

A DUALIDADE DA DEEP WEB

Caique Arthur Lopes da Silva Martins¹
Maria Helena Barriviera e Silva²

Tecnologia em Análise e Desenvolvimento de Sistemas
Faculdade de Tecnologia de Garça (FATEC)
Caixa Postal 17400-000 – Garça – SP – Brasil

`caique.martins@fatec.sp.gov.br`
`mhelena@fatecgarca.edu.br`

Abstract: *The deep Web (also called deep web, darknet, invisible web, hidden web, Tor network, and other variants) is characterized as a layer of the internet (or web surface) that can't be accessed so commonplace and as usual most people do daily. To access the deep web content it is necessary to use specific software and very good sense, it is possible to find topics of excellent quality and also the worst conceivable level. Thus, this article includes information on the deep web and its duality, ie the positive side and the negative side.*

Key-words: *Surface web. Deep web. TOR. Bitcoin.*

Resumo: A *deep web* (também denominada de *web* profunda, *darknet*, *web* invisível, *web* oculta, rede Tor, além de outras variantes) caracteriza-se como uma camada da *internet* (ou *surface web*) que não pode ser acessada de forma corriqueira e usual como a maioria das pessoas faz diariamente. Para acessar o conteúdo da *web* profunda faz-se necessário o uso de *software* específico e muito bom senso, pois é possível encontrar temáticas de excelente qualidade e também do pior nível imaginável. Assim este artigo contempla informações sobre a *deep web* e sobre a sua dualidade, ou seja, o lado positivo e o lado negativo.

Palavras-chave: *Surface web. Deep web. TOR. Bitcoin.*

1 Introdução

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

¹ Discente do curso de Tecnologia em Análise e Desenvolvimento de Sistemas na Faculdade de Tecnologia de Garça.

² Docente dos cursos de Tecnologia em Análise e Desenvolvimento de Sistemas e Tecnologia em Gestão Empresarial na Faculdade de Tecnologia de Garça. Mestre em Ciência da Computação pela Universidade de São Paulo *campus* São Carlos (USP/São Carlos).

Porém, a *internet* conhecida pela grande maioria é apenas parte do espaço virtual existente: “abaixo” dela existe uma “outra *internet*”, conhecida principalmente como *deep web*. Na verdade, esta última é constituída pelo conteúdo invisível aos buscadores comumente utilizados na *surface web*. Conhecedores da *web* oculta afirmam que a *surface web* detêm apenas 10% do total de conteúdo da grande rede, enquanto que os 90% restantes pertencem a esta camada “mais baixa” (PEREIRA, 2013-a), porém esses valores não são exatos, e muitas vezes mostram-se contraditórios. Por exemplo, Anonymous Brasil (2013) afirma que a *web* profunda representa de 70 a 75% do total do conteúdo da *internet*, ou seja, cerca de um trilhão de páginas não indexadas nos buscadores da *surface web*, e Mello (2013) afirma que “há quem diga que o Google só consegue rastrear 1% do que existe online. Os outros 99% estariam na chamada Deep Web”.

Existe também uma dualidade com relação ao teor do conteúdo da *web* invisível: de acordo com Estimulanet.com (2013), a *deep web* é um lugar misterioso, impossível de ser acessado por qualquer navegador e que ao acessa-la, o usuário pode estar na mira de investigações policiais, ser atacado por *hackers*, cair em *sites* com conteúdos proibidos de luxúria, depravação e psicopatias. Em contrapartida, Kohn (2013) ressalta a segurança e a privacidade da mesma, destacando-a como um local ideal para, por exemplo, armazenar bases de dados organizacionais que não estão em uso.

Assim, tem-se como objetivo principal um estudo detalhado sobre a *deep web* e suas características positivas e negativas, como forma de elucidação de mitos que acompanham o assunto, e de esclarecimentos sobre os reais riscos envolvidos nesse ambiente de navegação. Este artigo é resultante dos primeiros estudos sobre o tema, e contempla uma abordagem, ainda superficial, ao caráter da *web* profunda em relação à sua dualidade: o lado positivo *versus* o lado negativo. Desta forma, objetiva-se o aprofundamento nos estudos relacionados ao tema e a futura publicação de outros artigos com conteúdo mais avançado e específico. A justificativa para este estudo é a ausência de abordagens sobre o tema no formato de livros ou artigos científicos, bem como o crescente interesse sobre o assunto principalmente nos meios acadêmicos.

2 A Deep Web

A *deep web* caracteriza-se como o conjunto de conteúdos da *internet* que não podem ser acessados diretamente pelos mecanismos de busca normalmente utilizados no dia a dia, como por exemplo, o *Google*, pelo simples fato de não serem indexados por este mecanismo de busca.

Os motivos pelos quais esses conteúdos não são indexados são variados. Pode ser por opção de privacidade do próprio dono do *site*; por se caracterizar como conteúdo privado, sendo acessível somente com *login* e senha; por ser *internet* contextualizada, ou seja, de acordo com o *Intenet Protocol* (IP) apresentar conteúdos diferentes; ou por violação das regras dos buscadores, uma vez que, dentro dos motores de busca, existem vários fatores que categorizam um *site* como impróprio, o que pode ocasionar a penalização do mesmo. Esses fatores podem ser: conteúdo ofensivo e/ou duplicado, utilização de textos e imagens com direitos autorais, acessos não autorizados e acessos a informações confidenciais, dentre outros (AGRIPINO, 2013).

Quando pessoas ou organizações utilizam a *deep web* objetivando privacidade, elas podem ter motivação lícita, como por exemplo, a proteção de bases de dados organizacionais de *hackers* que utilizam a *surface web*, ou ilícitas, como por exemplo, quando pretendem realizar práticas ilegais, condenáveis ou bizarras, como acesso a informações sobre pedofilia ou comércio de drogas.

De acordo com Agripino (2013), os *browsers* comuns, utilizados pela maioria dos usuários da grande rede no dia a dia, como o *Google Chrome* e *Internet Explorer*, dentre outros, não são recomendados para navegar na *web* profunda, pois revelam a identidade do usuário através da identificação do endereço IP utilizado para o acesso.

O projeto TOR, inicialmente um acrônimo de *The Onion Routing*, e com outras propostas iniciais de uso (desenvolvido pelo Laboratório de Pesquisas da Marinha dos Estados Unidos), e que em 2006 foi transformado em Organização Não Governamental (ONG), “consiste em uma rede de túneis escondidos na *internet* em que todos ficam quase invisíveis” (PEREIRA, 2013-a).

Ainda segundo Pereira (2013-a):

Ao acessar um *site* normalmente, seu computador se conecta a um servidor que consegue identificar o IP; com o Tor isso não acontece, pois, antes que sua requisição chegue ao servidor, entra em cena uma rede anônima de computadores que fazem pontes criptografadas até o *site* desejado. Por isso, é possível identificar o IP que chegou ao destinatário, mas não a máquina anterior, nem a anterior, nem a anterior etc. Chegar no usuário, então, é praticamente impossível.

No *site* do projeto TOR é possível encontrar ferramentas que possibilitem um acesso mais seguro à *deep web*, como a versão portátil do *Firefox* já configurada para acesso anônimo e que não exige instalação. Vale ressaltar que a preocupação com segurança acaba ocasionando lentidão, pois, como já citado anteriormente, uma solicitação de acesso pode passar por diversos computadores/servidores, até mesmo em continentes diferentes, para depois ser enviado ao endereço IP destino.

Outra característica da *web* profunda é que os endereços *Uniform Resource Locator* (URL) mudam constantemente para não serem achados. Pode-se destacar também que a maioria dos *sites* tem o “.onion” no meio do URL pelo fato da utilização do TOR, mas existem *scripts* que configuram o navegador para que ele abra outras extensões, como forma de driblar o monitoramento da *surface web* (PEREIRA, 2013-a).

2.1 O lado positivo da *deep web*

Segundo Kohn (2013), um dos buscadores da *web* profunda é o *Torch*. Com a ajuda deste mecanismo de busca é possível encontrar serviços de mensagens instantâneas e bibliotecas com livros raros sobre religião, psicologia e outros assuntos curiosos, além de acervos de músicas e filmes, porém, todos sem procedência. Por este motivo ressalta-se a necessidade de cuidado com as palavras e atenção com os *links* listados nos resultados de busca. É possível também encontrar fóruns de discussões que vão desde política internacional até técnicas de programação, porém todos precisam de cadastro, que pode ser feitos gratuitamente pelo *Tor Mail*, serviço dotado de encriptação e segurança máxima.

Agripino (2013) destaca alguns mecanismos de busca da *deep web*, os quais apresentam como característica a especificidade a determinados assuntos: o *InfoMine* é um mecanismo de busca específico para conteúdo de bibliotecas universitárias norte-americanas, entre elas a Universidade da Califórnia; o *Intute* permite acesso ao conteúdo de todas as universidades da Inglaterra; o *Compleat Planet* dá acesso a assuntos diversos, como militares, comidas ou meteorologia para agricultores; o *IncyWincy* possui busca por imagens; o *DeepWebTech* permite acesso a temas como medicina, negócios e ciências; o *Scirus* é direcionado para assuntos científicos, como jornais, *homepages* de cientistas, materiais didáticos e patentes; o *TechXtra* é direcionado para áreas exatas, como matemática, engenharia e computação; e o *Hidden Wiki*, que é o mais famoso, é direcionado ao conteúdo mais agressivo, como por exemplo, pornografia, pedofilia, tráfico de drogas e venda de armas.

Há também aqueles que usam a *web* invisível para armazenar informações que não precisam gerar tráfego, como por exemplo, resultados parciais de pesquisas, e o simples armazenamento de bases de dados organizacionais que não estão sendo utilizadas no momento.

Assim como na *surface web*, também existe o consenso de que na *deep web* é possível encontrar todo tipo de informação, ficando a critério do usuário a seleção.

2.1 O lado negativo da *deep web*

Obviamente, a *web* profunda, por se caracterizar como um ambiente reservado, também chama a atenção de criminosos pelo fato de não poderem ser rastreados, destacando-se a facilidade de encontrar informações e conteúdos como contrabandos, drogas, pedofilia, armas etc, conforme ilustra a Figura 1.

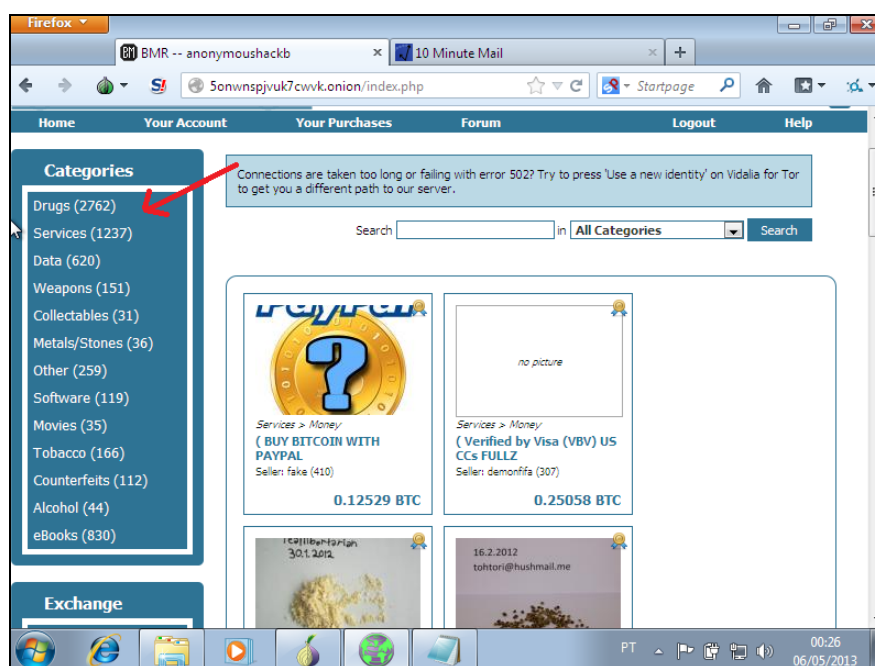


Figura 1: Categorias de itens disponíveis para comércio na *deep web*

De acordo com Kohn (2013):

Com a alta privacidade, a *deep web* atraiu grupos famosos. O *Wikileaks* e o *Anonymous*, por exemplo, refugiaram documentos sigilosos ali. E alguns revolucionários, que participaram da Primavera Árabe, usaram a rede paralela para facilitar a articulação dos rebeldes e complicar o trabalho da inteligência policial. Jornalistas, militares e políticos também se comunicam pela teia misteriosa e acobertam suas ações na rede – o que a torna um local muito mais rico em informações do que se imagina ou é comentado.

Como citado por Kohn (2013), o *Hidden Wiki* é o caminho mais conhecido para o conteúdo mais agressivo. Através desse mecanismo de busca é possível encontrar todo tipo de oferta de serviços e/ou comercialização de itens, desde os mais bizarros até os mais condenáveis, como por exemplo, *sites* de comercialização de conteúdo acerca de parafilias, a saber: pedofilia, necrofilia e zoofilia, dentre outros.

Segundo Pereira (2013-b), algumas páginas da *darknet*:

[...] ao serem carregadas, revelavam nada mais do que uma imagem estática, ou uma porção de códigos ininteligíveis, ou, então, nada. Às vezes recarrega o endereço e a página simplesmente não existe mais. Há muito disso na *deep web*, principalmente quando se trata de conteúdo inapropriado [...]

Esse tipo de ação é feito propositalmente para proteger tanto quem publica quanto quem foi parar por ali, muitas vezes, por acaso. Sobre esse procedimento, Pereira (2013-b) complementa que:

Há, sim, *links* que chegam facilmente a conteúdo pouco usual, mas a maioria do material está bem escondida por esse esquema de camadas. Quando você se depara com uma página aparentemente sem sentido, provavelmente há algo a mais para ser mostrado, mas que só pode ser acessado com a chave certa - que pode ser, por exemplo, uma letra ou um número diferente na URL. E nem sempre basta passar da primeira camada para chegar ao conteúdo; há quem diga que existem *sites* com até oito páginas falsas na frente.

Além de conteúdos inapropriados e extremistas como canibalismo, tráfico humano, turismo sexual, terrorismo e nazismo, dentre tantos outros, destacam-se o comércio de armas de fogo e de produtos roubados, além do tráfico de drogas. Assassinos de aluguel e “cybercriminosos” também oferecem seus serviços na *web* profunda. A comercialização de documentos falsos também é possível (PEREIRA, 2013-b).

Na *darknet* as transações são realizadas com a utilização do *Bitcoin*, que é uma moeda digital que torna as transações mais seguras e garante o anonimato. Segundo Bitcoin Brasil (2013), essa moeda digital é obtida em um procedimento chamado “garimpar”, promovido pela rede *Bitcoin*, onde a mesma cria e distribui lotes de *bitcoins* novas aproximadamente a cada 10 minutos, de maneira aleatória, entre os usuários que estão rodando no modo de “geração de moedas”. A quantidade de *bitcoins* que cada usuário recebe é diretamente proporcional ao poder de processamento de sua máquina

em contribuição para a rede, ou seja, o usuário empresta poder de processamento em troca de *bitcoins*. Pereira (2013-b) afirma que, nos Estados Unidos, é possível comercializar produtos como celulares, computadores, armas de fogo e até mesmo carros – tudo de procedência duvidosa – utilizando *bitcoins*.

3 Considerações finais

Conclui-se que a *deep web* é, basicamente, uma parte obscura da grande rede. Essa afirmativa, muitas vezes não é novidade para os iniciados nos assuntos de *internet*, porém, muita gente ainda ignora que esses conteúdos existam.

O conteúdo da *web* profunda é, de certa forma, protegido, podendo ser acessado somente por *browsers* específicos, e o usuário precisa se preocupar com a segurança, visto que está propenso a todo tipo de ação, desde a infecção de seu equipamento por vírus, até invasões *hackers*, além da possibilidade de acessar conteúdos indesejados. De forma semelhante, ela pode também disponibilizar conteúdo de excelência, como o acesso a bibliotecas e a material de universidades reconhecidas mundialmente. Obviamente, a escolha com relação a qual conteúdo acessar é do usuário.

No que diz respeito a trabalhos futuros, novas pesquisas estão sendo realizadas visando apontar quais os melhores *softwares* (*browser*, antivírus, *firewall* etc) e configuração ideal dos mesmos para acesso seguro a essa camada da rede. Outro tópico de pesquisa diz respeito ao *bitcoin*, suas formas de aquisição e utilização na *deep web*. A utilização da *web* profunda como local de investigações pelas agências de segurança também será contemplada em novos estudos.

Referências

AGRIPINO, Caroline. Deep web, a internet que o Google não vê. 2012. Disponível em: <<http://www.enlinkbuilding.com.br/blog/deep-web-a-internet-que-o-google-nao-ve/>>. Acesso em: maio/2013.

ANONYMOUS BRASIL. Deep Web: Entenda. 2013. Disponível em: <<http://www.anonymousbr4sil.com/2013/04/deep-web-entenda-e-acesse.html>>. Acesso em: abr/2013.

BITCOIN BRASIL. O que é Bitcoin? Disponível em: <<http://bitcoin-brasil.com/o-que-e-bitcoin/>>. Acesso em: maio/2013.

ESTIMULANET.COM. Deep web Verdades e Mentiras. 2012. Disponível em: <<http://www.estimulanet.com/2012/08/Deepweb-verdades-e-mentiras.html>>. Acesso em: abr/ 2013.

KOHN, Stephanie. OLHAR DIGITAL – Twitter, livros e música: o lado ‘cult’ da deep web. Dez/2012. Disponível em: <http://olhardigital.uol.com.br/produtos/digital_news/noticias/nem-so-de-bizarrices-vive-a-deep-web>. Acesso em: maio/2013.

MELLO, João. REVISTA GALILEU – Nem tudo são trevas: o lado bom da Deep Web. Maio/2013. Disponível em:
<<http://revistagalileu.globo.com/Revista/Common/0,,EMI331438-17770,00-NEM+TUDO+SAO+TREVAS+O+LADO+BOM+DA+DEEP+WEB.html>>. Acesso em: maio/2013.

OLHAR DIGITAL – Você sabe o que é a deep web? Jan/2012. Disponível em:
<http://olhardigital.uol.com.br/jovem/central_de_videos/voce-sabe-o-que-e-a-deep-web>. Acesso em: abr/2013.

PEREIRA, Leonardo. OLHAR DIGITAL – Deep web: saiba o que acontece na parte obscura da internet. Dez/2012. Disponível em:
<http://olhardigital.uol.com.br/produtos/digital_news/noticias/deep-web-saiba-o-que-acontece-na-parte-obscura-da-internet>. Acesso em: maio/2013-a.

PEREIRA, Leonardo. OLHAR DIGITAL – Nas entranhas da deep web: o que há de bizarro na ‘parte de baixo’ da internet. Dez/2012. Disponível em:
<http://olhardigital.uol.com.br/produtos/digital_news/noticias/nas-entranhas-da-deep-web-o-que-ha-de-bizarro-na-parte-de-baixo-da-internet>. Acesso em: maio/2013-b.