



EIXO TEMÁTICO:
Organização e Representação da Informação e do Conhecimento

A DARK WEB E SEU CONTEÚDO INFORMACIONAL

THE DARK WEB AND ITS INFORMATION CONTENT

Richele Grenghe Vignoli - rivignoli@gmail.com

Silvana Drumond Monteiro - drumond@gmail.com

Resumo: Existe no ciberespaço uma web escura e escondida denominada Dark Web. Nesse viés, esta pesquisa objetivou compreender o que representa a Dark Web e o que existe de conteúdo informacional nos seus ambientes. O estudo foi caracterizado como documental e exploratório. A Dark Web foi discutida como a web mais profunda e escura do ciberespaço, possível por meio de redes anônimas como o Tor, Freenet e I2P. Os principais resultados demonstram que os conteúdos informacionais da Dark Web são em sua maioria de má índole com envolvimento de crimes e atos ilícitos. No entanto, os pontos positivos da Dark Web são refletidos na possibilidade de navegação anônima, livre de espionagens, propagandas comerciais e comércio de informações gerados por buscas. De modo sumário, a Dark Web apresenta pluralidade em conteúdos informacionais, muitos restritos por incapacidade ou indisponibilidade dos mecanismos de busca em indexar ou recuperar esses conteúdos. Acredita-se que os resultados alcançados com este estudo possam contribuir com a Ciência da Informação, como campo informacional profícuo para novas pesquisas a respeito da temática que é inédita no Brasil.

Palavras-Chave: Web Visível. Web Invisível. Deep Web. Dark Web.

Abstract: There is in cyberspace a dark and hidden web called Dark Web. In this bias, this research aimed to understand what the Dark Web represents and what exists of informational content in its environments. The study was characterized as documentary and exploratory. The Dark Web has been discussed as the deepest and darkest web of cyberspace, possible through anonymous networks like Tor, Freenet and I2P. The main results show that the informational content of the Dark Web are mostly ill-natured involving crimes and illicit acts. However, the positive aspects of the Dark Web are reflected in the possibility of anonymous surfing, free of espionage, commercial advertisements and information trade generated by searches. Briefly, the Dark Web has plurality in information content, many restricted by inability or unavailability of search engines to index or retrieve such content. It is believed that the results obtained with this study may contribute to Information Science, as fruitful informational field for further research about the topic that is unprecedented in Brazil.

Keywords: Visible Web. Invisible Web. Deep Web. Dark Web.

1 INTRODUÇÃO

Em um contexto atual e intrínseco da Pós-modernidade, problemas contemporâneos existentes no ciberespaço passam a fazer parte de uma sociedade de sujeitos híbridos e cada vez mais conectados.

Dessa forma, a *web* em que todas as pessoas navegam, ou ainda, a única aparentemente existente é caracterizada na literatura científica, por *Web Visível*, da Superfície (*Surface Web*) (BECKETT, 2009) ou Indexável, a que todos veem e utilizam. Da mesma forma, os conteúdos invisíveis em uma busca podem compor a *Web Invisível* (SHERMAN; PRICE, 2001) ou *Deep Web* (BERGMAN¹, 2001). Apesar de os principais fatores acerca da *Web Invisível* ser do começo da década, razão pela qual alguns números estão desatualizados e portanto não citados neste trabalho, são obras basilares a respeito do tema.

Em sua gênese, conforme abordado na seção 3, a *Dark Web* foi resultante de um estudo acadêmico que previa uma internet que operasse de forma invisível aos rastreamentos comuns na superfície. Assim, essa *web* foi idealizada para que houvesse liberdade de expressão e o intercâmbio de informações de forma livre e não rastreável (MONTEIRO; FIDÊNCIO, 2013). De qualquer forma, as potencialidades acadêmicas dessa *web*, evidentemente existem e persistem. Em busca realizada pelo termo *Dark Web* no *Google Scholar* e *Google Acadêmico*, nos periódicos brasileiros A1, nos Diretórios dos Grupos de Pesquisa do Brasil do CNPq e no Portal Capes em 2013 e 2014, pouquíssimos artigos são recuperados, dados que evidenciaram o ineditismo da temática, principalmente na Ciência da Informação (CI).

Diante do panorama da *Dark Web* na literatura científica e do seu potencial acadêmico e impactos sociais/informacionais, questionou-se (em pesquisa de mestrado, que aqui compreende apenas uma parte): que tipo de espaços representa essa *Web* e o que há de conteúdos informacionais nesse ambiente.

Desse modo, o trabalho tem como objetivo responder essas questões dentro

¹ Segundo Bergman (2001), o mais adequado é *Web Profunda*, uma vez que o termo invisível não seria adequado, pois a invisibilidade é apenas uma questão tecnológica ou mesmo política de indexação dos mecanismos de busca. Já Sherman e Price (2001), na descrição das várias camadas da *Web*, deixam perceber que o termo invisível não é exatamente a dicotomia da *Web Visível*, mas apenas a existência de planos de invisibilidade. Para aprofundamento das questões conceituais ver Monteiro e Fidêncio (2013).

dos parâmetros de uma pesquisa documental e exploratória para apresentação e discussão dos resultados.

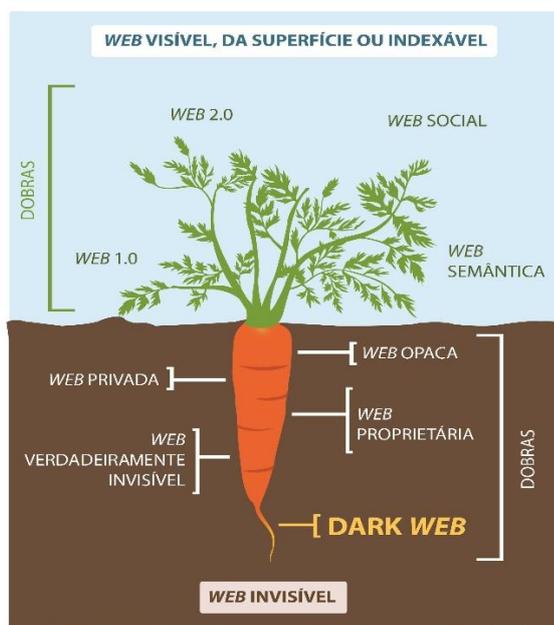
2 DA *WEB* VISÍVEL A INVISÍVEL

A *Web* Visível (também conhecida por *Web* da Superfície ou Indexável) é facilmente percebida ao acessar o ciberespaço por meio dos *sites* que milhares de pessoas utilizam diariamente, como por exemplo, o Google ou *Facebook*. O conteúdo visível é recuperado por intermédio de mecanismos de busca convencionais, o que torna a *Web* Visível presente na Superfície porque seus conteúdos foram indexados, por isso também conhecida como *Web* Indexável. Entretanto, os conteúdos que não foram ou não são indexados fazem parte do escopo da *Web* Invisível. O termo *Web* Invisível – *Invisible Web* para Sherman e Price (2001) ou *Web* Profunda – *Deep Web* para Bergman (2001), foi cunhado em 1994 por Jill Ellsworth para designar conteúdos que os mecanismos de busca tradicionais não conseguiam recuperar.

Não obstante, a *Web* Visível e a Invisível representam para os sujeitos navegadores duas *webs*: a primeira com seus conteúdos indexados e a segunda com conteúdos não indexados por motivos diversos, como dificuldades do robô de busca para indexar páginas com comandos que proíbem a ação; limitação na indexação de páginas por políticas de exclusão de conteúdos; proibição de conteúdos que não podem ser indexados, como perfis ou *sites* com propriedade estabelecida ou simplesmente porque os mecanismos não podem indexar (SHERMAN; PRICE, 2001).

Se o bem mais cobiçado da Era da Informação é a informação, então o conteúdo da *Web* Profunda é imensurável declara Bergman (2001) que em sua pesquisa demonstra além da variedade de assuntos encontrados nas dobras profundas do ciberespaço, a grande quantidade de Base de Dados existentes na *Web* Profunda. Entretanto, a principal constatação da pesquisa de Bergman (2001) é que 95% dos *sites* da *Web* Profunda são gratuitos, o que acentua ainda mais os prejuízos para qualquer sujeito que busca por informações na *web*. Porém, de maneira ainda mais profunda, existe a *Dark Web* que está localizada nas camadas da *Web* Invisível ou *Deep Web*, e representa a *web* mais densa, obscura e misteriosa de todas. A figura 1 demonstra, por meio de uma metáfora, a *Dark Web* no contexto da *Web* Invisível e suas dobras (camadas) do ciberespaço.

Figura 1 – A metáfora da cenoura: a localização da *Dark Web*



Fonte: Elaborado por Vignoli (2014).

Com base na figura 1, é possível observar que as folhas verdes da cenoura, que aparecem sobre a superfície, representam as *Webs* Visíveis do ciberespaço. Essas *webs* são facilmente identificadas pela *Web* Visível, da Superfície ou Indexável ou ainda por meio da *Web* 1.0, *Web* 2.0 ou Social, pela *Web* 3.0 ou Semântica, entre outras, todas passíveis de navegação pela superfície e principalmente de indexação por mecanismos de busca.

Abaixo da linha marrom que intenciona demonstrar a terra, estão as *Webs* Invisíveis. Na metáfora da cenoura, cada sulco existente no fruto alaranjado do vegetal representaria um tipo de *web* invisível, como por exemplo: a *Web* Invisível, a *Web* Opaca, a *Web* Privada, a *Web* Proprietária, a *Web* Verdadeiramente Invisível, entre outras (SHERMAN; PRICE, 2001). Porém, ainda na metáfora da cenoura, seria no último fio do fruto que se encontraria a *Dark Web*, a mais escondida e escura das *webs* existentes e objeto desta pesquisa. Com base na metáfora da cenoura, buscou-se tornar compreensível a localização da *Web* Visível e da *Web* Invisível assim como da *Dark Web* no ciberespaço.

3 A DEFINIÇÃO DE *DARK WEB*

Segundo Chen (2012), as pesquisas a respeito da *Dark Web* têm recebido destaque nas manchetes de importantes meios de comunicação pelo mundo, como

no *Washington Post*, *Fox News*, BBC, *PBS New Hour*, *National Public Radio*, *Science News*, *Toronto Star*, *Bulletin* (Austrália), entre outros canais principalmente nos EUA. A evidência noticiosa torna inquestionável a importância dos estudos acerca da *Dark Web*. Chen (2012) expõe também um fator interessante nas pesquisas da *Dark Web* que possui financiadores como a própria *Library of Congress*, a *National Science Foundation*, o *Air Force Resource Lab*, a *Defense Threat Reduction Agency* e o *Dept. of Homeland*. No Brasil, não foram encontrados nenhum tipo de financiamento para experimentos científicos na *Dark Web*.

A *Dark Web* ou *Web Escura* teve início com a tese de doutorado intitulada de *Distributed Decentralised Information Storage and Retrieval System* de Ian Clarke na *Edinburgh University*, em 1995. Mais adiante, precisamente em 2000, o *download* do *software* desenvolvido por Ian foi nomeado de *Freenet*, um programa gratuito que previa o acesso à internet, aos *websites*, *chats* ou compartilhamento de arquivos de forma anônima na rede. O *Freenet* teve nos seus primeiros nove anos de existência mais de dois milhões de *downloads*, principalmente na Europa e EUA (BECKETT, 2009). Com a tese de Ian foi possível a construção de uma rede paralela para acessar a internet, a *web* e o ciberespaço sem que essa navegação fosse rastreada. *A priori*, faz-se necessário esclarecer que a nomenclatura *Deep Web* seria utilizada para caracterizar a *web* invisível de forma geral, esta com todas as *webs* invisíveis citadas. No entanto, a *Dark Web* que também pertence a *Deep Web*, seria a sua camada mais profunda.

Por conseguinte, Fidêncio e Monteiro (2013, p. 692, grifos dos autores) especificam que “[...] é bastante seguro considerar a *Dark Web* como uma nova ramificação da *Web* Invisível: suas características são próprias; sua filosofia é própria e, além de tudo, seu conteúdo é o mais enigmático e desordenado de todas as ramificações.” Para Monteiro e Fidêncio (2013), o conteúdo da *Dark Web* permanece na invisibilidade porque grande parte de seus conteúdos são judicialmente ilegais. Ortega y Ortis (2013) explica que a parte de baixo do *iceberg* (figura largamente utilizada para demonstrar o tamanho da *Deep Web* em relação à *Web* da Superfície) existe por deficiência da parte de cima e por seu uso comercial excessivo. A menção do autor está relacionada às inúmeras propagandas direcionadas e a falta de privacidade existente na *Web* da Superfície que tanto incomoda sujeitos que não desejam se tornar fonte de informação e de lucros comerciais para os mecanismos de

busca convencionais.

Ainda para Fidêncio e Monteiro (2013, p. 693, grifos dos autores) “[...] na *Dark Web* o anonimato é desejável aos utilizadores, principalmente por causa de posições filosóficas dos usuários ou alguma posição contrária às normas sociais.” As razões pelas quais as pessoas optam por acessar a *Dark Web* são diversas, mas nem sempre estarão guiadas para atos ilícitos, e esse pressuposto deve acompanhar o conceito da camada mais incompreendida do ciberespaço.

Segundo Everett (2009), a *Dark Web* representa redes que compreendem múltiplos servidores escuros que são utilizados por todo tipo de ativistas políticos, cibercriminosos, serviço de inteligência internacional, agências que se comunicam e trocam informações secretamente, assim como para o comércio *online*. Ainda de acordo Everett (2009), a *Dark Web* acontece quando qualquer servidor *web* não pode ser encontrado por mecanismos de busca como o Google. Esse cenário poderia surgir também a partir do conteúdo de um servidor *web* individual que não contenha *hiperlinks* ou que é gerado dinamicamente a partir de um banco de dados, o que os tornará ilegível para os *spiders* da *web*, afirma a autora. No entanto, e como complemento de Everett (2009), a *Dark Web* é responsável também pela liberdade em comercializar e/ou publicar conteúdos de forma virtual sem censuras e em ambiente altamente criptografado e amorfo judicialmente.

Chen (2012, p. 93, grifo do autor, tradução nossa) possui uma visão esvaziadora da *Dark Web* porque a conceitua como se sua existência se baseasse no terrorismo: “Nós definimos este lado da Web reversa como a ‘Dark Web’, a porção da World Wide Web utilizada para ajudar a atingir os objetivos sinistros de terroristas e extremistas.” Em outro momento, Chen (2012, p. 220, tradução nossa) argumenta que:

Além de mau uso, sob a forma de engano, roubo de identidade, e vendas e distribuição de software pirata, a Internet também se tornou um popular meio de comunicação e refúgio para grupos extremistas e de ódio. Esta faceta problemática da Internet é frequentemente referida como a Dark Web.

As afirmações de Chen (2012) são arbitrárias, visto que os crimes descritos pelo autor ocorrem também na *Web* Visível. No entanto, não se pode subestimar a importância da falta de rastreamento dos sujeitos e de seus computadores como agente facilitador para pessoas que desejem cometer crimes. Em pesquisa anterior,

Chen *et al.* (2008) relataram que a *Dark Web* é utilizada por Organizações terroristas, Grupos extremistas, Grupos de ódio e Grupos de Supremacia Racial que se aproveitam do anonimato do ambiente para propagar suas ideias, conseguir novos adeptos e confabular ataques. Dessa forma, as pesquisas de Chen (2012) e Chen *et al.* (2008) são fundamentadas principalmente em estudos focados no *Jihad*, entre outros extremistas e ávidos por terrorismo contra os EUA.

Nas pesquisas de Chen (2012) e Chen *et al.* (2008) não são encontrados artigos que retratem outros assuntos ou outras abordagens para a *Dark Web*. Apesar dos autores possuírem dezenas de publicações a respeito da *Dark Web* (o que resultaria em avanços científicos significativos para a compreensão do ambiente) o objetivo é sempre entender o terrorismo discutido virtualmente contra os EUA. L' Huillier *et al.* (2010, Não paginado) também definem a *Dark Web* como a "Internet baseada em fóruns ou plataformas de terroristas ou cibercriminosos." No entanto, os autores incluem que o ambiente escuro é igualmente povoado por fãs-clubes de artistas ou comunidades que preferem a comunicação livre. Em pesquisa realizada em 2010, L' Huillier *et al.* analisaram redes de terrorismo na *Dark Web* com a utilização de Mineração de Dados e Análise de Redes Sociais como método científico o que é frequente nos estudos também de Chen (2012).

Diferentemente da *Web* Visível, em que a indexação de conteúdos é dificultada pela diversidade de formatos, na *Dark Web* é possível encontrar arquivos com dimensões muito variadas, demonstra Chen (2012): arquivos indexáveis: HTML, Word, PDF, Text, Excel, PowerPoint, XML; arquivos dinâmicos: PHP, ASP, JSP; arquivos em multimídia: imagem, áudio e arquivos de vídeo; arquivos compactados: RAR ou ZIP; arquivos com conteúdo em 2D e 3D além de arquivos com formatos não reconhecidos. Como muito pouco conteúdo da *Dark Web* é indexado (na *Web* Visível), qualquer tipo de formato pode ser utilizado para publicar e compartilhar conteúdos no ambiente que possui autonomia até mesmo nas mídias e padrões das informações.

Todas as conceituações e termos encontrados na *web* ou na literatura perpetuam a dificuldade e a necessidade em desmitificar a *Dark Web*. A esse respeito, Monteiro e Fidêncio (2013, p. 37, grifos dos autores) discursam que:

Como nada é tão simples nos objetos contemporâneos, outra *Web* emerge, considerada *Dark Web* (the dark side of the cyberspace) ou a invisível de fato, posto que servidores e a navegação feita sob o anonimato fazem a dobra underground do ciberespaço.

Nesta pesquisa, a *Dark Web* é definida a partir do momento em que é necessário utilizar proxy para acesso, em que sujeitos se depararem com conteúdos pesados, impróprios ou ilegais e que a *web* não seja indexada a risca. Diante desse cenário, conceitua-se que a *Dark Web* é composta por conteúdos não indexáveis por mecanismos de busca convencionais por motivos legais e porque os mecanismos simplesmente não conseguem indexar.

Igualmente, acredita-se que a *Dark Web* representa a *web* verdadeiramente livre e invisível e que apesar de ser utilizada também para o mal, exerce a liberdade de navegação, de expressão e de comunicação. Nesse pensamento, “A *Dark Web* ilustra a tensão entre a privacidade e a publicidade: a liberdade de expressão e até valores maniqueístas do bem e do mal, arquétipos humanos ressignificados ou virtualizados no ciberespaço.” (MONTEIRO; FIDÊNCIO, 2013, p. 44, grifos dos autores).

Navegar na *Dark Web* é lidar com a liberdade de expressão vestida pelo anonimato, o ambiente é a representação do que o ser humano pensa e faz na forma mais transparente, tanto para o bem quanto para o mal. Para acessar a *Dark Web*, o uso de proxy para camuflar o IP de um computador se faz indispensável. Uma vez que na *Dark Web* existem muitos conteúdos considerados impróprios ou secretos e que a sua principal característica é a privacidade de navegação, navegar sem registros do sujeito e de seu computador são imprescindíveis.

Para navegar na *Dark Web*, três *softwares* dispostos em *browsers* estão disponíveis no ciberespaço para *download* e acesso, são eles: o Freenet, que foi o pioneiro; o I2p que é uma iniciativa do Grupo Anonymous e o Tor que é proveniente de iniciativa da marinha americana e é o mais conhecido e utilizado de todos os recursos. O Tor possui uma rede de sujeitos cadastrados assim como de produtos e serviços na *Dark Web* com proporções desconhecidas, porém, astronômicas. De forma sumária, ao realizar o *download* de um dos três *softwares*, o sujeito navegador está ou estará pronto para navegar nos ambientes da *Dark Web*.

4 OS CONTEÚDOS EXISTENTES NA DARK WEB

A partir do método indutivo, foi possível levantar os conteúdos da *Dark Web* por meio de observação e navegação em dois ambientes: a *Hidden Wiki* e o *Tor Links*. A

Hidden Wiki é o endereço mais conhecido para acessar a *Dark Web* e o domínio do *Tor Links* foi encontrado durante a pesquisa por meio da rede Tor. Os dois *sites* funcionam como direcionadores com indicação de *hiperlinks* por assuntos com acesso direto e apresentam conteúdos iguais ou parecidos, porém ao contrário do que a literatura diz (FRANCO, 2013), o *Tor Links* referencia materiais mais pesados, principalmente para *hackers* e para pervertidos sexuais. Dessa forma, os resultados encontrados nos dois *sites* da *Dark Web* foram categorizados por temas e subtemas de forma simultânea.

Infelizmente, a maioria dos conteúdos da *Dark Web* é de baixa qualidade, ilegais e quase sempre desnecessários. Segundo Franco (2013), os ambientes escuros da *web* são divididos em duas camadas, uma que está a *Hidden Wiki* e outra que engloba *sites* com conteúdo fechado e para grupos específicos que são escondidos por mais camadas escuras. Os conteúdos encontrados na *Dark Web* que na qualidade de ruins ou não, não perdem a classificação de conteúdos informacionais, que assim foram classificados:

Crimes bancários: venda de contas bancárias com senhas; lavagem de dinheiro; venda de contas de cartões de crédito; tutoriais de roubo de cartões de crédito;

Tráfico: comércio internacional de armas; venda de armas militares; venda de munições; venda de drogas e diversos tipos de entorpecentes;

Mercado de contrabando: venda de eletrônicos em geral; lojas especializadas em aparelho celular de última geração; lojas especializadas em *videogames* de última geração; loja especializada em produtos da Apple; loja especializada em produtos da Samsung; venda de TVs de plasma e/ou *Full HD*; *softwares* da *Microsoft*; comércio de Viagra; comércio de animais raros; comércio de charutos cubanos;

Falsificações: falsificação de passaporte; falsificação de cidadania, inclusive americana; falsificação de dinheiro de diversas nacionalidades; confecção de Carteiras de Habilitação falsificadas; trabalhos acadêmicos;

Invasões de privacidade: venda de contas do *Twitter*; venda de resultados executivos; diversos tipos de espionagem; arquivos e informações secretas; interceptação telefônica;

Sexo e pornografia: zoofilia; parafilia; necrofilia; pedofilia; sadomasoquismo; sexo heterossexual; *snuffs* (que são vídeos com cenas reais, gravadas no ato da ação)

de sexo; contrato de companhia *gay* para negócios, amizade ou qualquer outra coisa; sexo com câmera escondida, inclusive de esposas e expostas por seus maridos sem consentimento; voyeurismo; prostituição; vídeo de estupradores e sexo forçado; pornografia de jovens, ninfetas e *top models*; mutilação de órgãos genitais; turismo sexual;

Religião e credences: *snuffs* espirituais; satanismos; financiamento de luta islâmica; exorcismos; serviços paranormais; informação esotérica (previsões do futuro);

Terrorismo: *snuffs* de ataques terroristas; *snuffs* de homem-bomba; tutoriais para a construção de bombas; muitas páginas para terrorismo disponível para israelenses; grupos de extremistas como nazistas e contra raças, negros ou *gays*; bioterrorismo e armas nucleares (CHEN, 2012);

Outros tipos de crimes: comércio de números de loteria; contratação de assassinos; tortura real de animais; destravamento de *videogames* bloqueados; rádio clandestina; fórum de *hackers*, *crackers*, programadores e anti-forenses; teste de vírus potentes; experiências médicas; manifestos, conspirações diversas que geram violência; lavagem de dinheiro; canibalismo ao vivo (ARAÚJO, 2012). Como visto, a diversidade temática é frequente na *Dark Web* para quem deseja realizar cibercrimes ou agir de forma ilícita e esses fatos podem ser comprovados por Chen (2012) e sua equipe que estudam o ambiente há algum tempo. Com base nas informações, afirma-se que se um sujeito realiza compras de produtos contrabandeados ou roubados, ou pratica outras ações ilegais na *Dark Web*, este se torna criminoso, cúmplice ou partícipe.

De qualquer forma, Bergman (2001, Não paginado) ao dissertar a respeito da *Dark Web* explica que “Se você está lendo isso, está na *Dark Web*.” A afirmação do autor parece uma forma ideal para a constatação de que a navegação está ocorrendo na *Dark Web*. Após diversos acessos no ambiente, é possível assegurar que Bergman (2001) foi assertivo, já que na *Dark Web* os conteúdos são expostos sem qualquer tipo de pudor e a verdade acerca do que acontece também na *web* escura.

Nesse contexto, o que mais impressiona nos crimes disponíveis por meio da variedade dos *hiperlinks* da *Dark Web*, é o teor das ações que ali podem ser praticadas e as propagandas para que crimes aconteçam por intermédio de uma página escolhida, como por exemplo: *Contas de Paypal, cartões de crédito, nós temos tudo!*

Preço baixo, delivery discreto e a melhor qualidade! Estoque fresco de contas bancárias a cada dois dias! Livre-se dos seus problemas! Entrega gratuita! Viagra com 50% de desconto! Foi enganado? Vamos encontrar o seu criminoso! Precisa de acesso a uma rápida conta? Podemos ter acesso a qualquer coisa! Sem perguntas. Você tem algum problema? Nós resolvemos pra você! Todas essas frases surgem como propostas de *marketing* para os serviços e produtos oferecidos que envolvem inescrupulosamente a vida humana.

O ser humano é comercializado nos ambientes da *Dark Web* de maneira abissal, sem hesitações ou qualquer tipo de respeito à raça humana ou mesmo animal. O desrespeito ao ser humano atinge o seu auge no comércio de órgãos ou nas mutilações de partes do corpo humano, além do canibalismo que ocorre por quem come ou vice-versa (ARAÚJO, 2012). O comércio de drogas e entorpecentes, tão comum na vida física e virtual, ganha proporções astronômicas na *Dark Web* que só na *Hidden Wiki* e no *Tor Links* são vendidos em cerca de 60 *hiperlinks* diferentes. Franco (2013) elucida que existe inclusive indicação dos melhores *sites* para a compra de drogas na *Dark Web*. Diante desses fatos, acredita-se que verdadeiros traficantes são formados unicamente de forma virtual na rede escondida.

Assassinos de aluguel oferecem seus serviços com tabela de preços: de 20.000 a 150.000 reais, inclusive com valores diferenciados para o assassinato de políticos ou pessoas famosas (ARAÚJO, 2012). Mercadorias são contrabandeadas e produtos são repassados a mercê da lei e de padrões de conduta e moral perante a sociedade. Não se sabe a procedência dos aparelhos eletrônicos ou dos medicamentos comercializados no ambiente, mas para Franco (2013) trata-se de objetos roubados. É preocupante cogitar a ideia de que pessoas honestas têm seus aparelhos eletrônicos roubados para serem vendidos no comércio negro do ciberespaço e que pessoas se predispõem a isso.

Os *snuffs* (vídeos em tempo real) atestam para imagens inimagináveis e incompreensíveis de apreciação por quem quer que seja. O prazer em ver pessoas sendo mortas ou agredidas não parece fazer sentido de nenhuma forma. O terrorismo tem proporções assustadoras na *Dark Web*, segundo Chen (2012) em sua pesquisa foram encontrados e observados: 1000 *sites* com 10.000 *hiperlinks* em 10 línguas distintas; 300 fóruns de terroristas com 30.000 membros e 1.000.000 de *posts* e 1.000.000 de imagens e 100.00 vídeos de terrorismo. O bioterrorismo (armas

biológicas) e a discussão acerca de armas nucleares causa espanto em qualquer pessoa. As discussões a respeito de terrorismo, fortemente pesquisada por Chen (2012) e sua equipe, são muito presentes na *Dark Web*. Na *Hidden Wiki* somente um endereço para discussões a respeito de terrorismo foi encontrado, no entanto, no *Tor Links* aproximadamente quinze endereços discutem a respeito. De fato, os dados são alarmantes e mantêm pesquisadores muito atentos a novos ataques terroristas contra o EUA e países de todo mundo, inclusive o Brasil.

A invasão de privacidade, de contas bancárias e ainda a interceptação telefônica fazem com que a insegurança já vivenciada diariamente por sujeitos do mundo todo, seja onipresente até mesmo no acesso a redes sociais como o *Twitter*, que possuem versão plagiada na *Dark Web* e também suas contas vendidas. Sonhos são despedaçados pelo mercado de números da loteria e pela propagação de informações privadas que podem roubar objetos de um sujeito trabalhador ou a inocência de uma criança violentada sexualmente. Os fóruns dedicados a *hackers* no *Tor Links* chegam a contabilizar um total de trinta endereços. Nesses *sites* destinados a *hackers*, todo tipo de crime é discutido.

Ainda que também existentes na superfície, os conteúdos da *Dark Web* são sem dúvida perturbadores e acabam por demonstrar o quão assombroso o ser humano por ser. Pensamentos desarranjados surgem ao se questionar ou afirmar que todas as excentricidades existentes na *Dark Web* sempre existiram, mas, não tinham ambiente tão propício para acontecer. De qualquer forma, ruins ou não, os conteúdos da *Dark Web* se caracterizam como informacionais. Entretanto, nem tudo que existe na *Dark Web* são conteúdos ruins, o que significa que os conteúdos informacionais da *Dark Web* serão muito semelhantes à *Web* Visível ou da Superfície. Muitos dos conteúdos da *Dark Web* retratam pirataria ou apropriação ilegal de conteúdos por meio de *downloads*, o que não é bom e nem novidade nem nas *webs* escuras nem ou da superfície. Entretanto, de forma mais branda, outros assuntos encontrados na *Dark Web* são apresentados também por temas e subtemas conforme se destaca:

Notícias: novidades em provedores; *sites* de notícias;

Conteúdos informacionais: filmes diversos e censurados; bibliotecas; livros proibidos, censurados, raros ou esgotados, todos para *download*.

Redes Sociais: *blogs* e *wikis*; *Torbook* (*clone do Facebook*); *Tor Fóruns*; *Torboks* (serviço de favoritos); *TorStatusNet* (*clone do Twitter*); fóruns diversos;

Ciberativismo: hacktivismo ético; *Wikileaks*; *Anonymous*; Manifestações, discussões e conspirações em geral;

Serviços ou produtos: compartilhamento de arquivos em *torrent* e em P2P; serviços de *e-mail*; hospedagem de *sites* e conteúdos; mecanismos de busca.

Como dito anteriormente, muitos dos conteúdos da *Dark Web*, às vezes apenas remetem a materiais menos agressivos. *Downloads* de livros ou filmes podem ser equiparados à compra de filmes piratas em camelôs do mundo todo, mas ainda assim, não deixam de ser crime. Livros banidos ou filmes censurados podem ser facilmente baixados em PDF e lidos ou assistidos pela rede. Também é possível baixar ou assistir filmes que ainda estão em cartaz nos cinemas pela rede Tor.

Algumas bibliotecas foram encontradas na *Dark Web*, inclusive com livros em português. No entanto, os *hiperlinks* apresentam dificuldades para serem abertos e os materiais desaparecem da mesma forma que reaparecem, sem aviso prévio. Na *Tor Library* (uma biblioteca virtual da rede Tor) existem livros para *download*, mas o comércio de drogas em vários idiomas foi descoberto com surpresa no ambiente. Franco (2013) explica que nem tudo que parece é, na *Dark Web*. O autor está correto porque as descrições para conteúdos comuns ou brandos na verdade, muitas vezes apresentam conteúdos ruins disfarçados. Isso acontece com frequência na navegação da *Dark Web*, como ocorreu no acesso a *Tor Library*.

Mas nem tudo que há na *Dark Web* é ruim já disse Ortega y Ortis (2013). Manifestações contra sistemas totalitários do mundo todo acontecem no ambiente. Franco (2013) articula ainda que até mesmo empregados descontentes utilizam os ambientes escuros para protestarem e desabafarem em silêncio. Todo tipo de manifestações e conspirações podem ser encontradas na *Dark Web* como a respeito de UFOs, ciências ou casos policiais. Neste momento, por exemplo, discussões e denúncias a respeito da Copa do Brasil 2014 estão acontecendo na *Dark Web*.

Muitas discussões acontecem por pessoas que pertencem a países cujo regime de liberdade de expressão é fortemente censurado, como a China. Segundo o *Anonymous* (2013), a Primavera Árabe foi discutida essencialmente na *Dark Web*. O próprio *Anonymous* conseguiu detectar uma rede de mais de 40 *sites* de pedofilia com cerca de 1.500 pedófilos denunciados para a polícia. Em 2012, a legião iniciou uma rede de ataques contra pedófilos intitulada de *Operação Pedo Chat* que já derrubou diversos *sites* com pornografia infantil (ANONYMOUS, 2012). A legião de ativistas

comprova que boas ações podem acontecer por meio da *Dark Web*. A equipe de Chen (2012) também tem conseguido acompanhar discussões acerca de centenas de grupos extremistas ou de ódio como o *Jihad* no ambiente. No entanto, com o sistema de criptografia robusta, fica quase impossível para a polícia encontrar os cibercriminosos.

Outro caso muito conhecido nas principais mídias do mundo foram as denúncias de Júlio Assange na *Wikileaks*. As informações publicadas na *Wikileaks* dissertam a respeito de crimes e arquivos secretos que envolvem o governo americano, além de denúncias de muitos outros países, como do Brasil. Diferente da maioria dos *sites* da *Dark Web*, a *Wikileaks* possui uma interface bastante agradável e muito parecida com o perfil de páginas da superfície, além da própria *wiki* – *Wikileaks* – que segue os moldes da *Wikipédia*.

As redes sociais também estão presentes nos ambientes escuros da *web*. *Blogs*, *wikis* e fóruns que discutem assuntos triviais (ou não) como na superfície são bastante comuns na *Dark Web*. A diferença é que participar ativamente de um desses recursos na *Dark Web* garantirá o anonimato para os sujeitos navegadores. É preciso entender que muitas vezes a escolha pelo anonimato presente na *Dark Web* é somente uma opção em não se expor virtualmente, o que nem sempre ensejará a ideia de um crime. O destaque para as redes sociais da *Dark Web* está no *Torbook*, um *Facebook* que opera na rede Tor. A ferramenta possui o mesmo *layout* da rede social e copia inclusive a cor azul que representa o recurso 2.0. Outras ferramentas 2.0 muito semelhantes as da superfície também são encontradas na *Dark Web*, como é o caso do *Starboks*, um serviço de *bookmarks* para hospedagem e compartilhamento de favoritos e o *TorStatusNet*, um *Twitter* da rede Tor.

Na *Dark Web* também é possível hospedar páginas diversas, como *sites*, *wikis*, imagens ou fóruns com temas específicos. Na hospedagem de páginas, tem-se uma situação antagônica: conteúdos bons ou ruins podem ser hospedados sem restrições ou censuras. Os serviços de *e-mail* disponibilizados para os sujeitos na *Dark Web* podem ser analisados como ferramentas interessantes na prevenção e exposição que por ventura ocorram na superfície. Foram encontrados quatorze serviços que mesclam *e-mail* e serviço de mensagens instantâneas, dentre esses, três ferramentas são destacadas por sua imanência no ambiente: o URSSMAIL, o *Anonmail* e o *Onion Mail*.

Notícias e novidades a respeito de assuntos diversos que não remetam a formas de cometer crimes, assim como os serviços de *e-mail* e *sites* que não propagem atos desleais podem ser considerados como conteúdos do lado da pílula azul na *Dark Web*. Importante destacar que existe a possibilidade em acessar qualquer conteúdo da superfície pela rede Tor a fim de tentar garantir privacidade nas navegações pelo ciberespaço.

Autores como Franco (2013) esclarecem que existem muitas bases de dados científicas na *Dark Web*. Mas conteúdos acadêmicos/científicos atuam como se fossem conteúdos ilegais na superfície, são muito difíceis de serem encontrados. Franco (2013) elencou alguns *sites* classificados como bases de dados ou enciclopédias que foram “acessados” tanto na superfície quanto na *Dark Web* o que, portanto, não foi considerado como conteúdo exclusivo da *web* escura. Dessa forma, encontrar informações científicas na *Dark Web* não é tarefa fácil, a menos que a busca seja realizada simultaneamente com a *Web* Visível. Outro ponto necessário de destaque é a forma como os mecanismos de busca da *Dark Web* funcionam, como os cinco encontrados: o *Ahmia. Fi*, o *Tor Search*, o *Duck Duck Go*, o *Torch*, o *Tor Find*. Se na superfície os buscadores mais tradicionais como o Google não conseguem ou não querem recuperar conteúdos invisíveis, quiçá os mais escuros, na *Dark Web* acontece exatamente o contrário. Uma *query* na *Dark Web* é pesquisada tanto nos ambientes escuros quanto na superfície, o que é intrigante para uma pesquisa científica por exemplo. Nesse raciocínio, uma busca de informações na *Dark Web* poderá recuperar resultados muito mais completos e variáveis que na superfície. Sem dúvida, a capacidade de recuperação da informação da *Dark Web* é um ponto muito positivo para o ambiente.

Todos esses fatores demonstram que as dobras/camadas escuras do ciberespaço inclinam para uma tendência futura para acesso, disponibilização de informações ou pesquisa. Dessa forma, considera-se que o lado realmente útil da *Dark Web* está no acesso à internet, a *web* e ao ciberespaço de forma anônima, como para que os sujeitos não sejam bombardeados por propagandas, invasões de privacidade ou distribuição e comercialização involuntária dos dados das buscas realizadas diariamente. As possibilidades em realizar buscas por informações nas duas *webs*, visível e invisível também merecem destaque e atenção para a CI, seus profissionais e pesquisadores.

5 CONSIDERAÇÕES FINAIS

No estudo das *webs* invisíveis, aquelas que não são indexadas, foram conceituadas a *Web Invisível* ou *Deep Web* com conteúdos que não são recuperados pela maioria dos mecanismos de busca da superfície. E ainda, a realmente invisível e profunda, a *Dark Web* que se torna possível e localizável por meio de *softwares* que garantem navegação anônima como o Tor, *Freenet* ou I2P. Com esta pesquisa, julga-se que o objetivo em explorar seus ambientes e se aprofundar nas *webs* escuras e muito profundas como a *Dark Web* foram atingidos com êxito. Infelizmente, constatou-se que a maioria de seus conteúdos não se refere a materiais bons (sem conteúdo ilegal ou impróprio), que poderiam ser “acessados” sem problema algum, como acontece na superfície. Definitivamente, a *Dark Web* destoa da superfície em questão de conteúdos, *layouts* e conteúdo informacional, já que nesta *web*, não há restrições.

Todos os crimes e discussões ilegais que ocorrem no ambiente, fazem o sujeito crer que o mundo e a sua vida estavam alienadas a um mundo senão perfeito, menos ruim até o encontro com maioria dos *sites* e serviços da *Dark Web*. Mesmo assim, toda essa faceta do ciberespaço precisa ser conhecida por profissionais que lidam com a informação. Claramente com intenção de informar as pessoas e de lhes apresentar esse mundo paralelo que também possui suas vantagens. Conteúdos bons ou neutros também existem na *Dark Web*, embora sejam muito mais difíceis de encontrar. No entanto, é possível realizar uma busca por informações entre e nas camadas visíveis e invisíveis simultaneamente, porque os mecanismos da superfície não indexam os conteúdos escuros e invisíveis, mas o contrário acontece. Navegar anonimamente na rede, discutir a respeito de assuntos entre pessoas específicas e não ser alvo de propagandas e principalmente de espionagem formam o pacote de benefícios em navegar nas dobras escuras e na *Dark Web*. Quem deseja privacidade, deseja uma navegação nas camadas escuras. Quem deseja realizar pesquisas/buscas mais completas, precisa conhecer as camadas escuras do ciberespaço.

A CI que ao lidar com informação e conhecimento e as formas de organizá-los e difundi-los não pode estar aquém das *webs* invisíveis do ciberespaço. Se isto for, a área padecerá por não estudar o maior lado do ciberespaço, em que de fato está a maioria das informações disposta de forma virtual. Ainda que contenha conteúdos

ruins como os ilegais, a *Dark Web* possui potencial para que muitas outras pesquisas sejam realizadas em seus ambientes por pesquisadores da CI. A diversidade temática e informacional da *Dark Web* e das dobras invisíveis do ciberespaço é, quem sabe, o mais novo desafio dos Profissionais da Informação, que precisam conhecer os caminhos que os levam até a informação. Espera-se que por meio dessa pesquisa, o objeto central que foi a *Dark Web* possam inclusive ser conhecidos pela sociedade em geral. A informação não pode ser negada a espaços informacionais públicos, como são os invisíveis e escuros.

REFERÊNCIAS

- ANONYMOUS. **Anonymous declara guerra a pornografia infantil #OPPEDOCHAT**. 2012. Disponível em: < <http://www.anonymousbrasil.com/mundo/anonymous-declara-guerra-a-pornografia-infantil-opedochat/> >. Acesso em: 15 mar. 2016.
- ARAÚJO, J. P. **Invisível, oculta ou profunda?: a web que poucas ferramentas enxergam**. 2012. Disponível em: < www.comunicar.pro.br/artigos/weboculta.htm >. Acesso em: 22 mar. 2016.
- BECKETT, A. **The dark side of the internet**. 2009. Disponível em: < <http://www.guardian.co.uk/technology/2009/nov/26/dark-side-internet-freenet> >. Acesso em: 27 abr. 2016.
- BERGMAM, M. K. White paper: the deep web surfacing hidden value. **Journal of Electronic Publishing**, v. 7, n. 1, 2001. Disponível em: < <http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104> >. Acesso em: 12 abr. 2016.
- CHEN, H. **Dark web: exploring and data mining the dark side of the web**. Nova York: Springer, 2012.
- CHEN, H. *et al.* Uncoverin the Dark web: a case study of Jihad on the web. **Journal of the American Society for Information Science and Technology**, EUA, v. 8, n. 59, p. 1347-1359, 2008. Disponível em: < <http://www.w.icadl.org/intranet/papers/H%20Chen%20and%20W%20Chung%202008.pdf> >. Acesso em: 12 mar. 2016.
- COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR (CAPES). **Portal de periódicos**. Disponível < <http://www.periodicos.capes.gov.br/> >. Acesso em: 02 set. 2013 e 14 mar. 2014.
- CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO (CNPQ). **Diretórios dos grupos de pesquisa no Brasil**. Disponível em: < <http://dgp.cnpq.br/buscaoperacional/> >. Acesso em: 09 set. 2014 e 14 jun. 2016.

EVERETT, C. Moving across to the dark site. **Network Security**, set. 2009.

FIDÊNCIO, M. V.; MONTEIRO, S. D. Web invisível: compreendendo a invisibilidade no ciberespaço. In: SEMINÁRIO EM CIÊNCIA DA INFORMAÇÃO – SECIN, 5., Londrina, 2013. **Anais eletrônicos...** Londrina: SECIN, 2013. Disponível em: <<http://www.uel.br/eventos/secin/ocs/index.php/secin2013/secin2013/paper/view/107>>. Acesso em: 23 mar. 2016.

FRANCO, D. P. Deep web: mergulhando no sub-mundo da internet. **Revista Segurança Digital**, n. 10, abr. 2013.

FREENET PROJECT, THE. **The free network**. Disponível em: <<https://freenetproject.org/>>. Acesso em: 25 abr. 2016.

HIDDEN WIKI. 2014. Disponível em: <<http://zqkltwi4fecvo6ri.onion/>>. Acesso em: 14 mar. 2016.

L'HUILLIER, G. *et al.* Topic-based social network analysis for virtual communities of interests in Dark Web. **SIGKDD Explorations**, v. 12, n. 2, p. 66-73. 2010. Disponível em: <<http://dl.acm.org/citation.cfm?id=1938615>>. Acesso em: 17 fev. 2016.

MONTEIRO, S. D. A dobra semiótica e os agenciamentos maquínicos: por uma ontologia das tecnologias da informação e comunicação. In: CERVANTES, B. M. N. (Org.). **Horizontes da organização da informação e do conhecimento**. Londrina: EDUEL, 2012. p. 63-96.

_____. Por uma cartografia conceitual da web invisível: a dobra oculta do ciberespaço. **Informação e Sociedade: estudos**, João Pessoa, v. 23, n. 3, p. 23-31, set./dez. 2013. Disponível em: <<http://periodicos.ufpb.br/ojs2/index.php/ies/article/view/16512>>. Acesso em: 01 fev. 2016.

MONTEIRO, S. D.; FIDÊNCIO, M. V. As dobras semióticas do ciberespaço: da web visível à invisível. **TransInformação**, Campinas-SP, v. 1, n. 25, p. 35-46, jan./abr. 2013. Disponível em: <<https://www.puc-campinas.edu.br/periodicocientifico>>. Acesso em: 28 fev. 2016.

ORTEGA Y ORTIS, J. **Você sabe o que é a Deep Web?** 2013. Disponível em: <<http://olhardigital.uol.br/video/voce-sabe-o-que-e-a-deep-web/32156>>. Acesso em: 24 fev. 2016.

SANTAELLA, L. **Navegar no ciberespaço: o perfil cognitivo do leitor imersivo**. São Paulo: Paulus, 2004. (Comunicação).

SHERMAN, C.; PRICE, G. **The invisible web: uncovering information sources: searches engines can't see**. Medford: Cyberage Books, 2001.

VIGNOLI, R. G. **A topografia da Dark Web e seus não lugares: por um estudo das dobras invisíveis do ciberespaço**. 2014. 154 f. Dissertação. (Mestrado em Ciência da Informação) – Universidade Estadual de Londrina, Londrina, 2014