não possui uma delegacia de polícia dedicada, você deve encontrar a delegacia mais próxima e denunciá-la. Para conduzir a investigação mais eficaz, muitas pessoas acham que a primeira reação após a invasão do dispositivo é reiniciar o dispositivo. Portanto, este é o primeiro aviso: não reinicie o dispositivo invadido, pois isso pode destruir os rastros deixados pelos criminosos e, assim, perder algumas provas importantes que podem ser usadas como evidência em processos futuros. Nesse caso, um especialista forense com todo o seu conhecimento, é designado para coletar dados e rastrear os rastros deixados pelos cibercriminosos. (SAFERNET, online).

CONCLUSÃO

O trabalho realizado, foi de grande relevância para o maior conhecimento acerca de um tema tão conhecido mundialmente. Muito ainda há de ser feito por todas as grandes nações mundiais, tendo em vista que as leis existentes, são bastante escassas, como estudado. Mas levando em consideração que a internet é como um espaço infinito, sem início ou fim, é compreensível que a jurisdição ainda não esteja a acompanhando no mesmo ritmo, Lewis Mumford, um historiador famoso, disse uma vez que (1922) “a tecnologia ensinou uma lição a humanidade: nada é impossível”.

No primeiro capítulo, tratou-se sobre o conceito, e de como a internet surgiu. Também sobre seus segredos, que trafegam por vários cabos que podem até ser visíveis, mas o conteúdo que os contém, não. Boas atitudes podem surgir da internet, e é notável que ela é a grande responsável por vários avanços mundiais, tanto na área profissional, quanto em áreas científicas, biológicas e até mesmo físicas.

Caminha-se para uma era totalmente virtual, como foi discutido em todos os capítulos. Estamos vivemos em meio ao trabalho remoto, educação escolar e universitária por meios eletrônicos, o que deixa a população ainda mais dependente de aparelhos eletrônicos. Os cuidados com a segurança da vida privada, devem ser estritamente tomados para que a estatística de crimes cibernéticos não aumente, tomando precauções necessárias como as descritas no último tópica desta monografia.

Todo o conhecimento adquirido no decorrer da confecção deste artigo, irá

me ser útil por toda a vida, e espero que possa enriquecer o conhecimento de outras pessoas com a curiosidade acerca do tema objeto dessa pesquisa. Parafraseio aqui por fim, para encerrar esse memorável e significante artigo desenvolvido, Guimarães Rosa (1956, p.31), a beleza não está na partida nem na chegada, mas na travessia.

REFÊRENCIAS

ALEX, Tony. 2020. **Anonymous Invade Rádio da Polícia de Chicago**. Disponível em: https://www.tenhomaisdiscosqueamigos.com/2020/06/01/anonymous-hacker-policia-chicago/. Acesso em 05 de junho de 2020.

ANGELUCI, Regiane Alonso. SILVA, Edevaldo Alves e SANTOS, Cariolano Aurélio de Almeida Camargo. **Sociedade da Informação: O mundo Virtual Second Life e os Crimes Cibernéticos.** Disponível em: http://www.oabsp.org.br/comissoes2010/gestoes-anteriores/direito-eletronico-crimes-alta-tecnologia/artigos/2010-2012/SL_Iccbyer_final0311.pdf. Acesso em: 17 de setembro de 2019.

AQUIM, Teixeira. 2017. **Proteção de Dados: um Desafio Para os Data Centers. Disponível em:** http://www.datacenterdynamics.com.br/focus/archive/2017/04/prote%C3%A7%C3%A3o-de-dados-um-desafio-para-os-data-centers. Acesso em: 16 de novembro de 2019.

BARATTA, Alessandro. **Criminologia e Crítica do Direito Penal Introdução à Sociologia do Direito Penal.** 3. Ed. Rio de Janeiro: Revan, 2002.

BARRETO, Alessandro. BRASIL, Beatriz Silveira. **Investigação Cibernética à Luz do Marco Civil da Internet.** Editora: Brasport. 2016.

BARRETO; CASTELLI; WENDT, **Investigação Digital em Fontes Abertas**. 2ª ed. Rio de Janeiro: Brasport, 2017.

BARROS, Alberto Felipe Friderichs. **Crimes na Internet**. Instituto Federal Santa Catarina. S/d. Disponível em: https://albertofelipeblog.files.wordpress.com/2016/07/crimes-na-internet.pdf. Acesso em 12 de novembro de 2019.

BASSO, Maristela; ALMEIDA, Guilherme Assis. 2010. **É preciso difundir mentalidade digital nas empresas.** Disponível em: https://repositorio.usp.br/item/002184406. Acesso em 30 de novembro de 2019.

BBC News. 2014. **Um Ano Depois, Pai Relata Suicídio da Filha Após Cyberbullying.** Disponível em: https://www.bbc.com/portuguese/noticias/2014/04/140403_bullying_suicidio_canada_fl#:~:text=O%20caso%20da%20jovem%20Rehtaeh,punir%20este%20tipo%20de%20crime. Acesso em 29 de maio de 2020.

BBC. **Deep Web: O Comércio Criminoso que Prospera Nas Áreas Ocultas da Internet.** 2016. Disponível em: https://www.bbc.com/portuguese/geral-36920676. Acesso em: 03 de fevereiro de 2020.

BRAMBILLA, Júlia Fernandes. **Falsa Identidade nas Redes Sociais.** 2020. Disponível em: https://juliafbrambilla.jusbrasil.com.br/artigos/831606853/falsa-identidade-nas-redes-sociais?ref=feed. Acesso em 04 de maio de 2020.

CÓDIGO PENAL BRASILEIRO. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848. Acesso em 25 de maio de 2020.

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA BRASILEIRA. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em 21 de dezembro de 2019.

CONVENÇÃO DE BUDAPESTE. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 10 de maio de 2010.

COSTA, Juliane. **Top 10: Os Maiores Hackers da História.** 2011. Disponível em: https://www.techtudo.com.br/noticias/noticia/2011/06/top-10-os-maiores-hackers-da-historia.html. Acesso em: 12 de maio de 2020.

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

CROCE, Delton; JÚNIOR, Croce Delton. **Manual de Medicina Legal.** 2004. 5ª Ed. São Paulo. Editora Saraiva.

D'URSO, Filizzola Luiz. **Em Tempos de Cibercrimes.** 2019. Disponível em: https://www.migalhas.com.br/dePeso/16,MI310551,31047-Em+tempos+de+cibercrimes. Acesso em 11 de novembro de 2019.

DAMÁSIO DE JESUS apud ARAS, **Vladmir. Crimes de informática: Uma nova criminalidade.** Disponível em https://www.google.com/search?q=o+que+significa+apud+em+uma+cita%C3%A7%C3%A3o&oq=o+que+significa+apud+em&aqs=chrome.1.69i57j0l7.7890j1j4&sourceid=chrome&ie=UTF-8. Acesso em 01 de dezembro de 2014.

DECRETO Nº 8.539/15. 8 de outubro de 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/d8539.htm. Acesso em 23 de janeiro de 2020.

DIAS, Camila Barreto Andrade. **CRIMES VIRTUAIS: as inovações jurídicas decorrentes da evolução tecnológica que atingem a produção de provas no processo penal.** Disponível em: http://repositorio.uniceub.br/bitstream/235/5977/1/20888860.pdf. Acesso em: 01 de março de 2020.

DINIZ, Carine Silva**. Os crimes virtuais: as condutas delituosas perpetradas através da Internet**. 2006. Disponível em: https://aplicacao.mpmg.mp.br/xmlui/bitstream/handle/123456789/970/3.4.4%20Os%20Crimes%20Virtuais.pdf?sequence=1. Acesso em: 15 maio 2020.

DORIGON, Alessandro e SOARES, Renan Vínicius de Oliveira. **Crimes Cibernéticos: Dificuldades Investigativas na Obtenção de Indícios de Autoria e Prova da Materialidade.** 2018. Disponível em: https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade/2. Acesso em 28 de dezembro de 2019.

EMAG, Escola de Magistratura da 3ª Região. Diretor: Desembargador Federal Carlos Muta. 2017. São Paulo**. Investigação e Prova nos Crimes Cibernéticos.** Disponível em: https://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em 24 de maio de 2020.

FAGUNDES, Eduardo. **Como Funciona a Internet?** S/D. Disponível em: https://efagundes.com/artigos/como-funciona-a-internet/. Acesso em 31 de janeiro 2020.

FEDERAL BUREAU OF INVESTIGATION. Internet Crime Report. 2015. Disponível em: https://pdf.ic3.gov/2015_IC3Report.pdf. Acesso em 19 de maio de 2020.

FERREIRA, Ivette Senise. **A Criminalidade Informática. Direito & Internet – Aspetos Jurídicos Relevantes.** Editora Edipro, 2011.

FILHO, Eduardo Tomas, **Marco Civil da Internet: uma lei sem conteúdo normativo**. 2016. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269 Acesso em 26 de maio de 2020.

FOGLIATTO, Juliana. **Os Crimes Cibernéticos e os Meios que a Polícia Utiliza Para a Identificação dos Criminosos**. 2019. Disponível em: https://www.conjur.com.br/2011-fev-23/possivel-verificar-autenticidade-prova-documental-eletronica. Acesso em 19 de janeiro de 2020.

FRAGOMENI, Ana Helena. **Dicionário Enciclopédico de Informática.** Vol.I. Rio de Janeiro: Campus, 1987.

GIACCHETTA, André Zonaro e MENEGUETTI, Gabrielle Pamela. **Privacidade do Usuário vs. Investigação Criminal – A Extensão e Alcance do Artigo 10, § 3º, do Marco Civil da Internet.** Disponível em: https://www.migalhas.com.br/depeso/220995/privacidade-do-usuario-vs-investigacao-criminal-a-extensao-e-alcance-do-artigo-10-3-do-marco-civil-da-internet. Acesso em 35 de janeiro de 2020.

GIMENES, Emanuel Alberto Sperandio Garcia. 2013. **Crimes Virtuais.** Disponível

em:http://www.revistadoutrina.trf4.jus.br/index.htm?http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html. Acesso em: 14 de novembro de 2019.

GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet.** Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.
HOESCHL, Hugo Cesar. **Elementos de Direito Digital.** ANO. Disponível em: https://egov.ufsc.br/portal/sites/default/files/elementosdedireitodigital_0.pdf. Acesso em 21 de dezembro de 2019.

HOLTHAUSEN, Fábio Zabot. **Inversão do ônus da prova nas relações de consumo: momento processual**. Unisul, 2006.

JUSTIFICANDO. **Crimes Digitais: Quais São, Quais Leis os Definem e Como Denunciar.** Disponível em: http://www.justificando.com/2018/06/25/crimes-digitais-quais-sao-quais-leis-os-definem-e-como-denunciar/. Acesso em: 23 de agosto de 2019.

KAMINSKI, Omar. Internet Legal. **O direito na tecnologia da informação.** 1ª ed. Curitiba: Juruá, 2003.

LEI DO MARCO CIVIL NA INTERNET, LEI Nº 12.965/2014 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 19 de maio de 2020.

LEI DO SOFTWARE. LEI N° 9.609/98. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9609.htm. Acesso em 21 de maio 2020.

LEI DOS CIBERCRIMES LEI N° 12.737/12. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 24 de maio de 2020.

LEI DOS DIREITOS AUTORAIS. LEI N 9.610/98. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Acesso em 23 de maio de 2020.

LEI Nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação dos crimes cometidos eletronicamente. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 24 de agosto de 2019.

LEMOS, André L. M. **Estruturas antropológicas do ciberespaço. Textos de Cultura e Comunicação**. Disponível em: http://www.facom.ufba.br/pesq/cyber/lemos/estrcy1.html. Acesso em 16 fevereiro de 2020.

LINS, Luis Fernando; VILLELA, Felipe; AZEVEDO, Vitor de. 2018. **Deep Weeb**. Disponível em: https://www.gta.ufrj.br/ensino/eel878/redes1-2018-1/trabalhos-vf/deepweb/historia.html. 30 de março de 2020.

LOCAWEB. **Você Sabe o que é e Como Funciona um Data Center**. 2014. Disponível em: https://blog.locaweb.com.br/geral/voce-sabe-o-que-e-e-como-

funciona-um-data-center/. Acesso em: 14 de novembro de 2019.

MAMFORD, Lewis. 1922. **The Story Of Utopias.**

MARQUES, Pablo. **Brasil é o 2° país com mais casos de bullying virtual contra crianças**. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/brasil-e-o-2-pais-com-mais-casos-debullying-virtual-contra-criancas-11072018. R7 notícias. Acesso em 20 de maio de 2020.

MARTINELLI, João Paulo Orsini. **Aspectos relevantes da criminalidade na Internet.** Disponível em http://jus2.uol.com.br/doutrina/texto.asp?id=1829. Acesso em 28 de maio de 2020.

MARTINS, Geiza. **O Que é o Marco Civil da Internet.** 2015. Disponível em: https://super.abril.com.br/mundo-estranho/o-que-e-o-marco-civil-da-internet/ Acesso em 19 de dezembro de 2019.

MASSON, Cleber. **Código Penal Comentado**. 2. ed. rev., atual. e ampl. - Rio de Janeiro: Forense; São Paulo: MÉTODO, 2014.

MEDIDA PROVISÓRIA. Nº 2.200/01. 27 de julho de 2001. Disponível em: http://planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-1.htm. Acesso em 24 de janeiro de 2020.

MELO, Adriana Zawada. **Crimes Cibernéticos. Manual Prático de Investigação.** 2006. Disponível em: http://tmp.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1tica-versaofinal.pdf. Acesso em 07 de março de 2020.

MELO, Guilherme Tomé; SOUZA, João Pedro Rosa de. 2019. **Lucro Indireto Online por Violação de Direitos Autorais.** Disponível em: https://jus.com.br/artigos/74348/lucro-indireto-online-por-violacao-de-direitos-autorais. Acesso em 04 de maio de 2020.

MELO, Sagmeister Isadora; GREGÓRIO, João Paulo. **A Relação Entre o Compartilhamento dos Dados Bancários e Fiscais do Contribuinte Obtidos pela Receita Federal sem Autorização Judicial e a Lei Geral de Proteção de Dados**. 2020. Disponível em: https://www.migalhas.com.br/depeso/323510/a-relacao-entre-o-compartilhamento-dos-dados-bancarios-e-fiscais-do-contribuinte-obtidos-pela-receita-federal-sem-autorizacao-judicial-e-a-lei-geral-de-protecao-de-dados. Acesso em 10 de maio de 2020.

MINISTÉRIO PÚBLICO FEDERAL, 2ª CÂMARA DE COORDENAÇÃO E REVISÃO, **Crimes Cibernéticos, Coletânia de Artigos**, vol. 3, 2018. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes. Acesso em 22 de maio de 2020.

MONTEIRO, Neto. **Aspectos Constitucionais e Legais do Crime Eletrônico**. 2008. Disponível em: http://www.dominiopublico.gov.br/download/teste/arqs/cp055676.pdf. Acesso em 11 de novembro de 2019.

MONTEIRO, Neto. **Aspectos Constitucionais e Legais do Crime Eletrônico.** Fortaleza, 2008.

NETO, João Araújo Monteiro. 2003. **Crimes Informáticos uma Abordagem Dinâmica ao Direito Penal Informático.** Disponível em: https://periodicos.unifor.br/rpen/article/view/736/1598. Acesso em: 07 de setembro de 2019.

NORTHFLEET, Ellen Gracie. **O Marco Civil da Internet sob o Prisma da Constitucionalidade – Parte I**, 2020. Disponível em: https://www.conjur.com.br/2020-fev-19/ellen-gracie-constitucionalidade-marco-civil-internet. Acesso em 18 de maio de 2020.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. Rio de Janeiro, Editora Forense, 11 Ed., 2015.

NUCCI, Guilherme de Souza. **Provas no processo penal.** São Paulo: Revista dos Tribunais, 2009.

PAYÃO, Felipe. **As Operadoras Estão Esfolando Nosso Dinheiro.** 2017. Disponível em: https://www.tecmundo.com.br/seguranca/123670-operadoras-esfolando-nosso-dinheiro-diz-hacker-capitao-crunch.htm. Acesso em: 23 de fevereiro de 2020.

PEREIRA, Leonardo. **Deep Web: O que é, Como Entrar e o Que Acontece na Parte Sombria da Internet.** 2019. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/deep-web-saiba-o-que-acontece-na-parte-obscura-da-internet/31120. Acesso em: 18 de setembro de 2019.

PEREIRA, Murilo Cezar Antonini. **Golpes Patrimoniais Envolvendo Cartões Bancários Clonados.** 2013. Disponível em: https://jus.com.br/artigos/26261/golpes-patrimoniais-envolvendo-cartoes-bancarios-clonados. Acesso em 20 de maio de 2020.

PROCURADORIA GERAL DA REPÚBLICA. **MPF defende adesão do Brasil à Convenção Internacional para Combate a Crimes Cibernéticos.** 2018. Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/mpf-defende-adesao-do-brasil-a-convencao-internacional-para-combate-a-crimes-ciberneticos. Acesso em 10 de maio de 2020.

RAMOS, Edí Patrícia. Sem data. **Vivendo Uma Nova Era: a Tecnologia e o Homem, Ambos Integrantes de Uma Sociedade que Preogride Rumo ao Desenvolvimento**. Disponível em: http://www2.seduc.mt.gov.br/-/vivendo-uma-nova-era-a-tecnologia-e-o-homem-ambos-integrantes-de-uma-sociedade-que-progride-rumo-ao-desenvolvimen-1. Acesso em 15 de dezembro de 2019.

REPORT, Security. **Brasil é o 2º País que mais Perdeu Dinheiro com Cibercrimes em 2017**. Disponível em: http://www.securityreport.com.br/destaques/brasil-e-o-2o-pais-que-mais-perdeu-dinheiro-com-cibercrimes-em-2017/#.XdNzCldKjIU. Acesso em 12 de novembro de 2019.

ROHR, Altieres. **Deep Web, O Que é e Como Funciona.** 2018**.** Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/deep-web-o-que-e-e-como-funciona-g1-explica.html. Acesso em: 16 de janeiro de 2020.

ROMANO, Raquel Alexandra**. Documento Eletrônico Pode Ser Utilizado Como Prova.** 2011. Disponível em: https://www.conjur.com.br/2011-fev-23/possivel-verificar-autenticidade-prova-documental-eletronica. Acesso em 14 de fevereiro de 2020.

ROMANO, Rogério Tadeus. 2014. **Furto de Fios Telefônicos.** Disponível em: https://jus.com.br/artigos/32600/furto-de-fios-telefonicos. Acesso em 20 de maio de 2020.

ROMANO, Tadeu Rogério. **Convenção de Budapeste e Cibercrimes.** 2019. Disponível em: https://jus.com.br/artigos/72969/convencao-de-budapeste-e-cibercrimes. Acesso em 10 de maio de 2020.

ROSA, Guimarães. **Grande Sertão: Veredas.** 1956. Editora: José Olympio.

ROSA, Fabrízio. **Crimes da informática.** 1ª Ed. Campinas: Bookseller, 2008.

ROSA, Fabrizio**. Crimes da Informática**. 2ª Ed. Campinas. Bookseller 2006.

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal.** São Paulo: Memória Jurídica, 2009.

SAFERNET BRASIL. **Associação Civil de Direito Privado de Proteção dos Direitos Humanos na Sociedade da Informação.** Disponível em: http://www.safernet.org.br. Acesso em: 14 de setembro de 2019.

SAFERNET BRASIL. **Delegacias Cibercrimes**. Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em 08 de junho de 2020.

SARTÓRIO, Giovanna. Crimes Virtuais: **Entenda o que são e Saiba Como recorrer.** Disponível em: http://www.joaquimnabuco.edu.br/noticias/crimes-virtuais-entenda-o-que-sao-e-saiba-como-recorrer. Acesso em 13 de novembro de 2019.

SCHREINER, Priscila Costa, OLIVEIRA; Neide M. C. Cardoso; BLAGITZ Melissa; MAGNO, Helder Magno; PIZA, Daniela Sueira Toledo; ILHA, Ângelo e FALCÃO JR, Alfredo Carlos. **O Combate aos Crimes Cibernéticos no Brasil e o Papel Desenvolvido Pelo MPF**. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/dados-da-atuacao/eventos-2/eventos-internacionais/crimesciberneticos.odp. Acesso em 04 de março de 2020.

SCOFIELD, Bruno Lauar. 2015. **Análise dos Tipos Penais: Art. 184 a 207 do Código Penal.** Disponível em: https://brunoscofield.jusbrasil.com.br/artigos/192928216/analise-dos-tipos-penais-art-184-a-207-do-codigo-penal. Acesso em 02 de junho de 2020.

SILVA, André Luiz Neto da. **Deep Web, o Inferno é Aqui e Agora.** 2015. Disponível

em: https://www.dm.jor.br/opiniao/2015/03/deep-web-o-inferno-e-aqui-e-agora/. Acesso em 27 de maio de 2020.

SILVA, Gama Reny. **Crimes da Informática**. 2000. Disponível em: http://underpop.online.fr/d/direito/crimes-da-informatica.pdf. Acesso em: 26 de agosto de 2019.

SILVA, Rosane Leal e VERONESE, Josiane Rose Petry. **Os Crimes Sexuais Contra Crianças e Adolescentes no Ambiente Virtual.** 2009. Disponível em: https://ambitojuridico.com.br/edicoes/revista-69/os-crimes-sexuais-contra-criancas-e-adolescentes-no-ambiente-virtual/. Acesso em: 21 de setembro de 2019.

SILVA, Werner Leonardo. Folha de São Paulo. **Internet Foi Criada em 1969 com o Nome de "Arpanet" nos EUA.** 2001. Disponível em: https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml. Acesso em 11 de novembro. 2019.

SOUZA, Júlio Cesar. **Investigação Criminal Pela Polícia Militar e Sua Inconstitucionalidade.** 2012. Editora: Clube de Autores.
Supremo Tribunal Federal. **Notícias STF**. 2019. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=431123&caixaBusca=N. Acesso em 12 de abril de 2020.

TAVARES, Adriano Lopes e REIS, Rafael rocha. **Crimes de Informática.** Disponível em:http://revistas2.unievangelica.edu.br/index.php/revistajuridica/article/view/1070/1012. Acesso em: 15 de setembro de 2019.

TEFFÉ, Chiara Spadaccini; SOUZA, Carlos Affonso. 2017**. Responsabilidade dos Provedores Por Conteúdos de Terceiros na Internet.** Disponível em: https://www.conjur.com.br/2017-jan-23/responsabilidade-provedor-conteudo-terceiro-internet. Acesso em 17 de maio de 2020.

TEIXEIRA, Ronaldo de Quadros. **Os Crimes Cibernéticos no Cenário Nacional.** Escola superior aberta do Brasil – ESAB, 2013 (Curso de pós-graduação lato sensu em engenharia de sistemas).

TEIXEIRA, Tarcísio, **Direito Eletrônico**. 4º Ed. São Paulo: Joarez de Oliveira, 2007.

TEIXEIRA, Tarcisio. **Curso de Direito e Processo Eletrônico, Doutrina, Jurisprudência e prática.** São Paulo. Editora: Saraiva. 2015. 3° Edição.

VADE MECUM. 2020. 29º Ed. Editora Saraiva. Vários autores.

VELASCO, Ariane. **Conheça os 10 Hackers Mais Famosos da História da Internet.** 2019. Disponível em: https://canaltech.com.br/hacker/conheca-os-10-hackers-mais-famosos-da-historia-da -internet-155459/. Acesso em 22 de maio de 2020.

VENÂNCIO, Pedro Dias. **Investigação e Meios de Prova na Criminalidade** Informática. Disponível em: https://www.verbojuridico.net/doutrina/tecnologia/meiosprovacriminalidadeinformatica.pdf Acesso em: 20 de setembro de 2019.

VIANA, Marco Túlio; apud, CARNEIRO, Adeneele Garcia. 2003. **Fundamentos de direito penal informático. Do acesso não autorizado a sistemas computacionais.** Rio de Janeiro, Editora Forense.

VILAS BOAS, Aline Hamdan e MACIEL, Álvaro dos Santos. II CONINTER-CONGRESSO INTERNACIONAL INTERDISCIPLINAR EM SOCIAIS E HUMANIDADES**. Os Dilemas do Direito ao Acesso A Informação e A Defesa Do Direito Autoral de Obra Literária Na Internet**. 2013. (Congresso).

WENDT, Emerson e NOGUEIRA JORGE, Higor Vinicius Nogueira. 2017. Editora Braspot. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação** – 2º Edição.

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

WENDT, Emerson e NOGUEIRA JORGE, Higor Vinicius. **Crimes Cibernéticos, Ameaças e Procedimentos de Investigação.** 1ª Ed. São Paulo, Editora Brasport, 2012.

WENDT, Emerson e NOGUEIRA JORGE, Higor Vinicius. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação.** 2ª Ed. São Paulo: Editora Brasport, 2012.

ZANIOLO, Pedro Augusto. **Crimes Modernos, o Impacto da Tecnologia no Direito.** São Paulo. Editora: Jurá. 2012. 2ª Edição.