A CRIMINALIDADE NA *DEEP WEB*

Flaviano de Souza Alves*

RESUMO
O homem consegue conversar com o mundo inteiro por meio da Internet, fazendo despertar para esta era de inovações e crescimento tecnológico. Embora pareça que, com o surgimento dessas redes, tenha-se estreitado laços entre pessoas de diversas partes do mundo, ao mesmo tempo, esta prática tem aumentado a vulnerabilidade das pessoas. O trabalho tem como objetivo mostrar a rede de atos criminosos existentes dentro da *Deep Weeb.* A justificativa para este estudo é o crescente interesse sobre o assunto, sobretudo nos meios acadêmicos, militares, nas áreas de Defesa e Segurança e em áreas policiais, visando também à grande necessidade de informar, analisar, investigar e alertar todos os cidadãos sobre os perigos e os riscos aos quais toda a sociedade está exposta. É necessário continuar com novas pesquisas e apontar novos mecanismos de combate para esses crimes cibernéticos, desenvolver melhores *softwares* (*browser,* antivírus, *firewall* etc.) e a configuração ideal desses *softwares* para acesso seguro a essa camada da rede. Na *Deep Web* depende de cada um escolher o que buscar.
Palavras-chave: *Deep Web*. Crimes Cibernéticos. Segurança.

THE CRIME IN THE DEEP WEB

ABSTRACT
Man mange to communicate with the entire world through the Internet and have awaked to this era of innovations and technological growth. Although it seems that ties between people from several parts of the world have been strengthened with the emergence of such networks, at the same time, this practice has increased the vulnerability of people. The paper aims to show the criminal acts network within the Deep Web. The rationale for this study is the rising interest on the subject, especially in the academic, military, defense and security areas and in police areas, seeking as well the great need to inform, analyze, investigate and alert all citizens about the dangers and the threats society has been exposed to. It is a need to continue with new researches and point out original mechanisms to combat these cyber crimes, develop better software (browser, antivirus, firewall, etc.) and its ideal configuration for a secure access to this network layer. At Deep Web, the search depends on everyone's choice.
Keywords: Deep Web. Cyber Crimes. Security.

* Doutorando pela Universidade Federal do Rio de Janeiro(UFRJ), Mestrado pela Universidade Federal de Campina Grande (UFCG), Especialista em Análises de Riscos pela Universidade Estadual da Paraíba (UEPB), Geógrafo pela UEPB, Pesquisador da Escola Superior de Guerra (ESG), atuando na Divisão de Fundamentos, Planejamento e Gestão (DFPG), Pesquisador dos Laboratórios de Estudos sobre Sociedade e Defesa (LABSDEF) e de Estudos Políticos de Defesa e Segurança Pública (LEPDESP). Contato: <flavianoeng@hotmail.com >.

LA CRIMINALIDAD EN LA DEEP WEB

RESUMEN
El hombre logra comunicarse con el mundo entero a través de *Internet*, haciendo despertar para esta era de innovaciones y crecimiento tecnológico. Aunque parezca que con el surgimiento de esas redes ha estrechado lazos entre personas de diversas partes del mundo, al mismo tiempo, esta práctica ha aumentado la vulnerabilidad de las personas. El trabajo tiene como objetivo de mostrar la red de actos criminales existentes dentro de *Deep Weeb*. La justificación para este estudio es el creciente interés sobre el tema, sobre todo en los medios académicos, en los militares, en las áreas de Defensa y Seguridad y en áreas policiales, buscando también la gran necesidad de informar, analizar, investigar y alertar a todos los ciudadanos sobre los mismos peligros y los riesgos a los que toda la sociedad está expuesta. Es necesario continuar con nuevas investigaciones y apuntar nuevos mecanismos de combate para esos crímenes cibernéticos, desarrollar mejores softwares (navegador, antivirus, firewall, etc.) y su configuración ideal para acceso seguro a esa capa de la red. En *Deep web* depende de lo que cada uno elija.
Palabras clave: *Deep web*. Crímenes Cibernéticos. Seguridad.

1 INTRODUÇÃO

A sociedade em que estamos inseridos passa por constantes mudanças dentro do processo de desenvolvimento com o avanço da tecnologia digital. Isso provocou uma grande revolução nas relações sociais. O uso do computador e dos dispositivos móveis como – *Smartphone*; Telemóvel (pt)/Celular (br); Console portátil; *Ultra Mobile PC*; *Ultrabook*; *Notebook*; *Netbook*; *Laptop*; Coletor de dados; *Smartwatch* e outros aparelhos, especialmente, a *Internet* – transforma vidas. Vivemos a era das tecnologias informatizadas, da informação, da cibernética – que consiste no estudo interdisciplinar da estrutura dos sistemas reguladores. Essa era cibernética, que está estreitamente vinculada à teoria de controle e à teoria geral de sistemas. Tanto nas suas origens como na sua evolução, na segunda metade do século XX. Os sistemas complexos afetam o seu ambiente externo e, logo a ele se adaptam. Em termos técnicos, centram-se em funções de controle e comunicação: ambos os fenômenos externos e internos do/ao sistema. Essas inovações propiciaram muitos benefícios ao homem; cada vez mais a era da informática traz consigo grandes descobertas e facilita as relações e estudos da sociedade em si.

O homem consegue se comunicar com o mundo inteiro por intermédio das redes da *Internet*, despertando para uma era de inovações e crescimento tecnológico. Segundo Noêmia Lucas e Martins (2013), o crescimento acelerado da tecnologia e consequentemente do uso das "redes sociais" alterou o comportamento do homem o que se reflete em toda sociedade.

Embora pareça que com o surgimento dessas redes tenha-se estreitado laços entre pessoas de diversas partes do mundo, ao mesmo tempo, esta prática tem aumentado a vulnerabilidade das pessoas, expondo-as a um perigo inimaginável. O portal de estudos e estatísticas divulgou uma lista de redes sociais mais acessadas no mundo e o número de usuários ativos, esses dados são referentes a abril de 2018, publicados no dia 13 de abril de 2018. *Ranking* das maiores redes sociais: 1) *Facebook:* 2.234.000.000**;** 2) *WhatsApp*: 1.500.000.000**;** 3) *Facebook Messenger*: 1.300.000.000**;** 4) *Youtube*: 1.500.000.000**;** 5) *Wechat:* 980.000.000**;** 6) QQ: 783.000.000**;** 7) *Instagram*: 813.000.000; 8) *Qzone:* 563.000.000; 9) *Tumbrl:* 550.000.000**;** 10) *Twitter:* 330.000.000**;** 11) *Sina Weibo*: 392.000.000**;** 12) *Baidu Tieba:* 300.000.000**;** 13) *Snapchat*: 255.000.000**;** 14) *Skype:* 300.000.000**;** 15) *Viber:* 260.000.000**;** 16) *Line:* 203.000.000**;** 17) *Pinterest:* 200.000.000**;** 18) *Linkedin:* 260.000.000**;** 19) *Telegram*: 100.000.000.

Infelizmente, o ser humano pensa diferente e de diversas formas, como existe o bom uso dessas tecnologias, existe também o uso errôneo dessas redes sociais, do computador, da *Internet* para a prática de novos delitos ou novas formas de praticar os já conhecidos tipos penais, surgindo os crimes cibernéticos, aumentando a criminalidade e desafiando os mecanismos de segurança propostos em todo o sistema de informação e nas redes computacionais, ou por meio destes, compreendendo as infrações praticadas contra os dispositivos e seus acessórios. Incluem-se, nesse conceito, as violações praticadas pela I*nternet,* já que para acessar a rede é necessária a utilização de um computador ou dispositivos.

Com base no exposto, é mister mostrar neste trabalho a rede de atos criminosos existentes dentro da *Deep Weeb,* e alertar todos os usuários do sistema de informação sobre a importância do bom uso das tecnologias e os perigos reais na divulgação e propagação de matérias ocorridas ao longo dos últimos anos.

2 IMPORTÂNCIA DO ESTUDO DA *DEEP WEB*

Este artigo é resultante de estudos sobre o tema, que contempla uma abordagem, ainda que superficial da *D*eep *W*eb, visando mostrar em específico o lado negativo, embora para muitos haja também pontos positivos, o que não é o objetivo deste artigo.

Dessa forma, objetiva-se aprofundar os estudos relacionados ao tema e à futura publicação de outros artigos com conteúdo mais avançado e específico. A justificativa para este estudo é o crescente interesse sobre o assunto, em especial nos meios acadêmicos, militares, nas áreas de Defesa e Segurança e em áreas policiais, visando também à grande necessidade de informar, analisar, investigar e alertar todos os cidadãos sobre os perigos e os riscos aos quais toda a sociedade está exposta. Realizou-se uma pesquisa bibliográfica sobre o tema, consulta a fontes e entrevistas com especialistas das áreas de Defesa e Segurança, que atuam

diretamente com a fiscalização e com a investigação do objeto de estudo, e uma coleta de dados minuciosa em toda a rede de *Internet.*

3 A INTERNET

Segundo Martins e Silva (2013), no mundo contemporâneo, a *Internet* pode ser classificada como uma ferramenta transformadora da sociedade. Por meio de sua expansão grandiosa e de sua democrática popularização, ocorrida especialmente na primeira década deste novo século, ela disponibiliza aos cidadãos e às organizações um extenso e rico local de acesso a informações, entretenimentos, comunicações e uma imensa possibilidade de realização de negócios, exercendo inclusive um importante papel no desenvolvimento econômico e social do país e do mundo.

A *Internet*, tal qual hoje é conhecida, originou-se em 1960, na Guerra Fria, com os conflitos entre os Estados Unidos e a União Soviética, já que os militares norte-americanos precisavam de um sistema que possibilitasse comunicação em longas distâncias, sem que esta pudesse ser cortada ou extraviada. Foi então que Paul Baran teve a ideia de criar uma rede com vários trajetos para que pudesse chegar ao seu destino, assimilando-se a uma teia, por isso a expressão *Web* que, em inglês, significa "teia de aranha". O primeiro experimento recebeu o nome de *packet switching*, ou "troca de pacotes", em português (MARCON; DIAS, 2014).

Em 1980, a *Internet* começou a ganhar espaço entre as "pessoas comuns", com a criação das "salas de bate-papo" (*chat rooms*). Com o passar dos anos, criou-se a possibilidade de se navegar de um *site* para o outro com a invenção do *HTTP* e *HTML*, o *WWW* (W*orld Wide Web*) conquistou cada vez mais adeptos e a *Internet* começou a se expandir amplamente, com milhões de usuários, em pouco tempo chegando a toda tecnologia que se encontra hoje.

Existem, contudo, situações nada agradáveis na *Internet,* pois há quem queira cometer crimes cruéis e bárbaros, mas, como fazê-lo impunemente? Umas das possibilidades é a *Internet*, e, pensando nesses indivíduos mal-intencionados, criou-se um local específico na *Internet* em que o anonimato é 100%, denominado *Deep Web,* e sobre o qual serão tecidos mais comentários adiante.

4 DEEP WEB: DEFINIÇÕES

E o que seria *Deep Web*?

Segundo Marcon e Dias (2014); Alves e Fernandes (2013), a *Deep Web* é um nível da *Internet* no qual não existem limites para os atos que são lá praticados: fotos e vídeos de muita violência, espalhados sem nenhum tipo de filtro. O que existe de mais perigoso na *Deep Web* é o seu anonimato, pois, quem a utiliza, dificilmente é rastreado, posto que muitas ferramentas são usadas para esconder a verdadeira identidade e localização do usuário. Com o passar dos anos, as

histórias encontradas na *Deep Web* vêm assustando pessoas em várias partes do mundo.

Segundo Pompéo e Seefeldt (2013), a expressão *Deep Web* foi criada por Michael K. Bergman, fundador do programa Bright Planet, software especializado em coletar, classificar e procurar conteúdo nessa esfera da Web. A expressão *Deep Web*, traduzida ao português, remete ao significado de profundeza, tanto que fixada em oposição a Surface Web, vocábulo que visa dar a ideia de superficialidade.

Outro termo pelo qual a *Deep Web* é conhecida é *Under Web*, que faz referência à posição entre os dois grupos, ficando a *Surface Web* por cima e a *Under Web* por baixo, com a forma de um *iceberg*. *Web* Oculta, em razão da dificuldade em localizar e acessar as páginas – já que se encontram camufladas –, é outra acepção possível.

Como, segundo especialistas, apenas 20% das páginas da rede estão presentes na *Surface Web*13, existem algumas analogias que se dedicam a explicá-la. A primeira delas é a do *Iceberg*, figura 1, em que a *Surface Web* é representada por seu topo, de fácil acesso e que salta aos olhos, embora pequena em termos de conteúdo; enquanto a *Deep Web* é representada como a sua base, pois se sabe que existe, mas não se tem a medida exata de seu tamanho, sabendo-se que é pouco visível e, por isso, de curto alcance.

Figura 1 - Analogia da *Deep Web*

Fonte: DESCONHECIDA, 2017.

Michael K. Bergman (2013) afirma que informações públicas na *Deep Web* são comumente de 400 a 500 vezes maiores que as definidas da *World Wide Web*. A *Deep Web* contém 7.500 *terabytes* de informações comparadas a 19 *terabytes* de informação da *Surface Web*. Contendo aproximadamente 550 bilhões de documentos individuais comparados com 1 bilhão da *Surface Web*. Existem mais de 200.000 *sites* atualmente, 06 das maiores enciclopédias da *Deep Web* contém cerca de 750 *terabytes* de informação, o suficiente para exceder o tamanho da *Surface Web* em 04 vezes. Em média, os *sites* recebem 50% mais tráfego mensal, ainda que não sejam conhecidos pelo público em geral, sendo a categoria que mais cresce no número de novas informações sobre a *Internet.* Essa rede tende a ser mais estrita, com conteúdo mais profundo do que *sites* convencionais. A profundidade de conteúdo de qualidade total é de 1.000 a 2.000 mil vezes maior que a da superfície. O conteúdo é altamente relevante para todas as necessidades de informação, mercado e domínio. Mais da metade desse conteúdo reside em tópicos específicos em bancos de dados.

A *Deep Web* – também denominada de *Web* Profunda, *Darknet*, *Web* invisível, *Web* oculta, rede *Tor*, além de outras variantes – caracteriza-se como uma camada da *Internet* – ou *Surface Web* – que não pode ser acessada de forma corriqueira e usual como a maioria das pessoas faz diariamente. Para acessar o conteúdo da *Web* Profunda faz-se necessário o uso de software específico e muito bom senso, pois é possível encontrar temáticas de excelente qualidade e também do pior nível imaginável.

Esta rede profunda engloba bancos de dados cujo conteúdo não está indexado e, por essa razão, não pode ser acessado por ferramentas de busca como o *Google*.

Imagine, por exemplo, um *site* de venda de carros de segunda mão. As informações sobre os carros estão no *site*, mas você só tem acesso a elas quando preenche um formulário dizendo que tipo de carro está procurando.

Também podemos incluir nessa *Web* Profunda uma porção da rede em que a publicação de conteúdos, bem como o acesso a eles, acontece de forma anônima. Essa é a *Dark Web,* ou *Internet* obscura. A *Dark Web* inclui, por exemplo, redes como a *Tor Network*. Para acessá-la, é preciso baixar o *Tor Browser*. Esse *browser* torna o endereço do seu computador indetectável. Você viaja anônimo, tanto pela *Internet* regular quanto pela rede obscura.

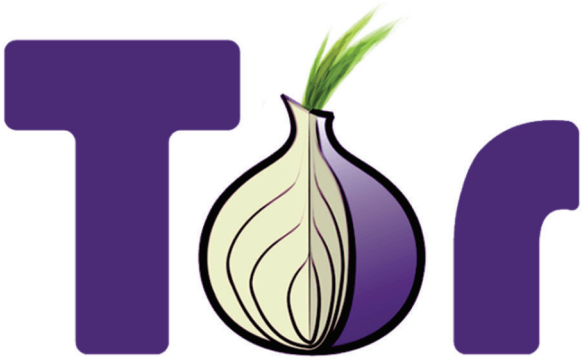
Da mesma maneira, se você cria um *site* na rede *Tor*, o conteúdo fica lá, mas sua identidade, não. Um dos especialistas na área de segurança foi bem claro em suas colocações: "Se crio um site, tenho de registrá-lo e criar um IP *address*, para identificação", explica Marcon e Freire (2014). Mas essas redes criam o IP (Internet Protocol) address e ninguém sabe quem eu sou".

Essa *Internet* anônima é usada para todo tipo de atividade ilícita e, hoje em dia, há um aumento considerável da criminalidade por causa do anonimato. Um desses *sites*, o supermercado de drogas *Silk Road*, operou na rede *Tor* durante mais de dois anos, até ser fechado pelo *Federal Bureau of Investigation* (*FBI*). Mas

a *Tor* também é usada por militantes, intelectuais e outros grupos que precisam permanecer anônimos para sua segurança pessoal. Obviamente, se o *FBI* é capaz de *hackear* o *Tor* e a *Deep Web,* então isso apresenta um problema enorme para o futuro da *Deep Web* e o navegador como seu único ponto de acesso e que, agora, ninguém estaria mais completamente anônimo.

A *Deep Web* é composta por várias redes separadas que não conversam entre si. No entanto, em 2006, foi lançada uma versão do projeto para fins não governamentais, intitulada de *TOR* – sigla de *The Onion Routing* –. A palavra "*onion*" significa "cebola", em português, fazendo alusão às várias camadas que existem na cebola, semelhantes às camadas que um internauta deve atravessar para chegar ao conteúdo desejado em algum *site* da *Deep Web*.

Figura 2 - Logomarca do software



Fonte: THE TOR PROJECT, 2018.

O *Federal Bureau of Investigation*, "Agência Federal de Investigação", em português, une esforços com outras instituições para vigiar a *Deep Web*, tentando capturar criminosos ou solucionar crimes que são expostos nos fóruns da "*Internet* invisível". Um especialista em segurança, chamado Brian Krebs, afirmou que o *malware* que estava rastejando através do *Firefox* não executa, realmente, quaisquer comandos, mas apenas descobre os verdadeiros endereços *Internet Protocol* (*IP)* dos usuários, o que faz sentido neste contexto. Esse não é um problema para a maioria de nós que não usamos a *Internet* para atividades ilegais, mas, obviamente, será preocupante para usuários do *Tor* e os usuários regulares da *Deep Web*.

Como o *Tor* é ainda mais seguro e mais anônimo do que qualquer outro navegador de *Internet*, por isso, provavelmente, ainda vá ser usado por um longo, longo tempo; ou, pelo menos, até que algo mais anônimo seja inventado – o que não deve aconter em breve.

Segundo Pompéo e Seefeldt (2013), a *Deep Web* é usualmente classificada em camadas. Quando o usuário adentra à *Deep Web*, ele possui acesso gradual. A

primeira camada concentra a maioria das informações necessárias aos iniciantes, mas, desde que se tenha um conhecimento mais avançado de informática e outros requisitos exigidos, é possível ir mais além.

Já Bergman (2013) acredita que existem, no mínimo, dez camadas de conteúdo da *Deep Web.* Dentro das acepções de arquitetura da rede, a configuração dessas páginas pode se dar por inúmeros conteúdos: conteúdo dinâmico, conteúdo isolado, conteúdo de acesso limitado, conteúdo de *script*, conteúdo não H*TML/* texto, conteúdo antigo, *Web* contextual e *Web* privada.

O que acontece na *Deep Web* é a inexistência de "filtros" como os disponíveis no *Google*, o que possibilita encontrar vídeos e fotos de crimes, assassinatos, estupros, experiências ilegais, crueldades com animais, pedofilia, venda de drogas, tutoriais sobre como fazer bombas, *hackers* e muitas pessoas que oferecem esses serviços, por isso é altamente recomendável não acessá-la, repita-se, o acesso a ela configura conduta criminosa em vários países. Porém, nem só coisas ruins podem ser encontradas, existe muito conteúdo interessante por lá. A grande questão é o que se quer encontrar? Mesmo que o indivíduo navegue buscando o lado positivo, é perigoso acabar sendo atraído pela curiosidade e entrar em um oceano de criminalidade.

Existe uma página da *Deep Web,* no Brasil, (Figura 3) com mais de um milhão de curtidas e, recentemente, foi disponibilizado nas bancas um periódico falando sobre o assunto e ensinando passo a passo como navegar por ela, intitulado de "Guia Proibidão" (Figura 4).

Figura 3 - Página da Rede Social da Deep Web no Brasil

Fonte: DEEP WEB (Brasil), 2018

Figura 4 – Exemplar "Guia Proibidão"

Fonte: EBOOK KINDLE [56], 2018**.**

Da mesma forma que as mais diversas relações sociais e econômicas se expandiram com o avanço das tecnologias de comunicações e transportes, os crimes também ultrapassaram fronteiras, eis que intimamente ligados à vida em sociedade, não se tratando só de uma patologia, mas também de fato social "normal". Dito isto, imperioso destacar, então, que, com o advento da globalização, surgiu um novo fenômeno: a criminalidade global (POMPÉO; SEEFELDT, 2013); (ALVES, 2013).

Conforme Castells (1999), a prática criminosa transnacional passa a existir de duas formas: A primeira emana após o enraizamento em uma determinada localidade de uma organização criminosa dita tradicional, por motivos históricos, culturais, étnicos ou socioeconômicos, e expande-se para outros países para assimilar diferentes associados e aumentar sua zona de atuação. Portanto, essas organizações não enfraquecem com a globalização, mas se fortalecem. A segunda decorre da criação de operações criminosas locais, geralmente fundadas em populações de baixa renda, que vendem seu crime para mercados de todas as partes do planeta.

Segundo Aragão (2013), obviamente, devido à intensa supervisão das autoridades policiais, a comunicação entre essas organizações criminosas não se

56 EBOOK KINDLE , editora on line – 04 de junho de 2018.

dá por meio da *Surface Web*. Por isso, muitas delas se utilizam da *Deep Web* para criptografar e enviar dados, trocar informações com suas associadas e propagar suas atividades nos mais diversos cantos do mundo. Tanto que, por isso, a *Deep Web* já ostenta inúmeros casos conhecidos, a exemplo do famoso *Wikileaks* e *Anonymous,* os quais tiveram a gênese de suas atividades ligadas à invisibilidade da rede. Com o conhecido *The Pirate Bay*, *site* destinado a *uploads* e *downloads* de arquivos protegidos por direitos autorais, não foi diferente.

Segundo Castells (1999); Alves e Fernandes (2013); Pompéo e Seefeldt (2013) e Marcon e Dias (2014), entretanto, não são esses os casos que apresentam maior periculosidade para a sociedade civil. O contrabando de mercadorias e de materiais radioativos, órgãos humanos, lixos orgânicos e inorgânicos, prostituição adulta e infantil, organização de jogos de azar, sequestros, compra e venda de assassinatos, extorsão, falsificações das mais diversas espécies, inclusa a de moedas em curso ou cartões de crédito, de identidades civis ou seu tráfico de informações, de tecnologias, objetos de arte estão entre as principais ações dessa rede criminosa que envolveu, de maneira global, o crime.

Por isso, não restam dúvidas de que essa globalização do crime, que se serve de forma maciça da *Deep Web*, abala profundamente a segurança transnacional, as políticas nacionais, a economia e a cultura dos povos. Em destaque nesse cenário, a lavagem de dinheiro revela-se o maior mal de todo esse contexto, constituindo-se na raiz de todos os demais delitos, já que destes decorre o sustento financeiro daqueles.

O sucesso e a expansão de atividades criminosas transnacionais ocorrem com a versatilidade e flexibilidade de sua composição, mas, sobretudo, da *Deep Web* enquanto ferramenta que sustenta de modo invisível suas articulações. Tal e qual um líquido, o qual se forma conforme o ambiente e se maneja sorrateiramente pelas beiradas e infiltrações, os perigos desse novo mal pós-moderno alcança toda a sociedade em rede e seu sucesso necessita de uma interligação global e silenciosa, em que os envolvidos se encontram muitas vezes invisíveis à fiscalização do Estado.

5 ARMAS E TERRORISMO

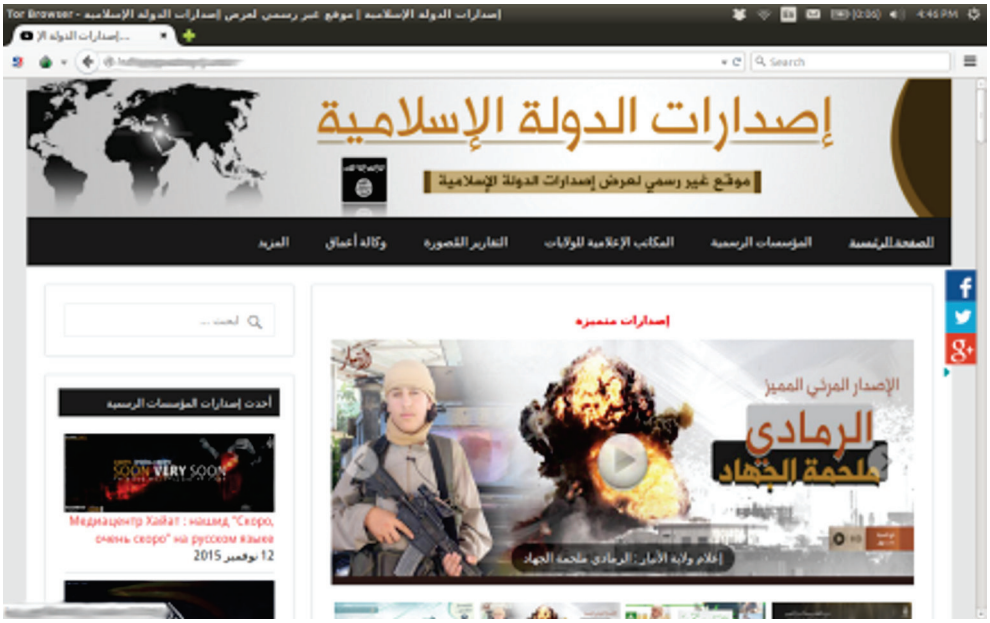
"Certamente, as vendas de armas são anunciadas e parece que algumas pessoas conseguiram obtê-las dessa forma, mas muitas vezes são fraudes", conta o Especialista Scot Terban.

O Estado Islâmico (EI) tem *site* nas profundezas da *Internet* (figura 5). Um *mirror* do *site* do EI na *Web* normal na rede anônima *Tor,* no que parece uma tentativa de tornar seu material de propaganda mais resistente às derrubadas e, de quebra, mais propício para preservar as identidades de seus membros e simpatizantes.

O pesquisador de terrorismo *on-line* Scot Terban postou no seu *blog* que o *Al-Hayat Media Center*, afiliado ao EI, "publicou um *link* e explicação sobre como

acessar seu novo endereço na *Deep Web segundo o site Infotecnogame (2015)*" em um fórum associado ao grupo.

Figura 5 - Página do Estado Islâmico e *links* de acessos



Fonte: ANONYMOUS, 2015.

Links que levam ao *site* também foram publicados por uma série de contas no *Twitter* com conexões *jihadistas*, de acordo com investigação do *Motherboard*.

O Jornal *Epoch Times* publicou, em 17 junho de 2016, uma matéria em que o Estado Islâmico teria divulgado uma "lista da morte" que inclui brasileiros; no total, a listagem ordena o assassinato de 8.318 pessoas do mundo todo, a grande maioria de americanos; a organização terrorista não anunciou precisamente quantos brasileiros foram "marcados para morrer", mas calcula-se que a lista pode conter até 39 pessoas. A relação foi encontrada pelo grupo *Vocativ*, *expert* em investigações da conhecida *Deep Web,* a área da *Internet* que não está acessível aos mecanismos de busca.

Também é vendido um grande número de armas, bombas e realizado inclusive recrutamento de jovens de todos os lugares.

6 PORNOGRAFIA INFANTIL

A *Deep Web* também é o lugar em que muitos pedófilos compartilham pornografia infantil. Em 2014, uma investigação da *British Broadcasting Corporation*

(BBC, 2016) descobriu que dezenas de milhares de pessoas usam a rede secreta para essa finalidade. Uma das páginas envolvidas recebia cerca de 500 visitas por segundo, apontou a pesquisa.

Para versar sobre esses e outros crimes, o Reino Unido criou uma célula de operações conjuntas que até agora "envolveu mais de 50 *sites* que têm o abuso sexual de crianças como atrativo, embora seja provável que esse tema represente uma pequena parte dos sites que a agência conhece".

No Brasil, a Policia Civil, por meio da "Operação *DarkNe*t" (MARCON, 2014) cumpriu mais de 100 mandados de prisão contra pessoas que utilizaram a *Deep Web* para crimes de pedofilia, "quebrando" o sistema que camuflava a localização e encontrou tais usuários, bem como mais de 90 indivíduos que compartilhavam material com pornografia infantil. "No decorrer da investigação iniciada há um ano, pelo menos seis crianças foram resgatadas de situações de abuso ou de iminente estupro, em diversos locais do Brasil. Em um dos casos, um pai relatava que abusaria da filha assim que ela nascesse" (MARCON, 2014).

7 EXPERIÊNCIA HUMANA

Segundo Lucas (2016); Alves e Fernandes (2013); Falconer (2013) assim como a Pornografia Infantil, há também pessoas fazendo experiências cirúrgicas de todos os tipos em humanos vivos, que são, na maioria, pessoas desabrigadas escolhidas nas ruas.

Há *sites* em que rapazes costumam apreender órfãos e outras pessoas das ruas e vendê-los como bonecos sexuais. Neste ponto, começa a ficar perturbador. Eles cortam-lhes os braços e as pernas, fecham todas as "aberturas", que são os olhos, a boca e os ouvidos.

E não acaba, já que eles também oferecem as opções de ter ganchos instalados para que seja possível pendurar a boneca sexual em qualquer lugar.

Nenhum órgão governamental conseguiu localizar a origem dos *Dolls Makers*. As informações são escassas e todas as transações monetárias são realizadas via *Bitcoins*, tudo muito sigiloso, não deixando qualquer rastro. Porém, sabe-se que não são um ou dois grupos e, sim, dezenas deles, oferecendo o serviço na *Deep Web*.

As bonecas sexuais humanas são geralmente crianças entre 8 e 10 anos, compradas de famílias miseráveis em países onde a pobreza extrema atinge a maioria da população. Por centenas de dólares, essas crianças são adquiridas pelos *Dolls Makers*. Em seguida, acredita-se que são levadas a centros cirúrgicos clandestinos e transformadas em bonecas vivas, que não apresentem resistência às perversões sexuais dos seus donos. Seus membros, braços e pernas, são amputados e substituídos por próteses de silicone. As cordas vocais são retiradas e os dentes arrancados e trocados por imitações de borracha. Todo procedimento dura de duas

a três semanas e só se inicia depois de a *"*boneca*"* ter sido encomendada. O preço varia entre 40 mil dólares e 700 mil dólares, dependendo das exigências. A boneca ainda viria com uma espécie de manual de instruções, informando como alimentá-la e realizar as demais necessidades básicas humanas para a sobrevivência, já que dependeria do dono para tudo a partir daí. A estimativa de vida seria reduzida há um ano após o início dos procedimentos cirúrgicos. O caso que ficou famoso na *Surface* das bonecas sexuais foi o da *Lolita Slave Toys*.

Acredita-se que o filme "O Albergue" lançado em 06 de janeiro de 2006, do diretor e roteirista Eli Roth, ao que se sabe, baseou-se em casos reais, investigados pela polícia de Nova Déli, na Índia, onde foram descobertos clubes secretos, nos quais ricos e poderosos assistiam a espetáculos de tortura de crianças e adolescentes. Situações similares a essa foram encontrados na Ásia, África e Europa, mesmo com uma forte rede de segurança por trás dessas páginas. Experimentos científicos realizados com humanos e até mesmo culto ao canibalismo são práticas que já foram igualmente desvendadas na imersão das profundezas da rede.

A *Deep Web* é, portanto, o mecanismo mais seguro para que se possam atingir as finalidades ilícitas arquitetadas por esses grupos.

8 SEGREDOS DE GOVERNO

Para Lucas (2015) e Munson entrevista da BBC em 2016, os que adoram pensar que tudo é uma teoria da conspiração, a *Deep Web* oferece a prova dessas teorias. E também há muitos segredos de governo. Recentemente, alguns foram retirados pelo FBI. Os *hackers* conseguem invadir diversos bancos de dados contendo informações secretas, operações, planilhas e até mesmo localidades e indivíduos envolvidos em missões, tudo isso em troca de quantias expressivas de dinheiro.

9 MATADORES DE ALUGUEL

É possível ver o nível de detalhamento que a *Deep Web* pode oferecer, pessoas que se escondem no anonimato e que realmente entendem do negócio. Ter alguém morto não é barato, mas, aparentemente, eles levam o trabalho a "sério". Tudo sem saber quem seja o mandante, ou quem quer que sejam as vítimas ou grupos (LUCAS, 2015).

10 TRÁFICO DE ORGÃOS E PESSOAS

Segundo Aragão (2013); Falconer (2013), a Organização das Nações Unidas (ONU**)** define o tráfico de pessoas como quando a vítima é retirada de seu ambiente, de sua cidade e até de seu país e fica com a mobilidade reduzida, sem liberdade de sair da situação de exploração sexual ou laboral, ou do confinamento para remoção

de órgãos ou tecidos, na qual a mobilidade reduzida é caracterizada por ameaças ou danos físicos e mentais. Normalmente, o tráfico de pessoas ocorre em regiões pobres, como certos lugares da Ásia, Europa Oriental e África, um exemplo de país é a Tailândia. Pelo fato de essas regiões serem pobres, familiares vendem outros familiares, como a mãe vendendo o filho – triste realidade!

Raramente, alguns casos que foram revelados da *Deep Web* chegam à mídia, mas de acordo com o site *Mother Board*, um dos casos foi o de Nicole, americana, de apenas 18 anos, raptada em Paris. O anúncio do leilão pedia um lance inicial de 150 mil dólares – algo como 610 mil reais. O anúncio mostrava fotos dela, trajando apenas calcinha, com os braços amarrados e uma corda prendendo-a a uma estrutura de metal, nas imagens pode-se perceber que ela estava se debatendo e, ao fundo, pode-se observar a sombra de um homem. O grupo por trás desse leilão é conhecido por *Black Death*. Nicole estava sendo vendida em um endereço da *Dark Web* – hoje, o *link* se encontra *off-line*, lugar em que esse comércio movimenta milhares de dólares, e estima-se que cerca de 2,4 milhões de pessoas são traficadas por ano: 6 de 10 são mulheres.

Na verdade, muitas pessoas que são traficadas são compradas por quem deseja realizar o ato de torturá-las. A chamada "Tortura por Encomenda". Usa-se esse termo quando alguém é comprado por outra pessoa – sem o consentimento da vítima. Depois de ser raptada, logo depois da compra, o comprador tem o direito de fazer o que quiser com a vítima, no caso, seria a tortura, já que ele encomendou isso. Um verdadeiro mundo dos psicopatas.

Se com a expansão da *Internet,* vista por muitos como um progresso humano sem igual, poucos percebem que a própria *Surface Web* é um perigo, que dirá a *Deep Web,* que, além de pouco conhecida é vista com desconfiança – existe ou não? –, por esses poucos. Dessa forma, depois de compreender o que se entende por *Deep Web* e analisar como se caracteriza seu acesso, restou claro, com base em casos e estudos já conhecidos, a necessidade da tomada de decisões e medidas que possam coibir ações delituosas que surgem nesse espaço. Por se tratar de ponto fundamental da vida da sociedade em rede, é preciso conhecer e entender todas as facetas da *Internet.* Como demonstrado, a *Web*, tal qual um *iceberg*, possui uma pequena ponta visível, enquanto sua maior extensão é a base que, por submersa, é quase que totalmente desconhecida.

11 POLÍCIA FEDERAL X DEEP WEB X CRIMES CIBERNÉTICOS

De acordo com Martins (2013); Dias e Marcon (2014); Munson (2016) nos últimos anos, a Polícia Federal especializa-se no combate aos crimes praticados nesses territórios, os chamados Crimes Cibernéticos. Várias operações vêm sendo realizadas contra a pornografia infantil na *Deep Web*. A operação *Darknet* foi deflagrada simultaneamente por 44 unidades da Polícia Federal em 18 estados e no

Distrito Federal. 55 pessoas foram presas e, 106 ainda são investigadas. No decorrer da investigação, iniciada há um ano, pelo menos seis crianças foram resgatadas de situações de abuso ou de estupro, em diversos locais do Brasil. Assim como diversos indivíduos que estão sendo monitorados pela Polícia Federal por serem suspeitos de utilizar a *Deep Web* para cometer seus delitos.

De acordo com Diana Calazans, delegada da Polícia Federal, em uma entrevista em 2017 ressaltou: esse tipo de investigação divide-se em duas partes: uma parte cibernética, em que se usa conhecimentos avançados para identificar os computadores e dispositivos de origem; e a investigação tradicional, para chegar ao usuário.

Mas, a *Deep Web* também apresenta um lado positivo. Países como a Coreia do Norte e a China costumam controlar a *Internet* convencional. Nesse caso, ela seria uma forma de burlar a censura. Uma de suas funções é também proteger conteúdos confidenciais, como os de governos, bancos, empresas, forças militares e universidades. Você quer manter uma informação privada e você não tem como, aí a *Deep Web*, para muitos usuários é um espaço para isso.

E, como boa parte do conteúdo desse universo ainda se constitui de informações ilegais, Diana Calazans, delegada da Polícia Federal, diz que não há crime perfeito.

Os crimes cometidos através do computador deixam rastro. A Polícia Federal quer reunir esses elementos e fazer a identificação dos criminosos, com todas essas mudanças e acontecimentos no meio tecnológico, é notória também a mudança social abarcada pela globalização da *Internet*, que trouxe nova forma de comunicação e modificou essas relações sociais em todo o mundo, contudo, junto com tais benefícios, surgiram também novos riscos, impondo a necessidade do controle jurídico. O dinamismo e versatilidade, inerentes à *Internet*, tornaram-se foco de preocupação para o Poder Legislativo que editou as Leis 12.735/12, 12.737/12 (Lei Carolina Dieckman – altera os artigos 154, 266 e 298 do CP) e 12.965/14 (Marco Civil da Internet) (BRASIL, 2012, 2014).

Quanto à competência para o processamento dos crimes praticados pela *Internet,* algumas questões devem ser levadas em conta, como o local de transmissão e a existência, ou não, da transnacionalidade do delito. A jurisprudência (abaixo) aponta que para os crimes praticados através da rede mundial de computadores deve ser observado o local em que foi publicado o conteúdo criminoso. Não sendo identificado o local, a competência recairá ao juízo que iniciou as investigações correlatas. Nas hipóteses em que seja verificada a transnacionalidade do delito, a competência será da Justiça Federal.

O Supremo Tribunal Federal **(**STF) reconheceu a repercussão geral da matéria que trata da competência para o processamento e julgamento dos crimes de divulgação de imagens de crianças e adolescentes através da *Internet* (RE 628624).

A mídia na contemporaneidade, especialmente no que tange à *internet*, deve ser uma ferramenta de evolução do homem, e não de sua destruição. Se quando

se considera apenas as ações ocorridas na *Surface Web* já se discute a necessidade de (co)regulamentação do uso que se faz da rede, é claro e cristalino que, após a descoberta da transcionalização criminosa que se espalha entremeio a *Deep Web,*essa necessidade aumenta significativamente (POMPÉO; SEEFELDT, 2013).

12 CONSIDERAÇÕES FINAIS

Já diz o Especialista em Defesa e Segurança: *Internet* ainda é um espaço carente de regulamentação legal e, por mais que existam muitas tecnologias e vários especialistas, há pessoas que possuem vasto conhecimento da ferramenta que estão usando e sabem como não serem localizadas, não temendo o que pode acontecer, usando uma nova "identidade", em um ambiente virtual que possibilita ser "quem bem entender". Através desse trabalho, é possível conhecer e descobrir um pouco mais sobre a *Deep Web*, o uso errôneo das novas tecnologias para o aumento da propagação da criminalidade.

A importância deste estudo sobre esse tipo de prática torna-se cada vez maior, sendo necessários a divulgação e o conhecimento sobre os perigos e ameaças aos quais estamos expostos.

A rapidez com que tudo se propaga na rede contribui para coisas boas e também ruins: a quebra de fronteiras, a difusão da informação, o rompimento dos mecanismos de defesa e sua segurança, a importância de mais estudos aprofundados nesta área, por isso é que se chama a atenção para o desenvolvimento da tecnologia e para o treinamento das pessoas capazes de fazer algo juridicamente eficaz, ou seja, punir e capturar esses indivíduos que se utilizam da *Internet* para cometer esses inúmeros crimes.

A captura e punição dessas pessoas só se tornarão um fato prático em grande escala, com um trabalho em grupo, a sociedade: a família, as igrejas, os policiais e a Lei, juntos, serão capazes de realizar algo que surta efeito. Mas é necessário um esforço em grande escala para que se concretize e para que se possa, através da prisão desses usuários que se utilizam do lado sombrio e negativo da *Deep Web* como ferramenta de destruição, prevenir que novos crimes ocorram e que mais pessoas sejam prejudicadas, através dessa disseminação tão negativa.

Educar na sociedade da informação não é apenas investir em aparato tecnológico e ensinar a usá-lo. Não adianta o jovem saber como utilizar a ferramenta digital; é preciso educá-lo sobre como usá-la de maneira responsável, ética e segura. É dever de todos orientar o uso correto da rede, indicando as consequências da utilização inapropriada não só para o indivíduo, mas, também, para a sociedade. Os pais desempenham papel importante nesse processo, mas, muitas vezes, sentem-se perdidos em meio a tantas inovações tecnológicas, sem saber quais os limites a serem impostos, ou mesmo sem terem real conhecimento dos perigos que seus

filhos correm em virtude da descontrolada exposição *on-line*. Também restam confusos quanto aos papéis na educação, deixando a cargo da escola, até mesmo, o que deveria ser também sua obrigação.

Outro ponto a ser observado é o ensino sobre a diferença entre domínio público e ambiente público. Crimes são cometidos em *blogs* e comunidades virtuais (como as redes sociais) porque o usuário acredita que não será identificado se fizer uso da condição de anônimo. É importante lembrar que é perfeitamente possível identificar qualquer usuário na *World Wide Web* através do número de IP, que identifica cada um de nossos computadores conectados.

Segundo Munson (2016) especialista em segurança da informação no Distrito Federal: "Não é um ambiente pra que as pessoas comuns tenham acesso". É imprescindível, portanto, que sejam implementadas ações governamentais para regulamentar e vistoriar as possibilidades do completo uso da *Web.* Investimentos públicos na área da tenologia de informações, somados ao combate do desconhecimento da *Deep Web* e a desmistificação de que hoje em dia tudo se encontra no *Google*, podem se revelar como eficientes mecanismos de controle para vigiar, identificar e rastrear crimes na rede, uma vez que as transgressões envolvem não apenas direitos fundamentais como também a própria soberania nacional e segurança transnacional. Somente depois disso é que se poderá suscitar a criação de normas jurídicas eficientes na prevenção e punição dos delitos cibernéticos agasalhados na *Deep Web*, conduzindo-nos, assim, por um caminho mais risonho em contraponto à realidade problemática e perigosa que avança, por enquanto, sem freio, debruçada durante as noites e os dias.

É necessário continuar com novas pesquisas e apontar novos mecanismos de combate para esses crimes cibernéticos, desenvolver melhores *softwares* (*browser,* antivírus, *firewall,* etc.) e sua configuração ideal para acesso seguro a essa camada da rede. Na *Deep Web* depende de cada um escolher o que buscar, se a pessoa buscar conteúdo criminoso, ela encontrará; se buscar um livro, um *cd,* ou até mesmo filmes, jogos e demais, também encontrará ressaltando que a violação de direitos autorais também é crime previsto no artigo 184 do CP – Decreto Lei 2848/40 por isso, é importante focar bem o que se busca por lá, pois o acesso a um *link* errado pode levar a um caminho totalmente diferente do que se busca e, muitas vezes, sem volta.

A criminalidade existe de todo lado, inclusive na *web*, por isso, é importante ter um certo conhecimento para navegar nesse mundo oculto e perigoso.

REFERÊNCIAS

ALVES, F. S; FERNANDES, N. L. G. *Pornografia Infantil Virtual:* o mau uso das tecnologias**.** Flaviano de Souza Alves; Norma Lúcia Gomes Fernandes. 2º Congresso sobre Novas Tecnologias. Campina Grande – PB, 2013.

ARAGÃO, Alexandre. Nas profundezas da web. *Folha de São Paulo*, São Paulo, 18 fev. 2013. Caderno tec. p. F1-F3.

BBC (Brasil) (Ed.). *Deep web:* O comércio criminoso que prospera nas áreas ocultas da internet. 2016. Disponível em: <http://www.bbc.com/portuguese/geral-36920676>. Acesso em: 10 ago. 2017.

BERGMAN, Michael K. *The Deep Web:* Surfacing Hidden Value. 2001. Disponível em: <http://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf>. Acesso em: 16 abr. 2013.

BRASIL. Lei n. 12.737/12, DE 30 de novembro de 2012. *Tipificação criminal de delitos informáticos,* Brasília, DF, nov. 2012.

_____. Lei nº 12.735, de 30 de novembro de 2012, altera o decreto-lei n. 2.848, de 7 de dezembro de 1940 - código penal, o decreto-lei n. 1.001, de 21 de outubro de 1969 - código penal militar, e a lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em: 12 nov. 2012.

CASTELLS, Manuel. *Fim do milênio:* A era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra, 1999. 3 v.

FALCONER, Joel. *Mail-order drugs, hitmen & child porn:* A journey into the dark corners of the deep web. 2012. Disponível em: <https://thenextweb.com/insider/2012/10/08/mail-order-drugs-hitmen-child-porn-a-journey-into-the-dark-corners-of-the-deep-web/>. Acesso em: 23 abr. 2013.

HIGA, Paulo. *Como entrar na deep web utilizando o Tor*. Disponível em: <https://tecnoblog.net/189897/como-acessar-deep-web-links/>. Acesso em: 12 jun. 2017.

INFOTECNOGAME – infogametec.blogspot.com. novembro de 2015.

JORNAL *EPOCH TIMES [on line].* junho de 2018.

LUCAS, Adriano S. Top 10 coisas mais absurdas encontradas na deep web. 2017. Disponível em: <https://top10mais.org/top-10-coisas-absurdas-encontradas-na-deep-web/#ixzz4pUATVSwM>. Acesso em: 10 ago. 2017.

MARCON, J. P. F.; DIAS, T. P. *DEEPWEB***:** o lado sombrio da internet. Conjuntura Global, Curitiba, v. 3, n. 4, p.233-243, out. 2014. Quadrimestral.

MARTINS, Caique Arthur Lopes da Silva; SILVA, Maria Helena Barriviera e Silva. A dualidade da Deep Web. Revista da Faculdade de Tecnologia de Garça. Garça, SP, vol. 3, n.2, 2013, p. 1-7. Disponível em. Acesso em 12 set. 2016.

MELLO, João**.** Nem tudo são trevas: o lado bom da Deep Web. In. *Revista Galileu*. Maio / 2013.

MUNSON. L. *Deep web:* O comércio criminoso que prospera nas áreas ocultas da internet. Agosto/ 2016

POMPÉO, W.A.H; SEEFELDT, J.P*. Nem tudo está no Google*: Deep web e o perigo da invisibilidade. In: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 2., 2013, Santa Maria. **Anais...** Santa Maria, Rs: Ufsm, 2013. P. 436-449.

Recebido em: 16 jan. 2018
Aceito em: 15 maio 2018