INTRODUÇÃO

A *Web* é um instrumento imprescindível para concretização da maior parte das atividades cotidiana e profissional, essencialmente por permitir o entrelaçamento, no âmbito virtual e real, de quase todos os aspectos da vida em sociedade. Ocorre que nem tudo é seguro no mundo virtual, visto que é um ambiente propício a concretização da criminalização de certas condutas, dentre elas o terrorismo. Logo, urge investigar: como a *Dark Weeb* favorece a prática do terrorismo? Sustenta-se como hipótese que a *Dark Web* permite os terroristas se esquivarem do olhar dos Estados, bem como obter investimentos necessários para a consecução de seus atos.

Diante disso, o objetivo geral do presente estudo é analisar a natureza do ambiente das *Deep Web* e da *Dark Web* que favorecem a prática dos mercados ilícitos, o que inclui o financiamento ao terrorismo e a sua própria prática. Para a consecução do objetivo geral, dois objetivos específicos foram elencados: (i) verificar as distinções e semelhanças da *Deep Web* e da *Dark Web*, principalmente quanto aos aspectos que tornam a última profunda e obscura; (ii) analisar a *Dark Web* como instrumento de ocultação e financiamento do terrorismo em um mercado clandestino alimentado por criptomoedas. Por fim, o trabalho possui natureza exploratória, adota o método de hipotético-dedutivo, abordagem qualitativa e pesquisa bibliográfica-documental.

Deep Web e *Dark Weeb*: distinções e semelhanças

Compreender as camadas obscuras da *Web* no ciberespaço é de suma importância à contemporaneidade, sobretudo quanto ao contraterrorismo. A *Web* utilizada diariamente é denominada de *Visible Web* (Web Visível), as camadas mais profundas e obscuras são denominadas *Deep Web* e *Dark Web,* distintas em natureza, pois a possibilidade de encontrar conteúdos na *Deep Web* não pode ser confundida com a obscuridade exclusiva da *Dark Web*. Ademais, insta ressaltar, a *Deep Web* abriga distintas camadas obscuras do ciberespaço, sendo a mais obscura, a *Dark Web* (Chertoff e Simon, 2015).

A *Deep Web*, também denominada de *Invisible Web* e *Hidden Web,* refere-se à fração do ciberespaço com conteúdo não recuperáveis ou indexáveis pelos mecanismos de busca e não transitáveis, i. e., não acessados por instrumentos de buscas tradicionais. Além disso, a efemeridade das informações possibilita a alteração dos dados com frequência tornando ineficiente a atuação do buscador tradicional. Igualmente, site com senhas, *firewall*, páginas

dinâmicas e sem hiperlink, informações nas intranets ou redes sociais, marcas e patentes não estão localizados nos buscadores convencionais, portanto, são encontrados na *Deep Web* (Weber e Kruisbergen, 2019).

Praticamente todo aquele que possui login e senha está envolvido na *Deep Web*, mesmo por desconhecimento. Logo, muitos dados não são disponibilizados por direito de sigilo ou de segurança por serem considerados dados sensíveis. Estes, por sua vez, são informações íntimas e secretas de pessoas físicas e jurídicas, portanto, sigilosas. Destarte, por questões éticas e jurídicas, tais dados não podem ser compartilhados por administradores das páginas e outros que utilizam o serviço. Consequentemente, o sigilo de determinadas informações na *Web* é necessário sob diversos aspectos (Gehl, 2016).

Entretanto, a maioria dos sites da *Deep Web* são gratuitos e concentram uma informação pública maior àquela encontrada na *Visible Web*. Outrossim, indubitavelmente se caracteriza por possuir uma quantidade mais elevada de documentos e elementos informativos. São inúmeros os materiais ilícitos e antiéticos encontrados no universo da *Deep Web*, a saber: comércio de drogas, fraudes, lavagem de dinheiro, pedofilia, artigos científicos sem acesso livre (Chertoff e Simon, 2015).

Ian Clarke – ex-presidente da Sociedade de Inteligência Artificial em Estocolmo- em 2000, desenvolveu um *software* denominado *Freenet*, i. e., uma plataforma de comunicação que garante o anonimato e impossibilita a censura. O objetivo original era assegurar a liberdade de expressão com base no anonimato. Ocorre que isso favoreceu a criação de uma rede paralela à *Web*, que é a *Dark Web*, também denominada de *Darknet*, fundamentada na ideia de *Invisible Web*. Nesse sentido, é inegável que a *Dark* facilita a navegação tranquila, com altíssima privacidade, bem como dificulta a prática da espionagem. Nesse sentido, trata-se do verdadeiro tipo de *Web* profunda e obscura, com características próprias, que apenas pode ser acessada por meio de navegadores baseados em *proxy* que escondam o *Internet Protocol* (IP), favorecendo, inclusive, a prática de crimes (Chertoff, 2017).

A *Dark Web* é um ambiente que possui seus próprios instrumentos de pesquisas, comunidade, sistemas de classificação, moeda – *bitcoins*. Não é de surpreender que essa espécie de moeda, no cenário da *Dark*, é utilizada como instrumento de troca do comércio ilegal, uma vez que a sua criptografia não exige as formalidades do comércio legal, como a criação de uma conta bancária. A *Dark* encontra-se no próprio cenário da *Deep Web*, porém, em uma escala hierárquica no ciberespaço, encontra-se em um ambiente mais profundo, justamente por ser acessada apenas por meio de *proxy*, por isso, é a esfera verdadeiramente invisível do ciberespaço. Consequentemente, o rastreamento de quem a acessa exige um trabalho hércule,

haja vista a tarefa dificílima de romper a blindagem da criptografia e obter o rastreamento de usuários e dos IP. O conteúdo da *Dark Web* geralmente fica no anonimato porque grande parte são ilegais, uma vez que permite bens e serviços serem comercializados às pessoas que arriscam e estão disposto a pagar o preço (Weber e Kruisbergen, 2019).

Observa-se que a *Deep Web* não é de toda ruim. O fato de ser um banco de dados e de outros serviços não indexados pelos mecanismos de busca tradicionais não a torna algo diretamente ilegítimo ou ilegal; a questão é que a *Dark Web* possibilita um ambiente no qual operam *hackers*, gângsteres, terroristas, dentre outros indivíduos delituosos. O local se caracteriza como um mercado negro, sendo a moeda de troca as formas de criptomoedas. Além do mais, nada obsta a terceirização do trabalho neste local, razão pela qual alguns indivíduos são contratados para fazer o trabalho sujo (Gehl, 2016).

O acesso à *Deep Web* depende de um conjunto de *software* e roteadores, sendo o mais cobiçado o navegador TOR, bem como o Hornet TOR, sendo este mais seguro do que o primeiro modelo. Os modelos TOR (*The Onion Router*) - frutos dos desenvolvimentos dos técnicos do laboratório *US Naval Research Lab* - usam pontos de entrada aleatórios na rede *Onion*, além disso os dados são criptografados e encaminhados com o endereço final. O ponto de retransmissão subsequente descriptografa o endereço, criptografa a solicitação e encaminha novamente. Portanto, em cada ponto ao longo do caminho, os dados são criptografados entre os nós (Chertoff e Simon, 2015).

A rede passa por servidores e cria passagens virtuais dificultando o rastreamento de IP. A questão é que dificilmente o governo não tem ciência de que alguém baixou o TOR, por isso, os usuários do navegador eram identificados pela *National Security Agency - NSA* (Agência de Segurança Nacional). Os usuários do TOR são rastreados por meio da impressão digital do site, ou seja, o navegador revela padrões de tráfego imprimíveis que permitem que o adversário seja identificado com eficiência e precisão. Portanto, busca-se identificar a estratégia do invasor por meio de circuitos suspeitos e ocultos. Para isso, rastreia-se as teclas digitadas, devido a tendência de que todos tem de utilizar a mesma caligrafia, além de identificar quanto tempo cada tecla foi pressionada e quando foi liberada. Em suma, se é possível rastrear alguém usando um navegador TOR significa que nada é verdadeiramente anônimo (Gehl, 2016).

***Dark Web* como Instrumento do Terrorismo**

Com o advento da internet, a globalização proporcionou uma conexão social jamais premeditada desencadeando integrações únicas e desafios inimagináveis. Dentre eles,

obscuridades dignas de preocupação internacional com o adentrar dos níveis ou camadas. Ocultos pela escuridão da *Dark Web*, indivíduos a utilizam por motivos amplos: da satisfação pessoal ao planejamento de atos terroristas. Tornando-a um ambiente negativo, como escrevem Ehney e Shorter (2016, p. 38):

> Como as recentes atividades na *Dark web* provaram ser negativas e perigosas? Como afirmei anteriormente, há muitos personagens maliciosos e coniventes que gostam de usar a parte escura da *web* invisível. Podem ser indivíduos procurando satisfazer seus próprios prazeres, ou como a pesquisa mostrará, podem ser organizações terroristas, como o ISIS e a Al Qaeda, procurando recrutar e obter financiamento daqueles que estão dispostos a ajudar sua causa.

Por conseguinte, o que possibilita a garantia desse anonimato são instrumentos e ferramentas programados especificamente para ocultar a identidade daqueles que os utilizam. Ademais, tais recursos fomentam a ocultação de atos ilícitos de insurgências vigiadas por agências de inteligência em cooperação internacional devido à alta periculosidade de suas ações. Por exemplo, ferramentas de criptografia como a chamada *Mujaheideen Secrets*[1], que se revela meio eficiente para, conforme o nome representa, esconder segredos de agentes terroristas (Ehney e Shorteer, 2016. Apud Glasser, 2015).

Além disso, a comunicação, essencial ao planejamento de atividades terroristas é fomentado pelos serviços ofertados na rede oculta, como lecionam Ehney e Shorter (2016) "Eles também utilizam a *Dark Web* para se comunicar uns com os outros porque a *web* invisível os auxilia a ficar fora do olhar atento de autoridades governamentais." Outrossim, como expressa Paganini (2015) são vários os serviços disponíveis na *Deep Web* cuja oferta visa a comunicação segura além dessa camada propiciar a manutenção financeira terrorista mediante a transferência de moedas digitais. Suprindo então duas demandas das insurgências: rotas de fuga à prevenção governamental e investimentos mediante transferência de criptomoedas.

Quanto ao angariar de fundos, a difusão de mídia terrorista torna a *Dark Web* meio chave para a influência e manipulação de massas, de acordo com Ehney e Shorter (2016, p. 38) grupos terroristas são capazes de postar propagandas em lugares que a rede proporciona muito tráfego que associado à ampla aceitação de criptomoedas, como as *bitcoins*, meio de transação dominante na *Dark Web*, promovem a divulgação necessária para que o angariar de fundos seja

[1] ferramenta de criptografia (Ehney e Shorter, 2016). O substantivo próprio do aplicativo *Mujaheideen Secrets* é, conforme Gianluca Melis (2019, p. 06), derivado da forma plural do vocábulo "*mujahid*", que em árabe significa "combatente". A mesma palavra, além disso, é atribuído o significado "guerreiro santo", termo de identificação para os combatentes vinculados à ideologia islâmica, servindo de base, inclusive, para a inspiração dos mesmos.

massivo, permitindo o financiamento e recrutamento de soldados, como descrevem Ehney e Shorter (2016), até mesmo de países que já lideraram o *front* na guerra ao terror: Estados Unidos.

Inclusive, as trocas de mercadoria e investimentos em moeda não rastreável associados ao sigilo nas comunicações dificultam o propósito de romper recursos financeiros, o rastreio da troca de informações, a identificação e rompimento na organização de células terroristas por meio do sigilo nas comunicações, contribuem para o fomento da eficiência de grupos terroristas, tornando o contraterrorismo desafiador:

> É tremendamente difícil de ler ou rastrear a maioria das mensagens entre terroristas porque a maioria delas é destruída logo após serem recebidas e lidas apenas pelo receptor ao qual a mensagem foi destinada. Apenas aquele que estão enviando mensagens são capazes de ver a mensagem inteira utilizando chaves logarítmicas especiais. Existem, até mesmo, aplicativos para download em *smartphones* que possibilitam anonimato na comunicação entre indivíduos. (Ehney e Shorter, 2016, p. 38).

Insta ressaltar, o terrorismo no século XXI, é uma preocupação internacional ao ponto de instigar o terror com atentados, se organizar em países que se submetem à vista grossa de suas atividades, verdadeiros oásis para o terrorismo, visando o cumprir de sua finalidade: a difusão do terror. Como afirmou Koffi Annan, o Secretário-Geral da ONU na 60ª Assembleia Geral das Nações Unidas, de acordo com Facciolli (2017, p.24):

> Qualquer ação que atente causar mortes ou sério dano corporal a civis e não combatentes, quando o propósito de tal ação, por sua natureza ou contexto, é intimidar uma população ou compelir um governo ou uma organização internacional a agir ou se abster de agir.

Logo, diante da preocupação quanto a necessidade de prevenir e reprimir atividades terroristas associadas às redes ocultas. Infere-se como solução contraterrorista a utilização da mesma arma dos malfeitores, mediante infiltrações e, como afirma Stockley (2015) desenvolvimento de programas com o objetivo de burlar o anonimato proporcionado pela *Dark Web.*

São diversas as práticas a serem adotadas no objetivo de rastrear usuários, dentre as quais, destacam-se o mapeamento do diretório de serviço oculto, monitoramento de dados dos clientes, sites sociais e serviços ocultos, análise semântica da informação necessária sobre o site secreto e a definição do perfil de transações feitas nos mercados da *Dark Web* para recolher

informações sobre vendedores, usuários e mercadorias. Assim, perfis pessoais poderão ser construídos com o tempo (Ehney e Shorter, 2016).

A ameaça terrorista afeta, não somente nações ou especificamente a ideia de Estado de determinada nação, mas também, a população residente em determinado local, utilizando como arma a integridade e vida de seres materiais. Dito isso, pergunte-se quem são os alvos de uma insurgência terrorista e a resposta exaure-se em: todos, inclusive nós. O ataque terrorista destinado à um só indivíduo possui a finalidade voltada para um grupo maior, visando sua influência psicológica. Como argumenta Ângelo Facciolli (2017, p. 24), eis o texto do Departamento de Estado dos Estados Unidos da América (DE/EUA), em definição ao terrorismo:

> É a ameaça ou o emprego da violência com fins políticos, por indivíduo ou grupo, em favor ou contra autoridade governamental instituída, quando tais ações se destinam a influência um grupo alvo mais amplo do que a vítima ou as vítimas imediatas.

Os grupos terroristas existentes colocam a integridade de cada indivíduo em risco. Ademais, o esforço individual, ao ser realizado por um conjunto de indivíduos molda o esforço coletivo, permitindo o perfazer da esperança na luta contraterrorista. Infere-se, portanto, a necessidade da sociedade em buscar conhecimento acerca da realização de atividades terroristas, conscientização e autoconscientização, a denúncia de atos moldando o agir individual como dever social na luta ativa contra o terror. “Não pergunte o que sua nação pode fazer por você, mas o que você pode fazer por sua nação” John F. Kennedy (Ehney e Shorter, 2016).

CONCLUSÃO

Primeiramente, a análise das camadas e programas da *Invisible Web* permitiu estabelecer definições gerais e a caracterização de suas partes. Outrossim, foi possível delimitar uma orientação acerca da ambientação, no cyberespaço, a ser utilizado por usuários que, a depender da finalidade, tornarão os serviços ofertados pela *Dark Web* e *Deep Web*, meios de concretização para atividades ilícitas.

Por conseguinte, a incidência do terrorismo, acarreta preocupação e exaure esforços internacionais para sua repressão e prevenção visando a proteção da população e da ideia de Estado-nação. Constitui função precípua do estado, no sentido de garantia aos Direitos

Fundamentais, o cuidado com a sociedade visando o bem comum de todos, condição necessária para preocupação em relação ao *cyberespaço* e indivíduos cujos atos ensejam a obstrução de liberdades e garantias.

Em suma, a atuação terrorista na *Invisible Web*, demanda necessidade de cooperação internacional para o fim dessas atividades, por meio da conscientização e apoio populacional, mediante segurança público-privada, e a execução de ações de inteligência visando o bem coletivo dos afetados direta e indiretamente pela difusão do terror.

REFERÊNCIAS

CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017.

CHERTOFF, Michael; SIMON, Tobby. The impact of the Dark Web on internet governance and cyber security. **Global Comission on Internet Governance**, Waterloo, n. 6, 2015.

EHNEY, Ryan; SHORTER, D. Jack. Deep Web, Dark Web, Invisible Web and The Post Isis World. **Issues in Information Systems**, v.17, n.4, p.36-41, 2016.

FACCIOLLI, Ângelo Ferreira. **Introdução ao terrorismo: evolução histórica, doutrina, aspectos táticos, estratégicos e legais**. Curitiba: Juruá, 2017.

GEHL, Robert. Power/freedom on the dark web: a digital ethnography of the Dark Web social network. **New Media & Society, Newbury Park**, v. 18, p. 1219-1235, 2016.

MELIS, Gianluca. **Risposte Agli Attentati Terroristici di Matrice Islamica a Confronto**: Sistema Europeo e Sistema Israeliano. Analisi delle peculiarità e difficoltà di adeguamento tra le due metodologie. Roma: Università degli Studi Niccolò Cusano UNICUSANO, 2018-2019.

PAGANINI, Pierluigi. The ISIS advances in the DeepWeb among Bitcoins and darknets. **Security Affairs**. [s. l.], 22 mai. 2015. Disponível em: https://securityaffairs.co/36961/intelligence/isis-in-the-Deepweb.html. Acesso em: 20 jul. 2023.

STOCKLEY, Mark. Can you trust Tor's entry guards? **Naked Security**. [*s. l.*], 03 ago. 2015. Disponível em: https://nakedsecurity.sophos.com/2015/08/03/can-you-trust-TORs-entry-guards/. Acesso em: 20 jul. 2023.

WEBER, Julia; KRUISBERGEN, Edwin. Criminal markets: the dark web, money laundering and counter strategies **Trends in Organized Crime**, Berlim, p. 347-356, 2019.