Data da aprovação: ____/____/____

INVESTIGAÇÃO POLICIAL NA *DEEP WEB*

Rafaela Guerra Barros[1]

Luiz Felipe Pinheiro Neto[2]

RESUMO

O presente trabalho tem como objetivo principal abordar a temática da investigação policial na *deep web.* Busca-se também apresentar, para o leitor, as principais técnicas investigativas utilizadas, conceitos iniciais sobre o fenômeno do *cybercrime* e as especificidades relacionadas a esse submundo da internet. Além disso, este trabalho objetiva elucidar quais são os principais delitos que ocorrem nesse meio. Ao longo dessa pesquisa, o texto terá um maior foco no contexto brasileiro, trazendo diversas legislações vigentes e realizando comparações com alguns países, que são referência no combate a esses delitos. Utiliza-se no desenvolvimento desta pesquisa exploratória o método dedutivo e a forma qualitativa de análise dos resultados e conclusões.

Palavras-chave: Deep web. Cybercrimes. Dark web. Investigação policial. Crimes de ódio. Exploração sexual infantojuvenil.

POLICE INVESTIGATION ON THE DEEP WEB

ABSTRACT

The present work has as main objective to approach the theme of police investigation on the deep web. It also seeks to present to the reader the main investigative techniques used, initial concepts about the phenomenon of cybercrime and the specifics related to this internet underworld.In addition, this work aims to elucidate which are the main crimes that occur in this environment. Throughout this research, the text will have a greater focus on the Brazilian context, bringing several

[1] Acadêmica do Curso de Direito do Centro Universitário do Rio Grande do Norte/UNIRN. E-mail: rafaelaguerra98@gmail.com

[2] Professor Orientador do Curso de Direito do Centro Universitário do Rio Grande do Norte/UNIRN. E-mail:professorluizpinheiro@gmail.com

current laws and making comparisons with some countries that are reference in the fight against these crimes. In the development of this exploratory research, the deductive method and the qualitative way of analyzing the results and conclusions were used.

Keywords: Deep web. Cybercrimes. Dark web. Police investigation. Hate crimes. Child sexual exploitation.

1 INTRODUÇÃO

A existência de crimes acompanhou a história evolutiva do homem, ao longo dos anos, diversos tipos de delitos surgiram para acompanhar as mutações da sociedade.

É válido pontuar que o surgimento da internet e das tecnologias de informação foi uma das maiores transformações sociais que a humanidade experimentou. Nesse sentido, os delitos acompanharam essa evolução tecnológica e com isso surgiu o conceito de crimes cibernéticos, com o advento desses crimes - no meio digital - as formas de prevenção, repressão, investigação e combate também necessitaram de uma atualização.

O objeto principal de estudo deste trabalho será a investigação policial na *deep web*. Esta consiste na parte indexada e de difícil acesso da internet, e, a investigação policial nesse meio é fundamental, pois objetiva o combate à proliferação de diversas condutas ilícitas que acontecem – cotidianamente - nessa parte da internet.

O segundo capítulo, deste estudo, aborda brevemente o surgimento e evolução dos crimes cibernéticos, além disso, o capítulo irá - por meio de dados de diversos estudos - demonstrar a enorme ascensão desses delitos, na contemporaneidade. Já o terceiro capítulo irá expor os diversos dispositivos legais que servem para reprimir as condutas ilícitas na internet.

Para que se consiga compreender esse estudo de uma forma eficaz, torna-se necessário conceituar e explicar os principais assuntos relacionados a *deep web,* além

disso, é importante também abordar os principais delitos que ocorrem nesse meio e as suas especificidades. Esses objetivos serão trabalhados no quarto e no quinto capítulo deste trabalho.

O importante tema da investigação policial e dos principais mecanismos adotados para combater esses delitos serão retratados no sexto capítulo deste artigo. Por fim, a conclusão desse estudo trará os variados resultados e as considerações finais obtidas por meio desta pesquisa.

Vale ressaltar, que foi adotada - na elaboração deste trabalho exploratório- a metodologia de pesquisa qualitativa pelo método dedutivo, devido à escolha desse método, o presente artigo buscará partir de um contexto mais universal do mundo do *cybercrime,* para chegar na especificidade do fenômeno da investigação policial, na *deep web.*

Além do mais, é válido pontuar que a abordagem metodológica adotada no presente trabalho, foi baseada em pesquisas bibliográficas, associadas a revisões de literatura nacional e estrangeira, diversos artigos e periódicos, sítios da internet, entre outros, foram fundamentais para a formulação da argumentação e a obtenção do respaldo científico.

2 SURGIMENTO E EVOLUÇÃO DOS CRIMES CIBERNÉTICOS

De início, mostra-se necessário comentar que, para que aconteça uma completa compreensão do fenômeno do *Cybercrime*[3], é válido iniciar com a exposição do seu contexto de surgimento e evolução.

A sociedade é dinâmica, ou seja, está em constante transformação. Essas transformações sociais fizeram com que os costumes, as formas de comunicação e o estilo de vida das pessoas mudassem.

Um desses fatores de transformação social - que trouxe diversas mudanças - foi a ascensão da internet e a naturalização do seu uso na vida cotidiana das pessoas. Lévy (1993, apud, Kohn ,2007, p.6) expõe que a interface digital alarga o campo do visível, evidenciando a emergente evolução que diversificou, facilitou e transmitiu as informações de forma instantânea e ampla.

[3] Do inglês, significa crimes cibernéticos. (tradução livre)

É válido pontuar que o crime, por ser um fato social[4], também muda e se adapta de acordo com as novas dinâmicas sociais. Devido a essas mudanças, os criminosos perceberam que este meio tecnológico seria muito proveitoso para seus objetivos e se adaptaram ao mundo digital. Assim, as práticas ilícitas na internet começaram a surgir e alcançaram um patamar inesperado. (Fernandes, 2013, p.143)

Esses delitos que acontecem no meio digital são chamados de crimes cibernéticos. Essas condutas típicas praticadas na internet trazem diversas consequências negativas - para a sociedade - e podem ser divididas em *cybercrimes* abertos e crimes exclusivamente cibernéticos (NOGUEIRA, WENDT, 2013).

Sobre isso, Nogueira e Wendt (2013) comentam que:

> Conforme anteriormente mencionado, os "crimes cibernéticos" em "crimes cibernéticos abertos" e crimes "exclusivamente cibernéticos". Com relação aos crimes cibernéticos "abertos", são aqueles que podem ser praticados de forma tradicional ou por intermédio de computadores, ou seja, o computador é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele. Já os crimes "exclusivamente cibernéticos" são diferentes, pois eles somente podem ser praticados com a utilização de computadores ou de outros recursos tecnológicos que permitem o acesso à internet.

Para ilustrar melhor os riscos de segurança e os riscos financeiros contemporâneos desencadeados pelo fenômeno dos crimes cibernéticos, mostra-se necessário elencar alguns dados importantes. Segundo Steve Morgan, editor chefe da *Cybersecurity Ventures*[5], há uma previsão de que os custos dos danos causados pelos *cybercrimes* vão custar ao mundo, o valor anual de U$ 6 trilhões, até o ano de 2021. (MORGAN,2020).

Outros dados alarmantes - retirados de um levantamento da SaferNet[6] Brasil - mostram que, diariamente, em média, são registrados 366 crimes cibernéticos no Brasil. Além disso, a SaferNet Brasil, em parceria com o Ministério Público Federal

---

[4] é fato social toda maneira de fazer, fixada ou não, suscetível de exercer sobre o indivíduo uma coerção exterior; ou ainda, toda maneira de fazer que é geral na extensão de uma sociedade dada e, ao mesmo tempo, possui uma existência própria, independentemente de suas manifestações individuais.(FONTES, 1999)

[5] A Cybersecurity Ventures é o pesquisador líder mundial e a Página UM para a cibereconomia global e uma fonte confiável de fatos, números e estatísticas sobre segurança cibernética. (MORGAN, 2020)

[6] A SaferNet Brasil é uma associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, sem vinculação político partidária, religiosa ou racial. Fundada em 20 de dezembro de 2005 por um grupo de cientistas da computação, professores, pesquisadores e bacharéis em Direito, a organização surgiu para materializar ações concebidas ao longo de 2004 e 2005, quando os fundadores desenvolveram pesquisas e projetos sociais voltados para o combate à pornografia infantil na Internet brasileira. (SAFERNET, 2008)

computou mais de 133.732 queixas de *cybercrimes* feitas em 2018 no Brasil.(ESTADO DE MINAS, 2019).

Esse mesmo estudo da “SaferNet Brasil” mostrou que o crime mais denunciado, em 2018, no Brasil foi o crime de pornografia infantil, seguido por apologia e incitação a crimes contra a vida, violência contra mulheres/misoginia, xenofobia (principalmente contra nordestinos), racismo, LGBTfobia e entre outros (SaferNet Brasil 2018).

Esses dados e estudos realizados, por diferentes organizações internacionais e nacionais, demonstram que o Cibercrime é um fenômeno marcante em ascensão e que está presente na realidade brasileira.

3 CONTEXTO BRASILEIRO E ASPECTOS JURÍDICOS RELACIONADOS AO FENÔMENO DO CYBERCRIME

Para que ocorra um completo entendimento do contexto dos crimes cibernéticos, mostra-se necessário comentar um pouco sobre a história desses crimes no Brasil e sobre as legislações existentes.

É imprescindível explanar que o Brasil, no quesito legislação e investigação dos crimes virtuais, teve um início e desenvolvimento tardio, em comparação a outros países, como os Estados Unidos, que teve a sua primeira legislação[7], tratando de crimes cibernéticos, aprovada - no ano de 1980 - pelo congresso americano. Já os países do continente europeu organizaram a importante Convenção de Budapeste ou Convenção sobre o cibercrime, no ano de 2001. (BORTOT, 2017, p.345-346)

Ainda sobre a legislação estrangeira, é importante destacar outras leis norte-americanas destinadas à repressão desses crimes. A Lei Fraude e Abuso de Computador (CFAA)[8] que foi publicada no ano de 1986 (mil novecentos e oitenta e seis) sofreu diversas emendas, mas ainda está vigente.

Outra forma importante de combate aos cibercrimes foi o Plano de Ação Nacional de Segurança Cibernética. Esse plano foi feito na administração do

[7] A primeira legislação tratando dos crimes cibernéticos foi aprovada no final da década de 1980, pelo Congresso americano, e foi chamada de Electronic Communication Privacy Act (ECPA3 - Lei de Privacidade de Comunicação Eletrônica), sendo amplamente utilizada pelo FBI e a National Security Agency (NSA4 - Agência de Segurança Nacional), além de servir como ponto de partida para a legislação de outros país es. (BORTOT, 2017)

[8] Computer Fraud and Abuse Act- CFAA.

presidente Barack Obama e promoveu por meio de diversos investimentos um maior fortalecimento da segurança cibernética dos Estados Unidos (BORTOT, 2017, p.344-345).

Além da importante convenção de Budapeste organizada no continente europeu, a Europa detém o importante Centro Europeu da Cibercriminalidade, que trabalha no combate efetivo dos *cybercrimes*.

Além disso, é mister salientar que o conselho europeu possui diversas outras convenções importantes para um efetivo enfrentamento aos delitos cibernéticos, entre essas convenções, mostra-se necessário destacar a Convenção para a Prevenção do Terrorismo (2005) , que contem dispositivos específicos relacionados a condutas criminosas de terrorismo na internet, a Convenção de Lanzarote (2007), que traz dispositivos relacionados a práticas criminosas ligadas à exploração sexual infanto-juvenil no meio digital e a Convenção de Proteção de Dados, que também é extremamente importante (CONSELHO EUROPEU, 2020).

Sobre a convenção de Budapeste, é mister esclarecer que o Brasil passou um longo período de tempo sem participar dessa aliança. Mas, no ano de 2019, a República Federativa do Brasil recebeu um convite para aderir a famosa convenção e está realizando o processo de adesão. Essa adesão é muito importante, visto que irá ajudar na realização de um combate mais efetivo aos crimes cibernéticos e irá proporcionar um acesso mais ágil das provas que se encontram sob jurisdição estrangeira. (BRASIL, SECRETARIA GERAL, 2020)

Bortot (2017, p.346) traz um importante comentário sobre essa fundamental convenção:

> Após a análise supra, torna-se necessário reconhecer a importância da Convenção de Budapeste, visto que nos últimos anos ela teve um impacto global e resultou numa legislação mais forte e mais harmonizada no domínio da cibercriminalidade a nível mundial, numa cooperação internacional mais eficaz na investigação e na instauração de processos penais contra crimes cibernéticos e em parcerias público-privadas mais estreitas. Assim, 15 anos após sua adoção, a Convenção de Budapeste continua sendo o tratado internacional mais eficaz em matéria de crimes cibernéticos e do Estado de Direito no ciberespaço. Este fato é resultado da consciência excepcional dos redatores da Convenção, pois eles sabiam que estavam escrevendo algo que não seria alterado em poucos anos, e assim, a convenção deveria ser um instrumento estável. Para tanto, eles redigiram brilhantemente em antecipação ao futuro, acomodando novas tecnologias.

Apesar do desenvolvimento tardio brasileiro, o país possui algumas legislações específicas importantes para o combate e prevenção, no cenário nacional. Entre elas a lei 12.735/2012, a qual tipificou algumas condutas praticadas contra

sistemas informatizados. Além disso, é válido falar sobre a lei 12.737/201216, popularmente conhecida como “Lei Carolina Dieckmann[9]”, que foi importante para tipificar condutas de invasão de computadores e de obtenção, alteração ou destruição ilícita de dados” (BORTOT, 2017, págs, 350-351).

Posteriormente, surgiu a lei 12.965/2014, que é conhecida como o marco civil da internet ou constituição da internet brasileira. Sobre essa legislação Nascimento (2019) comenta que:

> Em 2014 foi aprovado no Congresso Nacional a Lei 12.965/2014, o Marco Civil da Internet (MCI, que ficou conhecido como a Constituição da Internet Brasileira), apresentando de maneira sistematizada dez princípios elaborados pelo Comitê Gestor da Internet brasileira. Um dos objetivos do Marco Civil foi definir em lei os direitos oriundos da utilização da internet, prevendo o que se pode ou não fazer no âmbito civil, antes de se criminalizar condutas praticadas na internet. Até certo ponto a Lei do Marco Civil foi produzida como um movimento antagônico aos projetos de crimes na internet que tramitavam no Congresso Nacional e que acarretaram na criação da Lei 12.737/2012.

Além dessas leis específicas, o Brasil possui alguns outros dispositivos que ajudam a tipificar condutas ilícitas, praticadas no meio digital. Sobre essas outras legislações Bortot (2017, p.349) expõe que:

> Além dessas legislações supracitadas, que serão tratadas de forma mais abundante, ainda tem-se a Lei nº 11.829/2008, que combate a pornografia infantil na internet; a Lei nº 9.609/1998, que trata da proteção da propriedade intelectual do programa de computador; a Lei nº 9.983/2000, que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da Administração Pública; a Lei nº 9.296/1996 disciplinou a interceptação de comunicação telemática ou informática; e a Lei nº 12.034/2009, que delimita os direitos e deveres dentro da rede mundial, durante as campanhas eleitorais

Também, se mostra importante comentar, brevemente, sobre a importância da colaboração internacional investigativa para a repressão de diversos delitos, no mundo digital. Visto que, o maior alcance mundial de pessoas proporcionadas pela internet acarretou uma maior interligação criminosa entre diversos países.

Alguns mecanismos auxiliam no combate e na investigação internacional dos crimes cibernéticos, um deles é o fato de que o Brasil está sob jurisdição do Tribunal

[9] No fim de novembro a Presidente da República sancionou às pressas a Lei nº 12.737/2012, apelidada de Lei Carolina Dieckmann, já que o assunto passou a ser tratado em regime de urgência após o episódio em que fotos íntimas da famosa atriz vieram a público em razão da invasão de privacidade e extorsão a que fora submetida a estrela global (RIBAS, 2020).

Penal Internacional, esse importante tribunal procura julgar os crimes internacionais na insuficiência das legislações nacionais.

Também, é válido comentar sobre a INTERPOL, que é a Organização Internacional de Polícia Criminal que possui um eficiente banco de dados com informações de criminosos procurados e outras ferramentas que auxiliam a investigação e repressão criminal.

Ressalta-se que, apesar da existência de diversas legislações específicas sobre os crimes cibernéticos, há uma enorme lacuna legislativa atual e um combate deficiente aos *cybercrimes* no país, principalmente, nos delitos que ocorrem na chamada *deep web*[10]. Essas falhas brasileiras não estão conseguindo acompanhar – efetivamente - a proliferação dos delitos virtuais e isso acaba criando um ambiente com um clima de impunidade e insegurança.

4 DEEP WEB: O SUBMUNDO DA INTERNET

Para entender mais sobre os crimes cibernéticos, é imprescindível comentar sobre a *deep web*, expondo os seus conceitos, especificidades, os principais delitos que ocorrem nesse meio e os desafios enfrentados na sua investigação.

É válido expor que a internet pode ser dividida em *deep web* e *surface web.* A *surface web* é a parte mais visível da internet, que é acessada facilmente, e, diariamente, pelos usuários. Já a *deep web* tem o seu conteúdo não indexado, "invisível", impossibilitado de ser encontrado pelos navegadores[11] comuns. Normalmente, para acessar a *deep web,* são utilizados programas de rede anônima que permitem o compartilhamento anônimo de arquivos e a navegação incógnita. Os exemplos mais famosos desses *softwares*[12] que facilitam a entrada nesse submundo da internet *são*: o Tor, i2P e o FreeNet (BARRETO; SANTOS, 2019).

---

[10] Do inglês, significa internet profunda. (tradução livre)

[11] Basicamente, os navegadores transformam as páginas codificadas em HyperText Markup Language (HTML) para uma visualização compreensível para o usuário comum. O HTML é um padrão de marcação de hipertexto (textos, imagem, vídeo e áudio) que define como os elementos de uma página devem ser exibidos. Assim, ao invés dos usuários de Internet terem que entender o comando navegador (marcação que faz a palavra aparecer em negrito), o navegador exibe a palavra navegador em negrito, facilitando a compreensão dos usuários. (BOZZA, 2011)

[12] O software é todo programa rodado em um computador, celular ou dispositivo que permita ao mesmo executar suas funções. Eles vão desde sistemas operacionais, como Windows, macOS, iOS e Android aos apps que você usa todos os dias. (GOGONI,2020)

Mostra-se necessário falar um pouco sobre as suas características principais, entre elas é válido destacar a segurança, o anonimato, a existência de um código aberto e a descentralização dos nós de conexão[13]. (BARRETO; SANTOS, 2019)

Sobre essas características principais da *deep web*, Barreto; Santos (2019) expõe que:

> a) Anonimato: O principal objetivo da utilização de redes cujo conteúdo não é indexado na surface web é proporcionar anonimato a seus usuários. Nesse cenário podemos destacar: pessoas comuns na busca de conteúdo com garantia de privacidade; blogueiros, ativistas e jornalistas, para a publicação de suas opiniões, ideias e críticas e denúncias, principalmente em regiões do globo onde a censura governamental, política e de grupos extremistas não permite que certos conteúdos sejam levados ao conhecimento das pessoas de outros países, além de criminosos que buscam meios para não serem alcançados pela aplicação da lei penal.
> b) Segurança: essa peculiaridade decorre da conexão criptografada entre os nós componentes de rede[...]
> c) código aberto: [...] um software de código aberto ou *open source* é aquele que pode ser manipulado por um usuário/ programador de forma a eliminar suas vulnerabilidades e/ou problemas e propor novas funcionalidades e melhoramentos, a fim de beneficiar a comunidade de usuários.

Outro conceito relevante que precisa ser esclarecido é o conceito de *darknet.* A *darknet* ou *dark web* nada mais é do que uma parte da *deep web* ainda mais "profunda" e criptografada, com domínios que dificultam ainda mais o acesso e garantem ainda mais o anonimato e a segurança dos usuários. É nessa parte da rede que ocorrem a maiorias dos delitos cometidos na *deep web.* (BARRETO; SANTOS, 2019)

É necessário deixar claro que navegar pela *deep web* e pela rede *dark web* não se configura uma conduta ilícita e criminosa, visto que, diversos usuários utilizam a *deep web* como uma ferramenta de busca, aquisição de conteúdo, livros, filmes, aprendizado e de exercício da liberdade de expressão. Entretanto, como foi citado anteriormente, inúmeras condutas típicas são cometidas – diariamente - na *deep web* e isso gera diversos malefícios para a sociedade. (KUMMER, 2017)

A respeito desses ilícitos cometidos na *deep web*, é mister explanar que nesse "submundo da internet" são encontradas diversas páginas destinadas a grupos

[13] as Redes Descentralizadas que trataremos neste post não necessitam que os dispositivos que a compõem estejam conectados a um servidor central e não "somam forças" de processamento ou colaboram entre si como na rede distribuída. É a rede que promove a famosa "liberdade" (SAISSE,2019).

terroristas, grupos neonazistas[14], extremistas, canibais, vendas de armas, documentos falsificados, informações confidenciais, tutoriais de haking e de criações de virus, tráfico de drogas, tráfico humano, pornografia infantil, assassinos de aluguel e entre outros.(MARRIEL; CÁSSIA, 2019)

5 ESPECIFICIDADES DOS PRINCIPAIS CRIMES ENCONTRADOS *NA DEEP WEB*

Para que ocorra um real entendimento dos possíveis crimes existentes nesse meio, novamente é imprescindível pontuar a diferença entre os crimes exclusivamente digitais, que são aqueles crimes que só podem ocorrer na internet e os crimes cibernéticos abertos, que podem acontecer tanto no meio não digital, como no meio digital como por exemplo: a extorsão, os crimes de ódio, o tráfico de drogas e de armas e entre outros. Nesse caso, a internet seria só um meio de cometimento desses delitos.

Assim, neste capítulo será brevemente retratado os principais delitos encontrados no submundo da internet, esses crimes de maior incidência na *deep web* são em sua grande maioria crimes cibernéticos abertos. É válido pontuar que essa breve explicação irá promover uma maior compreensão sobre o fenômeno da *deep web* e do *cybercrime.*

5.1 TRÁFICO DE DROGAS

Primeiramente, é válido expor o crime de tráfico de drogas está previsto na lei de número 11.343/06, em seu artigo 33:

> Art. 33. Importar, exportar, remeter, preparar, produzir, fabricar, adquirir, vender, expor à venda, oferecer, ter em depósito, transportar, trazer consigo, guardar, prescrever, ministrar, entregar a consumo ou fornecer drogas, ainda que gratuitamente, sem autorização ou em desacordo com determinação legal ou regulamentar:
> Pena - reclusão de 5 (cinco) a 15 (quinze) anos e pagamento de 500 (quinhentos) a 1.500 (mil e quinhentos) dias-multa. [...]

[14] Nazismo é crime no Brasil. O artigo 20 da lei 7.716/1989 ressalta que "fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo", é passível de "reclusão de dois a cinco anos e multa". O material deve ser recolhido imediatamente, e as mensagens ou páginas respectivas na internet devem ser retiradas do ar (VEIGA, 2020).

Essa é uma conduta criminosa plenamente conhecida pelo povo brasileiro. Devido a sua grande ocorrência e influência na nossa sociedade. É válido comentar que o crime de tráfico de drogas pode ser praticado, em diversos meios diferentes, inclusive no meio digital.

A ocorrência desse crime, no meio digital, acontece principalmente na *darknet*, parte mais "obscura" da *deep web* em que ocorrem a maioria dos ilícitos. Existem na *dark web,* vários sites e os famosos *black markets*[15] que são utilizados para o gigantesco e lucrativo comércio de diversas substâncias ilícitas, principalmente as drogas sintéticas como: Ecstasy, MDMA, LSD e NBONE e entre outras.(BARRETO; SANTOS, 2019)

Sobre o assunto, é válido pontuar que muitos criminosos utilizam da característica do anonimato e segurança da *deep web*, aproveitam da menor vigilância e da maior facilidade para ocorrência do crime e aplicam diversas ferramentas como a tecnologia *mirror,* que consiste em vários endereços possíveis para acessar o mesmo site e as criptomoedas [16]que dificultam o trabalho de investigação policial. Entretanto, a polícia investigativa - ao redor do mundo - já conseguiu acabar com diversos mercados ilícitos e conseguiram prender alguns criminosos (BARRETO; SANTOS, 2019).

Um exemplo famoso de investigação policial em mercados de vendas de drogas na *deep web,* foi o que aconteceu com a conhecida *Silk Road*[17]*.* A *Silk Road* era um dos principais sites de comércio de drogas ilícitas da *darknet* e o FBI[18] conseguiu prender e condenar o seu principal dono e tirar o site original do ar.

5.2 TRÁFICO DE ARMAS

Inicialmente, é válido explanar que não tem um artigo específico sobre o tráfico de armas no Código Penal brasileiro, mas a previsão dessa conduta ilícita se

[15] Do inglês, significa mercado negro (tradução livre)
[16] As criptomoedas nada mais são do que moedas virtuais, utilizadas para a realização de pagamentos em transações comerciais. Ou seja, possuem a mesma função de comprar mercadorias e serviços que as moedas já conhecidas por nós, como o Real e o Dólar.Além do fato de serem completamente virtuais, existem três características básicas que diferenciam as criptomoedas das moedas regulares: a descentralização, o anonimato e custo zero de transação.(SCHIOCHETTI, 2019)
[17] Do inglês, significa rota da seda (tradução livre)
[18] *sigla de* Federal Bureau of Investigation. Serviço Federal de Investigação dos Estados Unidos da América (tradução livre).

encontra na Lei 10.826/03 (estatuto do desarmamento), mais especificamente, nos seus artigos 18º a 21º. Sobre isso, é válido expor os artigos 18º e 19º:

> Art. 18. Importar, exportar, favorecer a entrada ou saída do território nacional, a qualquer título, de arma de fogo, acessório ou munição, sem autorização da autoridade competente:
> Pena - reclusão de 4 (quatro) a 8 (oito) anos, e multa.
> Art. 19. Nos crimes previstos nos arts. 17 e 18, a pena é aumentada da metade se a arma de fogo, acessório ou munição forem de uso proibido ou restrito.

O tráfico de armamentos possui uma enorme incidência nos mercados negros da *deep web,* inúmeros vendedores e compradores se aproveitam da falta de fiscalização e do menor preço para poder adquirir armas de fogo, acessórios e munição, sem autorização das autoridades competentes. Além da problemática da compra de armamentos de uso restrito[19] e de uso permitido sem autorização, um dos maiores problemas decorrentes dessa prática ilícita no mundo digital, é a enorme quantidade de grupos criminosos que aproveitam da compra facilitada desses armamentos para se equiparem com armas de grande potência e realizarem as suas atividades criminosas (BARRETO; SANTOS, 2019).

5.3 EXPLORAÇÃO SEXUAL INFANTIL

Como já foi exposto anteriormente, a navegação pela *deep web* garante uma maior segurança, anonimato e uma "falsa" sensação de impunidade aos seus usuários. Essas são características que facilitam uma maior ocorrência de crimes. Sobre isso, é válido pontuar que um dos crimes com maior repercussão e ocorrência no submundo digital é o crime de abuso e exploração sexual de crianças e adolescentes.

A ocorrência desse delito é tão grande na *deep web,* que segundo uma pesquisa realizada pela Universidade de Portsmouth[20], 80% do tráfego na *deep web* estava relacionado à pornografia infantil. Esse estudo foi feito por meio de uma longa

[19] Na leitura das regras, não sabemos o que é uma arma de fogo, o que é uso permitido, o que é uso restrito ou até o que é um calibre, uma munição ou um acessório, razão pela qual precisamos alicerçar nosso estudo ao Decreto 3.665/2000, ao Decreto 5.123/2004 e ao Decreto 9.493/2018 (que revoga o primeiro), que tratam da fiscalização de produtos controlados, dentre outros, e definem diversos conceitos referentes a armas de fogo.(SCHAUN,2019)

[20] A Portsmouth é uma das melhores entre as universidades consideradas modernas do Reino Unido. (GRADEUP, 2020)

análise de sites que possuem a ferramenta Tor, que é um *software* que facilita a navegação no submundo da internet. (GARCIA, 2015)

A SaferNet[21] traz outros dados alarmantes sobre a ocorrência de delitos relacionados à pornografia infantil, segundo essa renomada organização, em 14 anos, a Policia Federal do Brasil recebeu e processou em média 180.009 (cento e oitenta mil e nove) denúncias anônimas do crime de pornografia infantil, esses crimes ocorreram em média em 48.995 (quarenta e oito mil novecentos e noventa e cinco) endereços de rede diferentes. Esses dados demonstram mais uma vez a enorme incidência dessas condutas ilícitas na contemporaneidade. (SAFERNET, 2019).

Mostra-se válido expor os principais dispositivos legais que tipificam algumas condutas ilícitas praticadas contra as crianças e adolescentes, no âmbito do abuso e da exploração sexual infanto-juvenil. Esses dispositivos dispõem, principalmente, sobre a distribuição, publicação, venda, inclusive no meio digital, de registros fotográficos, vídeos de pornografia infantil e procuram criminalizar a aquisição e a posse desses materiais e outras condutas relacionadas à pedofilia na internet.

> ECA - Lei nº 8.069 de 13 de julho de 1990
> Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências.
> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008)
> 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: (Incluído pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)

Para que seja possível uma ampla compreensão a respeito desse delito, é necessário um esclarecimento sobre a faixa etária do sujeito passivo do crime em questão. Sobre isso, Pinheiro e Sadalla (2019, p.4) expõe que:

> Para melhor entendimento, o art. 2º do Estatuto da Criança e do Adolescente (ECA) define como criança o indivíduo de até doze anos de idade, e

[21] A SaferNet Brasil é uma associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, sem vinculação político partidária, religiosa ou racial. Fundada em 20 de dezembro de 2005 por um grupo de cientistas da computação, professores, pesquisadores e bacharéis em Direito, a organização surgiu para materializar ações concebidas ao longo de 2004 e 2005, quando os fundadores desenvolveram pesquisas e projetos sociais voltados para o combate à pornografia infantil na Internet brasileira. (SAFERNET, 2008)

> adolescente aquele entre doze e dezoito anos. A delimitação etária é importante para enfrentar o crime de pornografia infantil, tipificado no Brasil, especificamente, pela Lei n° 8.829/08, tendo em vista que as previsões do Código Penal, no art. 217-A e no recente 218-C, referentes ao Estupro de Vulnerável e Pornografia Infantil, respectivamente, limitam-se ao menor de 14 anos (BRASIL, 2018). Logo, a faixa etária da vítima determinada no ECA é mais abrangente, oferecendo maior proteção infanto-juvenil.

Além do mais, é imprescindível relatar que outros dispositivos legais - do ordenamento jurídico brasileiro - tipificam condutas de exploração sexual e trazem diversas disposições com o intuito de proteger as crianças e os adolescentes. Entre essas normas legais, é válido comentar que a Constituição Federal do Brasil busca proteger a dignidade da pessoa humana, a integridade física, psíquica e moral da criança e do adolescente e aborda - expressamente - em seu artigo 227,§ 4º que a lei irá punir de maneira severa o abuso, a violência e a exploração sexual da criança e do adolescente.

Outra lei que tipifica essas condutas ilícitas é o artigo 217 do Código Penal Brasileiro que dispõe sobre o delito de estupro de vulnerável, esse crime pode ocorrer inclusive sem contato físico, facilitando ainda mais a sua incidência no meio digital. Sobre isso, Soares e Martins (2017, p.225) expõe que:

> No tocante ao crime de estupro de vulnerável, previsto no art. 217-A do CP, recentemente, a Quinta Turma do o Superior Tribunal de Justiça (STJ) adotou o entendimento pela dispensabilidade do contato físico para a caracterização deste crime. Neste caso, a decisão do STJ, certamente orientará decisões similares dos juízes e juízas de todo país. É por isso que entendemos que, desde que as vulneráveis também podem ser vítimas do estupro virtual, desde que sejam forçadas, chantageadas ou ameaçadas, por meio virtual, a praticar atos libidinosos consigo mesmas a fim de transmitir ou enviar para o sujeito do crime.

5.4 CRIMES DE ÓDIO

Primeiramente, mostra-se necessário conceituar os chamados crimes de ódio ou os crimes motivados pelo preconceito, esses crimes são normalmente direcionados às minorias e consistem em algum tipo de violência, podendo ser física, psíquica ou moral, direcionada a algum grupo específico (ORTEGA, 2015).

Sobre isso, Ortega (2015) comenta que:

> os grupos afetados por esse delito discriminatório são os mais variados possíveis, porém o crime de ódio ocorre com maior frequência com as chamadas minorias sociais. são consideradas minorias sociais aqueles

> conjuntos de indivíduos que histórica e socialmente sofreram notória discriminação. como exemplo podemos citar as vítimas deracismo, homofobia, xenofobia, etnocentrismo, intolerância religiosa e preconceito com deficientes. o crime de ódio é mais do que um crime individual; é um *delito que atenta à dignidade humana e prejudica toda a sociedade e as relações fraternais que nela deveriam prevalecer*. ele produz efeito não apenas nas vítimas, mas em *todo o grupo a que elas pertencem*. assim sendo, podemos classificá-lo como um crime coletivo de extrema gravidade.

Ainda sobre esse assunto, é importante expor que o Brasil não possui, em seu ordenamento jurídico, uma lei clara e concisa que trata de forma específica dos crimes de ódio, o que acontece no país é a utilização da lei 7.716/89, que trata do preconceito de raça e cor, etnia, religião e também serve para criminalizar a conduta da LGBTfobia[22], visto que o Supremo Tribunal Federal equiparou as duas condutas. (NUCCI, 2019)

Além disso, também são utilizados alguns dispositivos do Código Penal, como por exemplo aqueles que trazem a tipificação da conduta do feminicídio[23]. A reprovação às condutas relacionadas aos crimes de ódio, também recebem amparo na Constituição Federal do Brasil, na Declaração Universal dos Direitos Humanos e em outros dispositivos do ordenamento jurídico brasileiro. (NUCCI, 2019)

É imprescindível comentar que pela forte possibilidade do anonimato, essas condutas violentas que disseminam ódio a diferentes minorias, ocorrem de maneira intensa na internet, principalmente, em fóruns e grupos de discussão ocultos na *deep web*.

Alguns dados são importantes para demonstrar a grande intensidade da ocorrência desses delitos no ciberespaço, em um período de catorze anos a SaferNet Brasil recebeu e processou 239.240 denúncias anônimas de condutas neonazistas e nesse mesmo período foram recebidas e processadas 139.847 denúncias anônimas relacionadas à ocorrência de homofobia na internet.

---

[22] O termo LGBTfobia não é tão conhecido, já que outro é normalmente usado como sinônimo para se referir ao ódio à população LGBT: a homofobia. Nesse sentido, Maria Berenice Dias – presidente da Comissão da Diversidade Sexual do Conselho Federal da OAB –, define a homofobia como o “ato ou manifestação de ódio ou rejeição a homossexuais, lésbicas, bissexuais, travestis e transexuais”. (FIGUEIREDO,2020)

[23] Para se enquadrar o assassinato de uma mulher como crime de feminicídio, é necessário que o autor tenha cometido o ato em razão de violência doméstica e familiar, menosprezo ou discriminação à condição de mulher. Dessa forma, nem todos os assassinatos de mulheres são considerados feminicídios. (MINAS GERAIS, TRIBUNAL DE JUSTIÇA, 2019)

Esses dados alarmantes demonstram que os crimes motivados pelo preconceito precisam de uma maior atenção da sociedade, uma legislação mais específica e um combate mais efetivo para minimizar a sua incidência.

6 INVESTIGAÇÃO POLICIAL NA *DEEP WEB*

Para entender mais sobre os delitos presentes na *deep web* e o processo de investigação policial, mostra-se necessário abordar alguns conceitos iniciais do processo penal e explorar um pouco o mundo prático das investigações policiais no submundo da internet.

6.1 INVESTIGAÇÃO POLICIAL

Inicialmente, é importante começar explicando de uma forma breve como funciona uma investigação policial e qual é a sua utilidade para a sociedade. A investigação policial procura, por meio de diversas técnicas de várias áreas diferentes, descobrir como e onde ocorreu o crime e também busca juntar indícios de autoria delitiva para descobrir a possível autoria do delito. (SILVA, 2006, págs,103-104)

Outro conceito que precisa ser apresentado, é o de inquérito policial, esse procedimento dirigido pela polícia judiciária[24] e presidido pela figura do delegado de polícia tem caráter administrativo, informativo e sigiloso e procura por meio da chamada justa causa, formar a opinião do membro do Ministério Público para entrar com a ação penal. Além do mais, é mister explicar que o inquérito policial também serve para colher as provas irrepetíveis, que são aquelas provas que são perecíveis e são extremamente importantes para a investigação criminal (SILVA, 2006, págs, 103-104).

É importante expor que segundo a maioria da doutrina que a investigação pode ser dividida em três categorias principais (administrativas, legislativas e judiciárias) e possui diversos métodos diferentes de funcionamento (MARQUES, 2018).

[24] Às polícias civis, dirigidas por delegados de polícia de carreira, *incumbem*, ressalvadas a competência da União, as funções de polícia judiciária e a apuração de infrações penais, exceto as militares. (CONSTITUIÇÃO,1988)

Além disso, é interessante abordar como ocorre a chamada *notitia criminis,*[25] a notícia do crime é a forma com que a autoridade policial obtém o conhecimento de um possível fato criminoso, esse conhecimento pode ser obtido por meio de diversas formas, visto que a notícia crime pode ser espontânea, coercitiva, provocada e até anônima (VARGAS, 2020. P.6).

Sobre o assunto de *notitia criminis* Távora e Alencar (2016, p.165) comentam que:

> É o conhecimento pela autoridade, espontâneo ou provocado, de um fato aparentemente criminoso. A ciência da infração penal pode ocorrer de diversas maneiras, e esta comunicação, provocada ou por força própria, é chamada de notícia do crime. Normalmente é endereçada à autoridade policial, ao membro do Ministério Público ou ao magistrado. Caberá ao delegado, diante do fato aparentemente típico que lhe é apresentado, iniciar as investigações. O MP, diante de notícia crime que contenha em si elementos suficientes revelando a autoria e a materialidade, dispensará a elaboração do inquérito, oferecendo de pronto denúncia; diante de notícia crime deficiente, poderá requisitar diligências à autoridade policial. Já o magistrado, em face da notícia crime que lhe é apresentada, poderá remetê-la ao MP, para providências cabíveis, ou requisitar a instauração do inquérito policial.

Alguns dispositivos do ordenamento jurídico exploram os assuntos relacionados aos processos de investigação policial, e sobre isso é válido expor o artigo 6° do Código de Processo Penal que fala - expressamente - sobre os procedimentos que a autoridade policial precisa realizar quando tiver o conhecimento da existência do delito.

> I – dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais; II – apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais; III – colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias; IV – ouvir o ofendido; V – ouvir o indiciado, com observância, no que for aplicável, do disposto no Capítulo III do Título Vll, deste Livro, devendo o respectivo termo ser assinado por duas testemunhas que lhe tenham ouvido a leitura; VI – proceder a reconhecimento de pessoas e coisas e a acareações; VII – determinar se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias; VIII – ordenar a identificação do indiciado pelo processo datiloscópico, se possível, e fazer juntar aos autos sua folha de antecedentes; IX – averiguar a vida pregressa do indiciado, sob o ponto de vista individual, familiar e social, sua condição econômica, sua atitude e estado de ânimo antes e depois do crime e durante ele, e quaisquer outros elementos que contribuírem para a apreciação do seu temperamento e caráter.

Ainda sobre os dispositivos presentes no ordenamento jurídico brasileiro sobre os processos de investigação criminal, Marques (2018) expõe que:

[25] Do latim, significa notícia do crime. (tradução livre)

> Há ainda, outros atos de investigação criminal em leis esparsas, como, por exemplo, a obtenção de informações bancárias, fiscais e financeiras, a realização de interceptação de comunicações telefônicas e dados conforme dispõe a Lei 9.296/1996, a infiltração de agentes de polícia ou de inteligência, prevista na lei que pune o crime organizado Lei 12.850/13 e Lei de drogas 11.343/2006, etc, porém, este assunto deve ser explorado com mais profundidade no estudo específico da cada lei que será tema de outro trabalho.

6.2 TÉCNICAS DE INVESTIGAÇÃO POLICIAL NA *DEEP WEB*

Os delitos acompanham a sociedade e sofrem diversas mutações, ao longo dos anos. Devido a isso, as técnicas de investigação policial precisam de mecanismos atualizados e eficientes para o combate aos diversos crimes existentes.

É válido pontuar, novamente, que o Brasil possuiu um desenvolvimento tardio no combate e na repressão dos crimes cibernéticos. Entretanto, apesar da enorme dificuldade de investigar os delitos na *dark web*, o país possui várias ferramentas que auxiliam nas investigações e conseguiu solucionar diversos crimes nessa parte da internet.

Entre as técnicas mais utilizadas para essas investigações, é válido destacar a infiltração policial, essa importante técnica que está prevista na lei 12.850/13(lei das organizações criminosas), na lei 11.343/06 (lei de drogas) e em alguns outros dispositivos do ordenamento jurídico brasileiro, consiste na infiltração de agentes de polícia, após prévia autorização judicial, em organizações criminosas e em outras situações com o intuito de conseguir provas lícitas que ajudem na investigação policial de diversos delitos. (ANSELMO, 2017)

Sobre o assunto, é mister comentar que devido às mutações das formas e dos ambientes de cometimento dos crimes, a técnica da infiltração policial precisou se atualizar e com isso surgiu a infiltração virtual de agentes.

Essa modalidade digital da infiltração policial surgiu, inicialmente, na forma da lei 13.441/17 que instituiu essa nova modalidade no estatuto da criança e do adolescente. Sobre essas modificações da lei 13.441/17, Hoffmann (2017) dispõe que:

> Admite-se a infiltração policial virtual basicamente em 3 categorias de delitos (artigo 190-A do ECA):
> a) pedofilia (artigos 240, 241, 241-A, 241-B, 241-C e 241-D do ECA);
> b) crimes contra a dignidade sexual de vulneráveis: estupro de vulnerável (artigo 217-A do CP), corrupção de menores (artigo 218 do CP), satisfação de lascívia (artigo 218-A do CP) e favorecimento da prostituição de criança ou adolescente ou de vulnerável (artigo 218-B do CP);

> c) invasão de dispositivo informático (artigo 154-A do CP).

Além disso, também é importante expor as mudanças implementadas pelo pacote anticrime[26] (Lei 13.964/2019) na lei das organizações criminosas, o pacote anticrime, também, trouxe a possibilidade da figura do agente infiltrado virtual na lei 12.850/13 e com isso possibilitou uma nova forma de obtenção de provas. (LIMA, 2019, págs, 551-553).

Entre alguns dispositivos adicionados pelo pacote, é importante destacar:

> Art. 10-A. Será admitida a ação de agentes de polícia infiltrados virtuais, obedecidos os requisitos do caput do art. 10, na internet, com o fim de investigar os crimes previstos nesta Lei e a eles conexos, praticados por organizações criminosas, desde que demonstrada sua necessidade e indicados o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas.

A possibilidade do mecanismo de infiltração policial virtual (cibernética ou eletrônica) é uma técnica investigativa que pode ser extremamente útil nas operações policiais, devido à possibilidade dos agentes se infiltrarem em organizações criminosas, fóruns de exploração sexual infanto-juvenil e entre outras situações que possibilitem uma maior apuração de provas lícitas e que facilitam a descoberta da identidade verdadeira dos criminosos. (LIMA, 2019, p.554)

Para que seja possível a ocorrência da infiltração policial, sem a ocorrência da nulidade das provas colhidas, eles devem respeitar diversos requisitos jurídicos, como por exemplo, a necessidade de uma prévia autorização judicial, que deve ser circunstanciada, sigilosa e motivada.

Outro requisito importante é a questão da limitação temporal, visto que a infiltração não pode durar mais de 720 (setecentos e vinte) dias, além disso também é mister destacar o requisito da indispensabilidade da existência de indícios de crimes praticados por organizações criminosas, a comprovação do risco da não realização da infiltração policial, no caso específico e a indispensabilidade da infiltração. (LIMA, 2019, págs. 554-556)

---

[26] O chamado “Pacote Anticrime” do Governo Federal se refere a um conjunto de alterações na legislação brasileira que visa a aumentar a eficácia no combate ao crime organizado, ao crime violento e à corrupção, além de reduzir pontos de estrangulamento do sistema de justiça criminal.(BRASIL, MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, 2020)

Também é mister pontuar sobre a existência do direito de escolha do agente policial de participar ou não da infiltração e do direito de pedir para parar a sua atuação na operação sem sofrer consequências profissionais. Além disso, é importante comentar que o agente infiltrado não é uma figura provocadora de delitos, mas sim uma figura que deve agir majoritariamente de maneira passiva e investigativa. (LIMA, 2019, p.556)

Outra ferramenta utilizada nas investigações na *dark web* é a NIT- *Network Investigative Technique*[27]*.* Essa técnica muito utilizada em vários países, consiste na implantação de um *software* em um dispositivo informático de um terceiro que está sendo investigado, com o objetivo de conseguir diversas informações eficientes para identificar a autoria e existência do delito.

Entre essas informações que são possíveis de serem descobertas com essa ferramenta, é mister destacar o endereço Mac, os registros de conexão e entre outras. Ainda sobre isso, mostra-se necessário comentar que para a instalação dessa ferramenta, é necessária uma prévia autorização judicial. (NOGUEIRA; WENDT, 2019)

Além dessas técnicas investigativas utilizadas, é imprescindível comentar sobre as fontes de OSINT, que são fontes abertas de inteligência que servem como ferramentas informativas disponíveis legalmente*.* Sobre isso, Davies (2020) comenta que:

> Uma das técnicas de policiamento mais comumente usadas em todas as investigações cibernéticas, incluindo aquelas na dark web, é o uso de inteligência de código aberto. OSINT são dados e informações que são coletados legalmente de recursos abertos e disponíveis publicamente. A obtenção das informações não requer nenhum tipo de esforço clandestino e é recuperada de forma legal e em conformidade com os requisitos de direitos autorais. Há uma ampla gama de ferramentas OSINT disponíveis, algumas das quais específicas para a dark web. As fontes OSINT exigem que os policiais vasculhem a web em busca de migalhas de informações que levem ao desmascaramento de identidades geralmente deixadas por erro humano. Isso pode vir de postagens em fóruns em comunidades baseadas na web, contatos gerados por usuários, sites de redes sociais, wikis, blogs e fontes de notícias, entre outros. (tradução livre)

Ainda sobre o assunto, é mister expor que além dessas técnicas de investigação criminal, diversas outras ferramentas investigativas cotidianas dos policiais podem e são implementadas nas investigações na *deep web*.

[27] Do inglês, significa técnica de investigação de redes. (tradução livre)

6.3 OPERAÇÃO DARKNET

A operação Darknet foi a primeira investigação policial brasileira na *deep web* realizada na rede Tor, essa operação durou dois anos, teve o objetivo de investigar crimes de pornografia infanto-juvenil e foi executada pela Polícia Federal com uma parceria com o Ministério Público Federal (Ministério Público Federal, 2020).

Essa foi uma operação bastante complexa e importante, devido ao seu pioneirismo, no país, e por causa da dificuldade legislativa, visto que foi necessária uma complexa análise de adequação da legislação brasileira. Outra grande dificuldade presente na Darknet foi a dificuldade técnica, isso ocorreu por causa da necessidade de familiarização com a rede Tor e com os protocolos da *deep web* (Ministério Público Federal, 2020).

Sobre essa operação, o Ministério Público Federal esclarece que:

> Depois da obtenção dos respectivos endereços de IP, a fim de melhor realizar a individualização da autoria, ocorreu a quebra do sigilo dos dados cadastrais do usuário de internet, visando também a identificação do local no qual houve o compartilhamento do material contendo pornografia infanto-juvenil, indicando, assim, a competência territorial para a expedição de mandado de busca e apreensão e demais medidas decorrentes. Somente após a coleta dessas informações, ocorreu o declínio de competência às respectivas Subseções Judiciárias. Destaca-se que, durante o período da colheita da prova através da ferramenta da PF, identificaram-se, também, alvos que estariam não só compartilhamento pornografia infanto-juvenil, mas possivelmente abusando sexualmente de menores, conforme o teor das postagens e imagens publicadas. Nesses casos específicos, não se aguardou a deflagração da operação, mas agiu-se pontualmente caso a caso, compartilhando as informações imediatamente com o juízo territorialmente competente. Com isso, foram resgatas 5 crianças em situações de abuso.

No final, a operação Darknet obteve um sucesso bastante considerável, foram 37(trinta e sete) subseções judiciárias, alcançando 17 (dezessete) estados brasileiros e atingindo uma grande repercussão internacional, com a identificação de vários criminosos no exterior (Ministério Público Federal, 2020).

O Brasil participou de várias outras operações policiais investigativas, no submundo digital e obteve várias apreensões importantes que repercutiram também internacionalmente. Outra operação importante que merece a atenção, foi uma operação realizada, em 2019, pela Polícia Federal em parceria com o FBI, que prendeu um indivíduo responsável por um sítio localizado na *dark web,* destinado à prática de diversos crimes como por exemplo: tráfico de drogas e armas, contrabando

e lavagem de dinheiro e possível envolvimento com o crime de exploração sexual infanto-juvenil (Divisão de Comunicação Social da Polícia Federal, 2019).

7 CONSIDERAÇÕES FINAIS

Com base no que foi apresentado, conclui-se que o fenômeno do *cybercrime* está presente - em grande escala - na realidade brasileira, esses crimes que acontecem no meio digital podem tanto ocorrer na *surface web* como na *deep web,* que é a parte mais indexada da internet, que facilita o anonimato e a prática de vários delitos. Entre os delitos de maior ocorrência nesse submundo da internet, é válido destacar, o tráfico de armas, os crimes de ódio, o tráfico de drogas, crimes financeiros e a exploração e abuso sexual infanto-juvenil.

Além do mais, foi observado que apesar da enorme incidência dos crimes cibernéticos, a realidade legislativa brasileira possui algumas lacunas preocupantes e leis amplamente dispersas, em comparação com outros países, que possuem uma história mais longa, no combate a esses delitos.

Entretanto, apesar de algumas dificuldades técnicas e legislativas o país - nos últimos anos - vem obtendo avanços significativos em técnicas investigativas e operações policiais importantes com grande respaldo internacional.

Por fim, conclui-se que com o provável avanço tecnológico exponencial, nos próximos anos, esses *cybercrimes* estarão ainda mais presentes na realidade mundial, necessitando assim que as formas de prevenção, combate e investigação desses delitos acompanhem as possíveis atualizações. Alertando, também a necessidade de um maior envolvimento operacional internacional para um combate mais eficiente.

REFERÊNCIAS

ANSELMO, Márcio Adriano. **A infiltração policial no combate aos crimes de corrupção.** 2017. Disponível em: https://www.conjur.com.br/2017-out-24/academia-policia-infiltracao-policial-combate-aos-crimes-corrupcao#:~:text=A%20infiltra%C3%A7%C3%A3o%20policial%20(t%C3%A9cnica%20conhecida,criminosas%E2%80%9D%2C%20embora%20apenas%20mencionasse%20o. Acesso em: 16 nov. 2020

BARRETO, Alesandro Gonçalves; SANTOS, Hericson dos. **DEEP WEB:** investigação no submundo da internet. Rio de Janeiro: Brasport, 2019. *E-book*

BORTOT, Jessica Fagundes. **Crimes cibernéticos**: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. 2017. 25 f. TCC (Graduação) - Curso de Direito, A Faculdade Mineira de Direito da Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2017.

BRASIL. Artigo 217 do **Decreto Lei nº 2.848** de 07 de dezembro de 1940. 2020. Disponível em: https://www.jusbrasil.com.br/topicos/10611447/artigo-217-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940. Acesso em: 11 nov. 2020.

_____. **Lei 11829/08 | Lei nº 11.829**, de 25 de novembro de 2008. 2020. Disponível em: https://presrepublica.jusbrasil.com.br/legislacao/92844/lei-11829-08#comments. Acesso em: 11 nov. 2020.

_____. **Ministério da Justiça e Segurança Pública**. Pacote anticrime agora é lei. 2019. Disponível em: https://www.justica.gov.br/seus-direitos/elaboracao-legislativa/projetos/anticrime-1. Acesso em: 17 nov. 2020.

_____. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

_____. **Secretaria geral**. Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética. Disponível em: https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica. Acesso em: 19 set. 2020.

Conselho europeu. Ação do Conselho da Europa contra o crime cibernético. 2020. Disponível em: https://www.coe.int/en/web/portal/coe-action-against-cybercrime. Acesso em: 16 nov. 2020.

DAVIES, Gemma. **Iluminando o Policiamento da Dark Web**: Uma Análise dos Poderes de Investigação do Reino Unido. 2020. Disponível em: https://journals.sagepub.com/doi/full/10.1177/0022018320952557. Acesso em: 16 nov. 2020.

Divisão de Comunicação Social da Polícia Federal. PF e FBI combatem a prática de crimes na internet e Dark Web. 2019. Disponível em: http://www.pf.gov.br/imprensa/noticias/2019/05/pf-e-fbi-combatem-a-pratica-de-crimes-na-internet-e-dark-web. Acesso em: 17 nov. 2020

DURKHEIM, Émile. **As regras do método sociológico**. 2º. ed. São Paulo: Martins Fontes, 1999. p. 13

ESTADO DE MINAS. **Crimes cibernéticos disparam e expõem fragilidade tecnológica no Brasil.** 2019. Disponível em: https://www.em.com.br/app/noticia/politica/2019/08/04/interna_politica,1074689/crim

es-ciberneticos-disparam-expoem-fragilidade-tecnologica-no-brasil.shtml. Acesso em: 15 set. 2020.

FERNANDES, David Augusto. **Crimes cibernéticos: o descompasso do estado e a realidade.** 2013. 40 f. Tese (Doutorado) - Curso de Direito, Ufmg, Belo Horizonte, 2013

FIGUEIREDO, Danniel; MORAIS, Pâmela. **LGBTfobia no Brasil**: fatos, números e polêmicas. Disponível em: https://www.politize.com.br/lgbtfobia-brasil-fatos-numeros-polemicas/. Acesso em: 11 nov. 2020.

GARCIA, Gabriel. **80% do tráfego da deep web é gerado por sites de pedofilia**. 2015. Disponível em: https://exame.com/tecnologia/80-do-trafego-da-deep-web-e-gerado-por-pedofilia-dizestudo/. Acesso em: 11 nov. 2020.

GOGONI, Ronaldo. **O que é software?** 2020. Disponível em: https://tecnoblog.net/311647/o-que-e-software/. Acesso em: 20 set. 2020.

GRADEUP (org.). **University of Portsmouth**. 2020. Disponível em: https://gradeup.com.br/universidade/university-of-portsmouth/. Acesso em: 11 nov. 2020

HOFFMANN, Henrique. **Lei 13.441/17 instituiu a infiltração policial virtual**. 2017. Disponível em: https://www.conjur.com.br/2017-mai-16/academia-policia-lei-1344117-instituiu-infiltracao-policial-virtual. Acesso em: 17 nov. 2020.

LIMA, Renato Brasileiro de. **Pacote anticrime**: comentários a lei 13.964/2019 artigo por artigo. Salvador: Editora Juspodivm, 2019.

KOHN, Karen. **O impacto das novas tecnologias na sociedade**: conceitos e características da Sociedade da Informação e da Sociedade Digital. UFSM/Cesnors. Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação. XXX Congresso Brasileiro de Ciências da Comunicação – Santos – 29 de agosto a 2 de setembro de 2007. Disponível em: www.intercom.org.br/papers/nacionais/2007/resumos/R1533-1.pdf

KUMMER, Fabiano R. Direito penal na sociedade de informação. Paraná: Edição do Autor, 2017. *E-book*

MARQUES, José Guilherme Pereira da Silva. **As modernas técnicas de investigação policial**: a nova visão da polícia investigativa e suas modernas técnicas no combate ao crime. A nova visão da polícia investigativa e suas modernas técnicas no combate ao crime. 2018. Disponível em: https://jus.com.br/artigos/64402/as-modernas-tecnicas-de-investigacao-policial. Acesso em: 16 nov. 2020.

MARRIEL, Gleiciane; CÁSSIA, Júllia. **A Deep Web e os limites do anonimato**. 2019. Disponível em: http://universo.ufes.br/blog/2019/05/a-deep-web-e-os-limites-do-anonimato/.

MINAS GERAIS. TRIBUNAL DE JUSTIÇA. (org.). **Justiça pela Paz em Casa**: entenda o que caracteriza o feminicídio. 2019. Disponível em: https://www.tjmg.jus.br/portal-tjmg/informes/justica-pela-paz-em-casa-entende-o-que-caracteriza-o-feminicidio.htm#.X6wy1WhKhPY. Acesso em: 11 nov. 2020.

Ministério Público Federal. **Operação darknet**. 2020. Disponível em: http://www.mpf.mp.br/rs/sala-de-imprensa/docs/outros-documentos/operacao-darknet. Acesso em: 17 nov. 2020.

MORGAN, Steve. **About us.** 2020. Disponível em: https://cybersecurityventures.com/our-company/. Acesso em: 12 set. 2020.

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: 19 set. 2020.

NUCCI, Guilherme. **Crimes de ódio:** Uma tipificação necessária para o Brasil. 2019. Disponível em: https://migalhas.uol.com.br/depeso/309333/crimes-de-odio--uma-tipificacao-necessaria-para-o-brasil. Acesso em: 11 nov. 2020.

ORTEGA, Flávia. **O que são os crimes de ódio?** 2015. Disponível em: https://draflaviaortega.jusbrasil.com.br/noticias/309394678/o-que-sao-os-crimes-de-odio. Acesso em: 11 nov. 2020.

PINHEIRO, Débora Hiromi Sawaki Mouta; SADALLA, Nachara Palmeira. **O crime de pornografia infantil na deep web**: medidas legais para combate e proteção infantojuvenil. 2019. 36 f. TCC (Graduação) - Curso de Direito, Unama, Belém, 2019.

RIBAS JUNIOR, Douglas. **Lei Carolina Dieckmann e o sistema penal brasileiro**. 2020. Disponível em: https://canaltech.com.br/juridico/Lei-Carolina-Dieckmann-e-o-sistema-penal-brasileiro/. Acesso em: 19 set. 2020.

SAFER NET (org.). **Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. 2019**. Disponível em: https://indicadores.safernet.org.br/. Acesso em: 11 nov. 2020.

SAFER NET (org.). **Quem Somos**. 2008. Disponível em: https://www.safernet.org.br/site/institucional. Acesso em: 15 set. 2020.

SAISSE, Renan. **Um Mergulho na Deep Web: Redes Descentralizadas, FREENET, TOR, I2P**. 2019. Disponível em: https://www.profissionaisti.com.br/um-mergulho-na-deep-web-parte-25/. Acesso em: 21 set. 2020

SANTOS, Márcio Teixeira dos; DIGIÁCOMO, Murillo José. **Posição oficial:** Exploração sexual de adolescentes. 2009. Disponível em: http://crianca.mppr.mp.br/pagina-249.html. Acesso em: 11 nov. 2020.

SCHAUN, Guilherme. Uso permitido, uso proibido, munição, acessório, arma de fogo: definições. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 24, n.

5852, 10 jul. 2019. Disponível em: https://jus.com.br/artigos/73025. Acesso em: 9 nov. 2020.

SCHIOCHETTI, Rafaela; CUSTÓDIO, Ana Carolina. **Criptomoedas: o que são e como funcionam?** 2019. Disponível em: https://www.politize.com.br/criptomoedas-o-que-sao-e-como-funcionam/. Acesso em: 22 set. 2020.Acesso em: 21 set. 2020.

SILVA, Marcio Cesar Fontes. **A investigação criminal, a polícia judiciária e o ministério público**. 2006. 190 f. Dissertação (Mestrado) - Curso de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2006. Disponível em: http://livros01.livrosgratis.com.br/cp009108.pdf. Acesso em: 15 nov. 2020.

SOARES, Gabriella Ribeiro; MARTINS, Mikely Dayane Freire. **Frente às novas tecnologias: a configuração do crime de estupro em meio virtual.** 2017. 11 f. Tese (Doutorado) - Curso de Direito, Ufmg, esdhc, Belo Horizonte, 2017. Cap. 11. Disponível em: http://conpedi.danilolr.info/publicacoes/6rie284y/t3m9n6k4/aX082puAZFS1117y.pdf. Acesso em: 11 nov. 2020.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de direito processual penal.** 11. ed. Salvador: Editora Juspodivm, 2016.

VARGAS, Douglas. **Direito processual penal**: inquérito policial. Distrito Federal: Gran Cursos, 2020. 71 p.

VEIGA, Edison. **Dados indicam crescimento do neonazismo no Brasil**. 2020. Disponível em: https://www.dw.com/pt-br/dados-indicam-crescimento-do-neonazismo-no-brasil/a-53985901. Acesso em: 21 set. 2020.

VIEIRA, Luciana. **Com Tor, navegue totalmente em anonimato e ainda livre-se de malwares.** 2013. Disponível em: https://www.techtudo.com.br/tudo-sobre/tor.html. Acesso em: 20 set. 2020. I2P. O que a I2P pode fazer por você? 2020. Disponível em: https://geti2p.net/pt-br/about/intro. Acesso em: 20 set. 2020.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos:** ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: Brasport, 2013. *E-book*