DEEP WEB – O LADO SOMBRIO DA INTERNET

Edilberto Strauss
Ph.D. em Ciência e Tecnologia, ITLab/POLI da Universidade Federal do Rio de Janeiro(UFRJ), Rio de Janeiro, RJ, Brasil
estrauss@poli.ufrj.br

Manoel Villas Bôas Júnior
Mestre em Computação Aplicada, ITLab/POLI da Universidade Federal do Rio de Janeiro(UFRJ), Rio de Janeiro, RJ, Brasil
mvbjunior@poli.ufrj.br

Vinicius Drumond Gonzaga
Mestre em Ciência e Tecnologias Nucleares, Instituto de Engenharia Nuclear(IEN), Rio de Janeiro, RJ, Brasil
viniciusdgonzaga@gmail.com

Flávia Cristina Cabral Pereira
Master Business em Engenharia de Computação e Sistemas em TI pelo ITLab/POLI da Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro, RJ, Brasil
flavia.arrais92@gmail.com

RESUMO

O ato de abrir o navegador, escolher um site de busca e pesquisar por algum conteúdo, pode ser uma tarefa simples e rotineira para a maioria dos usuários, porém, existe um lado obscuro da internet que pode ser explorado pelos mais diversos tipos de curiosos, desde ativistas até criminosos. É uma internet que não está acessível através de mecanismos de busca, como o Google por exemplo. Nesta parte obscura da internet, pode-se encontrar prática de crimes de todo teor, como: tráfico de armas, tráfico de drogas, exploração sexual infantil, fóruns extremistas incentivando atos terroristas, venda de crianças e filmes com conteúdo de violência extrema. Atualmente, o termo *Deep Web* está associado a tudo que é criminoso na internet, porém, não é bem assim. Nela, constam todos os seus serviços de e-mail, de banco e de compartilhamento de arquivos, contudo, nenhum deles pode ser acessado pelos mecanismos de busca automáticos, poupando os usuários de marketing não solicitado e exposição dos seus dados, sendo um modo de navegação com mais privacidade. Com base nas informações mencionadas acima, este artigo aborda o conceito da *Deep Web*, suas características, o propósito de criação dessa rede "oculta" e como a criminalidade virtual foi aumentando através dela. Também será abordado as principais redes que operam na *Deep Web*, como: *Tor*, *Freenet* e I2P e como os criminosos as utilizam para atrair "clientes", entretanto, mesmo com toda essa criminalidade no ambiente virtual, há uma ativa atuação da polícia na investigação desses crimes, a fim de punir os responsáveis de forma devida. Entretanto, muitos desafios ainda precisam ser ultrapassados.

Palavras-chave: Deep Web, criminalidade, ambiente virtual, investigação policial.

STRATEGIC PLANNING AS A TOOL FOR STARTUPS COMPETITIVENESS.

ABSTRACT

The act of opening a browser, choosing a search engine, and searching for content may be a simple and routine task for most users, but there is a dark side of the internet that can be explored by various types of curious individuals, from activists to criminals. This is an internet that is not accessible through search engines like Google, for example. In this obscure part of the internet, one can find the practice of all kinds of crimes, such as arms trafficking, drug trafficking, child sexual exploitation, extremist forums encouraging terrorist acts, sale of children, and films with extreme violence content. Currently, the term Deep Web is associated with everything that is criminal on the internet, but that is not entirely true. It includes all of your email, banking, and file-sharing services, but none of them can be accessed by automated search engines, sparing users from unsolicited marketing and exposure of their data, being a mode of browsing with more privacy. Based on the information mentioned above, this article discusses the concept of the Deep Web, its characteristics, the purpose of creating this "hidden" network, and how virtual crime has been increasing through it. It will also address the main networks that operate on the Deep Web, such as Tor, Freenet, and I2P, and how criminals use them to attract "clients," however, even with all this virtual crime, there is an active police effort to investigate these crimes in order to punish those responsible appropriately. However, many challenges still need to be overcome.

Keywords: Deep Web, crime, virtual environment, police investigation.

1 INTRODUÇÃO

A internet tem sido uma ferramenta valiosa para o progresso humano, proporcionando avanços significativos em diversas áreas, desde a comunicação até a saúde. No entanto, como toda tecnologia, a internet também tem sido utilizada de forma indevida para práticas ilegais, prejudicando a segurança e a privacidade dos usuários. Um exemplo disso é o uso de plataformas ilícitas na *deep web*, que permitem que os usuários realizem delitos de forma anônima. Neste artigo, exploramos a natureza dessas plataformas e seus impactos na sociedade.

2 DESENVOLVIMENTO

A *deep web* é uma parte da internet que não é facilmente acessível e não está indexada pelos mecanismos de busca convencionais. Ela é composta por diversas redes derivadas, cada uma com diferentes níveis de permissão e conhecimento, tornando-as mais restritas e profundas. Dentre as redes que compõem a *deep web* estão as plataformas ilícitas, que são utilizadas por usuários com más intenções para praticar diversos tipos de delitos, como comércio ilegal de drogas, abuso e exploração sexual, violação de direitos autorais, entre outros.

Essas plataformas são construídas com o objetivo de manter o anonimato dos usuários, tornando difícil identificar e punir os responsáveis pelos delitos cometidos. Além disso, muitas delas são protegidas por sistemas de criptografia avançados, dificultando ainda mais a sua identificação e ação das autoridades.

Ainda assim, é importante destacar que nem toda a atividade realizada na *deep web* é ilegal ou mal-intencionada. Existem diversas comunidades e fóruns que têm objetivos benignos, como troca de informações e compartilhamento de conhecimento. No entanto, é necessário estar ciente dos riscos e perigos que podem ser encontrados na *deep web* e estar preparado para lidar com eles.

2.1 Deep Web, Surface Web e Dark Web

A internet pode ser divida em *Surface Web* e *Deep Web* onde a deep web possui uma subclassificação denominada *dark web*.

Conforme figura 1, podemos dizer que a surface web é formada por sites, conteúdos e páginas que utilizam a arquitetura cliente/servidor onde tal servidor tem a capacidade de fornecer serviços aos seus clientes. Estes servidores são capazes de hospedar páginas web, servidores de e-mail, banco de dados etc.

Já a *seep web*, embora o conceito seja relativamente novo, da década de 90, o termo "rede escondida" – *hidden web*, já era mencionado por alguns estudiosos, como por exemplo, em 1994, o termo "rede invisível" foi citado pela primeira vez pelo Dr. Jill Ellsworth, para fazer referência ao conteúdo de informação "invisível" para os mecanismos de busca convencionais. [1][2]

Segundo estudo realizado por Bergman (2001) [3], "[...] para ter acesso ao conteúdo "invisível" ou aos peixes raros, é necessário utilizar redes de pescas e equipamentos adequados para alcançar águas mais profundas, ou seja, a *deep web* [...]".

A *deep web* é constituída de redes de computadores caracterizada principalmente por seu anonimato, criptografia, descentralização e código aberto, cujo conteúdo não está disponível para as ferramentas de buscas tradicionais.

De acordo com a tabela 1, a arquitetura utilizada na *deep web* é a P2P, onde não se faz necessário o uso de um servidor central.

Figura 1 – Surface Web x Deep Web

Fonte: https://arikopel.com/2017/03/08/the-matrix-within-the-matrix/ [4].

Tabela 1: Características de redes que operam exclusivamente na *deep web*.

Rede/Sistema	Descentralizada	Segura	Anônima	Código Aberto
Stealhnet: sistema para compartilhamento de arquivos P2P anônimo	Sim	Sim	Sim	Sim
BitTorrent: protocolo para compartilhamento de arquivos via streaming (enxame). Permite aos usuários da rede fazerem download de arquivos em partes e de vários computadores	Sim	Não	Não	Sim
Zeronet: rede anônima para publicação de sites que utiliza criptografia e conexões P2P, funcionando semelhante ao BitTorrent	Sim	Sim	Sim	Sim
Resilio: rede para compartilhamento de arquivos, privada e descentralizada (P2P)	Sim	Sim	Não	Sim

Fonte – Livro: *Deep Web* – Investigação no submundo da Internet [3].

2.2 Características da Deep Web

A arquitetura utilizada nas redes *deep web* é a P2P (ponto a ponto), cuja necessidade de um servidor central é descartada, logo, é descentralizada. Seus componentes funcionam tanto como cliente tanto como servidor.

No momento da transmissão do arquivo, cada nó tem a possibilidade de oferecer partes menores desse arquivo, que ao final da transmissão, todas as partes serão unificadas, apresentando

o arquivo integralmente. Caso algum nó se desconecte da rede durante a transferência, o ponto solicitante irá receber a parte que foi perdida de outro nó conectado à rede.

A configuração da conexão e tráfego é gerenciada pelo software designado para navegação e transferência de arquivos em diversas redes operantes na *deep web*, garantindo a disponibilidade do serviço.

O que acontece de forma diferente na *surface web*, cuja arquitetura convencional deixa os clientes dependentes, aguardando respostas caso do servidor fique *off-line*. São destacadas três características das redes que operam na *deep deb* além da descentralização, que são:

Anonimato: Neste cenário encontramos pessoas comuns que buscam conteúdos com garantia de privacidade, como: blogueiros, ativistas e jornalistas, com o intuito de externarem suas opiniões, críticas e denúncias, principalmente em locais onde existem censura para publicação de determinados conteúdos.

Segurança: Existe um canal de comunicação que é criptografado ponto a ponto, e por mais que interceptem os pacotes em algum momento durante a conexão, eles continuarão cifrados e ilegíveis para quem tentar decifrar o conteúdo daquela comunicação.

Código Aberto: Possibilidade de alteração e otimização dos mecanismos de anonimato e segurança da rede, de maneira a exonerar vulnerabilidades e problemas, além de prover melhorias.[5][6][7].

2.3 As tradicionais redes da Deep Web

Não é possível determinar a quantidade exata de redes existentes na *deep web*, nem se há um mecanismo de busca como o Google ou Yahoo da Surface Web. A forma tradicional de localizar conteúdo na *deep web* é através de diretórios de links, que catalogam listas atualizadas de endereços de páginas com o conteúdo desejado. Outra forma é participar de fóruns de discussão com links de conteúdo desejado. Embora esses conteúdos possam ser publicados na Surface Web por meio de chat, Facebook ou WhatsApp, o link só pode ser acessado pelo software específico da rede, que requer permissão para acessar a *deep web*.

Para ilustrar, suponha um usuário que posta em seu Facebook um endereço fictício como “http://manuais6th6rtvc.onion”, contendo manuais raros de configuração de um rádio amador. Ao perceber a extensão ".onion", pode-se deduzir que se trata de uma *URL* da rede *TOR*, que opera principalmente na *Deep Web*. Este artigo se concentrará em três das principais redes da *deep web*: *Tor*, *Freenet* e I2P.

2.4 Rede Tor

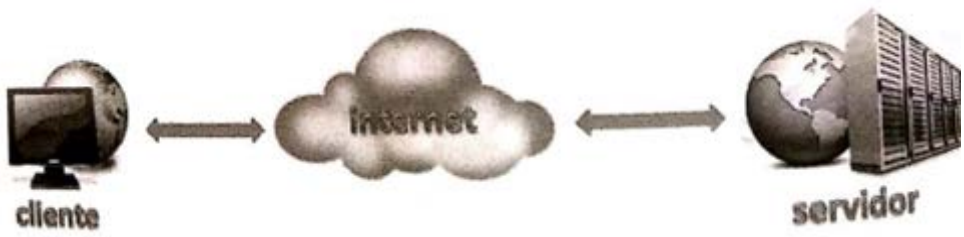
A rede Tor é uma rede descentralizada de computadores voluntários ao redor do mundo que permite aos usuários configurar seu nível de privacidade e segurança online. Embora a rede Tor seja confundida com a *deep web*, ela é definida como um software livre e de rede aberta que ajuda a contornar a censura na internet, protegendo o anonimato online. Os usuários estabelecem conexões por meio de diversos túneis virtuais, o que impede o rastreamento e garante a privacidade e segurança na navegação. No entanto, o uso da rede Tor também pode ser utilizado para atividades criminosas, como tráfico de drogas, transações financeiras ilícitas e abuso sexual infantil. A investigação policial pode ser prejudicada devido à facilidade de uso da tecnologia pelos criminosos, mas os policiais e agentes também podem usar a rede Tor para capturar informações em fontes abertas sem exposição de seus dados. É importante lembrar que navegar pela rede *Tor* não garante o anonimato do usuário, pois é necessário tomar os devidos cuidados e não expor dados pessoais durante a navegação.

2.4.1 Particularidades da rede Tor

A rede *Tor* é responsável por construir vias de comunicação entre o usuário e o computador destino, porém, diferentemente da internet comum, a conexão não é estabelecida no modo cliente/servidor.

Abaixo, nas figuras 2 e 3, são mostrados os dois modelos de rotas de comunicação. Da internet comum e da rede Tor.

Figura 2 – Modelo cliente/servidor da “internet comum”



Fonte: Livro: Deep Web – Investigação no submundo da Internet.[3]

Figura 3 – Modelo cliente/servidor da rede TOR

Fonte: Livro*: Deep Web* – Investigação no submundo da Internet.[3]

Na rede *Tor*, é criado um caminho sinuoso e aleatório, com “nós atravessadores” entre o cliente e o servidor, com o intuito de não deixar rastros das rotas que os pacotes percorreram até chegar ao destino.

Um dos grandes diferenciais da rede *Tor*, é a possibilidade de navegar pela *surface web* de forma anônima, não permitindo que grandes corporações coletem dados para serem utilizados posteriormente em propagandas ou spam, por exemplo.[8][3][4].

2.4 Rede Freenet

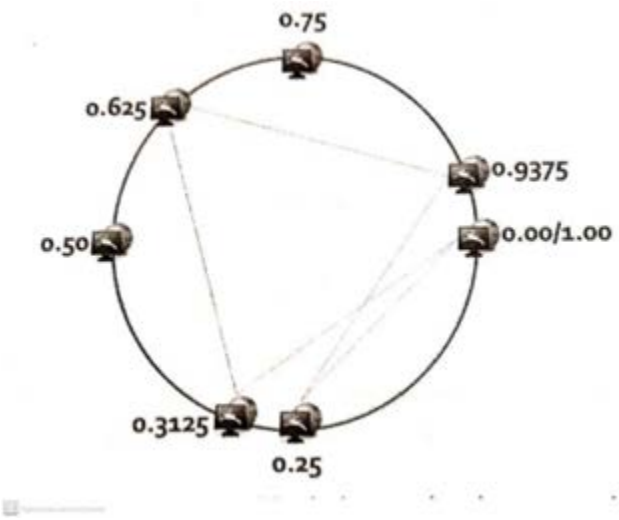
A rede *Freenet* é uma rede ponto a ponto projetada para atuar na *deep web*, com o objetivo de fornecer segurança e anonimato aos usuários, permitindo uma comunicação sem censura. Ao contrário da rede Tor, a *Freenet* não possui um navegador próprio e requer a instalação de um programa que funciona em conjunto com um navegador tradicional. O usuário também precisa configurar uma parte do disco rígido para armazenar conteúdo. Toda informação na *Freenet* é criptografada, e a rede também possui um cliente P2P que permite o compartilhamento de arquivos, preservando o anonimato. As conexões na rede *Freenet* são realizadas através de relés, e a requisição percorre um circuito constituído por N nós, afetando diretamente a velocidade de resposta da rede. A rede *Freenet* nos fornece várias opções de configuração, incluindo a definição de quantos saltos a requisição continuará viva na rede. Tudo isso é possível graças a canais criptografados com configuração avançada, garantindo descentralização, segurança e anonimato. A *Freenet* se baseia na ideia de que muitas pessoas são reprimidas em seus países ao expressarem livremente seus pensamentos e ideias, sendo censuradas por questões culturais, políticas ou religiosas. O download e instalação do software *Freenet* permitem que o usuário acesse o conteúdo disponível na rede de forma segura e anônima.

A rede *Freenet* é uma rede P2P formada por conexões fechadas por meio de nós, sendo

uma rede descentralizada. Quanto mais nós (computadores) conectados, melhor será a sua funcionalidade.

Cada usuário ou relé (nó) é reconhecido por uma variável denominada location(localização) assim que se conecta na rede. A arquitetura foi construída de maneira que cada nó localize o outro em um circuito circular, onde cada um recebe um número decimal entre 0 e 1, sendo assim identificado de forma única na rede. Devido ao mapa da rede ter formato circular, logo o identificador entre 0 e 1 também é, onde a maior distância entre dois nós, sempre 0,5, conforme mostrado na figura 4.

Figura 4 – Modelo simplificado do mapa de rede com sete nós



Fonte: Livro: *Deep Web* – Investigação no submundo da Internet.[3]

A estabilidade da rede, no que diz respeito ao tempo de resposta de uma requisição, é diretamente impactada pela distância entre um nó e outro, por esse motivo, a *Freenet* mantém os nós que possuem o mesmo conteúdo agrupados, facilitando a recuperação dos dados e evitando saltos desnecessários e longos. A *Freenet* possui dois modos básicos de funcionamento:

- *Opennet* ou rede aberta: Disponibilizada para acesso livre e sem restrições (P2P), (BitTorrent, Gnutella etc.), é usada pela *Freenet*, por default, quando o usuário conecta à rede inicialmente, disponibilizando a ele um identificador de localização, entre 0 e 1 aleatoriamente. Essa nova conexão estará conectada a vizinhos desconhecidos, o que a deixa suscetível a ser monitorada, embora isso seja pouco provável, devido à criptografia.
- *Darknet* ou rede obscura: Também denominada de F2F (*Friend to Friend*), a *Darknet* faz exigência do uso de credencial de acesso e o grupo de usuários nela conectado, trocam suas chaves de segurança, o que resulta numa rede totalmente secreta e invisível para os demais usuários

da *Freenet*. É de extrema importância que os usuários estabeleçam uma relação de confiança, a fim de não ocorres quebra do sistema de segurança.[3].

2.5 Rede I2P

Invisible Internet Project é o significado da sigla I2P, que traduzindo significa, "Projeto Internet Invisível".

Semelhante a rede *Freenet*, a I2P faz exigência de instalação de um software e requer configurações adicionais no browser para o seu funcionamento. A I2P conta com quatro camadas de criptografia e tem como agregadores de links principais o I2P Planet e o *Eepstatus*.

Conceitualmente, a I2P é uma rede anônima que utiliza a troca de mensagens entre pares, conservando o princípio da descentralização de servidores através de túneis criptografados em quatro camadas. Tem como objetivo de prover um meio de comunicação para a proteção da intimidade e da privacidade de seus internautas.

O anonimato fornecido pela rede I2P é relativo, ou seja, fica à mercê de como o internauta irá utilizar a rede.

Essa rede nasceu em 2003, oriunda de um projeto de pesquisa acadêmico, sustentado por um grupo dedicado de colaboradores em todo o mundo. Toda codificação utilizada para desenvolver a rede I2P é aberta, por isso, disponível gratuitamente. Atualmente, já existem vários softwares que foram desenvolvidos exclusivamente para operar nesta rede.

O software I2P é multiplataforma, ou seja, pode ser instalado em diversos sistemas operacionais distintos, como: Windows, Mac OS X, Linux (Debian e Ubuntu), BSD e Solaris, além da versão mobile para Android.

Após a instalação do software I2P, o internauta será capaz de gerar e usufruir de uma conta de e-mail privativa dessa rede. Não obstante, terá a possibilidade de navegar e publicar websites anônimos com a extensão ".i2p" na *Deep web*, e por último, essa rede fornece a possibilidade de se usar clientes IRC (Internet Relay Chat), que é um protocolo de comunicação utilizado como bate-papo e troca de arquivos, além da integração com as plataformas de compartilhamento de arquivos "P2P" e "Donkey", "gnutella" e "BitTorrent".

A i2p se auto conceitua como um *middelware*, um software que faz o meio de campo entre o usuário solicitante de uma informação e o destinatário, fornecendo um canal de comunicação seguro e criptografado, já a *Freenet* é retratada como um sistema de armazenamento distribuído e

possibilita a recuperação de conteúdo publicado mesmo que o internauta esteja off-line, por isso, diversas vezes surgem comparações entre as duas redes.

Para sanar as dúvidas de possíveis comparações, abaixo segue a tabela 2 que mostram as diferenças e semelhanças entre as duas redes:[9][3].

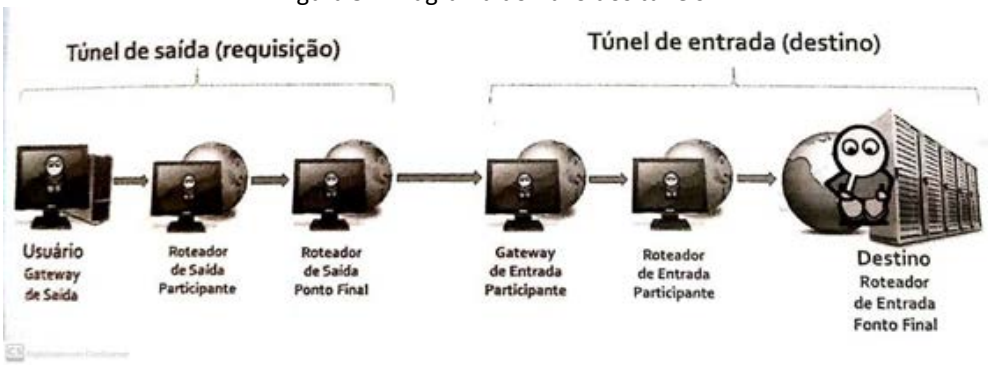
Tabela 2: Comparação das principais redes da *deep web*.

	I2P	**Freenet**	**Tor**
Página	Eepsite	Freesite	Site
Extensão	.i2p	Sequência de chaves (SSK)	.onion
Nome do nó	Roteador	Node	Relé
Objetivo	Comunicação anônima e segura	Armazenamento Distribuído	Comunicação anônima e segura
Comunicação	Criptografada	Criptografada	Criptografada

Fonte: Livro: Deep Web – Investigação no submundo da Internet [3]

- *Router* ou roteador: Os nós na rede I2P são denominados de “roteadores”, diferindo-se então da *Tor* e *Freenet*. Para cada tipo de ação realizada por um usuário na rede, um novo roteador é utilizado, fazendo com que haja um proxy (canal) para os servidores IRC (*chat*), outro para o servidor anônimo do usuário “*eepsite*” (termo utilizado para se referir a um site da rede anônima I2P), outro para o programa que compartilha arquivos etc.
- *Tunnel* ou Túnel: Conforme figura 5, um túnel criptografado é criado durante a comunicação entre os roteadores, neste cenário, é utilizada a criptografia em camadas, onde um roteador só consegue visualizar as informações que seus vizinhos estão transmitindo, assim como o IP do próximo roteador. O ponto de partida da mensagem se chama *gateway*, que é o primeiro roteador do túnel. Todas as mensagens só podem ser disparadas de uma única forma, por isso, a resposta necessariamente retornará por outro *gateway* (caminho).

Figura 5 – Diagrama do fluxo dos túneis I2P



Fonte: Livro: Deep Web – Investigação no submundo da Internet. [3]

3 PROBLEMAS IDENTIFICADOS NA DEEP WEB

A *deep web*, também conhecida como internet invisível, é uma parte da internet que não é acessível por meio dos motores de busca convencionais, e cujo acesso requer o uso de tecnologias como o Tor. A *deep web* é composta por sites que exigem autenticação, sites que não foram indexados pelos mecanismos de busca e sites que usam o anonimato para manter seus usuários seguros. No entanto, o uso da *deep web* não é restrito apenas a indivíduos que desejam manter sua privacidade, mas também a criminosos que buscam um ambiente propício para cometer ações ilegais.

Embora haja uma percepção generalizada de que a *deep web* é um lugar para atividades criminosas, isso não é verdadeiro. A motivação original para a criação da *deep web* era a privacidade, já que na superfície, é difícil manter a privacidade devido à coleta indiscriminada de informações pessoais a cada novo site visitado. No entanto, devido à oferta de privacidade irrestrita fornecida pela *Deep Web*, criminosos encontraram um ambiente consistente para cometer ações ilícitas.

Um dos problemas mais prevalentes na *deep web* é o tráfico de drogas. Há uma série de sites, especialmente na rede Tor, que vendem livremente drogas, principalmente as sintéticas, como MDMA e NBONe. Cada comerciante cria sua própria página hospedada localmente em seu próprio computador e disponibiliza o produto ao público. Existem até mesmo mercados negros, que reúnem diversos vendedores com uma variedade extensa de drogas e outros produtos ilegais ou falsificados. Inclusive, existem sites e fóruns de discussões gerenciados por brasileiros.

O *Wallstreet Market* é identificado como um dos principais e mais populares mercados negros da *deep web*. Ele pode ser encontrado na rede Tor, inclusive em língua portuguesa. A lista de endereços no *Mirrors* é atualizada com frequência, uma vez que os sites são armazenados localmente e, portanto, pode acontecer de um computador que está hospedando um desses endereços pare de funcionar por motivos indefinidos.

A página inicial do *Wallstreet Market* exibe uma lista de produtos disponíveis, com destaque para "Drogas", que conta com mais de seis mil produtos oferecidos, e "Falsificações", com mais de trezentos resultados. Além disso, a página também mostra os vendedores mais ativos desse mercado negro. O comércio de *ecstasy* é o produto mais rentável e lucrativo para os traficantes cibernéticos, pois é fácil de esconder e altamente consumido por jovens de classe média e alta, cujas encomendas são despachadas pelos correios sem levantar suspeitas.

No Brasil, um dos principais e mais populares sites de mercado negro está off-line desde 2018. Há boatos de que os responsáveis por eles foram presos, porém, sem confirmação pela

imprensa; outros afirmam que o site saiu do ar de forma proposital para reformas e ajustes e logo retornará às operações em outros endereços da *deep web*. No entanto, investigações mais profundas revelaram que, em diversos fóruns de origem nacional, os crimes continuam a todo.

4 INVESTIGAÇÃO POLICIAL

A crescente revolução digital e inclusão tecnológica nos últimos anos tem proporcionado muitos benefícios para as pessoas, mas, por outro lado, também tem havido um aumento das práticas criminosas no ambiente cibernético. O desenvolvimento do comércio eletrônico (e-commerce) tem permitido que os atos ilícitos praticados no ambiente físico migrem para o ambiente virtual. Os criminosos têm usufruído de diversos recursos disponíveis no meio virtual para tirar vantagem e cometer atividades ilegais.

No entanto, identificar os criminosos cibernéticos tem sido um grande desafio para os colaboradores da polícia judiciária, devido aos inúmeros serviços de proteção de privacidade e garantia de anonimato disponíveis, como na *deep web*. A falta de leis para dar suporte às novas tecnologias e a falta de capacidade investigativa no ambiente cibernético são alguns dos impasses encontrados.

Atualmente, existem usuários que fornecem seus dados e informações pessoais sem verificar a procedência de algumas aplicações de internet ou da segurança oferecida pelos sites. Por isso, os criminosos se aproveitam da vulnerabilidade desses usuários para potencializar suas ações.

A legislação brasileira possui diversas normas que podem ser usadas para dar suporte às investigações de crimes cometidos no ambiente virtual, como o tráfico de drogas na *deep web*, que possui lei própria há algum tempo. No entanto, o processo legislativo não consegue acompanhar os avanços tecnológicos, gerando um gap até mesmo para os usuários mais ativos na área. O processo investigativo não pode ser limitado por esse motivo.

Os investigadores relatam que os desafios enfrentados durante o processo de investigação são vários, uma vez que existem diversos tipos de delitos cometidos, desde os de menor potencial ofensivo, até graves crimes, como abuso e exploração sexual infantil, crimes de ódio, tráfico de drogas, armas e munições, venda de produtos farmacêuticos proibidos, controlados ou falsificados, crimes contra patrimônio, entre outros.

Por exemplo, o Estatuto da Criança e do Adolescente prevê que o praticante do delito seja notificado e, mesmo assim, não retire do ar ou desabilite o acesso a fotos, vídeos ou outro tipo de registro que contenha material de sexo explícito ou pornografia envolvendo criança ou adolescente,

fique sujeito a pena de três a seis anos de reclusão. Se o conteúdo estiver hospedado em um site ou rede social, não há nenhum impeditivo para que sejam removidos. No entanto, na *deep web*, a hospedagem fica sob controle do usuário, que está protegido pelo anonimato e por várias camadas de criptografia, tornando inviável a remoção deles.

É recomendada a instauração de inquérito policial para apuração do fato, independentemente da gravidade do delito. Embora a investigação de crimes cibernéticos ainda apresente muitos desafios, as polícias judiciárias brasileiras devem avançar na aplicação de novas metodologias para individualizar a autoria delitiva. Assim como diversos projetos foram desenvolvidos para tornar o ambiente cibernético mais seguro e estável.

5 PROPOSTA

A partir dos estudos teóricos descritos no capítulo 02, apresenta-se a primeira proposta de solução para o problema estudado.

5.1 Proposta 1: Fingir ser um usuário frequente da *deep web*

Esse método não é rápido nem fácil, e consiste em um policial especializado em desvendar crimes na *deep web* se passar por um usuário interessado em algum tipo de produto ou conteúdo, durante meses, para conseguir a confiança dos demais usuários da rede e até mesmo entrar em grupos fechados e participar de fóruns de discussões.

O investigador precisaria inclusive adquirir por meio de compra um dos produtos ou serviços durante um tempo, para convencer os demais usuários da rede que ele é um internauta rentável, frequente e de confiança.

Após se tornar um membro e se tornar “conhecido” entre os grupos fechados, o investigador criaria uma página para comercialização de drogas ilícitas de diversos tipos, para atrair o maior número de interessados possíveis. Quando uma venda é efetivada, existe um endereço de entrega registrado para os produtos, facilitando o trabalho do investigador.

Se não for possível encontrar o criminoso no endereço de entrega, pode-se imputar um rastreador no pacote e identificar posteriormente o produto para tentar achar alguma pista sobre o suspeito.

O transporte de drogas pela *deep web* é feito através de serviços de entrega tradicionais como os Correios, o que faz com que o remetente ou destinatário seja descoberto se o produto não

estiver cuidadosamente embalado. Daí, mais uma brecha para identificar o criminoso. Para estes casos, a polícia pode criar uma "entrega falsa", pegando o suspeito em flagrante.

Dado o seguinte cenário: Uma famosa página de venda de drogas ilícitas na *deep web*, na rede Tor, chamada *VisitMyDrugs*, comercializa livremente produtos como: *Ecstasy*, cocaína, maconha e remédios controlados, durante cinco anos, sem deixar rastros passíveis de identificação.

A polícia por sua vez, descobre um aumento significativo de indivíduos com overdose dessas drogas em hospitais e também boatos de alto consumo de *ecstasy* pelos jovens em festas, então, através de denúncias, um inquérito policial é aberto para investigação, onde policiais especializados tomam ciência por meio de depoimentos de testemunhas, que as drogas são compradas pelo mercado negro através do site *VisitMyDrugs*, porém, ninguém conhece os responsáveis pela criação do site e fornecimento das drogas.

A polícia especializada em crimes cibernéticos designa um profissional para se infiltrar nesta rede, a fim de identificar qualquer informação que o leve aos criminosos, então o policial durante o período de 6 meses, compra uma significativa quantidade de comprimidos de ecstasy e maconha todo mês, afirmando que irá comercializar para jovens em festas. Conforme as transações são realizadas de forma segura e anônima com o pagamento sempre em dia, o policial infiltrado passa a conquistar a confiança do vendedor, por ser considerado um "bom comprador", até que depois de três meses ele consegue entrar num grupo fechado que contém somente usuários de confiança. A partir daí, ele passa a ser convidado para fóruns próprios de discussões e dúvidas sobre as drogas, meio de entrega e etc.

Para não levantar suspeitas, o policial infiltrado não faz muitas perguntas, apenas lê os comentários e faz elogios aos produtos adquiridos.

Depois de uns meses, um site denominado *MetaBay* para venda de Metanfetamina é criado na rede Tor para que o policial infiltrado administre e tente atrair os clientes do *VistiMyDrugs*, já que sua "reputação" na rede estará em alta devido a um longo período de participação como usuário de confiança. Não sendo muito difícil, os usuários começam gradativamente a realizar seus pedidos pelo *MetaBay*, o policial utiliza um produto placebo para simular a Metanfetamina, contendo um microchip de metal capaz de rastrear o pacote em qualquer localização. Os funcionários dos correios precisarão garantir que o pacote chegue íntegro e no prazo para o comprador. Passando- se 24 horas, a polícia rastreia o microchip de metal e descobre a localização do comprador, que por sua vez, também está envolvido no *VistMyDrugs*, podendo contribuir com mais informações em troca de redução de pena.

Todo o processo de infiltração policial durou cerca de dois anos.

5.2 Proposta 2: Resolução através de software denominado IPED

Este software foi desenvolvido para auxiliar na operação Lava-Jato, porém, suas funcionalidades podem ser aplicadas para investigação de diversos crimes na *deep web*, conforme explicada no trabalho.

O IPED é um sistema para indexação e processamento de evidências digitais, que captura e organiza dados de interesse em arquivos visíveis ocultos, apagados e fragmentados que estejam em dispositivos com discos rígidos, *pendrives*, cartões de memória, SSDs, CDs, DVDs, entre outros.

Depois de coletar os dados, o IPED possibilita realizar pesquisas por meio de palavras-chave, além de recuperação de mensagens de chats, redes sociais e e-mails que já tenham sido gravadas e armazenadas no dispositivo, mesmo que de forma temporária.

O software permite também, a classificação e visualização rápida de conteúdos de imagem e vídeo.

Este software foi desenvolvido em Java e conta com uma interface simples e amigável.

O IPED tem alta escalabilidade e permite o processamento de dados em várias máquinas e possui uma taxa de processamento superior a 300GB/h e possibilita que dados sejam analisados de forma simultânea em até cem dispositivos diferentes.

Outra característica deste software é que os dados podem ser organizados por tipo e formato de arquivo, além de permitir que os arquivos sejam extraídos e exportados para posterior análise e possível inclusão de informações no laudo pericial.

Passando pela análise, o software conta com a possibilidade de geração de relatórios com os resultados obtidos. O programa ainda possui outras diversas funcionalidades interessantes, como por exemplo:

- Identificação de nudez: Essa funcionalidade é destinada para auxílio nas investigações relativas a pornografia infantil. O programa é capaz de fazer uma varredura e detectar imagens que contenham nudez.
- Indexação: Busca por palavras-chave nos dados capturados.
- Multiplataforma: O software é compatível com vários sistemas operacionais como: Windows, /Linux e Mac OS.
- Processamento em batch: Processamento e extração de dados automaticamente, em sequência e a qualquer hora.
- Recuperação de arquivos apagados: Através do recurso *data carving*, é possível recuperar mais de quarenta tipos de formatos de arquivos que foram apagados.

- Visualização de arquivos de imagens e vídeos: O software é capaz de exibir vários formatos diferentes de imagens e vídeos em miniatura durante a análise, com o propósito de gerar uma visualização geral da galeria de arquivos.

6 RESULTADOS OBTIDOS

Diante das propostas 1 e 2 apresentadas foram obtidos os seguintes resultados:

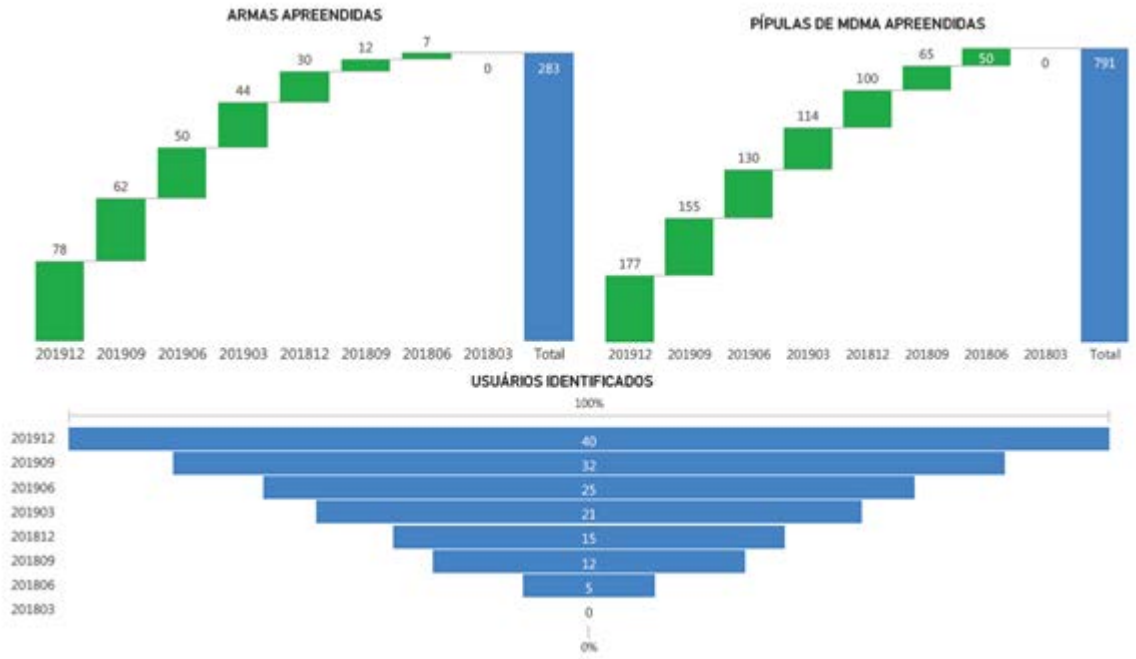
6.1 Resultado 1: Apreensão de criminosos, armas, drogas

As polícias gradativamente estão dando passos significativos no que diz respeito à repressão aos crimes praticados na *deep web*.

A primeira solução apresentada resultou no cumprimento de mais de cem mandados de busca e apreensão em diversos estados, resultando na individualização de mais de cinquenta usuários que exerciam e capitaneavam crimes no ambiente cibernético.

E, não somente criminosos que vendiam drogas foram capturados, como também foram identificados através das investigações, criminosos que praticavam delitos contra a dignidade sexual infanto-juvenil.

Figura 6 – Gráfico de Resultados obtidos da primeira solução proposta



Fonte: Autoria do pesquisador, 2020

A figura 6 mostra três gráficos referentes ao acompanhamento do desenvolvimento da primeira solução proposta. Este acompanhamento foi realizado

trimestralmente entre os anos de 2018 e 2019 e podemos ver desempenhos semelhantes nos três gráficos ao longo de dois anos.

No primeiro, após aplicação da primeira solução, notamos na cascata que o trimestre de melhor resultado foi o último (2019/10, 2019/11, 2019/12), com um crescimento exponencial de 61% a mais de armas apreendidas se comparado com o mesmo período do ano anterior.

Este resultado promissor se dá, devido à melhor aplicação da solução proposta, mais treinamentos e melhor entendimento do comportamento dos criminosos ao longo de dois anos. Não obstante, temos o resultado do segundo gráfico de apreensão de pílulas de MDMA, que com a proposta de fingir ser um usuário frequente na *deep web* para atrair traficantes e usuários, resultou num crescimento de 43% de pílulas apreendidas comparando o último trimestre de 2019 com o último trimestre de 2018.

Novamente, tal desempenho também se deu devido à melhor aplicação e entendimento da solução proposta.

Como consequência do bom desempenho da primeira solução proposta, a apreensão de usuários envolvidos (traficantes e compradores) cresceu significativamente, devido à entrega de outros participantes do esquema em troca de redução de pena, ou seja, um aumento de 79% (entre os anos de 2018 e 2019) de captura de usuários envolvidos em crimes de tráfico e compra de drogas pela *deep web*.

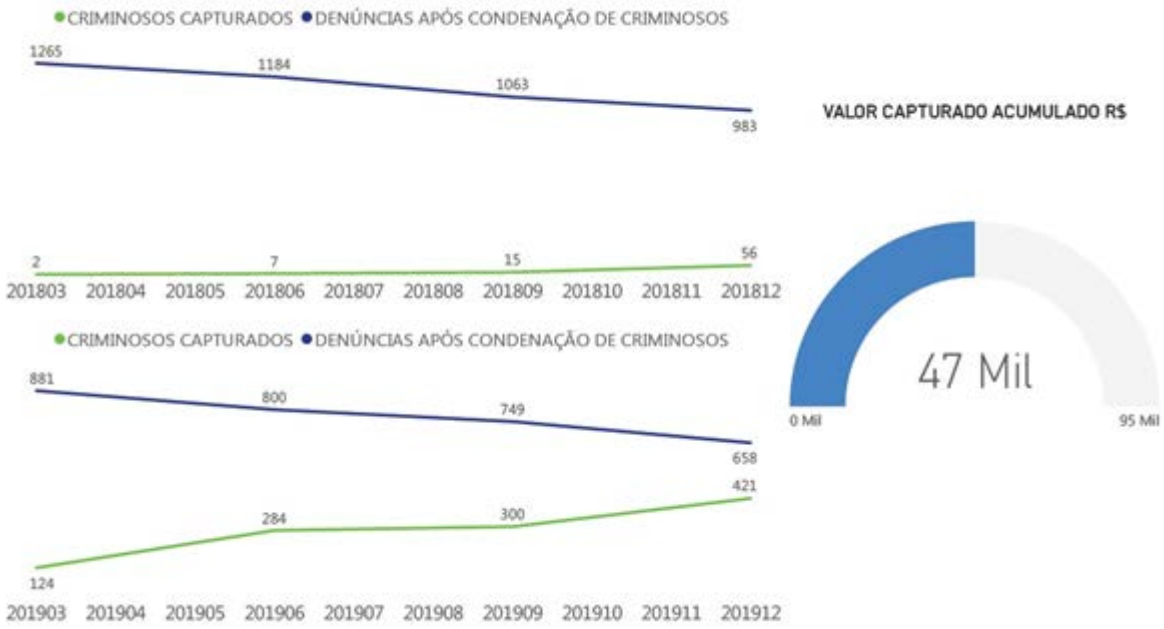
6.2 Resultado 2: Condenação de criminosos e recuperação de dinheiro

A aplicação do software IPED nas investigações de crimes na *deep web*, contou com a participação de dez peritos investigativos.

Na figura 7, contamos com dois gráficos, um para o ano de 2018 e outro para o ano de 2019, contendo o comparativo entre criminosos capturados e condenados após aplicação de solução com software IPED e a quantidade de denúncias recebidas após condenação destes criminosos.

No ano de 2018, de forma mais leve, podemos perceber que o número de denúncias relativas a crimes ocorridos na *deep web* diminuíra à medida que a quantidade de criminosos capturados aumentara.

Figura 7 – Gráfico de Resultados obtidos da segunda solução proposta.



Fonte: Autoria do pesquisador, 2020

Tal fato ocorreu, devido à eficiência provida pela ferramenta e pela aplicação de leis duras e penalidades irreversíveis ao envolvidos. Por exemplo, um criminoso capturado acusado de compartilhar e vender conteúdo pornográfico infantil, além de ser submetido ao código penal pertinente, ainda tem todo o seu "investimento" perdido com a condenação, e após a divulgação deste software na mídia, perceberam que é muito mais fácil e prático de identificar criminosos na *deep web* mesmo com todas as camadas de criptografia, poupando o trabalho de infiltração por longos anos. Com medo de serem identificados e presos, os praticantes de delitos cibernéticos passam a pensar duas vezes antes de comercializar conteúdo impróprio pelo ambiente virtual, daí com menos criminosos, menos denúncias.

No ano 2019, foi possível perceber esse contraste com mais força, pois com o devido treinamento e capacitação de pessoal especializado para operar a ferramenta, nota-se uma captura de criminosos com maior eficiência resultando no aumento de 92% de criminosos identificados de 2018 para 2019 e redução de 31% nas denúncias realizadas. A Operação no período de dois anos resultou na captura de mais de R$ 47.000,00 cujo montante foi aplicado no desenvolvimento de novas ferramentas de análise de big data a fim de produzir laudos periciais com maior agilidade.

7 CONCLUSÃO

É de extrema importância que o usuário da internet entenda o conceito de *deep web* e seu funcionamento. Com o surgimento de novas tecnologias, podemos ficar vulneráveis se nos expusermos a elas, sem conhecê-las.

Indefinida, inexplorada e misteriosa para a grande maioria dos internautas, é vista e caracterizada por leigos apenas como um território obscuro destinado somente para prática de atividades ilícitas.

Atualmente, os criminosos vêm buscando novas tecnologias e maneiras de fugir da aplicação da lei penal, sobretudo, dão de cara com as dificuldades de atribuição da autoria do crime, visto que existe uma robusta camada de criptografia "protegendo" esses delinquentes.

Nos dias que correm, as grandes organizações possuem o controle da internet (superfície) e mantém os usuários reféns de suas tecnologias, coletando seus dados e utilizando de forma a promover seus produtos e serviços. Daí, se encontra a necessidade de utilizar uma rede protegida e anônima (*deep web*).

Vale ressaltar que muitos profissionais liberais, jornalistas, blogueiros e ativistas buscam o anonimato e segurança fornecido pela *deep web* para expor suas opiniões e denúncias sem sofrerem censuras. Os especialistas de investigação nessa área precisam perseguir o caminho para enfrentamento dos crimes praticados na *deep web*, assim como seus autores.

REFERÊNCIAS

[1] Deep web: o que é, como entrar e o que acontece na parte sombria da internet https://olhardigital.com.br/fique_seguro/noticia/deep-web-saiba-o-que-acontece-na- parte-obscura-da-internet/31120 (Acesso em 08 de Janeiro de 2020).

[2] Gonçalves Barreto, Alesandro. Livro: Deep Web – Investigação no submundo da internet (Acesso em 10 de Janeiro 2020).

[3] Artigo publicado em 2001 por Michael K. Bergan intitulado de The Deep Web: Surfacing Hidden Value, cuja tradução livre para o português é "Rede profunda: Valores Escondidos da Superfície".

[4] Surface Web x Deep Web. https://arikopel.com/2017/03/08/the-matrix-within- the-matrix/

[5] GOODMAN, Marc. Future Crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. São Paulo: HSM, 2015, p. 188-189 (Acessado em 15 de Maio de 2020).

[6] O que é Deep Web? https://www.techtudo.com.br/noticias/2019/03/o-que-e- deep-

web.ghtml (Acesso em 12 de Fevereiro de 2020).

[7] Deep Web e Dark Web: qual a diferença? https://tecnoblog.net/282436/deep- web-e-dark-web-qual-a-diferenca/ (Acesso em 16 de Fevereiro de 2020).

[8] A diferença entre o Deep Web e o Darknet. https://www.cacatech.com/23817/a-diferenca-entre-o-deep-web-e-o-darknet.html (Acesso em 24 de Fevereiro de 2020).

[9] Navegue com privacidade. Pesquise com liberdade. https://www.torproject.org/pt-BR/ (Acesso em 12 de Março de 2020)

[10] Um Mergulho na Deep Web: Redes Descentralizadas, FREENET, TOR, I2P https://www.profissionaisti.com.br/um-mergulho-na-deep-web-parte-25/ (Acesso em 12 de Março de 2020). (Acesso em 03 de Agosto de 2020).