UNIVERSIDADE DE CAXIAS DO SUL
CAMPUS UNIVERSITÁRIO DA REGIÃO DAS HORTÊNSIAS
ÁREA DO CONHECIMENTO DE CIÊNCIAS JURÍDICAS
BACHARELADO EM DIREITO

DEIVID BRUSCH ETTER

CRIMES CIBERNÉTICOS, INVESTIGAÇÃO E O DESAFIO DA OBTENÇÃO DE PROVAS

CANELA, RS
2021

DEIVID BRUSCH ETTER

CRIMES CIBERNÉTICOS, INVESTIGAÇÃO E O DESAFIO DA OBTENÇÃO DE PROVAS

Trabalho de conclusão de curso de graduação da Universidade de Caxias do Sul – UCS, como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientador: Mestre Róbson de Vargas

CANELA, RS

2021

DEIVID BRUSCH ETTER

CRIMES CIBERNÉTICOS, INVESTIGAÇÃO E O DESAFIO DA OBTENÇÃO DE PROVAS

Trabalho de conclusão de curso de graduação da Universidade de Caxias do Sul – UCS, como requisito parcial para a obtenção do título de Bacharel em Direito.

Aprovado em: 06/07/2021

Banca Examinadora

_____

Prof. MSc. Róbson de Vargas

Universidade de Caxias do Sul - UCS

_____

Bruno Silveira Rigon

Universidade de Caxias do Sul - UCS

_____

Pedro Francisco Fernandes Pomnitz

Universidade de Caxias do Sul - UCS

Dedico este Trabalho de Conclusão de Curso primeiramente aos meus pais, base de todas as minhas conquistas, os quais me incentivaram e proveram o necessário para a conclusão desta etapa. À minha esposa, companheira, amiga, parceira, que sempre esteve ao meu lado, em todos os momentos.

AGRADECIMENTOS

Agradeço primeiramente à Deus, por ter me permitido chegar até aqui e por ter estado comigo nos momentos mais difíceis desta caminhada.

Agradeço imensamente aos profissionais da área do Direito aos quais tive o prazer de conhecer e obter como exemplos a serem seguidos na vida pessoal e profissional.

Agradeço aos professores que com seus ensinamentos e sabedoria puderam contribuir para que esse momento ocorresse de forma satisfatória.

RESUMO

O presente trabalho de conclusão de curso traz à luz a análise a respeito das práticas investigativas e o desafio na obtenção de provas nos crimes cibernéticos. Quando se fala em crimes cibernéticos deve-se conhecer algumas Leis que servem para nortear o tratamento dos agentes no que tange à investigação e suas limitações. O conceito histórico da internet, seu surgimento, as camadas mais profundas não disponíveis aos usuários comuns, conhecidas como e *dark web* e a decorrência da prática dos mais variados tipos e crimes são tratados no decorrer da presente pesquisa. Foram expostos pontos das Leis conhecidas como Lei Carolina Dieckmann, Marco Civil da Internet, Lei Geral de Proteção de Dados, Lei da Política Nacional de Informática, dentre outras. Ao final da pesquisa são tratados os temas de pedofilia e pornografia infantil, assuntos que mais têm repercussão mundial, assim como outros crimes praticados principalmente nas camadas da *deep web* e *dark web*. Este assunto traz à tona uma das operações realizadas em âmbito Nacional e que repercutiu mundialmente, chamada Operação Darknet, na qual foram cumpridos 70 mandados de busca e apreensão em 17 Estados.

Palavras-chave: Crimes Cibernéticos, Cibercrimes, Perícia Digital Forense, Marco Civil da Internet, Lei Carolina Dieckmann.

ABSTRACT

The present work of course completion brings to light the analysis of investigative practices and the challenge of obtaining evidence in cybercrime. When talking about cybercrimes, it is necessary to know some laws that serve to guide the treatment of agents with regard to the investigation and its limitations. The historical concept of the internet, its emergence, the deeper layers not available to common users, known as deep web and dark web and the result of the practice of the most varied types and crimes are dealt with in the course of this research. Points of the Laws known as Carolina Dieckmann Law, Marco Civil da Internet, General Data Protection Law, Law of National Informatics Policy, among others, were exposed. At the end of the research, the themes of pedophilia and child pornography are dealt with, subjects that have the greatest worldwide repercussion, as well as other crimes committed mainly in the layers of the deep web and dark web. This subject brings to light one of the operations carried out at the national level and which had repercussions worldwide, called Operation Darknet, in which 70 search and seizure warrants were carried out in 17 states.

Keywords: Cybercrimes, Forensic Digital Expertise, Civil Mark of Internet, Carolina Dieckmann Law.

LISTA DE SIGLAS

IP	Internet Protocol
ARPANet	Advanced Research Projects Agency Network
MAC	Media Access Control
VPN	Virtual Private Network
MPF	Ministério Público Federal

SUMÁRIO

1 INTRODUÇÃO 9

2 CIBERNÉTICA E OS CIBERCRIMES 11

2.1 INTERNET, *DEEP WEB* E *DARK WEB* 11

2.2 TIPIFICAÇÃO DOS CIBERCRIMES 15

3 AS PRÁTICAS INVESTIGATIVAS APLICADAS AOS CIBERCRIMES 19

3.1 FORMAS DE INVESTIGAÇÃO E SUAS CARACTERÍSTICAS 19

3.2 PERÍCIA INFORMÁTICA 22

3.3 DIFICULDADES NA INVESTIGAÇÃO CRIMINAL 25

4 A PRODUÇÃO DE PROVAS DOS CRIMES CIBERNÉTICOS 29

4.1 A PROBLEMÁTICA POR TRÁS DA COMPROVAÇÃO DE AUTORIA 29

4.2 PEDOFILIA E PORNOGRAFIA INFANTIL 32

4.3 OPERAÇÃO DARKNET 36

5 CONCLUSÃO 42

REFERÊNCIAS 44

1 INTRODUÇÃO

O presente trabalho tem por finalidade demonstrar os crimes cibernéticos de forma objetiva quanto à sua prática, bem como identificar as leis existentes em âmbito Nacional à fim de combatê-los, da mesma forma que será possível vislumbrar o conceito histórico e o surgimento da internet e suas particularidades quanto à navegação e seus lugares.

Foi realizada uma pesquisa através de revisões bibliográficas nas áreas de Direito Penal, conhecimentos em informática, estatísticas e legislação para crimes informáticos, sendo aplicada a metodologia bibliográfica, sendo examinados livros, artigos, manuais, informações extraídas de sites jurídicos e da legislação pertinente.

Buscou-se primeiramente, analisar historicamente o conceito e o princípio da internet, assim como suas camadas de difícil acesso como a *deep web* e a *dark web*, afim de demonstrar as situações em que ocorrem estes tipos de crimes. Desta forma nota-se o empenho dos investigadores e equipe de perícia na busca por vestígios e autoria destes delitos.

Com o surgimento de Leis específicas ao combate dos crimes cibernéticos, houve um avanço considerável, porém insuficiente, no que diz respeito à tipificação e configuração destes delitos. Se percebe a tentativa de evitar os crimes cibernéticos por meio da Lei Geral de Proteção de Dados, visto que o objetivo principal é garantir o uso e coleta de dados de forma consentida, bem como o direito de o usuário visualizar, corrigir e excluir esses dados.

De tal forma, percebe-se a dificuldade que a polícia encontra em determinadas circunstâncias, uma vez que o criminoso se encontra quase sempre em vantagem ao Estado. Nota-se que por muitas vezes é penoso o processo de criminalização aos infratores devida à lentidão do sistema judiciário no que diz respeito à expedição de mandado judicial e provimento na materialidade das provas.

Dividida em três capítulos, a pesquisa buscou demonstrar inicialmente ao leitor o conceito histórico desses tipos de crime tão presentes atualmente em nossa sociedade e quais as características mais relevantes encontradas na forma de atuação dos criminosos. Procurou-se demonstrar também, a forma como os órgãos públicos agem na investigação e combate aos delitos praticados por meio da internet. Não se pode deixar de lembrar que atualmente estes órgãos buscam traçar novos meios de encontrar vestígios deixados pelos criminosos, assim como devem

ser atualizados os meios de investigação, da mesma forma que evolui o sistema criminal.

Por fim, busca-se compreender e elucidar as ferramentas presentes para o processo investigativo em um meio volátil que é a internet. As possibilidades de infração e facilidade capazes de contaminar provas tornam este cenário muito suscetível a erros e assim, comprometendo a persecução penal.

Desta forma, busca-se analisar historicamente e socialmente como se dá o processo investigativo e a dificuldade e materialização de provas presentes nos crimes cibernéticos. Crimes que são presentes em todos os lugares e que desafiam os órgãos públicos em como agir, de forma precisa e dentro da Lei.

2 CIBERNÉTICA E OS CIBERCRIMES

2.1 INTERNET, *DEEP WEB* E *DARK WEB*

O conhecimento histórico da internet permite enxergar que a evolução da rede mundial de computadores foi estabelecida a partir dos experimentos iniciais em rede. Com o aumento gradativo dos primeiros computadores, nos anos 1950, primeiramente com fins profissionais e científicos, se percebeu a necessidade de uma forma de comunicação e interação entre um ou mais computadores.

O surgimento desta rede se deu pela necessidade de um meio de comunicação e de transmissão de informações entre os militares em determinadas ocasiões, por exemplo as situações críticas como um ambiente de guerra. Segundo Lígia Maria Ribeiro[1], o início das pesquisas surgiu no final dos anos 1960, onde o Departamento de Defesa dos EUA se interessou pelas redes de computadores, sendo então financiadas investigações para construção e utilização desta tecnologia, surgindo então a ARPANet.

Entre os anos 1980 e 1990, a capacidade de comunicação foi expandida entre indivíduos devido ao aumento de computadores conectados. Os militares, pioneiros nessa tecnologia, por medo de um possível ataque, não perderiam a conexão, pois ao invés de existir uma central, teriam as comunicações e informações interligadas por meio de computadores em uma rede. Francilaine Munhoz Moraes[2] destaca que com base nesses dados é possível observar que a internet é descentralizada desde sua criação.

Conforme Bernardo Felipe Estellita Lins[3], apenas a partir dos anos 1994 que o público em geral teve acesso à internet de forma aberta, antes disto, o uso deste serviço estava limitado apenas ao governo e às instituições de ensino superior.

Sob o amparo conceitual da internet e cibernética, aos olhos técnicos, deve-se atentar ao conjunto de ideias que evoluem de um contexto sempre presente na

---

1 RIBEIRO, Lígia Maria. **A História da Internet**. 1998. Disponível em: https://paginas.fe.up.pt/~mgi97018/historia.html. Acesso em: 05 mar. 2021.

2 MORAES, Francilaine Munhoz. **Discurso jornalístico on-line: a perspectiva crítica da narratividade**. Dissertação de Mestrado. Programa de Pós-Graduação em Comunicação da Universidade de Brasília, 2004. p. 34.

3 LINS, Bernardo Felipe Estellita. **A Evolução da Internet: Uma Perspectiva Histórica.** Cadernos ASLEGIS. Edição 48. 2013. p. 13.

sociedade, Pierre Lévy[4] vê uma forma de comunicação nova através da rede ou ciberespaço, de interconectar diferentes pessoas de diferentes culturas por meio da tecnologia. Acredita que através desta ferramenta surge uma nova forma de ver e entender o universo da comunicação e interação em ambiente global.

Com o uso da internet diariamente mais amplo para a realização de variadas atividades, através da interação entre vários sistemas e equipamentos. Para Miguel Maurício Isoni[5] é um fenômeno que necessita de extrema atenção por parte dos governos, empresas, instituições de pesquisa e universidades, uma vez que, relacionado a este crescimento, surgem as ameaças cibernéticas. Estas ameaças têm por objetivo o roubo de informações confidenciais e invasões a computadores através de acessos, que muitas vezes se beneficiam do anonimato que a internet propicia.

Com a evolução constante e disseminada da internet, surgiram ferramentas capazes de separar o que é a internet visível para todos, conhecida como S*urface Web*, ou internet superficial, ou seja, é aquela em que todos têm acesso, sem restrição de uso, e, as camadas abaixo da superfície, onde geralmente acontecem os mais variados tipos de crimes cibernéticos, que são a *deep web* ou internet profunda e a *dark web* ou internet obscura. De acordo com Fernanda Viero da Silva[6], as formas de acesso se dão somente com programas especializados em Redes Anônimas, procurados principalmente por quase não existir rastreamento. A ideia principal destes meios é o anonimato.

Comumente associada às práticas de crimes e atos ilícitos, a *deep web* é uma ferramenta que se difunde no nosso dia-a-dia, mesmo que indiretamente. Silvana Drumond Monteiro[7] entende que como o acesso a esta área da internet não é indexada, ou seja, não está interligada a buscadores de pesquisa como o Google, Yahoo, Bing, indiretamente ao navegarmos em sites da internet superficial com

---

[4] LÉVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. — São Paulo: Ed. 34, 1999. p. 116.

[5] ISONI, Miguel Maurício; VIDOTTI, Silvana Aparecida Borsetti Gregório. **E-crime em Ambientes Digitais Informacionais da Internet**. DataGramaZero – Revista de Ciência da Informação, v. 8, n. 2, 2007. p. 11.

[6] SILVA, Fernanda Viero da; FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. **Deep Web e Dark Web: Implicações Sociais e Repercussões Jurídicas**. Revista Eletrônica Direito e Sociedade, Canoas, v. 8, n. 2, 2020. p. 228-229.

[7] VIGNOLI, Richele Grenge; MONTEIRO, Silvana Drumond. **Deep Web *e* Dark Web: Similaridades e Dissiparidades no Contexto da Ciência da Informação**. *Transinformação*, v. 32, e190052, 2020. Disponível em: https://doi.org/10.1590/2318-0889202032e190052. Acesso em 12 abr. 2021.

direcionamento para logins com senhas e informações “ocultas” a outros usuários, estamos conectados em parte na *deep web*.

Em se tratando de *deep web*, no que tange aos filtros e à segurança, por não se enquadrar em informações que respeitem as diretrizes e normas impostas pela Lei do Marco Civil da Internet, no quesito de princípios e direitos, os conteúdos dispostos na *deep web* nem sempre são confiáveis e muitas vezes devem ser questionados, assim como há diversas páginas com muita informação proveitosa. Indo mais além, nas camadas da internet, se encontra o lado obscuro da Web, a não tão conhecida *dark web*. Segundo Braz Batista Vas[8], para o acesso à esta rede, se faz necessário o uso de ferramentas específicas, pois pelo fato de se valer de total anonimato e sem supervisão de conteúdo, torna-se ambiente propício para delitos.

Segundo o Centro de Recursos da renomada empresa de segurança cibernética Kaspersky,[9] a *deep web* é definida como uma camada da internet onde se encontram cerca de 90% de todos os sites existentes. É comumente usada a analogia de um iceberg, onde a maior parte do conteúdo existente se encontra “submerso na água”. O termo referido como “deep web” faz menção à todas páginas da Web que ficam invisíveis a mecanismos de busca, tornando estas páginas ocultas para proteção de informações e privacidade de usuários.

A *dark web* é estabelecida a partir do momento em que é necessário utilizar proxy para o acesso, onde possivelmente será encontrado material ilegal, impróprio e pesado e que a web não é indexada à risca. Silvana Drumond Monteiro[10] observa que os mecanismos de busca investem boa parte de recursos para um maior alcance de indexação de buscas em seus algoritmos, trazendo assim parte de arquivos que antes eram considerados não indexáveis à superfície, tornando-os “visíveis” aos sistemas de busca.

Richele Vignoli[11] em seu artigo exemplifica as individualidades da *deep web* e *dark web*, muitas vezes considerados demasiadamente parecidos, eles se diferem

---

8 NOGUEIRA, Cipriano Cássio; VAS, Braz Batista. **Percepções Sobre Ciberespaço e Territorialidade Digital: Estudo Exploratório com Foco em Aspectos Socioculturais Presentes Na Deep Web e Dark Web.** Revista Observatório, v. 5, n. 6, 2019, p. 22.

9 KASPERSKY. **O que é a Deep Web e a Dark Web?** Disponível em: www.kaspersky.com.br/resource-center/threats/deep-web. Acesso em: 27 mar. 2021.

10 MONTEIRO, Silvana Drumond; FIDENCIO, Marcos Vinicius. **As Dobras Semióticas do Ciberespaço: Da Web Visível à Invisível.** Transinformação, vol. 25, núm. 1, Pontifícia Universidade Católica de Campinas, Brasil. 2013. p. 37.

11 VIGNOLI; MONTEIRO, 2020, op. cit.

por características específicas. Segundo a autora[12], a *deep web* ainda é pouco aprofundada pelos pesquisadores, porém é considerado um campo repleto de desconhecimentos e prejulgamentos em relação ao seu conteúdo. Também define a autora, que o termo traduzido como "Rede Profunda" obteve essa definição em meados dos anos de 1994 por Jill Ellsworth, que também utilizava o termo Invisible Web ou Rede Invisível.

Vignoli[13] explica que, a *deep web* representa uma camada mais exposta do ciberespaço, e que, em sua maioria são conteúdos não recuperáveis, o que pode ocasionar um excesso de conteúdos não transitáveis, portanto, inacessíveis em alguns locais do ciberespaço.

A autora[14] ressalta, ainda, os motivos que fundamentam a ineficiência do buscador em relação a *deep web*, e por quais motivos a "Invisible Web" possui sites invisíveis para seus usuários. Ocorre que, segundo Vignoli, sites com senhas, com firewall, com metadado *noindex*, que não permite recuperação pelos buscadores, páginas dinâmicas, tarifas de acesso, entre outros, podem justificar a existência de certa dificuldade em acessar alguns sites relacionados a *deep web*.

Em relação à sua dimensão, a autora[15] traz dados sobre a compreensão territorial da *deep web* em comparação com a superfície. O estudo mais recente relata que as informações públicas são 400 a 550 vezes maior que a da superfície, a “Visible Web” teria 1 bilhão de documentos expostos enquanto a *deep web* teria 550 bilhões.

Em contrapartida, para Monteiro[16], utilizar o termo Web Invisível não seria correto, pois a invisibilidade é apenas questão tecnológica ou até mesmo política de indexação de links aos motores de busca. Segundo Monteiro, ao categorizar os mecanismos de busca deste “continente escuro” foi possível descobrir uma sobra, uma Web maior e oculta que mostra apenas uma pequena, porém, de grande extensão que é o ciberespaço.

Conforme a autora[17], a *dark web* surgiu como um projeto de nome *FreeNet*, de autoria de Ian Clarke, criado para garantir a liberdade de expressão e de conteúdo com informações livres e sem restrições para os usuários. Seria uma

---

12 Ibidem.
13 Ibidem.
14 Ibidem.
15 Ibidem.
16 MONTEIRO; FIDENCIO, 2013, op. cit., p. 36.
17 Ibidem.

internet integrada à própria rede de internet, onde os usuários, que quisessem privacidade não poderiam ser rastreados. Embora a iniciativa do projeto *FreeNet* tenha surgido com a intenção de liberdade, seu uso tem sido feito, em grande parte, para práticas de crimes cibernéticos.

2.2 TIPIFICAÇÃO DOS CIBERCRIMES

Segundo mencionado no site da Câmara dos Deputados[18], os primeiros crimes com relação à informática tiveram início nos Estados Unidos em meados dos anos de 1960, onde se cometerem crimes de sabotagem e espionagem. Vinte anos depois, em 1980 as ações criminosas foram se intensificando, principalmente se tratando de dados bancários, pirataria e pornografia infantil.

O início dos cibercrimes em âmbito Nacional se deu no final da década de 1990. Conforme Diego Medeiros[19], foram descobertas invasões em sites ligados ao governo, como por exemplo o site oficial do Supremo Tribunal Federal, ocorrido no dia 18 de junho de 1996, onde, a partir disto, a sociedade teve conhecimento deste tipo de crime.

No tocante ao termo específico “cibercrimes”, esta nomenclatura foi designada em reunião na França, onde membros do subgrupo das nações do G8, denominaram à crimes cometidos através de dispositivos eletrônicos conectados à internet. De acordo com Samir de Paula Nascimento[20], cibercrime é a atividade ligada diretamente a ação ilícita praticada através da internet, ou seja, consiste em fraudar a segurança dos dispositivos, sistemas de comunicação e redes corporativas. Sendo assim, o crime na internet nada mais é do que um ato ilegal cometido por meio de dispositivo eletrônico envolvendo informação digital através da internet.

---

[18] Agência Câmara de Notícias. **Conheça a Evolução dos Crimes Cibernéticos**. Disponível em: https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos. Acesso em: 23 jun. 2021.

[19] MEDEIROS, Diego. **Crimes Virtuais**. Disponível em: https://jus.com.br/artigos/42734/crimes-virtuais. 2015. Acesso em: 12 mar. 2021.

[20] NASCIMENTO, Samir de Paula. **Cibercrime: Conceitos, Modalidades e Aspectos Jurídicos-Penais**. 2019. Disponível em: https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais. Acesso em: 01 abr. 2021.

Tipificado no Art. 154 – A[21] do Código Penal, os crimes relacionados à informática dizem que:

> "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: (Incluído pela Lei nº 12.737, de 2012)".

Porém, trata-se mais especificamente, da tipificação da Lei dos Crimes Cibernéticos, Lei nº 12.737/2012[22], conhecida como Lei Carolina Dieckmann, onde o ato de invadir computadores, roubar senhas, violar dados de usuários e divulgar informações privadas configuram crime.

Segundo Erick Teixeira Barreto[23], a criação dessa lei federal ocorreu em uma tentativa de tipificar as novas condutas envolvendo a evolução tecnológica que se aproximava. Com a falta de punição muitas pessoas iniciaram práticas reprováveis por meio de computadores, com ou sem acesso à internet. Para a realização das condutas ilícitas, que já eram praticadas muito antes de existirem as redes e os meios eletrônicos, os agentes se utilizam de tais meios como facilitadores para suas práticas. O fato que deu apelido à Lei, ocorreu quando fotos íntimas da atriz Carolina Dieckmann foram expostas devido a uma invasão em seu dispositivo informático, onde o debate a respeito desse tipo de crime foi reacendido criando um ambiente propício para aprovação da lei.

Barreto[24] ainda ressalta que outros crimes surgiram em conjunto com a evolução tecnológica, que são os chamados crimes cibernéticos próprios, onde o sujeito ativo utiliza o sistema informático do sujeito passivo, no qual seja o computador, e utiliza como meio para a execução do crime. Exemplo desse tipo de crime seria a invasão de computadores ou celulares para roubo de dados ou informações pessoais. Devido ao rápido avanço tecnológico, tais crimes são de difícil conceituação jurídica, pois deixam lacunas na legislação que levam à impunidade.

---

[21] BRASIL. Decreto-Lei Nº 2.848, de 7 de Dezembro de 1940. Código Penal. Art. 154 – A.

[22] BRASIL. Lei Nº 12.737, De 30 De Novembro De 2012. Dispõe sobre a tipificação criminal de delitos informáticos.

[23] BARRETO. Erick Teixeira. **Crimes cibernéticos sob a égide da Lei 12.737/2012**. 2017. Disponível em: https://ambitojuridico.com.br/edicoes/revista-159/crimes-ciberneticos-sob-a-egide-da-lei-12-737-2012. Acesso em: 04 abr. 2021.

[24] Ibidem.

Outro exemplo destacado, de crime cibernético próprio é a Lei nº 9.983/2000 que tipificou as condutas de inserção de dados falsos em sistemas de informação e de modificação ou alteração não autorizada de sistemas de informação, incluídos pelos artigos 313-A[25] do Código Penal:

> "Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano." E

E pelo artigo 313-B[26]: "Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente." Barreto[27] ainda define o Marco Civil da Internet, com a criação da Lei 12.965/2014[28] houve um avanço considerável nesse sentido, pois ela estabelece princípios, direitos e deveres para os usuários da internet no Brasil. Em contrapartida, o autor destaca que ainda existe um vácuo legal perigoso no que diz respeito aos crimes virtuais, pois mesmo havendo inúmeros projetos e anteprojetos de leis que visam configurar penalidades mais rígidas sobre essas condutas nenhuma ainda está perto de ser aprovada.

No que tange aos crimes cibernéticos impróprios, Barreto[29] frisa que, em sua maioria, as condutas são puníveis com base no antigo Código Penal de 1940, como por exemplo os crimes contra a honra, fraude, furto, chantagem, falsificação, apropriação indébita, falsa identidade e entre outros. Nesse sentido, uma das leis pioneiras criada para a informática foi a Lei nº 7.232/1984[30] que estabelecia princípios e diretrizes sobre a Política Nacional de Informática (PNI) por intermédio da criação do Conselho Nacional de Informática (CONIN). Com isso, Barreto[31] informa que houve o surgimento das primeiras legislações que visavam proteger o bem jurídico informático e as relações do meio. A Lei nº 7.646/1987, revogada por meio da Lei nº 9.609/1998[32], falava a respeito da proteção intelectual de programas

[25] BRASIL, 2000, op. cit.
[26] Ibidem.
[27] BARRETO, 2017, op. cit.
[28] BRASIL, 2014, op. cit.
[29] BARRETO, 2017, op. cit.
[30] BRASIL, 1984, op. cit.
[31] BARRETO, 2017, op. cit.
[32] BRASIL, 1998, op. cit.

de computadores e sua comercialização no país, tipificando como crime essas violações.

De acordo com dados do Conselho Nacional da Justiça[33], as primeiras leis específicas com foco no combate a crimes cibernéticos são a Lei 12.735 de 2012, que *"tipifica condutas realizadas mediante uso de sistema eletrônico, digitais ou similares que sejam praticadas contra sistema informatizados"* e a Lei 12.737 de 2012, mais conhecida como Lei Carolina Dieckmann, à qual versa sobre invasão de computadores, violação de dados de usuários e de mecanismo de segurança sem autorização expressa. Já em 2014 surgiu a Lei 12.965/2014, conhecida como Marco Civil da Internet, que tem a competência de regular os direitos e deveres dos usuários, além de determinar que os Juizados Especiais têm a responsabilidade de decisão sobre ilegalidade dos conteúdos. Estas determinações são aplicadas nos casos de ofensa à honra ou injúria, com tratamento similar como ocorre nos crimes não praticados através da internet.

As formas mais comuns de crimes cibernéticos, segundo Neide Cardoso de Oliveira[34] são os crimes de estelionato e furtos eletrônicos, falsificação e supressão de dados, invasão de dispositivo informático e furto de dados, armazenamento, posse, produção, troca, publicação de vídeos e imagens contendo pornografia infanto juvenil, assédio e aliciamento de crianças, ciberterrorismo, ameaça, divulgação de estupro/pornografia adulta, interrupção de serviço, cyberbullying, incitação e apologia de crime, crimes de ódio, crimes contra a propriedade intelectual e artística e venda ilegal de medicamentos.

---

[33] CONSELHO NACIONAL DE JUSTIÇA. **Crimes digitais: O que São, Como Denunciar e Quais Leis Tipificam Como Crime?** 2018. Disponível em: https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime. Acesso em: 10 jun. 2021.

[34] OLIVEIRA. Neide Cardoso de. **Atuação do Ministério Público Federal no Combate aos crimes Cibernéticos**. 2019. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cspcco/apresentacoes-em-eventos/eventos-em-2019/AudinciaPblicaNeideMaraCavalcantiANPR.pdf. Acesso em: 19 mai. 2021.

3 AS PRÁTICAS INVESTIGATIVAS APLICADAS AOS CIBERCRIMES

3.1 FORMAS DE INVESTIGAÇÃO E SUAS CARACTERÍSTICAS

Os processos de investigação aplicados aos cibercrimes são de extrema importância no que se refere ao combate da criminalidade virtual, os meios aos quais se obtém sucesso ao investigar são de difícil acesso e nem sempre os usuários deixam rastros ou históricos para o prosseguimento das análises.

Com a facilidade e o baixo custo, o uso da internet vem aumentando frequentemente entre a população, não somente por lazer e diversão, mas também como meio de informação, de uso social e profissional. Enfim, a internet tem se tornado não somente essencial como primordial na relação entre as pessoas em seu cotidiano, interligando e conectando diversas informações ao redor do mundo.

Justamente pela facilidade que a internet nos proporciona em todas as circunstâncias, sendo em compras online, pagamentos via contas digitais e serviços disponibilizados de forma virtual, os perigos começam a surgir quando menos se espera. De acordo com indicadores da Central de Denúncias de Crimes Cibernéticos da SaferNet[35] – Associação civil de direito privado que atua na promoção e defesa dos Direitos Humanos na Internet no Brasil, e criadora da Central Nacional de Denúncias de Crimes Cibernéticos – foram registradas em 2018, 128.332 denúncias anônimas envolvendo crimes praticados através da internet. Estes números, considerados em âmbito Nacional, representam uma pequena parcela do que acontece no mundo inteiro, onde políticas de segurança e tratados para combater esses delitos devem ser considerados imediatos para a resolução destes crimes.

Diego Campos Salgado Braga[36] destaca que os métodos de investigação passaram por modernização assim como a tecnologia obteve sua evolução rapidamente. Hoje em dia, a informática permite atitudes demasiadamente invasivas como por exemplo programas espiões denominados trojan, que se articulam mediante o monitoramento.

---

[35] SAFERNET. **Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos**. 2018. Disponível em: https://indicadores.safernet.org.br. Acesso em 02 mai. 2021.

[36] BRAGA, Diego Campos Salgado Braga. **Métodos de investigações no âmbito cibernético**. 2019. Disponível em: https://jus.com.br/artigos/71463/metodos-de-investigacoes-no-ambito-cibernetico. Acesso em: 01 jun. 2021.

Segundo Braga[37], uma das maiores preocupações sociais a respeito do mundo cibernético é a vigilância sem freio e sem critério, que não é possível a identificação de quem vigia e por qual motivo o faz. De tal modo, a digitalização das imagens e as novas técnicas de reconhecimento facial auxiliam para extrair do desconhecido o indivíduo, identificá-lo e segui-lo.

No que se refere a investigação, em casos de ataque executado por meio de uma rede de informática de distribuição de conteúdo ilícito, ou de uso de rede informática como forma de comunicação entre criminosos, segundo Braga[38], seria fora da realidade confiar apenas nos meios tradicionais de investigação, por isso, a utilização de técnicas mais atuais é essencial na busca por provas e identificação da fonte do ataque.

Assim, da mesma forma que os indivíduos possuem números que os identificam como o CPF, os computadores e demais objetos tecnológicos conectados à uma rede de internet são identificados de maneira parecida, através de seu endereço IP (Internet Protocol ou Protocolo de Internet). Mas afinal, o que é um IP? De acordo com a empresa Kaspersky,[39] IP é:

> "Um endereço IP é uma sequência de números separados por pontos. O endereço IP é representado por um conjunto de quatro números: por exemplo, 192.158.1.38. Cada número do conjunto pode variar entre 0 e 255. Ou seja, o intervalo de endereçamento IP vai de 0.0.0.0 a 255.255.255.255."

Este número é um endereço exclusivo que identifica um dispositivo na internet ou em uma rede local, ou seja, é um localizador que permite a comunicação das informações entre dispositivos em uma rede. Além disso, tem o objetivo de distinguir diferentes computadores, roteadores e sites.

Com relação a esse assunto, Braga[40] destaca que as dificuldades da investigação se iniciam nas tentativas de descobrir o endereço de IP, pois apesar de haver essa possibilidade, obter os dados do usuário que estava acessando no momento do ato ilícito é complexo e burocrático, sem falar nas diversas ferramentas que o agente pode se utilizar para mascarar e dissimular o número do IP. Uma

---

37 Ibidem.
38 Ibidem.
39 KASPERSKY. **O que é Endereço de IP – Definição e Explicação**. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ip-address. Acesso em 07 jun. 2021.
40 BRAGA, 2019, op. cit.

dessas ferramentas seriam os proxies que conseguem ocultar o verdadeiro IP dificultando o rastreamento. Os servidores proxy facilitam o anonimato na internet, mesmo não sendo utilizados apenas com fim ilícito.

Uma vez obtido o endereço de IP o passo seguinte seria procurar o endereço físico do computador, chamado endereço MAC, para após identificar quem realizou o acesso e quem praticou o crime. Porém, Braga[41] ressalta que tal tarefa não é fácil quando a rede é aberta ao público, como por exemplo, em Shoppings, Universidades, Aeroportos ou Lan Houses, onde inúmeras pessoas acessam diariamente essas redes.

Com a chegada do Marco Civil da Internet, os provedores de conexão e de aplicação foram obrigados a guardar as informações de conexões de usuários que utilizaram determinado serviço, assim como a hora, data e fuso horário da conexão. Neste quesito, Adriana Shimabukuro[42] destaca que para a obtenção das informações para a resolução destes crimes é fundamental o acesso a estes dados pelo fato de que com estes registros é possível verificar e rastrear de onde surgiu determinada conduta ilícita, ainda que tais informações sejam fornecidas mediante ordem judicial. Por mais que esta regulamentação seja favorável aos agentes, as autoridades enfrentam mais um desafio, pois de acordo com o Marco Civil da Internet, estes dados devem ser excluídos assim que termine o prazo de retenção, ou seja, para provedores de aplicação 1 (um) ano e 6 (seis) meses para provedores de conexão.

As fontes de informações essenciais para investigação são as mais variadas, enquanto no local de um crime tradicional se encontram testemunhas, digitais, vestígios e indícios, nos crimes cibernéticos as provas são abrigadas em diversas formas como: computadores, telefones celulares, pen drives, máquinas fotográficas, provedores de internet, roteadores, servidores de e-mail, entre outros. As provas podem ser encontradas em diversas formas como arquivos digitais, histórico de navegadores, fotos ou vídeos. De acordo com a autora[43], a coleta dos vestígios digitais deve seguir rigorosos mecanismos de preservação, e além disto, ser o mais

---

41 Ibidem.

42 SHIMABUKURO, Adriana. **Cibercrime: Quando a Tecnologia é Aliada da Lei**. Investigação e prova nos crimes cibernéticos. Escola de Magistrados da Justiça Federal da 3ª Região. Cadernos de Estudos. São Paulo, 2017. p. 22.

43 Ibidem.

rápido possível, caso contrário, podem ser rapidamente danificadas ou alteradas, impedindo qualquer investigação ou identificação dos criminosos.

Entrando no mérito da coleta de provas, Lima[44] versa sobre o sigilo de informações pessoais e virtuais, o qual é inviolável se tratando da correspondência, das comunicações, de dados e telefônicas, o qual este último, é possível conseguir por meio de ordem judicial, se a lei estabelecer para fins de investigação. Assim, se demonstra difícil manter uma investigação de cibercrimes mantendo 100% em sigilo dados pessoais do indivíduo e principalmente da vítima, visto que todas as pessoas possuem redes sociais e acesso á internet na palma da mão.

Alexandre Rocha Almeida de Moraes[45] faz um comparativo no que tange ao tempo do crime, uma vez que, segundo o Código Penal é adotado a teoria da atividade, onde o tempo do crime é considerado o momento da ação ou omissão do agente, e utilizando a internet é peculiarmente difícil saber quando foi cometido o crime. Tal circunstância gera insuficiência de evidências e consequentemente a dificuldade de avaliar a imputabilidade e a prescrição, como também saber qual lei deve ser aplicada em cada caso.

Verificando tais informações, Moraes[46] relata que a Convenção de Budapeste para crimes cibernéticos, esta em que o Brasil ainda não participa, prevê a conservação expedita dos dados informáticos armazenados, sendo esta uma medida legislativa a ser adotadas pelos países que fazem parte. Tal afirmação se vale devido a interpelação do servidor, que se faz necessária uma vez que no Brasil não existe legislação que verse a respeito de obrigação ao tráfego de informações dos clientes. Da mesma forma, as polícias civil e federal, quando for necessário, devem ser acionadas, como também um perito, para que possam tomar as devidas providências com relação ao fato.[47]

3.2 PERÍCIA INFORMÁTICA

Uma das etapas mais importantes na investigação criminal cibernética é a perícia informática. É nela que se obtêm vestígios deixados em computadores e

---

[44] Ibidem.
[45] MORAES, Alexandre Rocha Almeida de; SILVA, Isabella Tucci; SANTIAGO, Bruno. Os Cibercrimes e a Investigação Digital: Novos Paradigmas Para a Persecução Penal. 2020. p. 13.
[46] Ibidem.
[47] Ibidem. p. 14.

mídias de armazenamento que auxiliam na investigação. Nestes casos, Márcio Rodrigo de Freitas Carneiro[48] aponta a importância da perícia de informática onde se realiza a extração dos dados dos computadores e mídias, aplicando filtros específicos ao contexto almejado. Destaca-se a necessidade de análise efetiva do conteúdo do material colhido por parte dos policiais e às partes envolvidas durante o processo criminal para que o perito tenha melhores resultados na busca de indícios.

Dentro do percurso investigativo criminal cibernético, Carneiro[49] demonstra que no momento que se identifica o endereço do imóvel ao qual partiu o acesso à internet, ou outra forma que tenha sido identificada a ação criminosa, se cumprem os mandados de busca e apreensão emitidos pelos juízes. Ainda, segundo Carneiro[50], apesar de o cumprimento de mandado de busca e apreensão não requerer a presença de um perito criminal, se tem papel importante por parte da Polícia Federal na capacitação técnica da equipe.

Conforme Adriano Mauro Cansian[51], ao encontrar-se em uma análise, o perito deve isolar e assegurar o perímetro, de modo que não se viole e não coloque em risco a coleta e a veracidade das informações. O perito deve estar atento que ao executar qualquer operação em determinado sistema, causará possivelmente uma alteração em seu estado. Deste modo, a forma como um perito computacional age é de conhecimento de atacantes hábeis, sendo assim, é importante que o perito desconfie de informações falsas que possam ser plantadas propositalmente, a fim de atrapalhar a investigação.

Os procedimentos realizados na busca, segundo Eleutério e Machado[52], de forma geral, são verificações no suposto local do crime, exames em dispositivos de armazenamento computacional, em aparelhos de telefone celular, sites da internet, mensagens eletrônicas (e-mails), entre outros. Segundo o artigo 158[53] do Código de Processo Penal, é indispensável o exame de corpo de delito nas condutas

---

48 CARNEIRO, Márcio Rodrigo de Freitas. **Perícia de Informática nos Crimes Cibernéticos**. Investigação e prova nos crimes cibernéticos. Escola de Magistrados da Justiça Federal da 3ª Região. Cadernos de Estudos. São Paulo, 2017. p. 37.

49 Ibidem.

50 Ibidem.

51 CANSIAN. Adriano Mauro. **Conceitos Para Perícia Forense Computacional**. UNESP – Universidade Estadual Paulista. p. 13.

52 ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a Computação Forense**. Editora Novatec. São Paulo. 2011. p. 20-21.

53 BRASIL. Decreto-Lei Nº 3.689, de 3 de Outubro de 1941. Código de Processo Penal. Art. 158.

investigativas por parte do perito, onde serão examinados os vestígios necessários para a produção de laudos que interessem à Justiça.

Dentre os conhecimentos necessários para a atuação de um profissional da perícia forense, deve-se destacar a importância de conhecimento do máximo possível das tecnologias da informática, dentre elas estão a Engenharia de Softwares, Bancos de dados, Redes de Computadores, Sistemas Distribuídos, Programação, Arquitetura de Computadores, destaca Gonçalves[54]. Para a perícia criminal da polícia, o trabalho pericial e de investigação fazem parte da computação forense, a fim de desvendar os crimes praticados através de um computador.

Cansian[55] afirma que se pode genericamente dividir o perfil dos atacantes em dois padrões: atacantes oriundos de meio interno, ou seja, de uma própria empresa ou instituição, e atacantes externos, normalmente provenientes da internet. Segundo o autor[56], os ataques mais sérios, onde envolvem perdas financeiras significativas, contam com a cooperação de alguém de dentro das próprias organizações, ao contrário do que se acredita, na maioria das vezes, serem provenientes de ataque decorrente da internet.

A perícia computacional, segundo Dan Farmer[57]:

> "Trata da captura e análise de evidências, tanto quanto possível livres de estarem distorcidas ou tendenciosas, de tal forma, a reconstruir determinados dados ou o que aconteceu num sistema no passado".

Desta forma, são inúmeros os percalços enfrentados pelos peritos. Devido ao tamanho dos sistemas, os fatos e evidências podem estar ocultos em qualquer lugar. Com isso, em função da quantidade de dados armazenados, se esbarra com a dificuldade e demanda de tempo para análise dos mesmos.

Na fase de exame pericial, deve ser respeitada a ordem dos fatores para melhor resultado posterior. É necessário ao analisar mídias de armazenamento de

---

[54] GONÇALVES, Márcio; AMADIO, Renato Arnaut; GAVILAN, Júlio César; SANTOS, Herlones Wuilles dos. **Perícia Forense Computacional: Metodologias, Técnicas e Ferramentas**. Revista Científica Eletrônica de Ciências Sociais Aplicadas da Eduvale. Jaciara/MT Ano V, Número 07, novembro de 2012. Disponível em: http://eduvalesl.revista.inf.br/imagens_arquivos/arquivos_destaque/LXkEA5FVHGZF1FB_2015-12-19-2-33-33.pdf. Acesso em 29 mai. 2021.

[55] CANSIAN. op. cit., p. 05.

[56] Ibidem.

[57] FARMER, Dan; VENEMA, Wietse. **Perícia Forense Computacional. Teoria e Pratica Aplicada**. Tradução Edson Furmankiewicz, Carlos Schafranski, Docware Traduções Técnicas; Revisão Técnica Pedro Luís Próspero Sanchez. São Paulo: Person Prentice Hall, 2007.

forma que não haja possível modificação nos dados, nesses casos é recomendado a duplicação dos arquivos para a análise no sistema do perito. De acordo com Petter Anderson Lopes[58], seguir e manter a cadeia de custódia atualizada é importante para registro e planejamento da melhor abordagem tomada na perícia. É fundamental o correto armazenamento das informações para garantir a veracidade e integridade das provas.

Ainda a respeito da proteção de dados, quando se fala em perícia informática Alexandre Rocha Almeida de Moraes[59] relata sobre o estado de São Paulo, o qual possui uma Lei Municipal nº 12.228/2006[60] a qual obriga “lanhouse”, “cibercafé” e outros ambientes com disponibilidade de acesso à computadores ligados á internet, a manter em arquivos todos os dados cadastrais dos usuários por prazo mínimo de 60 meses. Tal medida auxiliou para cercar infratores que utilizavam tais máquinas para o cometimento de ilícitos, tentando assim, dificultar futuras investigações policiais.

Rafael Nader de Almeida[61] discorre sobre a maneira correta de armazenar dados na perícia forense de computadores. No momento de efetuar cópias dos dados, o perito deve obter cuidado no processo de espelhamento e cópias de imagens, pois tal cópia deve ser feita de forma que nenhuma informação contida no material investigado seja adulterada. Outro fator deve ser analisado, é o tempo de uso do computador investigado, uma vez que quando um aparelho é utilizado para a prática de um crime, como meio ou ferramenta, os rastros dessa atividade são deixados no dispositivo e os mesmos podem ser apagados pelo usuário. Com o passar do tempo, conforme o aparelho for usado outras vezes, tais dados perdem cada vez mais as chances de serem recuperados, por isso o tempo se torna essencial nas investigações de crimes por meios virtuais.[62]

---

[58] LOPES, Petter Anderson. **Forense Digital**. 2018. Disponível em: https://jus.com.br/artigos/69827/forense-digital. Acesso em 05 jun. 2021.

[59] MORAES; SILVA; SANTIAGO, op. cit. p. 15

[60] SÃO PAULO. Lei Nº 12.228, de 11 de Janeiro de 2006. Dispõe sobre os estabelecimentos comerciais que colocam a disposição, mediante locação, computadores e máquinas para acesso à internet e dá outras providências.

[61] ALMEIDA, Rafael Nader de. Perícia Forense Computacional: Estudo das Técnicas Utilizadas Para Coleta e Análise de Vestígios Digitais. 2011. p. 20.

[62] Ibidem. p. 21.

3.3 DIFICULDADES NA INVESTIGAÇÃO CRIMINAL

Inúmeras são as dificuldades e problemas encontrados no combate aos cibercrimes, visando a punição dos mesmos. Com o dinamismo e a volatilidade que são dotadas as tecnologias de informação, maior é o impulsionamento para cometimento destes crimes, visto que a velocidade de combate é menor que as incontáveis formas de serem praticados. A internet vem evoluindo de forma rápida e junto aos meios de comunicação surgiram novas modalidades de crimes neste âmbito. Os criminosos se valem da vulnerabilidade dos sistemas e também dos usuários que circulam através da rede, onde se aproveitam das fraquezas de sistemas as vezes mal projetados e suscetíveis a falhas.

Devida a especialização que os infratores adquirem juntamente com o avanço da internet, os agentes responsáveis por solucionar e punir estas práticas não conseguem amparar o crescimento dos criminosos nessa área, conforme aumenta o número de dispositivos conectados à internet, maior é o número de práticas ilícitas presentes na sociedade. De acordo com Dorigon[63], vários são os meios utilizados para a perpetração da conduta ilícita pelo infrator, desde e-mails, redes sociais, malwares, sites falsos de comércio eletrônico ou instituições bancárias, situações dentre várias existentes no meio virtual.

A autoria dos crimes cibernéticos é o início dos problemas que a polícia investigativa se depara no momento da investigação. O primeiro passo de uma investigação de crime cibernético se dá pela identificação do endereço IP do dispositivo usado pelo autor do crime. Como já mencionado, o IP serve como identificador de um dispositivo eletrônico ou de uma conexão, onde somente com ele se consegue descobrir a autoria dos atos. É neste ponto que muitas vezes está a maior dificuldade na identificação do autor, pois além de morosa a quebra de sigilo dos dados telemáticos, muitas das vezes o usuário faz uso de meios que mascaram o IP, como servidores proxy, redes Wi-Fi abertas, ou VPNs.

As redes Wi-Fi abertas baseiam-se em locais que dispõe conexão à internet de forma gratuita no intuito de suprir a demanda de variados dispositivos eletrônicos como celulares, notebooks, tablets, entre outros. Desta forma, pela característica

---

[63] DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes Cibernéticos: Dificuldades Investigativas na Obtenção de Indícios da 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: 22 mai. 2021.

que valida a conexão, não se faz necessária a identificação do usuário que nela se conectar, sendo assim, se torna ineficaz a tentativa dos agentes na busca pelo endereço IP de quem cometeu algum delito. Conforme Jonatas Lucena[64], as empresas que disponibilizam as redes Wi-Fi públicas deveriam manter um controle de acesso, bem como armazenar os registros das atividades que ocorrem na rede. Acrescenta Lucena[65], a importância da solicitação do uso de senhas e o preenchimento de qualquer informação capaz de localizar os usuários através do dispositivo usado.

Outra maneira de mascarar o tráfego de dados e consequentemente o endereço IP é o uso de servidores proxy. De acordo com Motta[66] no manual prático de investigação, em determinadas circunstâncias o usuário pode utilizar um método de acesso indireto, ou seja, se conecta através de um servidor proxy que vai servir como “ponte” entre ele e o conteúdo desejado. Desta maneira, o servidor ao qual foi conectado utiliza um IP próprio e oculta o IP original do usuário, dificultando ainda mais as possibilidades de investigação de quem pratica um crime cibernético. Apesar de muitos usuários se valerem desta ferramenta para práticas ilícitas, os servidores proxy não têm esta finalidade, em grande parte, o objetivo destes serviços é de providenciar aos usuários proteção contra ataques invasivos, roubo de dados e envio de spams.

De todas as formas, além de dificultosos os passos da investigação criminal cibernética, conforme visto anteriormente, ainda deve-se contar com a colaboração dos serviços de provedores de conexão e dos servidores proxy para o andamento na persecução penal, visto que, segundo Yuri Saramago Sahione de Araujo[67], se faz necessário o pedido judicial de cumprimento de mandado judicial para obtenção destas informações, pois, do contrário, acarretará na ilegalidade da obtenção da provas e por consequência invalidando-a. Assim, é visto como o andamento das investigações deve seguir etapas respeitando as particularidades de cada caso

---

64 LUCENA, Jonatas. **Wi-Fi Público e os Crimes Virtuais**. Disponível em: https://www.drjonatas.com.br/wi-fi-publico-e-os-crimes-virtuais. Acesso em: 11 jun. 2021.

65 Ibidem.

66 KUROKAWA, Adriana Shimabukuro; SUIAMA, Sergio Gardenghi; NASCIMENTO, Ana Carolina Previtalli; KAHN, Karen Louise Jeanette; MOTTA, Eduardo Barragan Serôa da. Crimes Cibernéticos: **Manual Prático de Investigação**. Procuradoria da República no Estado de São Paulo. Abril de 2006. p. 39.

67 ARAUJO, Yuri Saramago Sahione de. **A Insuficiência de Proteção Legal e Desproporcionalidade das Sanções às Vítimas de Ataques Cibernéticos**. 2021. Disponível em: https://www.migalhas.com.br/depeso/338849/a-insuficiencia-de-protecao-legal-e-desproporcionalidade-das-sancoes-as-vitimas-de-ataques-ciberneticos. Acesso em: 13 abr. 2021.

específico, pois são variadas as formas de abordagem e verificação tanto do local suposto do crime, quanto aos variados dispositivos e meios de armazenamento de dados, assim como a quantidade de arquivos presentes.

4 A PRODUÇÃO DE PROVAS DOS CRIMES CIBERNÉTICOS

4.1 A PROBLEMÁTICA POR TRÁS DA COMPROVAÇÃO DE AUTORIA

Constatada a ocorrência de infração penal ligada ao uso da informática, conforme se estabelecem as características para a tipificação, surge a problemática presente nas configurações criminais. Na maioria das vezes o crime se camufla em identidades anônimas e em vários casos, estão escondidos na *deep web*, local onde a dificuldade é grande na investigação e materialização das provas. Segundo Rodiner Roncada[68], devida a problemática da comprovação da existência e de quem foi o autor, cabe aos órgãos encarregados juntarem as possíveis provas na intenção de demonstrar a materialidade e autoria do delito, dentro de meios legítimos.

Partindo do pressuposto de que para a firmação de veracidade e aceitabilidade das provas, há de se levar em consideração o exame de corpo de delito, princípio este que vem a ser realizado primariamente, sendo dispensado o exame pericial em caso de desaparecimento ou destruição de quaisquer indícios de objetos ligados à cena do crime. No que diz respeito aos crimes cibernéticos, deve-se levar em consideração que em casos específicos não há evidência material de crime, sendo este cometido diretamente pela internet. É neste momento que se deve atentar ao caminho que o criminoso levou até praticar o delito.

O maior desafio encontrado por parte das autoridades na busca por comprovação pelos delitos praticados através da internet se faz com o ordenamento jurídico. Ao que traz o Código de Processo Penal[69] no artigo 386, caso não seja comprovada de forma robusta a materialidade delitiva e a autoria, o juiz absolverá o réu nos termos da Lei. Não obstante as dificuldades dispostas, os meios de angariação de provas devem respeitar o princípio da legalidade, sendo assim, devem ser adquiridas de forma lícita, respeitados os dispositivos na forma da Lei.

Conforme Alessandro Dorigon[70] destaca, a autoria dos crimes cibernéticos seria o primeiro problema encontrado pelos investigadores, pois dificilmente os

---

[68] RONCADA, Rodiner. **A Prova da Materialidade Delitiva nos Crimes Cibernéticos**. Investigação e Prova nos Crimes Cibernéticos. Escola de Magistrados da Justiça Federal da 3ª Região. Cadernos de Estudos. São Paulo, 2017. p. 178.

[69] BRASIL,1941, op. cit.

[70] DORIGON; SOARES, 2018, op. cit.

criminosos se utilizam de sua verdadeira identidade na prática desses ilícitos. Desta forma, ao ser encontrado o endereço de IP, a investigação em fim caminha a elucidação. Em contrapartida, Dorigon[71] afirma que, mesmo diante da hipótese de ser encontrado o IP, em se tratando deste ser dinâmico ou estático, nenhum IP seria atribuído ao mesmo usuário, no mesmo horário ou mesma data, por isso, deve-se solicitar aos provedores de acesso quem teria utilizado aquele endereço de IP em data e hora específicas.

As provas são os meios pelos quais o investigador consegue demonstrar como, quando, onde e contra quem o autor cometeu o crime. Partindo da premissa de Jorge Luiz Silva da Silva[72] a prova não tem caráter absoluto, pois possui limites mesmo estando presente como uma garantia. Desta forma, a doutrina procurou distinguir os meios de provas dos meios de obtenção das mesmas, assim, Silva[73] afirma que os meios de prova servem para o convencimento do juiz a respeito da veracidade ou não dos fatos, os meios de obtenção servem basicamente como instrumento para a colheita de fontes ou elementos para integrar uma suposta autoria.

Conforme ditado no art. 225 do Código Civil Brasileiro:

> "As reproduções fotográficas, cinematográficas, os registros fonográficos, e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos não lhes impugnar a exatidão".

Desta forma, Silva[74] afirma que, é possível aceitar-se qualquer meio de prova, desde que, respeitados alguns limites técnicos na sua coleta e guarda, com objetivo de resguardar a integridade e a garantia de que a mesma não venha a ser questionada posteriormente quanto a sua validade ou licitude.

Em outro momento, o autor[75] versa a respeito da computação forense, uma especialidade que se enquadra na ciência criminalística que aborda as técnicas utilizadas nos crimes envolvendo a internet e seus meios. Esta técnica serve para identificar, analisar, coletar e preservar as provas ou informações que são

---

71 Ibidem.
72 SILVA, Jorge Luiz Silva da. **A Prova nos Crimes que se Utilizam das Redes Sociais**. 2016. Disponível em: https://ajufesc.org.br/wp-content/uploads/2017/02/Jorge-Luiz-Silva-da-Silva.pdf. Acesso em: 03 jun. 2021.
73 Ibidem.
74 Ibidem.
75 Ibidem.

armazenadas magneticamente ou codificadas. Levando em consideração que tal ciência abrange a perícia aplicada à informática, esta, segundo Silva, pode ser definida como “a aplicação de princípios das ciências físicas ao Direito na busca da verdade em questões cíveis, criminais e de comportamento social para que não se cometam injustiças contra qualquer membro da sociedade”.

Utilizando-se de tais terminologias, Mariana Maria Matos[76] destaca a respeito das provas ilícitas decorrentes de investigações criminais, as quais são inadmissíveis perante a Constituição Brasileira no seu art. 5º:[77]

> “Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: **LVI** - são inadmissíveis, no processo, as provas obtidas por meios ilícitos;

E no Código de Processo Penal em seu art. 157:[78]

> “São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais. (Redação dada pela Lei nº 11.690, de 2008).
> **§ 1o** São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras. (Incluído pela Lei nº 11.690, de 2008)
> **§ 2o** Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova. (Incluído pela Lei nº 11.690, de 2008)
> **§ 3o** Preclusa a decisão de desentranhamento da prova declarada inadmissível, esta será inutilizada por decisão judicial, facultado às partes acompanhar o incidente. (Incluído pela Lei nº 11.690, de 2008)
> **§ 5º** O juiz que conhecer do conteúdo da prova declarada inadmissível não poderá proferir a sentença ou acórdão. (Incluído pela Lei nº 13.964, de 2019)”. De tal maneira, é necessário que, assim como na quebra de registro telefônico, exista prévia autorização judicial para apurar dados nos crimes relacionados a meios virtuais.

Mariana Maria Matos[79] ainda aduz a respeito do órgão responsável pela atribuição de autenticidade, integridade e validade jurídica aos documentos eletrônicos no Brasil, o Instituto Nacional de Tecnologia. A utilização de documentos

---

[76] MATOS, Mariana Maria. **Da Produção e Colheita de Provas no Ambiente Cibernético**. 2014. Disponível em: https://marianamariam.jusbrasil.com.br/artigos/119753698/da-producao-e-colheita-de-provas-no-ambiente-cibernetico. Acesso em: 27 mai. 2021.
[77] BRASIL. Constituição da República Federativa do Brasil de 1988.
[78] BRASIL, 1941, op. cit.
[79] MATOS, 2014, op. cit.

eletrônicos como prova tem sido bastante discutida no ambiente jurídico. A autora afirma que, mesmo a maioria dos doutrinadores admitirem tais meios de prova, ainda existem discussões sobre se os documentos eletrônicos seriam provas documentais ou periciais. Segundo Matos[80], a teoria mais utilizada é a de que tais documentos serviriam como prova pericial pois necessitam de perícia técnica.

Neste sentido, a autora frisa que as provas encontradas nas redes correm sérios riscos de perecimento, por isso, devem ser coletadas e analisadas com cuidado e atenção, garantindo assim, que o autor seja encontrado, preso e que seja iniciado o devido processo legal.

4.2 PEDOFILIA E PORNOGRAFIA INFANTIL

Com o desenvolvimento tecnológico cada vez mais crescente, as crianças e adolescentes estão ainda mais expostos à crimes como pedofilia a abuso de menores. Laura Pereira do Nascimento e Rosane Leal da Silva[81] versam a respeito de como o fluxo de informações ao redor do mundo facilita a prática deste tipo de crime, principalmente no que tange a formas de entretenimento disponíveis no ciberespaço, tais formas chamam atenção principalmente de jovens e crianças. Uma pesquisa realizada no ano de 2012 pelo Comitê Gestor da Internet no Brasil mapeou os usos e atividades feitas pelo público infanto-juvenil, o que revelou que usuários entre 09 (nove) e 16 (dezesseis) anos confirmaram utilizar a internet para inúmeras tarefas.

De tal forma, as autoras[82] afirmam que foi possível perceber na presente pesquisa que, cerca de 70% desses jovens e crianças possuem perfil próprio nas redes sociais, expondo fotos que mostram claramente seus rostos, identidade, local onde moram e estudam. Ocorre que tais características são um “prato cheio” para criminosos, uma vez que pais e crianças não possuem a real noção dos perigos e riscos que rondam a internet e em consequência as redes sociais. Destaca-se que tais criminosos atuam de forma discreta e articulada, encontrando e atraindo suas vítimas facilmente por meio de perfis chamados “fake” ou “falso”.

---

[80] Ibidem.

[81] NASCIMENTO, Laura Pereira do; SILVA, Rosane Leal da. **Crianças e Adolescentes Internautas como Alvo da Criminalidade Online: Pedofilia e Pornografia na Internet**. 2014. Disponível em: https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/11741/1541. Acesso em: 13 mai. 2021.

[82] Ibidem.

Nascimento[83] demonstra que, segundo o psiquiatra Patrice Dunaigre, especialista em crimes de pedofilia, caracteriza tal prática criminosa como manifestações e práticas de desejo sexual que alguns adultos possuem em relação à crianças ou menores de idade, se tratando de uma transgressão singular totalmente contrária às regras estabelecidas pela sociedade. Por outro lado, a Organização Mundial da Saúde (OMS) dispõe de uma classificação clínica de tal distúrbio, onde conceitua como uma:

> "Ocorrência de práticas sexuais entre um indivíduo maior, principalmente do sexo masculino, como uma criança na pré-puberdade (13 anos ou menos), normalmente deve haver uma grande diferença de idade entre ambos".[84]

A Lei nº 11.829/2008[85] em seu art.1º (art. 240 e 241 da Lei nº8.069/1990) especifica que:

> Art. 240 - Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
> § 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.
> § 2º Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime: I – no exercício de cargo ou função pública ou a pretexto de exercê-la; II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou III – prevalecendo-se de relações de parentesco consanguíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento." (NR).

Tal artigo especifica, reforçando o que já dizia a Lei nº 8.069/1990, quais as atitudes e condutas que são caracterizadas como pedofilia infantil e abuso de menores de idade. Com o aumento da tecnologia foi necessário alterar a Lei e incluir as condutas descritas. Art. 241 - Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (NR).

---

[83] Ibidem.
[84] Ibidem.
[85] BRASIL. Lei nº 11.829, de 25 de Novembro de 2008. Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.

Este artigo demonstra que, apesar de não realizar a conduta típica do autor de pedofilia (ato sexual propriamente dito), expor o menor em fotografias, vídeos ou demais registros contendo relações sexuais envolvendo crianças e adolescentes também é conduta ilícita caracterizada como crime de pedofilia.

> Art. 241 – A - Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.[86]
> § 1º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.

O artigo acima demonstra também, que a conduta de simplesmente “passar a diante”, vender ou disponibilizar vídeos ou fotos com conteúdo sexual em que configurem como vítimas crianças e adolescentes será configurado como crime de pedofilia.

> Art. 241 – B - Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
> § 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
> I – agente público no exercício de suas funções;
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
> § 3º As pessoas referidas no § 2º deste artigo deverão manter sob sigilo o material ilícito referido.

Tal artigo versa a respeito de pessoas que no exercício de suas funções (agentes públicos, funcionários ou representantes de provedor de acesso à internet

[86] Ibidem.

entre outros) que armazenam ou mantem conteúdo sexual envolvendo crianças e adolescentes, não serão denunciados como autores caso tais informações tenham sido passadas às autoridades, ou seja, não eram com a finalidade de cometerem crime de pedofilia.

> Art. 241 – C - Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo.[87]
> Art. 241 – D - Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Nas mesmas penas incorre quem:
> I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso;
> II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita.
> Art. 241 – E – "Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais."

Os artigos mencionados à cima, fazem menção a demais condutas envolvendo crianças e adolescentes, exemplo da simples simulação de ato sexual, induzir a criança ou adolescente a se mostrar ou exibir de forma pornográfica, também configuram crime de pedofilia, mesmo que o agente nem encoste na vítima.

Vale destacar, de tal forma, segundo Laura Pereira do Nascimento[88] a internet, da mesma forma que impulsiona a prática do crime de pedofilia, ela também tem papel fundamental na incidência da pornografia, pois ela se tornou um dos principais meios de intercâmbio da pornografia infantil através de inúmeras técnicas, como por exemplo a codificação de dados e o reenvio anônimo. Segundo a autora, houveram avanços na identificação dos autores de crimes de pedofilia utilizando as redes de internet, algo positivo, porém que não depende exclusivamente dos agentes de investigação da polícia. Deve-se haver uma colaboração significativa das empresas provedoras de internet e computadores, pois com isso é possível haver a conservação das provas, ocorre que muitas grandes

[87] Ibidem.
[88] NASCIMENTO; SILVA, 2014, op. cit.

empresas se recusam a efetuar tal colaboração, se negando a passar informações e dificultando o trabalho dos investigadores.

No estado do Rio Grande do Sul, segundo Caroline Tentardini e Luana Rosales[89] dados da Secretaria Estadual de Segurança Pública (SSP) no ano de 2019 demonstram que 80% dos crimes virtuais estão relacionados à pedofilia. De acordo com o DECA (Departamento Estadual da Criança e Adolescente, a conduta mais frequente ligada a pedofilia seria o armazenamento e/ou compartilhamento de arquivos contendo pornografia infanto-juvenil, por meio da internet em forma de fotos, vídeos ou qualquer outro registro que contenha sexo explícito ou pornografia envolvendo crianças.

A autora[90] ainda traz a luz que números obtidos na pesquisa revelam que cerca de 551 ocorrências que envolviam o crime de pedofilia foram registradas no Rio Grande do Sul entre 2009 e 2018, uma média de 55,1 casos por ano. A pesquisa revelou também que o período mais expressivo foi o ano de 2018, quando foram contabilizadas 88 ocorrências. Já no ano de 2019, pelo menos 24 crimes relacionados à pedofilia no ambiente virtual já foram denunciados às autoridades.

Destaca-se, nesse sentido, a Operação permanente Luz na Infância[91], onde as Polícias Civis do Brasil têm como objetivo a busca e a prisão dos investigados por crimes virtuais que se relacionam com a pedofilia. Da mesma forma, as Delegacias de Proteção à Criança e ao Adolescente e de Repressão à Crimes Informáticos realizam a apuração, a instauração do inquérito e solicitam buscas junto à Justiça. Desde o início desta operação, nos 26 estados do país e no Distrito Federal, mais de 500 pessoas foram presas.

4.3 OPERAÇÃO DARKNET

Conforme o Ministério Público Federal[92] a operação Darknet consiste na primeira investigação realizada na *deep web* no Brasil, que tem por objetivo

---

89 TENTARDINI, Caroline; ROSALES, Luana. **80% dos Crimes Virtuais Investigados no RS Estão Ligados à Pedofilia**. 2019. Disponível em: https://www.sul21.com.br/ultimas-noticias/geral/2019/08/80-dos-crimes-virtuais-investigados-no-rs-estao-ligados-a-pedofilia. Acesso em: 17 abr. 2021.

90 Ibidem.

91 Ibidem.

92 MINISTÉRIO PÚBLICO FEDERAL. **Operação Darknet**. Disponível em: http://www.mpf.mp.br/rs/sala-de-imprensa/docs/outros-documentos/operacao-darknet. Acesso em 17 abr. 2021.

encontrar usuários que se utilizam das redes para realizar crime de pedofilia ou pornografia infantil. Em um primeiro momento foram utilizadas ferramentas desenvolvias pela Polícia Federal do Rio Grande do Sul onde esta conseguia detectar usuários que compartilhavam vídeos ou fotos contendo pornografia de crianças e adolescentes. Por tal motivo, o início das investigações se dera na cidade de Porto Alegre no final do ano de 2013, e assim foi deflagrada em duas etapas: 15 de outubro de 2014 e 22 de novembro de 2016.

O artigo destaca ainda, que houve necessidade de reconhecimento da *deep web*, o funcionamento da rede TOR, para se chegar na colheita de provas de forma lícita. A forma de trabalho utilizada foi fundamental, uma vez que, a Coordenação da Operação constatou de antemão todos os membros que receberam a materialidade delitiva, as peculiaridades diversas do caso bem como repassou cuidados que foram sugeridos para uso na colheita da prova digital, tal qual necessita de observações especiais onde, dependendo do caso, pode auxiliar na identificação dos criminosos.

Inicialmente, após transcorrido um período de tempo de mais ou menos 1 ano, na data de 15 de outubro de 2015 se encontrou deflagrada a primeira fase da operação ocorrendo o cumprimento de mais de 100 mandados de busca e apreensão das quais resultaram em 51 prisões ao todo no país. Já na segunda fase, houve investigação de 70 possíveis alvos compreendendo 17 estados além dos alvos da Subseção Judiciária de Porto Alegre que foi sede das investigações.[93]

A Lei 13.441/2017[94] versa sobre a Infiltração de Agentes de Polícia para a Investigação de Crimes Contra a Dignidade Sexual de Crianças e Adolescentes, ela diz: A infiltração de agentes de polícia na internet com o fim de investigar os crimes previstos nos arts. 240 , 241 , 241-A , 241-B , 241-C e 241-D desta Lei e nos arts. 154-A , 217-A , 218 , 218-A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) , obedecerá às seguintes regras:

> I – será precedida de autorização judicial devidamente circunstanciada e fundamentada, que estabelecerá os limites da infiltração para obtenção de prova, ouvido o Ministério Público;
> II – dar-se-á mediante requerimento do Ministério Público ou representação de delegado de polícia e conterá a demonstração de sua necessidade, o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas

[93] Ibidem.

[94] BRASIL. Lei nº 13.441, de 8 de Maio de 2017. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente.

> investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas;
> III – não poderá exceder o prazo de 90 (noventa) dias, sem prejuízo de eventuais renovações, desde que o total não exceda a 720 (setecentos e vinte) dias e seja demonstrada sua efetiva necessidade, a critério da autoridade judicial.
> § 1º A autoridade judicial e o Ministério Público poderão requisitar relatórios parciais da operação de infiltração antes do término do prazo de que trata o inciso II do § 1º deste artigo.
> § 2º Para efeitos do disposto no inciso I do § 1º deste artigo, consideram-se:
> I – dados de conexão: informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão;
> II – dados cadastrais: informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão.
> § 3º A infiltração de agentes de polícia na internet não será admitida se a prova puder ser obtida por outros meios."
> "Art. 190-B . As informações da operação de infiltração serão encaminhadas diretamente ao juiz responsável pela autorização da medida, que zelará por seu sigilo.
> Parágrafo único. Antes da conclusão da operação, o acesso aos autos será reservado ao juiz, ao Ministério Público e ao delegado de polícia responsável pela operação, com o objetivo de garantir o sigilo das investigações.[95]

Neste sentido, Felipe José Souza Rodrigues[96] cita que a Lei nº 13.441/2017 trouxe a discussão mais clara a respeito das infiltrações virtuais, a operação Darknet, por exemplo surgiu anteriormente à Lei e já trazia tal assunto à tona. Tal operação obteve embasamento nas diretrizes da Lei 12.850/2013[97], que versa a respeito de organizações criminosas, e exemplifica as hipóteses de infiltração de forma presencial. Esta mesma Lei, em seu §2º Inciso I diz*: Esta lei se aplica também: I- às infrações penais previstas em tratado ou convenção internacional quando, iniciada a execução no país, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente"*. Ou seja, esta lei pode ser aplicada para reprimir os crimes sexuais contra a criança e adolescente ocorridos através da internet a qual pode abranger países distintos e diversos.

---

[95] Ibidem.

[96] RODRIGUES, Felipe José Souza; CARDOSO, Sarah de Araújo Mendes; MARWELL, Tatiana Eulálio Dantas Guedes. **Utilização da Infiltração Virtual nas Operações Policiais Para o Combate ao Crimes Sexuais Contra Crianças e Adolescentes**. Research, Society and Development, v. 10, n. 7, e24710414152, 2021. p. 03.

[97] BRASIL. Lei nº 12.850, de 2 de Agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências.

Rodrigues[98] ressalta que no trâmite dos trabalhos de investigação da operação Darknet foram realizados relatórios no prazo de 60 dias, destes eram proporcionadas análises referentes ao desenvolvimento da ação. Tais relatórios eram periódicos e se encontram previstos no procedimento de infiltração da Lei nº 12.850/2013 a qual fundamentou o modus operandi da Darknet. Graças a esse trabalho e aos mandados realizados pela operação, diversas crianças foram retiradas de situações de abuso sexual contínuo, algumas até antes do cumprimento dos mandados.

Versando nesse mesmo sentido, os autores[99] ainda frisam que a operação Darknet possui reconhecimento mundial, uma vez que, segundo o MPF, foram identificados alvos que faziam transmissão de pornografia infantil no exterior, enviando a materialidade através da Interpol aos seus respectivos países, quais sejam Espanha, Portugal, Itália, México, Colômbia e Venezuela. Demais estudos foram feitos e aprofundados, com base na análise de acórdão publicado no Diário Eletrônico em 08 de janeiro de 2019, proferido pela egrégia 11º Turma do TRF da 3ª Região julgando o Recurso em Sentido Estrito nº 0013152-89.2014.4.03.6181/SP, como relator o Desembargados Federal José Lunardelli, diz a ementa:

> RECURSO EM SENTIDO ESTRITO. PORNOGRAFIA INFANTIL. ART. 241-A e ART. 241-B DA LEI Nº 8.069/90. RECEBIMENTO DA DENÚNCIA. OPERAÇÃO DARKNET. FLAGRANTE PREPARADO. AUSÊNCIA. NÃO CONFIGURAÇÃO DE CRIME IMPOSSÍVEL. RECURSO PROVIDO. 1. O inquérito policial que embasou a denúncia teve origem na Operação "Darknet", deflagrada no estado do Rio Grande do Sul, após notícia oriunda de outra operação, acerca da existência de pessoas utilizando a rede "TOR" ("The Onion Router"), que permite navegação anônima na "DeepWeb" ou internet profunda, para compartilhamento de arquivos cujo conteúdo envolveria pornografia infantil. Após autorização judicial para infiltração de agentes e criação do fórum "Forpedo Brasil" na "DeepWeb", o acusado foi identificado como sendo um dos usuários que compartilhou material pedófilo no referido ambiente, o que culminou com o seu rastreamento e cumprimento de mandado de busca e apreensão em sua residência. 2. Ausência do flagrante preparado ou provocado, eis que nenhum dos usuários foi induzido a praticar crimes pelos policiais infiltrados. Não houve convite ou qualquer outra forma de instigação, nem se fez nascer a intenção da prática dos delitos. Houve, sim, a criação de um fórum onde havia uma espécie de cadastro prévio, etapa que permitia a identificação dos IP's dos usuários, ante a dificuldade de rastreamento ao se utilizar a "DeepWeb" através do programa TOR. Constatada atividade suspeita pelo usuário, com a publicação de material que denotasse a prática de crimes, o IP era rastreado e a investigação prosseguia com o objetivo de averiguar elementos de autoria e materialidade. Os crimes foram efetivamente consumados, com o compartilhamento de material de cunho pedófilo, para só após se dar o

[98] RODRIGUES; CARDOSO; MARWELL, 2021, op. cit., p. 09.
[99] Ibidem.

> rastreamento e a identificação dos IP's. Os agentes policiais não fomentaram nem impediram a prática dos crimes, daí não se pode falar em crime impossível. A hipótese amolda-se ao que se entende pelo flagrante esperado, válido e aceito em nosso ordenamento jurídico. 3. A leitura da denúncia de fls. 265/266v revela que foram atendidos os requisitos previstos no art. 41 do Código de Processo Penal, estando ausentes, por outro lado, as hipóteses previstas no art. 395 do mesmo Diploma Legal. Assim, de rigor o retorno dos autos ao Juízo a quo para recebimento da denúncia e prosseguimento do feito. 4. Recurso em sentido estrito provido. (TRF-3 - RSE: 00131528920144036181 SP, Relator: DESEMBARGADOR FEDERAL JOSÉ LUNARDELLI, Data de Julgamento: 11/12/2018, DÉCIMA PRIMEIRA TURMA, Data de Publicação: e-DJF3 Judicial 1 DATA:07/01/2019).[100]

Conforme se pode analisar na ementa supracitada, os autores[101] fazem menção ao acusado José Afonso da Silva, o qual publicou e divulgou em um Fórum da internet imagens de conteúdo explícito de pornografia de menores. Além do mais, durante o cumprimento de mandado de busca e prisão expedido em seu nome, teriam encontrado cerca de 140 imagens e 3 vídeos no interior de seu computador em sua residência. Assim, a infiltração virtual deu-se de forma satisfatória para assegurar a autoria e materialidade delitiva do acusado.

Ao adentrar no ambiente dos investigadores, Felipe José Souza Rodrigues[102] discorre a respeito de relatos de uma agente da Polícia Federal que tem atuado como investigadora infiltrada após a Lei nº13.441/2017[103]. A agente relatou que, atualmente, o local de atuação dos investigados são os aplicativos de conversação, como Whatsapp e Telegram. Ao utilizar essas plataformas, os usuários se beneficiam das facilidades de comunicação que estes proporcionam pela criptografia das mensagens, proporcionando um ambiente propício para abusadores e pedófilos compartilharem arquivos com conteúdo ilícito. Ressalta-se, aproveitando o contexto, a Operação Protetor e a Operação Ades, duas operações iniciadas em 2018 com ênfase na elucidação de crimes virtuais de pedofilia e abuso infantil. A Operação Ades identificou um autor, o qual possuía inúmeras conversas com outros infratores nos aplicativos de conversas, este já conhecido no meio por conseguir arquivos inéditos e disponibilizar aos demais pedófilos. Desta forma a Operação Protetor foi iniciada com alvo utilizando o usuário do autor (já preso na Operação Ades) vinculado a diversas plataformas para ser possível conseguir dados de outros

---

[100] SÃO PAULO. Tribunal Regional Federal. (3. Câmara Criminal). Recurso em Sentido Estrito 00131528920144036181. Relator: Desembargador Federal José Lunardelli, data de julgamento: 11/12/2018. Publicado em: e-DJF3 Judicial 07/01/2019.

[101] RODRIGUES; CARDOSO; MARWELL, 2021, op. cit., p. 10.

[102] Ibidem.

[103] BRASIL, 2017, op. cit.

criminosos. Tal qual foi o contexto de uma investigação feita por um agente infiltrado, que utilizou o número de telefone do criminoso preso, com autorização judicial, dotado de credibilidade, para conversar e encontrar outros criminosos abusadores e pedófilos.

Contudo, Rodrigues[104] menciona a parte final da entrevista com a agente da Polícia Federal, onde a mesma afirma que ainda faltam normas específicas em nosso ordenamento jurídico regulamentando a infiltração virtual, o que, segundo ela, não deixa entendimentos diversos dos magistrados ou do Ministério Público durante o trabalho de investigação. Da mesma forma, a agente ressalta que a inovação legislativa trouxe alguns prejuízos como o prazo limitado, mas também elegeu benefícios ao procedimento do agente infiltrado, e finalizou argumentando que é necessário analisar a longo prazo, com amplitude de investigações se a nova norma, que futuramente virá, consiste em uma ótima regulamentação.

[104]RODRIGUES; CARDOSO; MARWELL, 2021, op. cit., p. 12.

5 CONCLUSÃO

Através da presente pesquisa, pode-se observar que a constante evolução tecnológica bem como o crescimento dos meios ligados à internet facilitam o cometimento de crimes por meio destes assim como, em alguns aspectos, dificultam a atuação da polícia investigativa no que tange a encontrar o autor do crime de pedofilia ou abuso sexual de crianças e adolescentes.

Inicialmente, relatou-se a respeito dos tipos de crimes cometidos no meio virtual, os chamados cibercrimes, e sobre suas subdivisões, assim como a *deep web* e a *dark web*, locais obscuros da internet onde criminosos aproveitam as facilidades inseridas nesses meios para o cometimento de seus ilícitos, levando em consideração a praticidade de fazê-los e de ocultar sua verdadeira identidade.

Em um segundo momento, abordou-se sobre as práticas investigativas e o desafio encontrado por parte dos agentes públicos no que concerne à limitação das Leis e na minuciosidade de detalhes que devem ser levados em consideração no momento da investigação. Dito isto, é evidente que o papel dos peritos é crucial no angariamento de provas, visto que devem ser observados critérios e respeitados os dispositivos legais, afim de não resultarem em ilicitude de provas. Salienta-se também a qualidade na capacitação de agentes de segurança e peritos por se tratar de crimes que necessitam de atenção redobrada para analisar os milhares de arquivos encontrados em um dispositivo de armazenamento.

Com isso, se percebe que os órgãos públicos têm papel primordial no combate aos crimes cibernéticos, porém esbarram na falta de leis mais específicas que tipifiquem estes delitos informáticos. Sabe-se que novas modalidades de crime surgem a cada momento, assim como evoluem os serviços dispostos nos meios virtuais.

É de se observar que em decorrência do Marco Civil na Internet, as autoridades ganham força pela obrigatoriedade de guarda de registros por parte dos provedores de internet, porém, em virtude da necessidade de autorização judicial para quebra de sigilo e de dados telemáticos, a demanda de tempo é inimiga dos órgãos competentes, pois é morosa a liberação judicial para mandados de busca e apreensão. Entretanto, ainda é necessário que sejam formuladas leis mais severas e meios mais precisos para que a polícia possa elucidar tais crimes com mais agilidade e precisão.

Por fim, conclui-se que, mesmo havendo operações importantes e significativas no âmbito dos crimes cibernéticos, como por exemplo as citadas Operação Darknet, Operação Ares entre outras, a melhor forma de se combater os crimes envolvendo crianças e adolescentes seria a precaução dos pais e responsáveis com relação às redes sociais e acessos desses menores à internet. Assim como, os adultos devem proceder com cautela quando acessarem sites duvidosos ou que peçam seus dados pessoais, com as crianças o cuidado deve ser redobrado. Avaliar as atividades destes e com quem se comunicam e porque é o ponto chave para se proteger, de alguma forma, os menores contra criminosos mal intencionados, que na maioria das vezes só necessita de um descuido destes pais para conquistar sua vítima.

REFERÊNCIAS

Agência Câmara de Notícias. **Conheça a Evolução dos Crimes Cibernéticos**. Disponível em: https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos. Acesso em: 23 jun. 2021.

ALMEIDA, Rafael Nader de. Perícia Forense Computacional: Estudo das Técnicas Utilizadas Para Coleta e Análise de Vestígios Digitais. 2011. p. 20.

ARAUJO, Yuri Saramago Sahione de. **A Insuficiência de Proteção Legal e Desproporcionalidade das Sanções às Vítimas de Ataques Cibernéticos**. 2021. Disponível em: https://www.migalhas.com.br/depeso/338849/a-insuficiencia-de-protecao-legal-e-desproporcionalidade-das-sancoes-as-vitimas-de-ataques-ciberneticos. Acesso em: 13 abr. 2021.

BARRETO. Erick Teixeira. **Crimes cibernéticos sob a égide da Lei 12.737/2012**. 2017. Disponível em: https://ambitojuridico.com.br/edicoes/revista-159/crimes-ciberneticos-sob-a-egide-da-lei-12-737-2012. Acesso em: 04 abr. 2021.

BRAGA, Diego Campos Salgado Braga. **Métodos de investigações no âmbito cibernético**. 2019. Disponível em: https://jus.com.br/artigos/71463/metodos-de-investigacoes-no-ambito-cibernetico. Acesso em: 01 jun. 2021.

BRASIL, Lei Nº 7.232, de 29 de Outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências.

BRASIL. Decreto-Lei Nº 2.848, de 7 de Dezembro de 1940. Código Penal. Art. 154 – A.

BRASIL. Decreto-Lei Nº 3.689, de 3 de Outubro de 1941. Código de Processo Penal. Art. 158.

BRASIL. Lei nº 11.829, de 25 de Novembro de 2008. Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à

produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.

BRASIL. Lei Nº 12.737, De 30 De Novembro De 2012. Dispõe sobre a tipificação criminal de delitos informáticos.

BRASIL. Lei nº 12.850, de 2 de Agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências.

BRASIL. Lei Nº 12.965, de 23 de Abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

BRASIL. Lei nº 13.441, de 8 de Maio de 2017. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente.

BRASIL. Lei Nº 9.609, de 19 de Fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.

BRASIL. Lei Nº 9.983, de 14 de Julho de 2000. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Art. 313-A.

CANSIAN. Adriano Mauro. **Conceitos Para Perícia Forense Computacional**. UNESP – Universidade Estadual Paulista. p. 13.

CARNEIRO, Márcio Rodrigo de Freitas. **Perícia de Informática nos Crimes Cibernéticos**. Investigação e prova nos crimes cibernéticos. Escola de Magistrados da Justiça Federal da 3ª Região. Cadernos de Estudos. São Paulo, 2017. p. 37.

CONSELHO NACIONAL DE JUSTIÇA. **Crimes digitais: O que São, Como Denunciar e Quais Leis Tipificam Como Crime?** 2018. Disponível em: https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime. Acesso em: 10 jun. 2021.

DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes Cibernéticos: Dificuldades Investigativas na Obtenção de Indícios da 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: 22 mai. 2021.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a Computação Forense**. Editora Novatec. São Paulo. 2011. p. 20-21.
FARMER, Dan; VENEMA, Wietse. **Perícia Forense Computacional. Teoria e Pratica Aplicada**. Tradução Edson Furmankiewicz, Carlos Schafranski, Docware Traduções Técnicas; Revisão Técnica Pedro Luís Próspero Sanchez. São Paulo: Person Prentice Hall, 2007.

GONÇALVES, Márcio; AMADIO, Renato Arnaut; GAVILAN, Júlio César; SANTOS, Herlones Wuilles dos. **Perícia Forense Computacional: Metodologias, Técnicas e Ferramentas**. Revista Científica Eletrônica de Ciências Sociais Aplicadas da Eduvale. Jaciara/MT Ano V, Número 07, novembro de 2012. Disponível em: http://eduvalesl.revista.inf.br/imagens_arquivos/arquivos_destaque/LXkEA5FVHGZF1FB_2015-12-19-2-33-33.pdf. Acesso em 29 mai. 2021.

ISONI, Miguel Maurício; VIDOTTI, Silvana Aparecida Borsetti Gregório. **E-crime em Ambientes Digitais Informacionais da Internet**. DataGramaZero – Revista de Ciência da Informação, v. 8, n. 2, 2007. p. 11.

KASPERSKY. **O que é a Deep Web e a Dark Web?** Disponível em: www.kaspersky.com.br/resource-center/threats/deep-web. Acesso em: 27 mar. 2021.

KASPERSKY. **O que é Endereço de IP – Definição e Explicação**. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ip-address. Acesso em 07 jun. 2021.

KUROKAWA, Adriana Shimabukuro; SUIAMA, Sergio Gardenghi; NASCIMENTO, Ana Carolina Previtalli; KAHN, Karen Louise Jeanette; MOTTA, Eduardo Barragan Serôa da. Crimes Cibernéticos: **Manual Prático de Investigação**. Procuradoria da República no Estado de São Paulo. Abril de 2006. p. 39.

LÉVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. — São Paulo: Ed. 34, 1999. p. 116.

LIMA, Adriano Gouveia; DUARTE, Adrienne. **Crimes Virtuais: Conceito e Formas de Investigação**. 2020. Disponível em: https://www.boletimjuridico.com.br/artigos/direito-penal/10382/crimes-virtuais-conceito-formas-investigacao. Acesso em 29 mai. 2021.

LINS, Bernardo Felipe Estellita. **A Evolução da Internet: Uma Perspectiva Histórica.** Cadernos ASLEGIS. Edição 48. 2013. p. 13.

LOPES, Petter Anderson. **Forense Digital**. 2018. Disponível em: https://jus.com.br/artigos/69827/forense-digital. Acesso em 05 jun. 2021.

LUCENA, Jonatas. **Wi-Fi Público e os Crimes Virtuais**. Disponível em: https://www.drjonatas.com.br/wi-fi-publico-e-os-crimes-virtuais. Acesso em 11 jun. 2021.

MATOS, Mariana Maria. **Da Produção e Colheita de Provas no Ambiente Cibernético**. 2014. Disponível em: https://marianamariam.jusbrasil.com.br/artigos/119753698/da-producao-e-colheita-de-provas-no-ambiente-cibernetico. Acesso em: 27 mai. 2021.

MEDEIROS, Diego. **Crimes Virtuais**. 2015. Disponível em: https://jus.com.br/artigos/42734/crimes-virtuais. Acesso em: 12 mar. 2021.

MINISTÉRIO PÚBLICO FEDERAL. **Operação Darknet**. Disponível em: http://www.mpf.mp.br/rs/sala-de-imprensa/docs/outros-documentos/operacao-darknet. Acesso em 17 abr. 2021.

MONTEIRO, Silvana Drumond; FIDENCIO, Marcos Vinicius. **As Dobras Semióticas do Ciberespaço: Da Web Visível à Invisível.** Transinformação, vol. 25, núm. 1, Pontifícia Universidade Católica de Campinas, Brasil. 2013. p. 37.

MORAES, Alexandre Rocha Almeida de; SILVA, Isabella Tucci; SANTIAGO, Bruno. Os Cibercrimes e a Investigação Digital: Novos Paradigmas Para a Persecução Penal. 2020. p. 13.

MORAES, Francilaine Munhoz. **Discurso jornalístico on-line: a perspectiva crítica da narratividade**. Dissertação de Mestrado. Programa de Pós-Graduação em Comunicação da Universidade de Brasília, 2004. p. 34.

NASCIMENTO, Laura Pereira do; SILVA, Rosane Leal da. **Crianças e Adolescentes Internautas como Alvo da Criminalidade Online: Pedofilia e Pornografia na Internet**. 2014. Disponível em: https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/11741/1541. Acesso em: 13 mai. 2021.

NASCIMENTO, Samir de Paula. **Cibercrime: Conceitos, Modalidades e Aspectos Jurídicos-Penais**. 2019. Disponível em: https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais. Acesso em: 01 abr. 2021.

NOGUEIRA, Cipriano Cássio; VAS, Braz Batista. **Percepções Sobre Ciberespaço e Territorialidade Digital: Estudo Exploratório com Foco em Aspectos Socioculturais Presentes Na Deep Web e Dark Web.** Revista Observatório, v. 5, n. 6, 2019, p. 22.

OLIVEIRA. Neide Cardoso de. **Atuação do Ministério Público Federal no Combate aos crimes Cibernéticos**. 2019. Disponível em:

https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cspcco/apresentacoes-em-eventos/eventos-em-2019/AudinciaPblicaNeideMaraCavalcantiANPR.pdf. Acesso em: 19 mai. 2021.

RIBEIRO, Lígia Maria. **A História da Internet**. 1998. Disponível em: https://paginas.fe.up.pt/~mgi97018/historia.html. Acesso em: 05 mar. 2021.

RODRIGUES, Felipe José Souza; CARDOSO, Sarah de Araújo Mendes; MARWELL, Tatiana Eulálio Dantas Guedes. **Utilização da Infiltração Virtual nas Operações Policiais Para o Combate ao Crimes Sexuais Contra Crianças e Adolescentes**. Research, Society and Development, v. 10, n. 7, e24710414152, 2021. p. 03.

RONCADA, Rodiner. **A Prova da Materialidade Delitiva nos Crimes Cibernéticos**. Investigação e Prova nos Crimes Cibernéticos. Escola de Magistrados da Justiça Federal da 3ª Região. Cadernos de Estudos. São Paulo, 2017. p. 178.

SAFERNET. **Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos**. 2018. Disponível em: https://indicadores.safernet.org.br. Acesso em 02 mai. 2021.

SÃO PAULO. Lei Nº 12.228, de 11 de Janeiro de 2006. Dispõe sobre os estabelecimentos comerciais que colocam a disposição, mediante locação, computadores e máquinas para acesso à internet e dá outras providências.

SÃO PAULO. Tribunal Regional Federal. (3. Câmara Criminal). Recurso em Sentido Estrito 00131528920144036181. Relator: Desembargador Federal José Lunardelli, data de julgamento: 11/12/2018. Publicado em: e-DJF3 Judicial 07/01/2019.

SHIMABUKURO, Adriana. **Cibercrime: Quando a Tecnologia é Aliada da Lei**. Investigação e prova nos crimes cibernéticos. Escola de Magistrados da Justiça Federal da 3ª Região. Cadernos de Estudos. São Paulo, 2017. p. 22.

SILVA, Fernanda Viero da; FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. **Deep Web e Dark Web: Implicações Sociais e Repercussões Jurídicas**. Revista Eletrônica Direito e Sociedade, Canoas, v. 8, n. 2, 2020. p. 228-229.

SILVA, Jorge Luiz Silva da. **A Prova nos Crimes que se Utilizam das Redes Sociais**. 2016. Disponível em: https://ajufesc.org.br/wp-content/uploads/2017/02/Jorge-Luiz-Silva-da-Silva.pdf. Acesso em: 03 jun. 2021.

TENTARDINI, Caroline; ROSALES, Luana. **80% dos Crimes Virtuais Investigados no RS Estão Ligados à Pedofilia**. 2019. Disponível em: https://www.sul21.com.br/ultimas-noticias/geral/2019/08/80-dos-crimes-virtuais-investigados-no-rs-estao-ligados-a-pedofilia. Acesso em: 17 abr. 2021.

VIGNOLI, Richele Grenge; MONTEIRO, Silvana Drumond. **Deep Web *e* Dark Web: Similaridades e Dissiparidades no Contexto da Ciência da Informação**. *Transinformação*, v. 32, e190052, 2020. Disponível em: https://doi.org/10.1590/2318-0889202032e190052. Acesso em 12 abr. 2021.