# *Deep Web* e *Dark Web*: similaridades e dissiparidades no contexto da Ciência da Informação

# *Deep Web and Dark Web*: *similarities and dissiparities in the context of Information Science*

Richele Grenge VIGNOLI[1] 0000-0003-1550-5258
Silvana Drumond MONTEIRO[2] 0000-0001-7228-1380

## Resumo

Neste artigo, objetiva-se desmitificar a *Deep Web* e a *Dark Web*, além de apresentar as principais similaridades e disparidades entre elas, essencialmente no que tange aos seguintes aspectos: (1) Termo; (2) Definição; (3) Localização metafórica no ciberespaço por meio de figura; (4) Tipos de conteúdos e (5) Formas de acesso. A pesquisa teve caráter documental e bibliográfico, com buscas realizadas na *Web of Science, Scopus Elsevier, Scientific Eletronic Library Online*, Base de Dados Referencial de Artigos de Periódicos em Ciência da Informação, *Science Direct, Google Scholar* e em periódicos científicos diversos. As principais relações similares e dissimilares entre a *Deep Web* e a *Dark Web* foram apresentadas no artigo. No entanto, propõe-se que novos e necessários estudos a respeito das camadas escondidas e profundas do ciberespaço sejam realizados e difundidos no campo da Ciência da Informação.

**Palavras-chave**: Ciberespaço. *Web* invisível. *Web* profunda.

## Abstract

*In this article, we aim to demystify the Deep Web and the Dark Web, in addition to presenting the main similarities and disparities between them, essentially in regard to their: (1) Term; (2) Definition; (3) Metaphorical location in cyberspace through figures; (4) Types of contents; and (5) Ways of access. The research was documental and bibliographic, with searches in the Web of Science, Scopus Elsevier, Scientific Eletronic Library Online, Base de Dados Referencial de Artigos de Periódicos em Ciência da Informação, Science Direct, Google Scholar, and various scientific journals. The main relationships (similar and dissimilar) between the Deep Web and the Dark Web are presented in the article. However, new and necessary studies on the hidden and deep layers of the cyberspace should be carried out and disseminated in the field of Information Science.*

***Keywords***: *Cyberspace. Invisible Wep. Dark Web.*

## Introdução

É possível afirmar que o conhecimento acerca de camadas e, principalmente, de frações obscuras da *Web* no ciberespaço já seja uma realidade nos caminhos que a *internet* percorre diariamente. A saber, a *Web* que milhares

[1] Universidade Estadual Paulista Júlio de Mesquita Filho, Faculdade de Filosofia e Ciências, Programa de Pós-Graduação em Ciência da Informação. Marília, SP, Brasil.

[2] Universidade Estadual de Londrina, Centro de Comunicação e Artes, Programa de Pós-Graduação em Ciência da Informação. Rod. Celso Garcia Cid, PR 445, Km 380, *Campus* Universitário, 86057-970, Londrina, PR, Brasil. Correspondência para/*Correspondence to*: S. D. MONTEIRO. *E-mail:* <silvanadrumond@gmail.com>.

Recebido em 10 de junho de 2019, reapresentado em 19 de maio de 2020, aprovado em 8 de junho de 2020.

Como citar este artigo/How to cite this article

Vignoli, R. G.; Monteiro, S. D. *Deep Web* e *Dark Weeb* similaridades e dissiparidades no contexto da Ciência da Informação. *Transinformação*, v. 32, e190052, 2020. https://doi.org/10.1590/2318-0889202032e190052

de sujeitos utilizam diariamente é denominada Visible *Web* (*Web* Visível), Surface *Web* (*Web* da Superfície) e Normal *Web* (*Web* Normal) (Bergman, 2001; Sherman; Price, 2001; East, 2017).

No entanto, nas camadas mais profundas e obscuras do ciberespaço, estão a *Deep Web* e a *Dark Web*, dois objetos distintos, por vezes conceituados como congêneres. Apesar de possuírem algumas semelhanças, não são, de fato, a mesma *Web*. De todo modo, o ciberespaço, em sua totalidade, teria sido pouco explorado em questões informacionais até o momento, pois a literatura que retrata tanto a *Deep* quanto a *Dark Web* é escassa em território nacional, especialmente no âmbito da Ciência da Informação (CI).

Dessa forma, a CI, campo científico profícuo a novos desafios, poderá investigar os entraves das camadas escuras do ciberespaço sob diversos aspectos científicos. Para tanto, este ensaio objetivou, além de desmistificar a *Deep Web* e a *Dark Web*, apresentar suas principais similaridades e dissiparidades, sob os seguintes aspectos: (1) termo; (2) definição; (3) localização metafórica no ciberespaço, por meio de discussões e de figura; (4) tipos de conteúdos e (5) formas de acesso. A necessidade de distinção entre as *Web* se faz latente e vital, pois há, na literatura, confusão e distorções generalizadas no que representa tanto a *Deep* quanto a *Dark Web*. Na urgência de aprofundamento e de prospecto de novos estudos a respeito da temática para a CI, esta pesquisa se justifica na tentativa de tornar cognocível a premissa básica direcionada à distinção conceitual e prática entre a *Deep* e a *Dark Web*, sua desmitificação, seus principais conteúdos e suas formas de acesso. Além disso, apresenta uma figura ilustrativa que objetiva demonstrar visualmente a verdadeira diferença entre as *webs*. Prospectar novas pesquisas nos entornos das camadas obscuras do ciberespaço sem a definição e a distinção nítida da *Web* é um erro crivo acentuado na literatura, essencialmente na internacional.

Considerando isso, foram utilizados os delineamentos da pesquisa documental e bibliográfica para a investigação. Os termos pesquisados para a busca bibliográfica foram *Deep Web* e *Dark Web*, com refinamento de pesquisa e com intuito de recuperar documentos que continham o termo no título e/ou como assunto. Assim, foram abordados os dois objetos de maneira distinta desde o levantamento bibliográfico, como propunha o estudo.

As bases de dados consultadas para esta pesquisa foram a *Web of Science, Scopus Elsevier, Scientific Eletronic Library Online*, Base de Dados Referencial de Artigos de Periódicos em Ciência da Informação, *Science Direct, Google Scholar* e periódicos científicos diversos. No levantamento bibliográfico, priorizou-se a busca em língua inglesa até 2020 e em língua portuguesa especificamente de 2014 (quando outras pesquisas acadêmicas da CI foram findadas a esse respeito) a 2020. As principais fontes bibliográficas consultadas em língua portuguesa no escopo da CI foram as citadas nos parágrafos seguintes.

Monteiro (2013) perscruta alguns conceitos de *Invisible Web* no campo semântico e apresenta, como metodologia, uma cartografia de análise conceitual, a partir dos princípios (deleuziano) da dobra, a saber: a dobra possui interior e exterior; alto e baixo, desdobra e o paradigma. A premissa da dobra serviu como aporte teórico e método, para estudar tanto o conceito da *Invisible Web* quanto do movimento dos platôs simbólicos que formam a *Invisible Web* no ciberespaço.

Monteiro e Fidencio (2013) realizam uma prospecção conceitual da *Invisible Web* e de alguns mecanismos de busca que fazem a dobra com essa *Web* no ciberespaço, com o objetivo de dirimir a polissemia do tema: que nome dar a esse (des)território? *Web* Invisível, Profunda, Oculta, Escura? Durante a pesquisa, descobriu-se uma *Web* verdadeiramente escura, a *Dark Web*, paralela e *underground*, utilizada para o bem e para o mal, como previsível da espécie humana.

Fidencio e Monteiro (2013) definem a *Invisible Web* como o conteúdo do ciberespaço não indexado pelos mecanismos de buscas. A metodologia empregada foi a pesquisa e a análise documentais para estudo do objeto específico. Fez-se a categorização dos tipos de invisibilidade descobertas na literatura: *Web* opaca, que mistura mídias; *Web* privada, restrita pelos seus mantenedores; *Web* proprietária, indexável, mas que possui propriedade de alguma organização e é acessível por senha; e a *Web* verdadeiramente invisível, excluída por política de exclusão

dos mantenedores ou por dificuldade de indexação. Em síntese, nos artigos supracitados, a *Dark Web* não foi objeto de investigação.

Vignoli (2014), em dissertação intitulada "A Topografia da *Dark Web* e seus não lugares: por um estudo das dobras invisíveis do ciberespaço", defendida na CI, buscou, com foco exclusivo na *Dark Web*, apresentar o ambiente e situá-lo enquanto conceito e espaço ocupado no ciberespaço. Além disso, objetivou demonstrar suas características como um não lugar em essência, segundo os aportes de Bauman (2001) e de Augé (2012) e os conteúdos benéficos e maléficos encontrados nessa *web*.

Vignoli e Monteiro (2015a) desenvolveram pesquisa com foco no prisma do conteúdo informacional recuperado no ambiente e interessante à CI como fonte de informação não explorada. O potencial informativo da *Dark Web* teceu a discussão principal do estudo.

Vignoli e Monteiro (2015b) discutiram mais especificamente as dobras/camadas da *Dark Web* e sua condição como não lugar no ciberespaço. Apesar de as últimas três pesquisas citadas terem sido desenvolvidas no núcleo da *Dark Web*, em nenhuma delas houve diferenciação precisa entre a *Deep* e *Dark Web*, corriqueiramente confundidas como sinônimos. Infelizmente, na CI brasileira, foi observada estagnação científica a respeito das camadas/dobras obscuras do ciberespaço desde o ano de 2015.

É, portanto, primordial que mais discussões a respeito da temática sejam realizadas, essencialmente porque o ciberespaço e suas camadas profundas, sempre em constante mutação e crescimento, apresentam-se como campo muito rico a ser investigado na CI sob diversos aspectos.

## *A Deep Web*

A *Deep Web*, ainda pouco difundida por pesquisas científicas, principalmente na CI, representa uma *Web* permeada por desconhecimento e prejulgamentos pejorativos em relação ao seu conteúdo. O termo, cuja tradução é "Rede Profunda", foi cunhado em 1994 por Jill Ellsworth (Bergman, 2001) e pode ser comumente denominado por *Invisible Web* (*Web* Invisível) (Sherman; Price, 2001; Fulton; McGuinness, 2016) e/ou *Hidden Web* (*Web* Escondida) (Hurlburt, 2017). Contudo, devido a confusões conceituais, alguns autores como East (2017) propagam que a Deep e a *Dark Web* significam a mesma *Web* e são apenas duas denominações para o mesmo objeto, afirmações contrárias a este estudo. Para Fulton e McGuinness (2016), não se pode confundir a dificuldade de localizar certos conteúdos e páginas na *Deep Web* com a obscuridade da *Dark Web*, assim também pensam também os autores Finklea (2017), Rouse (2019) e Zilman (2019).

A *Deep Web* representa uma camada exponente do ciberespaço que possui, na maioria das vezes, conteúdos não recuperáveis ou indexáveis pelos mecanismos de busca. O resultado da falta de indexação e posterior não recuperação da informação ocasiona uma quantidade significativa de conteúdos não transitáveis e, portanto, não acessados em todo o ciberespaço.

A *Deep Web*, para Sherman e Price (2001), significa que motores de busca gerais não podem ou não conseguem adicionar conteúdos e páginas em seus índices, seja por limitações técnicas, por escolhas definidas ou, ainda, por questões de tarifamento para acesso, conforme apontam Winkler e Gomes (2017). Bergman (2001) explica que os mecanismos de busca tradicionais criam seus índices nas páginas da superfície, o que comprova a disposição dos motores em não indexar e demonstra que essa indexação é deliberadamente superficial.

No entanto, outros motivos fundamentam a ineficiência do buscador e a falta de indexação dos conteúdos invisíveis, como a própria efemeridade das informações, no caso de horários de voos (Sherman; Price, 2001) ou de informações do mercado de ações (Fulton; McGuinness, 2016), dados alterados a todo momento. Nesse caso, a indexação se torna um trabalho desnecessário para sítios não especializados nesses ramos comerciais.

Céndon (2001) expõe outras justificativas técnicas que tornam páginas invisíveis aos mecanismos de busca, como: *sites* com senhas, com *firewall*, com o metadado *noindex*, que não permite recuperação pelos buscadores, páginas dinâmicas (criadas no momento da busca) e com *frames* ou com *image-maps* (com um URL para cada imagem/mapa), entre outros motivos. Fulton e McGuinness (2016) explicam que também são conteúdos da *Deep Web* as páginas sem *hiperlink* de entrada ou de saída, as que não possuem acesso direto e imediato por diversas razões, como tarifação no acesso, e, ainda, as informações advindas de *intranets* ou de comunicação via redes sociais. Marcas e patentes são outros fatores que dificultam acesso a páginas específicas (Niemeier, 2016).

Céndon (2001) acentua que importantes bancos de dados não fazem parte do escopo de resultados apresentados pelos mecanismos de busca convencionais. Materiais de referência como dicionários, catálogos *on-line* de bibliotecas, informações protegidas por *firewalls* e bancos de dados de assinaturas (com base em taxas) são outros exemplos de conteúdos encontrados na *Deep Web* (Rouse, 2019). Entretanto, a principal constatação da pesquisa de Bergman (2001) é a de que 95% dos *sites* da *Deep Web* são gratuitos, o que acentua os prejuízos para qualquer sujeito que busque por informações na *Web*.

Quanto à dimensão da *Deep Web*, Bergman (2001) traz dados fundamentais em busca da compreensão territorial entre as camadas invisíveis vs visíveis da *Web*. Apesar de já considerados antigos, dados mais recentes com a precisão de Bergman (2001) não foram encontrados na literatura. À época, o autor diagnosticou que na *Deep Web*: (a) a informação pública é de 400 a 550 vezes maior que a da superfície; b) a *Visible Web* teria 19 terabytes, contra 7.500 da *Deep Web* (Rouse, 2019); (c) a *Visible Web* teria 1 bilhão de documentos e, a *Deep Web*, 550 bilhões; (d) existem mais de 200.000 *sites*; (e) o conteúdo da *Deep Web* é de 1 a 2 mil vezes maior do que o da *Visible Web*.

Outrossim, autores como Atwood (2017), East (2017) e Rouse (2019) explicam que a *Visible Web* torna disponível apenas 4% de todo o conteúdo do ciberespaço. Rouse (2019) ao atualizar os dados expressos no pioneirismo de Bergman (2001), apresenta a seguinte fração da totalidade de conteúdos do ciberespaço em suas camadas: (a) *Deep Web* = 90% de todo o conteúdo do ciberespaço; (b) *Dark Web* = 6%; e (c) *Visible Web* = apenas 4%.

Segundo Zilman (2019), o conteúdo da *Deep Web* é formado por cerca de 7.500 *terabytes*, assim como apresentado por Bergman (2001). Cabe ressaltar que, conforme mencionado, a diversidade de conteúdos e de informações relevantes na *Deep Web* é imensa. Materiais inapropriados, como comércio de drogas, além de outros tipos de venda ilegal, fraudes de diversos tipos, lavagem de dinheiro, pedofilia e demais distúrbios sexuais, são, indubitavelmente, encontrados na *Deep* (e mais precisamente na *Dark Web*) como mercancias da *internet* desde sua criação e não como propriedade dessa ou de outra *Web*.

Outro tipo de conteúdo pertencente à *Deep Web*, de acordo com Fulton e McGuinness (2016), são os artigos e as publicações científicas sem acesso livre. Para se acessar bancos de dados científicos proprietários, por exemplo, práticas como cadastramento e/ou pagamentos são necessárias, o que acarreta a falta de indexação por mecanismos de busca da superfície.



Trata-se de prejuízos para a ciência e para pesquisadores de forma geral. Para os autores, o *Google Scholar* pode ser visto como uma espécie de buscador da *Deep Web*, pois possibilita acesso direto e imediato à informação científica. No entanto, como nem sempre consegue realizar essa tarefa, não se pode afirmar com precisão que seja um buscador da *Deep Web*. A esse respeito, para Zilman (2019), apesar do acesso dificultado, não é impossível recuperar textos e pesquisas de qualidade na *Deep Web*. Na intenção de auxiliar pesquisadores em buscas bibliográficas de qualidade no ambiente, a autora preparou uma espécie de guia com os principais pontos a serem observados quando na navegação do ambiente com fins acadêmicos/científicos. Outras dicas e instruções detalhadas podem ser igualmente acessadas em materiais correlatos na plataforma da *Association of Internet Research Specialist*, que disponibiliza, inclusive, materiais para navegadores iniciantes nas camadas obscuras do ciberespaço.

Invariavelmente, afirma East (2017, p. 16, tradução nossa)[3]: "Você deve estar ciente de que sua vida diária frequentemente envolve a *Deep Web* de alguma forma." Sob esse prisma, todo sujeito que acessa a *Web* e possui *login*, senhas ou cadastros acaba envolvido na *Deep Web* diariamente, ainda que por desconhecimento ou com preconceitos a seu respeito (Vignoli; Monteiro, 2015a).

Desse modo, os preceitos da *Deep Web* vão além de decisões ou de impedimentos técnicos, pois muitas informações simplesmente não podem ser disponibilizadas por questões de sigilo e/ou de segurança. É a condição de dados de *e-mail* e de *instant messages*, entre outros tipos de informações que não devem trafegar na *Web*, conhecidos igualmente por Dados Sensíveis. Dados Sensíveis são definidos por "Dados íntimos, secretos ou sigilosos de pessoal natural ou jurídica." (Vignoli; Vechiato, 2019, p. 296). Também é o caso de dados ocasionados por conteúdos tecnicamente limitados, como os que requerem a tecnologia CAPTCHA (teste de *Turing* público completamente automatizado para diferenciar computadores e humanos) e os textos existentes fora dos protocolos http: // ou https: // ou em bancos de dados convencionais (Rouse, 2019).

Os Dados Sensíveis não podem ser difundidos por questões de segurança, ética, privacidade e motivos legais, tanto para os administradores das páginas quanto para quem utiliza o serviço/produto oferecido. Há, nesse cenário, outro ponto a ser observado na *Deep Web*: a confiança depositada por sujeitos que aceitam os termos de uso de cada página. Nesse sentido, foi publicada a Lei Geral de Proteção de Dados Pessoais no Brasil em 2018, prevendo a relação legal de proteção aos Dados Pessoais e Sensíveis (Brasil, 2018).

Na União Europeia, as discussões acerca da proteção dos Dados Pessoais e Sensíveis ocorrem desde 1981 e, mais recentemente, por meio da atualização do Regulamento Geral de Proteção de Dados, publicado em 2016. Em relação aos direitos à privacidade, guarnecidos por leis e por regimentos nacionais ou internacionais, há, na *Deep* ou na *Dark Web*, diversas ilegalidades que inferem negativamente nos direitos dos cidadãos. Enquanto discussões e aparatos legais são desenvolvidos para a proteção dos Dados Pessoais e Sensíveis de forma geral, nas camadas obscuras do ciberespaço há dificuldade eminente de garantia desses direitos, tanto a pessoas físicas quanto jurídicas. Registros públicos de pessoas e de empresas (Rouse, 2019) são exemplos de dados e de informações sigilosas e sensíveis recuperadas na *Deep* ou na *Dark Web*, o que parece ser um desafio de difícil e longa dissolução. Isso se deve aos milhares de sítios existentes no espaço, já destinados a denúncias e à violação de privacidade e de identidade de forma proposital. Como é possível notar, a invisibilidade da *web*, e mais precisamente de seus conteúdos, dados ou informações, é, sob diversos ângulos, precisamente necessária.

A *Deep Web* representa uma camada exponencial de dados e de informações não indexadas e acessadas, e uma pluralidade de materiais aquém de criminalidade, com qualidade substancial (Vignoli, 2014; Vignoli; Monteiro, 2015a, 2015b; Niemeier, 2016; Zilman, 2019). O que tem ocorrido, no entanto, é que os conteúdos da *Deep Web* permanecem camuflados, mas, uma vez indexados ou encontrados, a invisibilidade é dissipada.

A saber, para acessar conteúdos da *Deep Web*, o sujeito precisa conhecer ou encontrar a URL correta, cadastrar-se ou realizar pagamentos para acesso, ou, ainda, utilizar mecanismos de busca específicos para o ambiente. O *Duck Duck Go* é um mecanismo de busca que retorna resultados, sejam estes da superfície ou não, amparados em navegação anônima, o que é pautado na privacidade do indivíduo que busca informações (Duck Duck Go, c2019). Por não ser recuperada em mecanismos de busca comuns como *Google* ou *Bing*, por exemplo, a *Deep Web* estaria metaforicamente localizada abaixo da Superfície (Figura 1) e abrigaria diversas outras camadas ainda mais profundas e obscuras no ciberespaço, como a *Dark Web*.

[3] No original: "*You should, however, be aware that your daily life frequently involves the dark web in some way*".

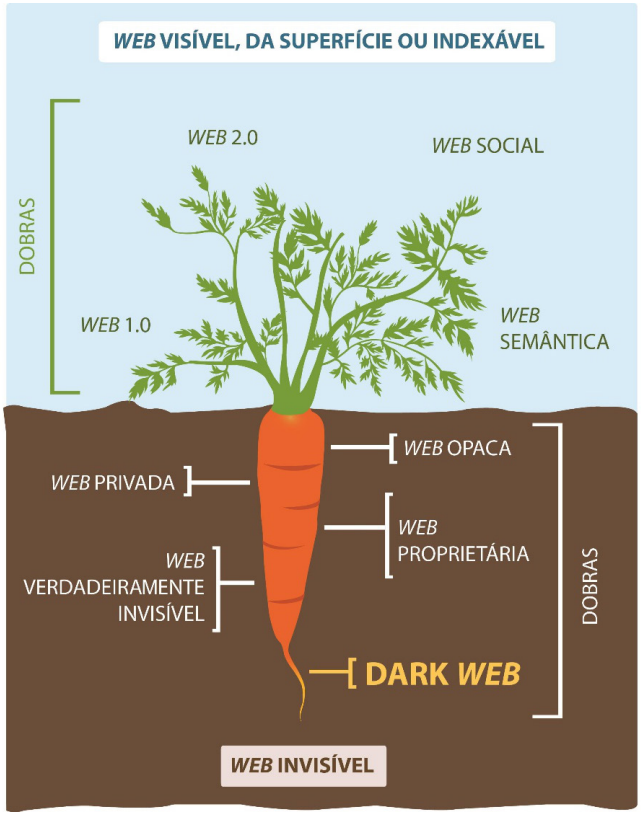


**Figura 1**. Dobras/camadas do ciberespaço: *Visible Web vs Inivisible Web*.
Fonte: Vignoli (2014).

## *A Dark Web*

A *Dark Web* ou *Web* Escura teve início com a tese de doutorado intitulada *Distributed Decentralised Information Storage and Retrieval System*, de Ian Clarke, na Edinburgh University em 1995 (Beckett, 2009). Mais adiante, precisamente em 2000, o *download* do *software* desenvolvido por Clarke foi nomeado de *Freenet* (Freenet, 2019), um programa gratuito de *proxy* que prevê acesso à *internet*, aos *websites*, aos *chats* ou ao compartilhamento de arquivos de forma anônima na rede. O *proxy* funciona como um intermediário entre computadores e *internet* ou entre usuários e servidores. Um *proxy* possibilita conexão de computadores locais com redes externas e "[...] impede que usuários externos acessem recursos existentes na rede interna ou saibam onde estão localizados." (Sawaya, 1999, p. 375). O *Freenet* teve, nos seus primeiros nove anos de existência, mais de dois milhões de *downloads*, principalmente na Europa e nos Estados Unidos da América (Beckett, 2009). A partir da tese de Clarke, foi possível a construção de uma rede paralela para acessar a *internet*, a *Web*, o ciberespaço e, essencialmente, a *Dark Web*.

Beckett (2009), Fulton e McGuinness (2016) e Hurlburt (2017) demonstram algumas nomenclaturas possivelmente encontradas para a *Dark Web*, como: (a) *Darknet* (*Net* escura); (b) *Deep Web* (*Web* profunda); (c) *Invisible Web* (*Web* invisível); (d) *Dark address space* (Espaço de endereço escuro); (e) *Murky address space* (Espaço de endereço sombrio); (f) *Dirty address space* (Espaço de endereço sujo).

A propósito das nomenclaturas, cada termo demonstrado pelos autores deve possuir suas próprias definições, nas quais se destacam a *Invisible Web* e a *Deep Web* (sinônimos com base na invisibilidade geral da *web*) e a *Darknet*, correspondente a um sinônimo de *Dark Web* e de redes de acesso às dobras *undergrounds*.

Para Atwood (2017), o conteúdo não pesquisável da *web* pode ser denominado *Deep Web*, *Dark Web*, *Invisible Web*, *Hidden Web* (*Web* escondida), *Dark Net* e *Black Web* (*Web* negra), mas o autor informa que, apesar das combinações entre os termos, somente a *Dark Web*, possível por meio de *proxy*, é a representação da *Web* verdadeiramente escura, assim como também para Fidencio e Monteiro (2013) e para Monteiro e Fidencio (2013).

Para Winkler e Gomes (2017, p. 73, tradução nossa)[4], "A *Dark Web* é aquela parte da *web* que se destina a ser anônima". Por conseguinte, Fidencio e Monteiro (2013, p. 692, grifo do autor) 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 Beckstrom e Lund (2019), a *Dark Web* representa um grupo coletivo de páginas da *Web* que só podem ser acessadas com uso de navegadores específicos (por meio de *proxy*). Com base nos autores, tanto a *Deep* quanto a *Dark Web* estão abaixo da superfície; no entanto, apesar de ser um desdobramento ou uma camada da *Deep Web*, a *Dark Web* é muito mais profunda e obscura, além de possuir sua gênese no anonimato, muitas vezes associado à ilegalidade.

Acerca disso, Hurlburt (2017) explica que o mercado subterrâneo é vasto o suficiente para conter seus próprios mecanismos de pesquisa, fóruns de comunidade e sistemas de classificação apenas com o www, além de sua própria moeda, os *bitcoins*. Estes foram aderidos em diversas movimentações comerciais legais e de maneira mundial, mas também se tornaram uma moeda facilitadora para transações comerciais ilegais, principalmente na *Dark Web*. Trata-se de uma moeda digital criptografada que dispensa formalidades, como conta bancária e/ou cartões de crédito (Bitcoin.Org, 2020), foi e é um recurso bem aceito essencialmente para aquisições de serviços e de produtos ilegais na *Deep* ou *Dark Web*. As informações registradas na cadeia de blocos (transações pela moeda) são os endereços de *bitcoin* do remetente e do destinatário, mas um endereço não identifica um *bitcoin* específico (Finklea, 2017).

A prerrogativa é que a *Dark Web* é uma *Web* ímpar, com suas peculiaridades e formas de acesso subjacentes. Nesta pesquisa, parte-se do pressuposto de que o acesso à *Dark Web* só é possível por meio de *proxy*, pois, do contrário, não se trata da mesma *Web*. Seus conteúdos só podem ser acessados por intermédio de *softwares* de *proxy* que camuflam o *Internet Protocol* (IP) de máquinas diversas e permitem adentramento ao ambiente.

Para compreensão mais clara, Hurlburt (2017) acentua que a *Dark Web* está embutida na *Deep Web*, em uma espécie de hierarquia entre as camadas do ciberespaço (Figura 1). Dessa forma, a *Dark Web* faz parte do escopo da *Deep Web* enquanto *Web* profunda, assim como é a própria *Deep*. Contudo, devido a sua relevante profundeza, a seu acesso realizado somente por meio de *proxy* e a seus conceitos e características distintos, trata-se, indiscutivelmente, de outra *Web*, da *Dark Web*.

A Figura 1 demonstra graficamente a *Visible* e a *Invisible Web*, além de outras denominações para *Web*, tanto da superfície quanto das camadas invisíveis. Para além das *Webs* mencionadas (Fidencio e Monteiro (2013), Monteiro e Fidencio (2013) e Vignoli e Monteiro (2015), a figura é utilizada para demonstrar, por meio do desenho de uma cenoura, a localização metafórica da *Deep* e da *Dark Web* no ciberespaço. Como é possível verificar, ambas estão abaixo da superfície, na terra, não facilmente visíveis. Entretanto, a *Deep Web* representa toda a camanda "enterrada" da leguminosa, e a *Dark Web* é ilustrada como a camada mais profunda do ciberespaço e da própria *Deep*.

Assim, considera-se que a Dark é uma *Web* ainda mais profunda e talvez a única verdadeiramente invisível (Fidencio; Monteiro, 2013; Monteiro; Fidencio, 2013). O rastreamento de quem a acessa é bastante dificultado devido aos processos de alta criptografia proeminentes no ambiente. Sobre a questão do rastreamento de usuários ou dos IP de seus computadores, Montieri *et al.* (2018) realizaram uma recente pesquisa com base no Traffic Classification dessas redes e concluíram que, embora o rastreamento seja extremamente difícil, a distinção entre as Redes de Anonimato utilizadas no ambiente é facilmente descoberta.

[4] No original: "*The dark web is that portion of the web that is intended to be anonymous*".

A falta de rastreamento, chamariz para a utilização da *Dark Web*, facilita a realização de crimes, mas proporciona, também, uma navegação tranquila, sem observadores em busca do melhor cliente para a aquisição de seus produtos e com elevada privacidade. Além disso, dificulta a espionagem e a invasão de privacidade recorrentes na superfície, bem como o conhecimento por parte das empresas sobre quem visita suas páginas, explica Heaven (2018). Winkler e Gomes (2017) acentuam que a camuflagem de IP em redes como o *The Onion Router* (TOR), por exemplo, não é perfeita, mas é razoável e cumpre o propósito prometido: ficar invisível na rede.

De todo modo, para acessar a *Dark Web*, são necessários *softwares* especializados em Redes Anônimas, com uso de *Anonymity Tools* (AT). As AT mais conhecidas para acesso à *Dark Web* são o *Tor*, o *Freenet*, o I2P e o *JonDonym* (anteriormente conhecido por JAP ou *Web-Mix*). Existem outras dezenas de AT, inclusive para dispositivos móveis, passíveis de *download* de forma simples, lícita e gratuita. As versões de AT para dispositivos móveis demonstram o avanço das redes escuras de forma rápida, além da crescente demanda por navegação privada e sigilosa. O *Orbot, software* de *proxy* da rede *Tor* já contabilizava, em abril de 2020, mais de 10 milhões de *downloads* no *Play Store* (The Tor Project, 2018). Navegar livremente no ciberespaço e em sua *Web* obscuras de forma móvel e privada parece ser uma tendência já palpável e em constante crescimento.

Após o *download* do *software* escolhido, a forma mais habitual e organizada de realizar pesquisas no ambiente tem sido por meio da *Hidden Wiki*, que lista diversos mecanismos de busca, escuros ou não, além de agrupar *hiperlinks* por temas. Beckstrom e Lund (2019) publicaram o livro *Casting L*: a *guide for safe exploration on the Dark Web*, que desempenha muito bem o papel de um verdadeiro e potente guia de acesso à *Dark Web*. No livro, os autores apresentam como utilizar o ambiente, navegar, recuperar informações, além de demonstrar endereços de sítios a serem visitados, e quais cuidados devem ser tomados em relação à segurança dos dados no acesso.

Alguns dos mecanismos de busca mais comuns da *Dark Web* são o *Torch*, o *Duck Duck Go* (se acessado na *Dark*, recuperará conteúdos ainda mais escondidos e sob o domínio da Rede de Anonimato escolhida), o Ahmia.if, entre muitos outros operantes na rede cuja interface é parecida com a do *Google*, por exemplo. Diversos mecanismos de busca da *Dark Web* podem ser acessados na superfície, no entanto, os resultados de busca obviamente não serão os mesmos. A navegação, para que possa ser segura, pode se tornar muito lenta devido às tecnologias empregadas para esse fim.

Diferentemente da *Deep Web*, na *Dark Web* é possível encontrar arquivos com dimensões muito variadas, como 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 e arquivos com formatos ainda não reconhecidos. Como nada na *Dark Web* é indexado (convencionalmente), qualquer tipo de formato pode ser utilizado para publicar e compartilhar conteúdos no ambiente, que possui autonomia até mesmo nas mídias e formatos das informações. *Hackers* e especialistas de alta tecnologia utilizam e projetam formatos e mídias especificamente para o ambiente que operam como um laboratório para novos produtos.

Para Monteiro e Fidencio (2013), o conteúdo da *Dark Web* permanece na invisibilidade, na maioria das vezes, porque seus materiais são judicialmente ilegais. Contudo, a ilegalidade não a representa em sua totalidade. Hurlburt (2017) explica que a *Dark Web* é imensa e que sua maior fração é relativamente benigna, mas sua notoriedade é destacada devido a lugares em que bens e serviços ilegais são vendidos a qualquer pessoa que deseje pagar o preço e assumir o risco.

Chen (2012) possui uma visão esvaziadora da *Dark Web*, porque a define como se sua existência se baseasse no terrorismo, no roubo de identidade, em vendas e na distribuição de *softwares* piratas, ou como meio de comunicação e refúgio para grupos extremistas e de ódio. Contudo, acredita-se que as afirmações de Chen (2012) sejam arbitrárias, visto que os crimes descritos pelo autor também ocorrem e sempre ocorreram na *Web* da superfície.

Em contrapartida, não se pode subestimar a importância da falta de rastreamento dos sujeitos e de seus computadores como agente facilitador para pessoas que desejam cometer crimes. Vignoli e Monteiro (2015b) demonstram o que pode ser encontrado na *Dark Web*: crimes bancários; tráfico de armas, de drogas e de animais; contrabandos; falsificações de identidades, de passaporte, de dinheiro, de trabalhos acadêmicos e/ou de diplomas; contratação de assassinos; vídeos e contatos para pedofilia e necrofilia, entre muitas outras situações desumanas e ilegais.

Apesar disso, é indiscutível a possibilidade de uma navegação livre para outros fins, como para a discussão de grupos diversos que não desejam ser observados, jornalistas com suas reportagens secretas, pesquisadores com dados inéditos, *etc*. O ambiente da *Dark Web* pode ser utilizado igualmente para burlar a censura, para acessar conteúdos bloqueados e para manter a privacidade de comunicações ou de planos de negócios confidenciais. Os indivíduos podem procurar um porto seguro para discutir questões particulares, como vitimização ou doenças físicas ou mentais. Eles também podem usar o *Tor* para proteger seus filhos *online*, ocultando os endereços IP nas atividades das crianças (Finklea, 2017).

Heaven (2018) explica que, para cada ato nefasto ocorrido na *Dark Web*, há, por outro lado, um benéfico. O autor cita a participação de importantes jornais como o *The New York Times* e o *The Guardian* que, por meio de seus perfis na rede escura, possibilitam a realização de *uploads* de documentos sigilosos e denunciativos que podem fundamentar reportagens renomadas e úteis à sociedade.

Temas muito discutidos na *Dark Web* envolvem denúncias de governos criminosos, política no geral, teorias da conspiração, entre outros assuntos, não somente relacionados à criminalidade virtual. Muitas pessoas residentes em países sem liberdade de expressão encontram refúgio na *Dark Web* para se comunicar ou acessar conteúdos proibidos por seus governantes, acentua Heaven (2018). L'Huillier *et al.* (2010) também definem a *Dark Web* como local baseado em fóruns ou em plataformas de terroristas ou cibercriminosos. Todavia, os autores mencionam que o ambiente escuro é igualmente povoado por fã-clubes de artistas ou comunidades que preferem a comunicação livre. Hulrburt (2017) evidencia que a *Dark Web* é capaz de atingir a economia global por meio do expansivo *e-commerce* ilegal movimentado por *bitcoins* e que empresas gastam milhares de dólares por ano para se prevenir contra roubo de informações provenientes do ambiente. Para East (2017), os ambientes da *Dark Web* são propícios para uma verdadeira economia liberal, não controlada pelos governos, uma tendência contemporânea.

Atwood (2017) demonstra outros pontos notáveis da *Dark Web*, como a liberdade de uma navegação limpa, na qual governos ou empresas não possam espionar o que os indivíduos fazem *on-line* ou redirecionar propagandas involuntárias. Segundo o autor, é na própria rede escura que novas técnicas e tecnologias são desenvolvidas para a proteção de dados no ciberespaço. Mas não se pode negar que a *Dark Web* é uma grande propagadora de Dados Sensíveis comercializáveis. Há sempre o bem e o mal na *Dark Web* (Vignoli, 2014; Vignoli; Monteiro, 2015b), já que existem *hackers* que auxiliam no desenvolvimento de recursos tecnológicos para a prevenção de crimes e os que se preocupam com inovações tecnológicas para não serem identificados e punidos.

Em outro momento, Atwood (2017) informa que os Estados Unidos da América já investiram quantias consideráveis para que a rede *Tor* elabore técnicas de espionagem ainda mais seguras para a proteção de movimentos democráticos em regimes autoritários. De qualquer modo, se uma nação deseja que suas informações sejam protegidas, provavelmente utilizará a rede escura para atingir seus objetivos. Segundo Fidencio e Monteiro (2013, p. 693, grifo do autor), "[...] 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, e nem sempre estarão guiadas para atos ilícitos. Essa pressuposição deve acompanhar o conceito da camada mais incompreendida do ciberespaço, pois nem todo o seu conteúdo deve ser compreendido como ilícito. Não obstante, desejar uma navegação segura, não espionável nem invasiva, não é crime.

Para Everett (2009) a *Dark Web* representa redes que compreendem múltiplos servidores escuros, 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*. 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 judicialmente amorfo. Hurlburt (2017) evidencia que na *Dark Web* existem Redes Sociais advindas do ambiente e que também é possível acessar as redes da superfície com privacidade, como *Facebook, Twitter, Youtube*, entre outras. Regras para uso e acesso de páginas, seja na superfície ou em *websites* escuros, na maioria das vezes não se aplicam à *Dark Web*.

Também por meio da *Dark Web*, muitos criminosos já foram encontrados e punidos de acordo com a gravidade de seus crimes e com a legislação de cada país. As redes de pedofilia são destaque nesse aspecto, pois se o ambiente é propício para esse tipo nefasto de crime, há os que utilizam a própria rede anônima para denunciar atrocidades. Assim, o *Federal Bureau of Investigation* e polícias federais monitoram a rede já há algum tempo, na tentativa de encontrar quadrilhas e criminosos.

Todas as conceituações e os termos encontrados na *Web* ou na literatura perpetuam a dificuldade em se desmitificar a *Dark Web* e a necessidade disso. A esse respeito, Monteiro e Fidencio (2013, p. 37, grifo do autor) 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 sob anonimato fazem a dobra underground do ciberespaço".

Diante desse cenário, conceitua-se que a *Dark Web*, possível somente por meio de *proxy*, é composta por conteúdos não indexáveis por mecanismos de busca convencionais, por motivos legais e porque eles simplesmente não conseguem indexar. Igualmente, acredita-se que a *Dark Web* representa a *Web* verdadeiramente livre e que, apesar de utilizada também para o mal, exerce a liberdade de navegação, de expressão e de comunicação.

A filosofia da *Dark Web* é ser livre, e navegar em seu ambiente é lidar com a liberdade de expressão sob o anonimato, representando o que o ser humano pensa e faz de forma vítrea, tanto para o bem quanto para o mal.

## Considerações Finais

Procurou-se distinguir as duas *Webs, Deep* e *Dark*, de maneira a elucidar seus conceitos, suas denominações, seus conteúdos e suas formas de acesso, além de sua localização metafórica no ciberespaço (Figura 1). Dessa forma, as principais disparidades entre a *Deep* e a *Dark Web* são: o termo *Deep Web* é confundido e ocasionalmente definido como sinônimo de *Dark Web* e de outras *Webs* e vice-versa; a *Deep Web* possui dimensão astronômica, que pode representar 96% de todo o ciberespaço, porém a *Dark Web* totalizaria apenas 6%; metaforicamente, no ciberespaço, a *Deep Web* está representada logo abaixo da superfície, e a *Dark Web* seria a camada mais profunda do ciberespaço; os conteúdos da *Deep Web* podem ser indexados, mas os da *Dark Web* provavelmente nunca serão; os conteúdos da *Deep Web* não são indexados por diversos motivos, inclusive técnicos, já os da *Dark Web* são (em muitos casos) escondidos intencionalmente; a *Deep Web* não costuma possuir variedade de formatos ou mídias substanciais em seus conteúdos, já na *Dark Web* são encontrados formatos e mídias muito distintos ou, até mesmo, desconhecidos; para acessar a *Deep Web* basta possuir a URL, *login*, senha ou realizar pagamento, por exemplo, mas, para acessar a *Dark Web*, é necessário o *download* de *proxy*, normalmente gratuito; na *Deep Web*, pode ocorrer a camuflagem do IP, mas, na *Dark Web*, a camuflagem é uma prerrogativa para acesso ao ambiente; a *Deep Web* é considerada como *Web* invisível, a *Dark Web*, como a verdadeiramente invisível.

Quanto às similaridades encontradas entre a *Deep* e a *Dark Web*, as principais são: ambas se localizam abaixo da superfície (*Surface Web/Visible Web*); representam mais uma camada (dobra) do ciberespaço; seus conteúdos não são indexados; possuem conteúdos com alto teor de qualidade; são consideradas como *Webs* invisíveis;

são comumente vistas com teor sujo e ilícito; representam camadas exponenciais do ciberespaço, muito pouco acessadas em relação à superfície; são camadas/dobras distintas do ciberespaço; podem ser objetos profícuos para investigações científicas, inclusive na CI.

Como visto, as diferenças se sobrepõem às semelhanças de uma *Web* e outra. Porém, o que mais distancia a *Deep Web* da *Dark Web* é, sem dúvida, a forma de acesso. De todo modo, ambas possuem potencial e motivos benéficos para acesso e reconhecimento, essencialmente científico.

A definição da *Deep Web* está associada a páginas não indexadas por diversos motivos e a conteúdos muito diversos, que também podem ser ilícitos, mas não representam toda essa camada do ciberespaço. Foi possível perceber que a invisibilidade da *Deep Web* pode ser temporária, pois o cadastro, o conhecimento da URL de uma página ou, ainda, o uso de mecanismos específicos para a navegação pode tornar a informação visível e disponível.

A *Dark Web*, camada apresentada normalmente na ilegalidade, expande suas definições arbitrárias em prol da navegação livre, privada e segura, e da descoberta de conteúdos lícitos. Em verdade, a *Dark Web* proporciona novos olhares à navegação para lazer, trabalho ou pesquisa. Muitas possibilidades se abrem aos sujeitos e à própria CI, que facilmente poderão abrigar a desmitificação e a valorização da *Dark Web* como objeto de estudo a ser amplamente explorado. Sua filosofia é outra: é pungente e, em momentos, arbitrária, mas necessária para a verdadeira liberdade de navegação e de expressão em toda a rede.

Espera-se que o aprofundamento de cada *Web*, assim como de suas peculiaridades, e sua representação visual (no desenho da cenoura) tenham sido demonstradas com clareza para que outras pesquisas a respeito da temática, pouco difundida na CI, possam ser realizadas.

Como pesquisa futura na *Deep Web*, poder-se-ão realizar estudos aplicados para identificar materiais acadêmicos porventura obscuros, a fim de propor difusão dessas informações, o que é pertinente à CI e a seus profissionais e pesquisadores. Outro estudo capital para a *Deep Web* poderá se dar no aprofundamento de mecanismos de busca especializados para o ambiente.

Como próximo trabalho com foco na *Dark Web*, pretende-se desenvolver estudos aprimorados a respeito das AT (*Anonymity Tools*) para *mobile*, com o intuito de verificar como a informação escura navega em serviços e em tecnologias móveis. A investigação para a localização de Bases de Dados científicas também se apresenta como tema promissor a novos estudos com foco para a CI.

Muitas outras possibilidades de pesquisas básicas ou aplicadas podem ser realizadas, no que se refere à *Deep* ou à *Dark Web* e no contexto da CI. O ciberespaço é imenso, assim como as possibilidades, e cabe à CI e a seus estudiosos se beneficiarem de todas as oportunidades científicas desses ambientes escuros, porém não perversos.

## Colaboradores

R. G. VIGNOLI e S. D. MONTEIRO participaram em todas as etapas de produção do artigo.

# Referências

Association of Internet Research Specialist. Ontario: Government of Canada. Available from: https://www.airsassociation.org/. Access on: Jul. 27 2020.

Atwood, M. The dark dialect: every aspect of human technology has a dark side, including the bow and arrow. *IEEE Espectrum*, New York, 22 Oct. 2017. Available from: https://s2.smu.edu/~fmoore/misc/IEEE-Spectrum-The-Dark-Dialect-Oct-2017.pdf. Access on: Apr. 25 2020.

Beckett, A. The dark side of the internet: in the deep web, Freenet software allows users complete anonymity as they share viruses, criminal contacts and child pornography. *The Gardian*, London, 26 Nov. 2009. Available from: http://www.guardian.co.uk/technology/2009/nov/26/dark-side-internet-freenet. Access on: Apr. 23 2020.

Beckstrom, M.; Lund, B. *Casting L*: a guide for safe exploration on the Dark Web. New York: Rowman & Littlefield Publishers, 2019.

Bergman, M. K. White paper: the deep web surfacing hidden value. *Journal of Eletronic Publishing*, v. 7, n. 1, 2001. http://dx.doi.org/10.3998/3336451.0007.104.

Bitcoin.org. Bitcoin para Pessoas Físicas. *Bitcoin.org.*, [*S.l.*], 2020. Disponível em: https://bitcoin.org/pt_BR/bitcoin-para-pessoas. Acesso em: 23 abr. 2020.

Brasil. *Lei n° 13.709, de 15 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei n° 12.965 de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 22 abr. 2020.

Céndon, B. V. Ferramentas de busca na web. *Ciência da Informação*, v. 30, n. 1, p. 39-49, 2001. Disponível em: http://www.scielo.br/pdf/ci/v30n1/a06v30n1. Acesso em: 23 abr. 2020.

Chen, H. Dark web: exploring and data mining the dark side of the web. New York: Springer, 2012.

Dark Web (darknet) *In*: WhatIs.com. Newton: WhatIs, 2019. Available from https://whatis.techtarget.com/definition/dark-web. Access on: Apr. 23 2020.

Duck Duck Go. *A ferramenta de busca que não rastreia você*. [*S.l.*], c2019. Disponível em: https://duckduckgo.com. Acesso em: 24 abr. 2020.

East, C. S. Demystifying the Dark Web. *ItNow*, v. 59, n. 1, p. 16-17, 2017. Doi: https://doi.org/10.1093/itnow/bwx007.

Everett, C. Moving across to the dark side. *Network Security*, v. 2009, n. 9, p. 10-12, 2009. Doi: https://doi.org/10.1016/S1353-4858(09)70099-6.

Fidencio, M. V.; Monteiro, S. D. Web invisível: compreendendo a invisibilidade no ciberespaço. *In*: Seminário em Ciência da Informação, 5., 2013, Londrina. *Anais* [...]. Londrina: Universidade Estadual de Londrina, 2013. p. 683-700. Disponível em: http://www.uel.br/eventos/cinf/index.php/secin2013/secin2013/paper/view/107. Acesso em: 25 abr. 2020.

Finklea, F. *Dark Web*. Washington: Congressional Research Service, 2017. Available from: https://fas.org/sgp/crs/misc/R44101.pdf. Access on: Apr. 22 2020.

Freenet. *Browse websites, post on forums, and publish files within Freenet with strong privacy protections*. [*S.l.*], 2019. Available from: https://freenetproject.org/author/freenet-project-inc.html/. Access on: Apr. 22 2020.

Fulton, C.; McGuinness, C. In too deep. *In*: Fulton, C.; McGuinness, C. (Org.). *Digital detectives*: solving information dilemmas in an on-line world. New Deli: Elsevier, 2016, p. 95-118. Doi: https://doi.org/10.1016/B978-0-08-100124-0.00007-6.

Heaven, D. Unpicking the mythologies around the dark web. *NewScientist*, v. 240, n. 3209-3210, p. 82-83, 2018. Doi: https://doi.org/10.1016/S0262-4079(18)32375-3.

Hurlburt, G. Shining light on the dark web. *Computer*, v. 50, n. 4, p. 100-105, 2017. Doi: https://doi.org/10.1109/MC.2017.110.

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. Doi: https://doi.org/10.1145/1938606.1938615.

Monteiro, S. D. Por uma cartografia conceitual da Web invisível: a dobra oculta do ciberespaço. *Informação & Sociedade*: *Estudos*, v. 23, n. 3, p. 23-31. 2013. Doi: https://doi.org/10.1590/S0103-37862013000100004.

Monteiro, S. D.; Fidencio, M. V. As dobras semióticas do ciberespaço: da web visível à invisível. *TransInformação*, v. 1, n. 25, p. 35-46, 2013. Doi: https://doi.org/10.1590/S0103-37862013000100004.

Montieri, A. *et al.* Anonymity services, Tor, I2p, Jondonym: classifyng in the Dark (Web). *In*: International Teletraffic Congress, 29., 2017, Paris. *Proceedings* […] New York: IEEE Xplore, 2017. Doi: https://doi.org/10.23919/ITC.2017.8064342.

Niemeier, C. Rolling in the deep not dark web: tips for accessing and searching the hidden web. *Aall Spectrum*, v. 20, n. 6, p. 22-25, 2016. Available from: http://epubs.aallnet.org/i/695274-aall-spectrum-july-august-2016-volume-20-number-6/23? Access on: Apr. 23 2020.

Sawaya, M. R. *Dicionário de informática e internet*. São Paulo: Nobel, 1999. 545 p.

Sherman, C.; Price, G. *The invisible web*: uncovering information sources: searches engines cant´s see. Medford: Cyberage Books, 2001.

The Tor Project. Orbot Proxy com Tor. Versão 16.0.5-RC-2-tor-0.3.4.9. [*S.l.*]: Guardian Project, 2018. Acesso em: 23 abr. 2020.

Vignoli, R. G. *A topografia da dark web e seus não lugares*: por um estudo das dobras invisíveis do ciberespaço. 2014. 153 f. Dissertação (Mestrado em Ciência da Informação) – Universidade Estadual de Londrina, Londrina, 2014. Disponível em: http://www.bibliotecadigital.uel.br/document/?view=vtls000191992. Acesso em: 23 abr. 2020.

Vignoli, R. G.; Vechiato, F. L. Dados pessoais, dados sensíveis e dados pessoais sensíveis: um contributo conceitual para a Ciência da Informação. *In*: Farias, G. B.; Farias, M. G. G. (Org.). *Competência e mediação da informação*: percepções dialógicas entre ambientes abertos e científicos. São Paulo: Abecin, 2019. Disponivel em: http://www.abecin.org.br/e-books/. Acesso em: 11 maio 2020.

Vignoli, R. G.; Monteiro, S. D. A Dark Web e seu conteúdo informacional. *In*: Seminário de Ciência da Informação, 5., 2015, Londrina. *Anais eletrônicos* […] Londrina: UEL, 2015a. Disponível em: http://www.uel.br/eventos/cinf/index.php/secin2016/secin2016/paper/viewFile/266/186. Acesso em: 8 jun. 2019.

Vignoli, R. G.; Monteiro, S. D. Dark Web e seus não lugares: por um estudo das dobras invisíveis do ciberespaço. *Liinc em Revista*, v. 11, n. 1, p. 140-166, 2015b. Doi: https://doi.org/10.18617/liinc.v11i1.798.

Winkler, I.; Gomes, A. T. Adversary infrastructure. *In*: Winkler, I.; Gomes, A. T. (Org.). *Advanced persistent security*: a cyberwarfare approach to implementing adaptive enterprise protection, detection, and reaction strategies. New Deli: Elsevier, 2017. p. 67-79. Doi: https://doi.org/10.1016/B978-0-12-809316-0.00007-5.

Zilman, M. P. Deep Web research and discovery resources 2019. *Law and Technology Resources for Legal Professionls*, [*S.l.*], 2019. Available from: https://www.llrx.com/2019/01/deep-web-research-and-discovery-resources-2019/. Access on: Apr. 23 2020.