universitári@
REVISTA CIENTÍFICA DO UNISALESIANO - LINS - SP
UniSALESIANO Centro Universitário
ANO 12 - Nº 23 - JANEIRO / DEZEMBRO 2021 ISSN 2177-4951

CRIMES VIRTUAIS E A DEEP WEB: O BENEFÍCIO DO ANONIMATO AO CRIMINOSO E A REALIZAÇÃO DA IDENTIFICAÇÃO DO AUTOR

VIRTUAL CRIMES AND THE DEEP WEB: THE BENNEFIT OF CRIMINAL ANONYMITY AND THE AUTOR RECOGNITION

Guilherme Hiibner Pereira – Graduando em Direito
UniSALESIANO Lins - gphiibner@gmail.com
Prof. Danilo César Siviero Ripoli– Mestre em Direito
UniSALESIANO Lins - danilo@unisalesiano.edu.br

RESUMO

O presente trabalho trata-se de pesquisa bibliográfica, com uso de método dedutivo, valendo-se de textos de doutrinas e normas, que tem como objetivo compreender a investigação policial nos crimes praticados na *deep web*, internet caracterizado pelo anonimato. O preparo e a realização de investigações em relação aos crimes virtuais na internet convencional, é uma tarefa árdua e dificultosa. Essa atividade torna-se mais espinhosa quando os crimes acontecem na internet profunda (*deep web)*, já que exige um preparo ainda maior para desvendá-los. O trabalho procura entender como acontecem essas investigações dentro da internet. A *deep web*, como a tradução sugere “internet profunda”, é um lugar de difícil acesso, onde o anonimato protegido por várias camadas de criptografia, facilita a prática de ilicitudes, pois dificulta o trabalho da investigação policial de identificar a autoria e materialidade dos crimes ocorridos na mesma. Este trabalho observa a *Network Investigative Technique* (Técnica Investigativa de Redes) e a infiltração policial como formas de investigações feitas na *deep web*.

Palavras-chave: INTERNET. DEEP WEB. CRIME VIRTUAL. INVESTIGAÇÃO POLICIAL.

ABSTRACT

The present work is bibliographical research, using a deductive method, using texts of doctrines and norms, which aims to understand the police investigation of crimes committed on the deep web, an internet characterized by anonymity. Preparing and carrying out investigations in relation to virtual crimes on the conventional internet, where the task is arduous and difficult, is characterized by greater difficulty when crimes take place on the deep web, which requires even greater preparation. The work seeks to understand how these investigations happen on the internet. The deep web, as the translation suggests “deep internet”, is a place of difficult access, where the anonymity protected by several layers of encryption facilitates the practice of illicit acts,

ANO 12 - Nº 23 - JANEIRO / DEZEMBRO 2021 ISSN 2177-4951

as it makes it difficult for the police investigation to identify the authorship and materiality of the perpetrators. Crimes were committed there. This work looks at the Network Investigative Technique and police infiltration as forms of investigations carried out on the deep web.

Keywords: INTERNET. DEEP WEB. VIRTUAL CRIMES. POLICE INVESTIGATIONS.

INTRODUÇÃO

A internet surgiu em 1969, na Guerra Fria, com o engenheiro Joseph Licklider do Instituto Tecnológico de Massachutsetts (MIT). Tinha o objetivo de criar um sistema de conexão em rede entre computadores. Após sete anos formou a ARPANET, rede de conexões da DARPA (Agência de Projetos de Pesquisa Avançada dos Estados Unidos), podendo dizer que com isso houve o surgimento da internet, com algumas semelhanças e muitas diferenças de como se conhece hoje. (BARROS, 2013).

A internet dá acesso a muitas ferramentas, podendo realizar um retrato falado online, com ferramentas similares às que a polícia utiliza; conversar com um robô, que se adapta aos linguajares e consegue dialogar com o internauta como se fosse uma pessoa, beirando a perfeição, entre outras utilidades que seriam desnecessárias mencioná-las aqui, pois é de conhecimento de todos. (FERNANDES, 2016).

O implemento de novas tecnologias, indubitavelmente, proporciona significativos avanços em diversas áreas. Não obstante, plataformas construídas com fins lícitos são utilizadas por criminosos e usuários mal-intencionados no incremento de seus atos. Nesse contexto, inserem-se diversos serviços disponíveis na *surface web*, a exemplo de redes sociais, serviços de e-mail e aplicativos de mensageria. O cenário não é distinto na *deep web*. (FERNANDES, 2016).

Apesar de ser citada desde a década de 90, a internet permanece desconhecida, nebulosa e eivada de lendas verdadeiras ou falaciosas perante a absoluta maioria dos usuários. Esse ambiente se apresenta propício para o criminoso alcançar mais vítimas, maximizar lucros e se furtar à aplicação da lei penal. Diversos são os delitos praticados nessa rede, especialmente apologia ao crime em fóruns de discussão, comércio ilegal de drogas, armas e munições, abuso e exploração sexual

ANO 12 - Nº 23 - JANEIRO / DEZEMBRO 2021 ISSN 2177-4951

infanto-juvenil, terrorismo, crimes de ódio e violação de direitos autorais. (BARRETO; SANTOS, 2019).

Para realizar uma pesquisa na internet utiliza-se as ferramentas que alguns sites disponibilizam, como Google, Yahoo, Ask, etc. Digita-se o que se está procurando e os resultados variam entre vídeos, artigos, entre outros, isso seria a "superfície" da internet, mas vai além disso, abaixo da "superfície" temos a *deep web* (internet profunda). (BERGMAN, 2001).

Bergman foi o primeiro a usar esse termo e para ele utilizar os sites de pesquisas convencionais tendo acesso a superfície, seria aquele pescador que lança sua vara ao rio e espera os peixes comuns fisgarem, mas para ter acesso aos "peixes especiais" ou "raros", seria necessário a utilização de redes de pesca e barcos mais adequados. (BERGMAN, 2001).

Com tantas vantagens e facilidades, a internet também se mostra muito perigosa. Quando estamos online a nossa segurança é garantida? A nossa privacidade é respeitada?

A Constituição Federal nos assegura o direito à privacidade em seu artigo 5º, inciso X, narrando que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". (BRASIL, 1988).

Segundo David Duarte e Tiago Mealha, a privacidade na internet é assunto de uma das grandes áreas de pesquisa, já que muitas pessoas ainda não têm o conhecimento de como funciona o compartilhamento de informações pela internet, muitas vezes aceitando acordo de termos de uso sem realmente saber o que está "assinando", como a venda de informação legal de dados compartilhados em redes sociais e o sistema de publicidade online. (DUARTE; MEALHA, 2016).

A grande maioria dos internautas não sabem o que está realmente acontecendo com seus dados, suas informações e isso facilita muito a exposição e a quebra de sua privacidade, surgindo como meio alternativo de navegação a *deep web*, tema que será discorrido de forma aprofundada no transcorrer do presente trabalho.

Por fim, de uma maneira específica, é abordada a investigação policial na *deep web*, as ferramentas disponíveis para o trabalho, como a criada pela PRODESP (Companhia de Processamento de Dados do Estado de São Paulo), PHOENIX, IPED

(Indexador e Processador de Evidências Digitais). Há técnicas de investigações dedicadas a internet profunda, como a Network Investigative Technique (NIT), podendo ser traduzida em forma literal como Técnica Investigativa de Redes, sendo utilizada mediante autorização judicial para instalar um programa em dispositivo alheio para ser feita a monitoração.

A infiltração de agentes será realizada também através de autorização judicial. O agente será introduzido na organização criminosa de forma infiltrada com o objetivo de recolher informações preciosas para a justiça combater a organização com informações privilegiadas.

1 *A DEEP WEB*

Tudo o que se consegue acessar de forma convencional é realizado na *surface web.* A simples tarefa de abrir o navegador, inserir o endereço de seu site de pesquisa favorito, acessar suas redes sociais, sites de notícias, etc., o usuário está acessando a *sufarce web*.

A popularização da internet atraiu também pessoas más intencionadas, já que seria mais fácil manter o anonimato na internet. O número de crimes cibernéticos vem crescendo, sendo que já é bastante comum o criminoso cibernético adaptar um crime que já existe no “mundo real” para o plano virtual, como pornografia infantil, apologia e incitação a crimes contra a vida, violência contra mulheres/misoginia, xenofobia, racismo, LGBTfobia, apologia ao nazismo, maus tratos contra animais, intolerância religiosa, tráfico de pessoas, etc. (ROSA, 2019).

A *deep web* pode ser entendida como uma camada profunda da internet, onde o anonimato é praticamente absoluto com criptografia de dados e o direito à privacidade respeitado. (BERGMAN, 2001).

A internet profunda ou *deep web* é utilizada por criminosos por razão do benefício da criptografia apresentada, realizada em várias camadas, onde é possível a prática de crimes com lojas com mercadorias ilícitas no catálogo e mídias de abuso sexual infantil.

2 A CRIPTOGRAFIA

ANO 12 - Nº 23 - JANEIRO / DEZEMBRO 2021 ISSN 2177-4951

Para um melhor entendimento de como funciona a *deep web*, é interessante entender o que é criptografia. É inevitável na vida de um internauta compartilhar documento pessoal ou arquivos pessoais, seja alguma digitalização de documentos para seu banco ou um arquivo por aplicativo de mensageria para alguém que confia, nessas ocasiões a criptografia se encontra presente.

A criptografia é uma ferramenta essencial para o uso da internet, com ela é possível ter acesso ao seu dinheiro, compartilhar dados e não ser possível um terceiro interceptar essas informações e usá-las como bem entender. (DUARTE; MEALHA, 2016).

Sendo uma codificação da informação, para somente o emissor e o receptor ter acesso a ela, os sites de banco possuem sistemas de criptografia e alguns aplicativos de mensageria também, como o WhatsApp. (ROMAGNOLO, 2017).

Pode-se imaginar várias chaves de códigos e somente os usuários que participam da conversa teriam as chaves corretas para ter acesso à mesma. Para Mealha e Duarte (2016), a criptografia segue quatro princípios, sendo eles:

a) Confidencialidade: somente o destinatário possui a chave que decifra a mensagem encriptada e a torna legível.

b) Integridade: o destinatário deverá saber se a mensagem sofreu alterações antes de chegar a ele.

c) Autenticidade: os usuários devem ser capazes de identificar o emissor da mensagem.

d) Irretratabilidade: o emissor não será capaz de negar o autor da mensagem. (DUARTE; MEALHA, 2016).

Em decorrência da criptografia, não seria surpresa se pessoas más intencionadas usassem a *deep we*b para ilegalidade, o que ocorre com bastante frequência. Quando na *sufarce web* os vários tipos de vírus seriam a forma de ilegalidade mais comum, criminosos usam a internet profunda para vender produtos ilegais, mídias com cenas de abuso sexual, incluindo infantil e outros crimes deploráveis. (BARRETO; SANTOS, 2019).

O tráfico de drogas na *deep web* é bastante comum. Muitos sites na rede Tor comercializam drogas com muita liberdade, sendo que os principais tipos de drogas

comercializadas são as drogas sintéticas, como o ecstasy. Tais drogas sintéticas são pequenas, sendo escondidas com mais facilidades, muito consumida por jovens, dessa forma, as encomendas são entregues por correios, sem levantar suspeitas. Feito de maneira muito organizada, assim é encontrado o Blackmarket (mercado negro), que será estudado no próximo tópico, mas que desde já há que ressaltar tratar-se de um ambiente virtual propício para o tráfico de entorpecentes. (BARRETO; SANTOS, 2019).

3 CRIMES PRATICADOS NA *DEEP WEB*

3.1 O *Blackmarket*

O *Blackmarket* é um mercado "aberto" na *deep web* para anunciar todos os tipos de ilegalidades. Para o tráfico de drogas, o maior e mais conhecido é o *Wallstreet* Market, presente na rede Tor, onde é criptografado em várias camadas. Tal mercado virtual é inclusive acessível aos brasileiros, sendo que a página se apresenta em idioma português. (BARRETO; SANTOS, 2019).

Como se trata de um site muito conhecido, os responsáveis fazem uma estratégia por meio de *mirror,* que significa espelho em português. Baseia-se em hospedar o mesmo site em diversos endereços para aumentar a dificuldade de o site ser tirado do ar. Acessando um endereço que o site se encontra indisponível, o usuário irá tentar outro *mirror* para conseguir o acesso. (BARRETO; SANTOS, 2019).

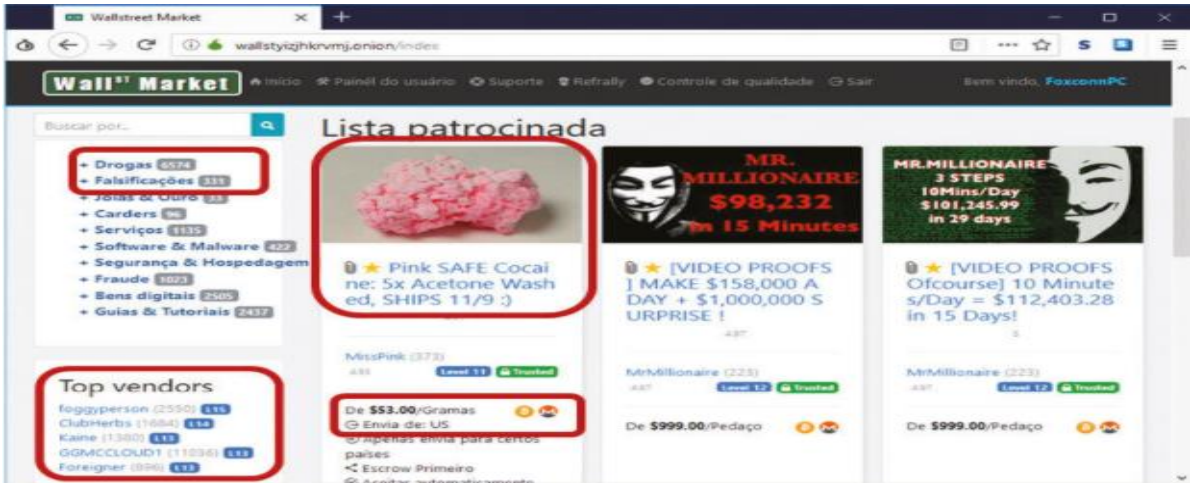
Os espelhos são atualizados constantemente, pois como na *deep web* o site é armazenado no próprio computador do criminoso, o mesmo pode ser desligado, no caso do agente ser preso, por exemplo. Assim, esta é uma forma como os negócios são continuados. (BARRETO; SANTOS, 2019).

O *Wallstreet Market* é bastante conhecido pelos criminosos brasileiros e numa "página inicial" do site, pode-se perceber que "drogas" e "falsificações" aparecem em grande número, em português. Também há os melhores vendedores, avaliados e mais confiáveis para realizar a compra. (BARRETO; SANTOS, 2019).

Por exemplo, a *Pink Cocaine* é uma droga muito alucinógena, que foi apreendida em 2016 em mãos de colombianos em Ibiza, na Espanha. A droga está sendo vendida na *deep web* por cinquenta e três dólares e o vendedor só aceita

bitcoins e *monero* como forma de pagamento, sendo tipos de moedas virtuais, e o montante a ser pago seria o equivalente ao valor pedido em dólares. O que infelizmente deixa claro é a maneira muito organizada das ilegalidades serem praticadas. (BARRETOS; SANTOS, 2019).

Figura 1 – Página do *Wallstreet Market.*



Fonte: BARRETOS; SANTOS, 2019.

Também se percebe na figura acima “cursos” sendo vendidos no intuito de ensinar o usuário adquirente a enriquecer com facilidade, com preço de mil dólares cada. Pode-se notar que o *print* (captura de tela) diz que o cliente que comprar o curso irá fazer praticamente cem mil dólares em quinze minutos.

3.2 O abuso sexual infantil na *deep web*

Um dos crimes mais deploráveis e praticados com muita frequência na *deep web* é o abuso sexual, principalmente infantil.

A pedofilia é caracterizada por anseio, fantasia sexual por crianças, ficando claro que não necessariamente precisa tocar na vítima para se tornar pedófilo, o ato de desejar sexualmente uma criança já o caracteriza como pedófilo. Não que haverá

consequências penais para punir pensamentos, mas a pessoa que imagina cenários sexuais com crianças já é socialmente um pedófilo. (ASSUMPÇÃO, 2014).

O Estatuto da Criança e do Adolescente prevê pena para a materialização destes pensamentos, onde expõe o referido assunto em seu artigo 241. (BRASIL, 1990).

Como nos crimes anteriormente relatados, aproveitam a privacidade dada pela internet para dificultar a descoberta da polícia, porém com a *deep web*, é ainda mais dificultoso. Passando por muitas camadas de criptografia, o rastreio é praticamente impossível, tornando o ambiente propício ao consumo e compartilhamento de conteúdo pornográfico infantil. (JI HOON YU, 2020).

A *deep web* se mostra um ambiente propício para o acesso à pornografia infantil, pois um conteúdo do gênero na *surface web* seria derrubado facilmente, tanto pelos esforços da polícia quanto da sociedade em denunciar com velocidade e eficiência. (BARRETOS; SANTOS, 2019).

Proprietários de sites da *deep web* com foco em pornografia infantil vendem o conteúdo por forma física usando CD's (Compact Disc) ou pendrives e também comercializam o acesso ao conteúdo de forma on-line. É numerosa a participação brasileira no mercado negro de arquivos de abuso sexual infantil, estes produzidos diariamente, comercializados ou compartilhados em fóruns da internet profunda. (BARRETOS; SANTOS, 2019).

4 FERRAMENTAS DISPONÍVEIS PARA A INVESTIGAÇÃO POLICIAL VIRTUAL

Existem diversas ferramentas disponíveis para a polícia, que lhe auxiliarão em sua função, com o objetivo de facilitar as buscas, enriquecendo o inquérito policial e os relatórios de investigação. Ferramentas que encontram valor também nos crimes virtuais, pois uma vez que há suspeitos, a dificuldade de encontrá-los e aplicar a pena é mais difícil que nos crimes "habituais", ou seja, não virtuais. A seguir serão citadas as principais ferramentas que auxiliam no âmbito virtual.

A PRODESP (Companhia de Processamento de Dados do Estado de São Paulo), é uma empresa que tem a função de gerenciar muitos bancos de dados de informações, como o cadastro de pessoa física e jurídica, carteiras de habilitação,

placas de veículos, cadastro criminal, entre outras informações. O programa Ômega desenvolvido pela PRODESP tem a funcionalidade semelhante, porém conta com uma ferramenta interessante, chamada de “investigador virtual”, em que é possível a autoridade policial inserir informações que estão procurando e, surgindo determinada ocorrência pesquisada, o policial será notificado. (MARQUES, 2019).

Também é possível citar o sistema da Polícia Civil do Estado de São Paulo denominado PHOENIX, que tem como diferencial o fato de que se baseia em fotos criminais previamente fornecidas. Esse programa está disponível para todas as seccionais e sedes de departamento. A máquina coleta desde impressões digitais até amostras de voz, além disso, cria retrato falado do criminoso. Um fato interessante é que o rosto humano tem dez pontos considerados imutáveis, mesmo após cirurgias plásticas, com isso o programa encontra uma eficácia ainda maior nas investigações policiais (MARQUES, 2019).

Especificamente para a *deep web*, onde o anonimato é o fundamento principal, a Polícia Federal desenvolveu uma metodologia complexa para a identificação de usuário. Segundo peritos, a identificação do criminoso é possível, porém é um árduo trabalho, pois é necessário mapear toda a estrutura envolvida na hospedagem de dados, passar por diversas camadas de anonimato, como anteriormente dito no presente trabalho. É preciso encontrar o servidor de hospedagem e após todo o mapeamento, a polícia precisa de autorização judicial para prosseguir e, assim, começa a apuração tradicional. (JOVEM PAN, 2019).

Uma dessas ferramentas usadas pela Polícia Federal é o IPED (Indexador e Processador de Evidências Digitais). As funções da ferramenta são encontradas no próprio “GitHub” do projeto. GitHub é um site de gerenciamento de projetos e também versões de códigos disponibilizado para desenvolvedores, é uma espécie de rede social para compartilhamento de projetos. (GITHUB).

As funções presentes no IPED são a decodificação de imagens; acesso a arquivos apagados e espaço não alocado; categorização por análise de assinatura e propriedades e filtro por categoria; expansão de containers; indexação e pesquisa por palavras-chave no conteúdo e propriedades dos arquivos; *Data Carving* (busca por arquivos deletados) eficiente sobre itens não alocados e alocados; visualização em árvore dos dados (não implementada para relatórios, atualmente); cálculo de *hash* (mapeador de grandes arquivos) e filtro de duplicados; OCR (reconhecimento ótico de

caracteres) de imagens e PDFs e detecção de imagens contento textos como digitalizações; detecção de documentos cifrados; consulta a base de *hashes* para alertar ou ignorar arquivos; visualização integrada de dezenas de formatos; visualizador de texto filtrado para qualquer formato; galeria *multithread* (vários núcleos de processamento) para visualizar miniaturas de dezenas de formatos de imagens; geração de miniaturas de vídeos; extração e reindexação de itens selecionados pela interface de pesquisa após análise do perito. (GITHUB).

De acordo com a própria Polícia Federal, os resultados são satisfatórios para o atendimento dos determinados objetivos, porém, nunca serão perfeitos, por conta de inúmeros tipos de arquivos para a realização dos tratamentos, podendo variar resultados de outras ferramentas forenses utilizadas. (POLÍCIA FEDERAL, 2018).

4.1 *Network Investigative Technique* (NIT)

Como apresentado no início do presente trabalho, o anonimato na internet é algo a se preocupar quando o assunto é crime e isso é ainda mais aprofundado quando a *deep web* está envolvida, pois uma técnica que seria eficiente na *surface web* passa a ser ineficaz na internet profunda. Sendo assim, a internet sempre estará à frente da legislação, já que o regulamento é incapaz de acompanhar todas as inovações da internet que acontece a todo momento. (VENTURA, 2017).

A *Network Investigative Technique* (NIT), que pode ser traduzida como Técnica Investigativa de Redes, tem sido uma grande aliada na investigação policial de crimes virtuais, no entanto, sua utilização só é possível, mediante autorização judicial. Consiste na instalação de um programa em dispositivo informático de terceiro, com o objetivo de extrair muitas informações do usuário daquele dispositivo, como: registros de conexão, endereço MAC, nome de usuário, histórico de navegação e demais informações necessárias para a materialização do delito e quanto a atribuição da autoria. (BARRETO; SANTOS, 2019).

A *Network Investigative Technique* vem sendo utilizada pelo Federal Bureau of Investigation (FBI) por mais de 25 anos. Em diversos casos foi necessária a sua utilização, como em abuso e exploração sexual infantil, terrorismo, extorsão, etc. Um dos casos conhecidos que se pode exemplificar melhor a utilização da NIT, foi o de

Buster Hernandez, de 26 anos, acusado de esconder seu IP e sua identidade utilizando o Tor, assim, ameaçava garotas menores com o objetivo de obter fotos íntimas delas. O FBI usando essa técnica, conseguiu quebrar seu anonimato. A tática do FBI foi colocar um vídeo como isca (sem qualquer tipo de pornografia infantil), certo que quando o acusado abriu o vídeo, a NIT foi um sucesso, revelando seu endereço IP, assim foi fácil rastrear seu endereço físico e seu uso da internet foi monitorado. (VENTURA, 2017).

A técnica de investigação de redes é bastante útil, sendo uma sugestão adotada até mesmo pelo FBI e é possível adaptá-la para a legislação brasileira, deixando a técnica mais versátil para a aplicação no Brasil. Segundo Santos e Barreto é um fato a se comemorar, pois nossa legislação ainda está carente de leis específicas para a investigação policial na *deep web*. (BARRETO; SANTOS, 2019).

4.2 Infiltrações de agentes na *deep web*

O conceito básico de investigação policial para a obtenção de provas seria o mesmo, tanto para a *surface web* quanto para a *deep web*, porém para identificar o autor na internet profunda, a capacidade técnica da investigação deve ser ainda maior, em virtude do enorme obstáculo do anonimato que a internet profunda oferece. Trata-se de um processo muito difícil, não havendo espaço para amadores.

Segundo o detetive Chris Purchas, da Seção de Exploração Infantil da Unidade de Crimes Sexuais do Serviço Policial de Toronto, no Canadá, a maioria dos criminosos da internet da superfície são “apenas” consumidores dos arquivos ilícitos, ou seja, eles baixam os arquivos, armazenando em suas máquinas, porém, na *deep web*, os criminosos criam esses conteúdos, disponibilizando mediante pagamento, em alguns casos até mesmo de graça, e assim esse tipo de material começa a circular também na *surface web*. (BARRETO; SANTOS, 2019).

A infiltração é uma técnica especial, excepcional e subsidiária da investigação criminal, somente permitida mediante autorização judicial, já que o agente será inserido no meio da organização criminosa, infiltrado com o objetivo de pegar informações valiosas e assim desestruturar a organização criminosa, sendo assim, com a reunião de provas suficientes, o processo penal será iniciado. Mesmo com leis

prevendo a infiltração policial, ainda restavam dúvidas de como inseri-las nos casos de crimes de abuso sexual e exploração infantil, sendo que assim foi sancionada a Lei nº 13.441, de 08 de maio de 2017, apresentando alterações no Estatuto da Criança e do Adolescente. (SANNINI, 2016).

Essa legislação tem como objetivo entregar uma melhor resolutividade em crimes que outras legislações não conseguiam alcançar, como o abuso sexual infantojuvenil praticado na *deep web*. (BARRETO; SANTOS, 2019).

As operações policias na *deep web* são diferentes das que acontecem fora da internet, já que o maior obstáculo é decifrar o IP do agente, pois usam formas de aumentar ainda mais o anonimato, como o uso do Tor, já mencionado anteriormente. (VENTURA, 2017).

Já são muitas as operações policiais realizadas na *deep web*, podendo citar, como exemplo a *darknet* e o famoso caso da escola de Suzano, cidade situada no Estado de São Paulo. E vários outros casos podem ser enumerados, como por exemplo a operação *Pacifier; Bayonet; Disarray; Underground 2*, entre outras. Todas seguindo os mesmos princípios de investigação policial na internet profunda. (BARRETO; SANTOS, 2019).

CONCLUSÃO

O presente trabalho apresentou brevemente o que seria a internet, quando foi criada, onde e sua função. Nos dias de hoje a internet é usada para diversas atividades e está presente em toda nossa vida. A internet é conhecida por todos, mas a internet profunda é um ambiente novo para muitos, onde é possível contemplar o mais alto tipo de anonimato, com dados criptografados, assim praticamente impossibilitando o rastreio ao autor do conteúdo.

A internet profunda não é usada apenas para crimes, ela exerce o direito à privacidade de forma que todos esperam, em virtude disso, se transforma em um ambiente propício à prática de crimes. Criminosos aproveitam o vasto anonimato para dificultar o rastreio ao agente. Na *deep web* é vendido todo tipo de mercadoria ilícita, como drogas, serviços, armas, mídias de pornografia infantil, entre outras.

A investigação neste ambiente é feita por profissionais especializados no assunto, eles utilizam programas de computador para retirar a criptografia em suas várias camadas, reunindo provas para chegar ao agente. Muitos casos de investigações na internet profunda foram positivos, alcançando o autor do crime. Mesmo sendo um árduo trabalho, com os profissionais certos e os devidos *softwares*, não é impossível chegar à origem do crime.

Com o NIT (Network Investigative Technique), a investigação é feita mediante autorização judicial, consistente em implantar um programa de computador, uma espécie de espião, coletando todas as informações do usuário que prática os crimes na *deep web*.

A infiltração também é feita mediante autorização judicial, consiste em inserir o agente na organização criminosa sem deixar suspeitas para os criminosos, assim coletando informações valiosas para a investigação.

Diante do fato que o tema tratado é muito novo e atualizado a todo instante, como já dito e a cada vez que a tecnologia alavanca, certamente os métodos delitivos também progredirão, motivo pelo qual, a temática enseja a continuidade da pesquisa científica de acordo com a evolução do mundo digital.

REFERÊNCIAS

ASSUMPÇÃO, Alessandra de Fátima Almeida. **Avaliação das abordagens terapêuticas para agressores sexuais portadores de transtornos parafílicos**. Dissertação de Mestrado. Universidade Federal de Minas Gerais. Belo Horizonte, MG, 2014.

BARRETO, ALESSANDRO; SANTOS, HERICSON. **Deep Web: Investigação no submundo da internet.** 1. ed. Rio de Janeiro: Brasport, 2019. 170 p. v. 1. Ebook

BARROS, THIAGO. In: **Internet completa 44 anos; relembre a história da web** [S. l.], 7 abr. 2013. Disponível em: https://www.techtudo.com.br/artigos/noticia/2013/04/internet-completa-44-anos-relembre-historia-da-web.html. Acesso em: 28 maio 2020.

FERNANDES, Thamyris. **10 coisas que você pode fazer na internet e nem desconfiava**. São Paulo, 1 set. 2016. Disponível em: https://www.fatosdesconhecidos.com.br/10-coisas-que-voce-pode-fazer-na-internet-e-nem-desconfiava/. Acesso em: 10 out. 2020.

JI HOON YU, Fernando. **Deep Web: Análise acerca do crime envolvendo pedofilia na internet**. São Paulo, 2020. Disponível em:

https://jus.com.br/artigos/81817/deep-web-analise-acerca-do-crime-envolvendo-pedofilia-na-internet. Acesso em: 28 out. 2020.

JOVEMPAN. In: **PF tem tecnologia para identificar usuários da 'deep web'**. [S. l.], 16 mar. 2019. Disponível em: https://jovempan.com.br/noticias/brasil/pf-tem-tecnologia- para-identificar-usuarios-da-deep-web.html. Acesso em: 28 maio 2020.

MARQUES, JOSÉ, **As modernas técnicas de investigação policial** –. Âmbito Jurídico. Disponível em: <https://ambitojuridico.com.br/cadernos/direito-penal/as-modernas-tecnicas-de-investigacao-policial/>. Acesso em: 8 Mar. 2021.

POLÍCIA FEDERAL :**IPED Indexador e Processador de Evidências Digitais Descrição**. [s.l.]: , [s.d.]. Disponível em: <https://servicos.dpf.gov.br/ferramentas/IPED/3.14.5/IPED-Manual_pt-BR.pdf>.

ROSA, NATALIE. In: **Brasil registra aumento de 1.600% em denúncias de crimes online contra mulheres.** [S. l.], 5 fev. 2019. Disponível em: https://canaltech.com.br/seguranca/brasil-registra-aumento-de-1600-em-denuncias-de- crimes-online-contra-mulheres-132103/. Acesso em: 28 maio 2020.

SANNINI NETO, Francisco. **Inquérito Policial e Prisões Provisórias** – Teoria e Prática de Polícia Judiciária. São Paulo: Ideias e Letras, 2014.

SANNINI NETO, Francisco **Infiltração de agentes é atividade de polícia judiciária**. Canal Ciências Criminais. Disponível em: <https://canalcienciascriminais.com.br/infiltracao-de-agentes-e-atividade-de-policia-judiciaria/>. Acesso em: 20 Mar. 2021.

SEPINF-INC. **sepinf-inc/IPED**. GitHub. Disponível em: <https://github.com/sepinf-inc/IPED>. Acesso em: 8 Mar. 2021.

VENTURA, FELIPE. **FBI usa vídeo infectado para revelar a identidade de suspeito na rede anônima Tor** | Internet | Tecnoblog. Tecnoblog. Disponível em: <https://tecnoblog.net/220857/fbi-nit-tor-anonimato/>. Acesso em: 20 Mar. 2021.