UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE HUMANIDADES
DEPARTAMENTO DE CIÊNCIAS DA INFORMAÇÃO
CURSO DE BIBLIOTECONOMIA

JACKSON CLAYTON DOS ANJOS LIMA

O ANONIMATO NA DEEP WEB E SUA DUALIDADE INFORMACIONAL

FORTALEZA

2018

JACKSON CLAYTON DOS ANJOS LIMA

O ANONIMATO NA DEEP WEB E SUA DUALIDADE INFORMACIONAL

Monografia apresentada ao curso Biblioteconomia, do Departamento de Ciências da Informação, da Universidade Federal do Ceará, como requisito parcial para obtenção do título de Bacharel em Biblioteconomia.

Orientador: Prof. Dr. Jefferson Veras Nunes

FORTALEZA
2018

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

L698a Lima, Jackson Clayton dos Anjos.
O anonimato na deep web e sua dualidade informacional / Jackson Clayton dos Anjos Lima. – 2018.
71 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Centro de Humanidades, Curso de Biblioteconomia, Fortaleza, 2018.
Orientação: Prof. Dr. Jefferson Veras Nunes.

1. Internet. 2. Deep web. 3. Conteúdo informacional. 4. Anonimato. 5. Vigilância. I. Título.

CDD 020

JACKSON CLAYTON DOS ANJOS LIMA

O ANONIMATO NA DEEP WEB E SUA DUALIDADE INFORMACIONAL

Monografia apresentada ao curso Biblioteconomia, do Departamento de Ciências da Informação, da Universidade Federal do Ceará, como requisito parcial para obtenção do título de Bacharel em Biblioteconomia.

Aprovada em: _____/_____/_____.

BANCA EXAMINADORA

_____

Prof. Dr. Jefferson Veras Nunes (Orientador)

Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Antônio Wagner Chacon Silva (Membro)

Universidade Federal do Ceará (UFC)

_____

Profª. Dra. Isaura Nelsivânia Sombra Oliveira (Membro)

Universidade Federal do Ceará (UFC)

AGRADECIMENTOS

Agradeço a Deus, por me dar força e tornar possível todos os meus sonhos.

À minha mãe, Leda Maria dos Anjos, que sempre me ajudou em toda minha vida. Obrigado, mãe, por toda sua generosidade e simpatia. Te amo.

Agradeço à minha família pelo apoio diante das dificuldades.

À minha namorada e amiga para todas as horas, Micaele dos Santos Oliveira, que me ajudou e me acompanhou durante esse trabalho. Beijo no coração. Te amo.

Agradeço à Universidade Federal do Ceará, pelo ambiente criativo e amigável que proporciona.

Agradeço a todos os professores do Departamento de Biblioteconomia e Ciência da Informação da Universidade Federal do Ceará por repassarem seus conhecimentos.

Aos professores Antônio Wagner Chacon Silva e Jefferson Veras Nunes que me fizeram abrir a mente sobre muitos assuntos que eu desconhecia, assim ampliando meu olhar crítico diante da sociedade.

Ao meu Orientador, Prof. Dr. Jefferson Veras Nunes, que me orientou e me ouviu todas as vezes que necessitei. Obrigado pela paciência e por acreditar na minha capacidade.

Obrigado!

Resumo

Esta pesquisa tem como objetivo principal o estudo das seguintes questões: como se dá o acesso à informação na deep web? Quais as motivações dos indivíduos para fugirem da exposição navegando em websites não indexados por mecanismos de busca convencionais? Que estratégias são adotadas para burlar a vigilância e preservar o anonimato na rede? Faz-se a revisão bibliográfica que abarca conceitos relativos à história da internet, web 2.0, comunidades virtuais, criptografia e vigilância na rede. Além disso, são trazidas discussões sobre a dualidade do anonimato e conteúdo informacional dentro da deep web. Em relação à metodologia, desenvolve-se uma pesquisa exploratória de cunho qualitativo no qual usou-se a entrevista como coleta de dados até a saturação das respostas e a técnica de analise de conteúdo. Conclui-se que os fatores que exercem a influência dos usuários ao uso da deep web são o anonimato como forma de se proteger contra a vigilância e os perigos da rede durante a navegação e, também, o conteúdo encontrado lá que, muitas vezes não é encontrado na surface web.

Palavras-Chave: Internet. Deep web. Conteúdo informacional. Anonimato. Vigilância.

Abstract

This research has as main objective the study of the following questions: How is access to information in the *Deep Web* ? What are the motivations of individuals to escape exposure by browsing on websites not indexed by conventional search engines? What strategies are used to circumvent surveillance and preserve network anonymity? A bibliographic review is carried out covering concepts related to the history of the internet, web 2.0, virtual communities, cryptography and surveillance in the network. In addition, discussions are brought about the duality of anonymity and informational content within the *deep web* . In relation to the methodology, an exploratory qualitative research is developed in which the interview was used as data collection until the saturation of the answers and the technique of content analysis. It is concluded that the factors that exert the influence of the users to the use of the *deep web* are the anonymity as a way to protect against the vigilance and the dangers of the network during navigation and also the content found there that, often is not found on the *Surface Web.*

Keywords: Internet. Deep web . Informational content. Anonymity. Surveillance.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Diante das evoluções tecnológicas e da comunicação, a internet pode ser considerada uma ferramenta que transforma a sociedade. Ela busca a conectividade entre várias pessoas de diferentes lugares do mundo, além do seu corpo informacional que está dividido nos seus diversos formatos e tamanhos. Usado para todos os fins e por diferentes pessoas, ela contribui de alguma forma com a socialização dos indivíduos dentro do cyberespaço.

A deep web está abaixo dessa “internet” que a maioria das pessoas acessa. A surface web apenas é uma parte do grande mar de informações que existe. Colaborando com isso (Santos e Marchi, 2013) “A deep web (DW) consiste numa área da internet onde o anonimato é o seu principal foco. Nela é possível encontrar diversos tipos de conteúdo no qual não podem ser encontrados na web convencional [...]”.

O interesse em desenvolver este trabalho surgiu ao constatar um preconceito diante da deep web por meio dos conteúdos encontrados lá. Além da curiosidade pelo ciberespaço. Interesse esse que adquiri no curso de Biblioteconomia, por meio das disciplinas Tecnologias da informação e Informação e sociedade.

O presente estudo será pautado pelas seguintes questões centrais: Como se dá o acesso à informação na deep web? Quais as motivações dos indivíduos para fugirem da exposição navegando em websites não indexados por mecanismos de busca convencionais? Que estratégias são adotadas para burlar a vigilância e preservar o anonimato na rede?

Desta forma este trabalho tem como objetivo geral: analisar os fatores preponderantes na decisão dos usuários para uso da deep web, considerando o anonimato em rede e o caráter informacional em relação à sua dualidade, de modo a assinalar alguns dos seus aspectos positivos e negativos. Deste objetivo geral, têm-se os seguintes objetivos específicos: analisar e descrever a importância do anonimato na deep web; identificar como se dá o uso de ferramentas adotadas para fugir da vigilância na rede e interpretar os sentidos que os indivíduos atribuem a essa fuga e, compreender de que maneira o uso da deep web favorece o livre acesso a conteúdos diversos impulsionando o conhecimento colaborativo.

Posto isso, esta monografia está distribuída em seis capítulos: o primeiro apresenta informações introdutórias sobre a temática, a questão de pesquisa, bem como a justifica, e os objetivos; o segundo traz as conceituações sobre o surgimento da internet, web 2.0, comunidades virtuais, composição de conceitos e comportamento do usuário na web 2.0; o terceiro se dá pela deep web, Tor project, vigilância, anonimato e criptografia; Cultura Hacker; o quarto traz a metodologia utilizada para aplicar esta pesquisa com os usuários da deep web por meio do telegram; o quinto apresenta a análise dos dados obtidos através de entrevista e a discussão dos resultados; e, por fim, a sexta traz as considerações finais.

2 INTERNET

A internet nos liga e nos reconecta junto a outras pessoas, lugares e culturas de qualquer parte do mundo. A internet se tornou algo fundamental nas nossas vidas, nos diversos ambientes, tanto profissional como no lazer. Tendo em vista organizar essa nova era informacional, ela visa nos conectar a rede global.

A internet teve início no contexto de Guerra Fria, entre os Estados Unidos e a União Soviética. Em setembro de 1969 surge a ARPANET, conhecida também como ARPA (Advanced Research Projects Agency), criada pelo departamento de defesa dos Estados Unidos. Segundo Castells (2003) o objetivo maior do programa era alcançar superioridade tecnológica militar em relação à URSS através do estímulo à pesquisa em computação interativa. Para montar uma rede interativa de computadores, a ARPA valeu-se da comutação por pacote desenvolvida por Paul Baran, que compreendia uma rede de comunicação descentralizada.

Diante disto, o passo seguinte da ARPANET foi a possível conexão entre outras redes de computação no qual foram a PRNET e a SATNET. Segundo Castells (2003) isso introduziu um novo conceito: uma rede de redes. Em 1973 surgiu, então, o protocolo de controle de transmissão (TCP), sendo acrescido pelo protocolo intrarede (IP), conhecido por nós até hoje como o padrão TCP/IP. Logo depois, a ARPANET mudou-se para a Defence Communication Agency (DCA) para que as forças armadas decidissem criar várias redes para seu próprio controle.

Conforme Castells (2003) Em 1990, a ARPANET já tinha virado uma tecnologia obsoleta e logo foi tirada de operação pelas forças armadas que, dali em diante, passou a responsabilidade para a National Science Foundation (NSF). Mas

diante da tecnologia estar sendo usada pelo domínio público e sua desregulação, a NSF tratou logo de privatiza-la.

Logo, provedores e serviços de internet estavam tornando a internet algo totalmente comercial.

> No início de 1990 muito provedores de serviços de internet montaram suas próprias redes e estabeleceram suas próprias portas de comunicação em bases comerciais. A partir de então, a internet cresceu rapidamente como uma rede global de computadores. O que tornou isso possível foi o projeto original da Arpanet, baseado numa arquitetura em múltiplas camadas, descentralizada, e protocolos de comunicação abertos. (CASTELLS, 2003, p.15)

Para falarmos sobre o desenvolvimento da internet e sua popularização por meio da *WWW*, em 1990, por Tim Berners-Lee, “Ele definiu e implementou o software que permitia obter e acrescentar informação de/e para qualquer computador conectado através da internet: HTTP, MTML, e URI (mais tarde chamado URL).” (CASTELLS, 2003, p. 18).

Berners-Lee, com a ajuda de Robert Cailliau, construiu o programa navegador que caracteriza por World Wide Web, uma rede mundial de hipertexto que foi lançado pelo CERN em agosto de 1991. Segundo Castells (2003) muitos hackers do mundo todo passaram a desenvolver seus próprios navegadores diante da iniciativa de Bernrs-Lee. Logo depois o Instituto de tecnologia de Helsinki e a universidade da Califórnia, produziram sua própria adaptação.

Dentre diversas versões modificadas da *WWW*, a mais orientada para o produto foi o mosaic. O mosaic tinha uma capacidade gráfica avançada e tinha uma ótima qualidade para transmitir, captar e distribuir imagens pela internet, com várias técnicas de interface e com um vasto campo de multimídia. Depois de vários processos empresariais, o mosaic começou a se chamar de netscape communications e em dezembro de 1995, lançaram o primeiro produto, o software Navigator, de forma gratuita pra fins educacionais e 39 dólares para uso comercial.

Graças ao sucesso do Navigator, a Microsoft descobriu a internet, assim em 1995, juntamente com o sistema operacional Windows 95, veio também o navegador Internet Explorer, baseado na tecnologia da empresa Spyglass.

Em 1990 a internet já tinha uma arquitetura aberta que permitia a interconexão entre diversas máquinas e redes em todo mundo. Segundo Castells

(2003) a *WWW* podia então funcionar com software adequado, e vários navegadores de uso fácil estavam à disposição do público.

Diante da fala de Castells (2003) a internet nasceu no interesse militar e da cultura libertária sobre a Big Science, no qual centros de pesquisa universitários e centros ligados à defesa queriam desenvolver interconexão mediante ao compartilhamento de computadores. Dessa forma, passaremos a falar um pouco mais sobre a Web 2.0

2.1 Web 2.0

A web ganhou notoriedade por ser a primeira geração de internet que tinha a característica de abranger grande quantidade de informação, tendo um papel fundamental no serviço distribuído de informação. Em primeiro caso, o usuário se destaca como espectador das páginas visitadas, sem o menor poder de editar o conteúdo, sendo ele um usuário passivo de conteúdo. De acordo com Meirelles e Moura (2007, p.12),

> Os usuários ou interatores, anteriormente denominados “navegantes” (internautas) da Web 1.0, transformaram-se em usuários (stricto sensu) de serviços on-line que, atualmente, podem dispensar a instalação de aplicativos nos micro – computadores. Podendo perceber, desse modo na Web 2.0 há ocorrência de modificações no papel do usuário, que passará a interagir selecionar e controlar as informações de forma a ampliar o seu papel de agente atuante.

Diante dos avanços tecnológicos na web, foi possível a criação de um espaço cada vez mais social e interativo entre os usuários. Tendo como foco principal a interação, transformação e a edição de material nesses ambientes hipertextuais, assim dando início a web 2.0.

De acordo Curty (2008, p. 56), o termo web 2.0 surge em 2004 durante uma sessão de brainstorming realizada pela empresa americana do setor de comunicação Reilly Media. Os membros Tim O´Reilly e Dale Dougherty foram os responsáveis pela propagação, dando forma ao termo e fazendo com que ele fosse amplamente utilizado. O termo começou a ocorrer desde 2004 com a realização da primeira edição da web 2.0 na conferência que reúne os líderes da indústria da internet. A publicação do artigo “What is web 2.0? Design patter and business models for the next generation of softwares” - outro fator marcante na propagação do

conceito da Web 2.0 – teve o propósito de esclarecer o significado do termo em face de diversas interpretações existentes.

A web 2.0 pode ser entendida como um avanço da web 1.0, uma nova versão da Web. Na web 1.0, seus programadores polarizavam a tecnologia responsável por conectar os usuários, enquanto que na web 2.0, as pessoas que se conectam através da tecnologia. Dessa forma, podemos entender que o termo web 2.0 busca uma forma de assumir um papel no processo de interação entre os usuários.

Blattmann e Silva (2007, p. 198) acreditam que:

> A web 2.0 pode ser considerada uma nova concepção, pois passa agora a ser descentralizada e na qual o sujeito torna-se um ser ativo e participante sobre a criação, seleção e troca de conteúdo postado em um determinado site por meio de plataformas abertas. Nesses ambientes, os arquivos ficam disponíveis on-line, e podem ser acessados em qualquer lugar e momento, ou seja, não existe a necessidade de ser gravado em um determinado computador os registros de uma produção ou alteração na estrutura de um texto. As alterações são realizadas automaticamente na própria Web.

Diante dessa perspectiva, nota-se que a web 2.0 é, sem dúvida, bem mais sociável por conta de existir mais pessoas compartilhando e elaborando conteúdos para o enriquecimento do espaço, deixando em segundo plano os conteúdos e tecnologias e, em primeiro plano, a própria interação entre os usuários.

Segundo Carvalho, Alcoforado e Santos (2013, p. 64) constatamos que:

> A Web 2.0 apresenta um conjunto de novas possibilidades e valores relacionado ao acesso, uso, compartilhamento e produção de informação, o que gera impactos na relação de indivíduos com a informação e a comunicação, produzindo novos comportamentos informacionais.

Sendo assim, a web 2.0 busca cada vez mais a interação desses usuários pelos mais variados tipos de canais existentes, tendo como principal característica um usuário mais ativo, que passa a ser um produtor e receptor das informações. Um fator de extrema importância nesse processo é a presença de uma inteligência coletiva, sendo assim a participação e colaboração dos usuários agregam valor para essa plataforma. Dentre alguns principais recursos presentes no ambiente da web 2.0 estão: redes sociais, *blogs,* wikis, youtube, telegram, whatsapp e entre outros.

Diante da evolução da web, nota-se que já existe uma nova versão para web, a web 3.0 também denominada Web semântica. Para Curty (2008) “é conceituada como uma extensão da Web atual em que se busca atribuir à informação significado definido de forma a interagir computadores e pessoas”. Logo, diante dos vários tipos de canais e a interação desse usuário no ciberespaço, falaremos sobre comunidades virtuais.

2.2 Comunidades virtuais

Durante os tempos as tecnologias da informação foram atuando e renovando os espaços e a forma de como a sociedade se estrutura. Os sites, comunidades e grupos virtuais têm a intenção de reunir o máximo de usuários para obterem novas trocas de informação. O usuário cria uma um perfil e preenche alguns dos dados para completar seu cadastro de forma simples e rápida. Cada comunidade, dependendo do tipo de tema, tem suas regras a serem seguidas, assim moldando o seu comportamento diante da forma de como o mesmo pode se portar diante de cada grupo que pertença.

Grupos, comunidades ou redes sociais podem ser caracterizados de acordo com Carvalho (2007, p.66).

> Agrupamentos de pessoas que se reúnem em função de suas afinidades e utilizam o ciberespaço como meio para intercambiar e difundir suas ideias, estabelecer relações sociais, realizar atividades conjuntas e lograr objetivos comuns. Oferecem o ambiente e suas ferramentas necessárias para que seus usuários interajam, de modo espontâneo e democrático, e se gere, armazene e difunda a informação associada aos processos de comunicação.

Um grupo virtual se organiza pela base de afinidade de algum interesse específico, afinidades e problemas no qual eles passam. Com isso, a distância deixa de ser um obstáculo. De acordo com Teixeira Filho (2002, p. 43) “apesar de não presentes, em uma comunidade virtual as pessoas encontram muitos elementos humanos de uma interação normal: paixões, ideias, apoio, solidariedade, conflitos, ódio, amizades, etc.”. A virtualização dos sentimentos humanos se passando por dados para melhor fluir a informação e a interação entre os mesmos. As conexões em uma comunidade virtual são constituídas de laços sociais que são formados por

interações entre os próprios usuários desse ciberespaço. As relações e os laços sociais são o resultado dessa interação.

Segundo Recuero (2009), a interação no cyberespaço pode ser compreendida como uma maneira de conectar usuários e verificar que tipo de relação eles possuem, estas podem ser diretamente relacionada às questões sociais. A participação em comunidades virtuais instiga a inteligência coletiva, onde os usurários recorrem à troca de informações e conhecimentos.

Segundo Lévy (2002), uma comunidade virtual, quando convenientemente organizada, representa uma importante riqueza em termos de conhecimentos disseminados. Representam o papel que nos ajudam a filtrar o excesso de informação. Diz Lévy (2002, apud COSTA, 2008, p. 44), “Uma rede de pessoas interessadas pelos mesmos temas é não só mais eficiente do que qualquer mecanismo de busca.” A forma de integração dentro da cibercultura é algo marcante e diferente em nossa história. Nesse ciberespaço é possível encontrar áreas de proximidades: usuários compartilham ideias, conhecimentos e informações sobre seus problemas e dificuldades.

De acordo com Teixeira (2002), a comunicação via Internet e as comunidades virtuais são uma forma de comunicação “muitos-para-muitos”, enquanto o telefone é “um - para- um” e os meios de comunicação clássicos – televisão, jornais e revistas – são “um- para- muitos”. A Internet ficou rapidamente famosa como comunicação em massa pelos usuário, trazendo uma transformação radical nas mídias. Fazendo com que não somente as pessoas, mas também as demais formas de comunicação se adaptem à Internet como um todo.

Segundo Teixeira Filho (2002, p. 50):

> O ciberespaço oferece instrumentos de construção cooperativa de um contexto comum em grupos numerosos e geograficamente dispersos. A comunicação não é apenas uma difusão ou transporte de mensagens, mas uma interação no meio de uma situação com a qual cada um contribui para modificar ou estabilizar.

Dessa forma, podemos dizer que é uma ligação que funciona como uma memória de troca comum, o ponto principal das comunidades virtuais é a partilha e reinterpretações sobre determinados assuntos entre eles em comum. Nesse contexto, podemos ver seis benefícios de uma comunidade virtual, da obra de Teixeira Filho (2002): reduz os custos de comunicação entre os membros da

organização; aumenta a produtividade na solução de problemas; favorece a criação de memória organizacional; favorece o processo de inovação de produtos e processos; facilita a cooperação entre os membros da organização; facilita o compartilhamento de conhecimentos.

2.3 Composição de conceitos

Diante da análise de uso da informação, nota-se um crescimento no enfoque nos estudos, partindo de uma visão limitada para uma mais ampla. Figueiredo (1994) compreende estudos de usuários como as investigações realizadas para conhecer as necessidades de informação dos usuários ou avaliar o atendimento das necessidades de informação pelas bibliotecas, centros de informações ou serviços de informações.

Wilson (1999) fez várias análises sobre o assunto e amplia sua ideia, no campo do comportamento humano e denominando “comportamento informacional”. Esse tipo de ação está voltado às atividades de busca, uso e transferência de informações no qual o usuário se esforça para satisfazer suas necessidades informacionais.

Wilson (1999 apud GASQUE, 2010, p. 22) propõe quatro definições que estão relacionadas ao comportamento informacional, sendo elas:

> **Comportamento informacional:** a totalidade do comportamento humano em relação ao uso de fontes e canais de informações, incluindo a busca da informação passiva ou ativa.
> **Comportamento de busca da informação**: a atividade ou ação de buscar informação em consequência da necessidade de atingir um objetivo.
> **Comportamento de pesquisa de informação:** O nível micro do comportamento, em que o indivíduo interage com os sistemas de informação de todos os tipos.
> **Comportamento do uso da informação:** constitui o conjunto dos atos físicos e mentais e envolve a incorporação da nova informação aos conhecimentos prévios do indivíduo.

Diante das ideias de Wilson (2000) estudiosos como Pettigrew, Fidel e Bruce (2001 apud GASQUE, 2010, p. 22) entendem “comportamento informacional” como sendo as atividades que envolvem as necessidades de sujeitos e de como procuram, utilizam e transportam a informação em diversos contextos. Dentro de suas investigações sobre o tema, esses pesquisadores perceberam três formas: a) Cognitiva – examina o comportamento a partir do conhecimento, convicções e

crenças que medeiam as percepções do mundo; b) Social – baseada nos significados e valores que vivem em vários contextos; c) Multifacetada – integra múltiplos pontos de vista para compreensão do comportamento informacional.

De acordo com Wilson (2000 apud MARTÍNES; SILVEIRA; ODDONE, 2007, p. 121), “Comportamento Informacional é todo comportamento humano relacionado às fontes e canais de informação, incluindo a busca ativa e passiva de informação e uso da informação”. Logo, é possível perceber que este processo está totalmente ligado à necessidade informacional do usuário relacionado ao interesse na sua pesquisa.

Diante das considerações comportamentais dos usuários, podemos analisar entre eles, sua área profissional, suas características informacionais que desejam encontrar e as fontes consultadas influenciam nesse comportamento informacional.

2.4 Comportamento do usuário na web 2.0

A facilidade do usuário com recursos da web 2.0 estimula a interação entre elas, tornando cada vez mais importante a criação, seleção e propagação de conteúdo, causando um impacto no comportamento informacional de uma gama de usuários.

No âmbito da web 2.0 existem novas possibilidades de se manifestar um comportamento informacional ativo no processo de geração e troca da informação. De acordo com Blattmann e Silva (2007, p. 198). “[...] o sujeito torna-se um ser ativo e participante sobre a criação, seleção e troca do conteúdo postado em um determinado site por meio de plataformas abertas.”

Assim, nota-se que o processo de construção de informação na web 2.0 destaca o papel do usuário com um protagonismo do seu próprio processo de evolução; levando em conta sua capacidade de gerar, selecionar, organizar, recomendar e alterar conteúdos no ciberespaço. Tendo em vista algumas caracteristicas, podemos classificá-los como usuários ativos que criam, selecionam e disseminam informação para que outros tenham acesso.

Diante disso, vemos a relação da web 2.0 que Pisani e Piotet (2010 apud CARVALHO; ALCOFORADO; SANTOS, 2013) analisaram e sugeriram o conceito de web atores; esses sujeitos que compreendem a web e a utilizam da mesma maneira

bidirecional, recebendo e mandando informação ao mesmo tempo, assumindo papel de consumidor/criador; leitor/escritor; ouvinte/ gravador; expectador/produtor. Dessa maneira, os usuários passam a se envolver na forma de administrar e organizar da informação.

Outra característica do processo é a armazenagem ao compartilharem suas produções através das ferramentas 2.0 e se ajudarem mutuamente a se acharem no ciberespaço. A maneira de interagir entre os usuários e conteúdo a partir dos recursos web 2.0 apresentam vários setores na realização de diversas atividades. Mudanças essas que formam a maneira como as pessoas estudam, trabalham, compram etc. Essas experiências de compartilhamento de informações e conhecimento estabelecem um importante processamento do conhecimento mútuo entre os membros dos cyberespaço.

Dessa forma, a participação na web 2.0 é algo crescente, o comportamento dos usuários das comunidades virtuais e de seus criadores ainda é algo limitado. Vemos isso através do estudo “The 90-9-1 Rule for Participation Inequality in Social Media and Online Communities”. Segundo Jakob Nielsen (2006), os usuários de comunidades online seguem um princípio de desigualdade, isso implica dizer que a participação segue uma regra de 90-9-1.

> **90%** constituem a audiência, são pessoas que observam e apenas leem, mas não contribuem de maneira ativa na comunidade.
> **9%** são editores, essas contribuem algumas vezes modificando ou adicionando texto a um artigo já produzido.
> **1%** são usuários criadores e responsáveis pela maior parte das contribuições. Frequentemente essas pessoas estão conduzindo um vasto percentual, novos comentários e atividades no site.

Nesse contexto, vemos o usuário tornando-se um ser ativo e participante sobre a criação, seleção e troca do conteúdo postado por meio de plataformas abertas no ciberespaço como um todo. Até mesmo na Deep Web, no qual falaremos mais adiante.

3 DEEP WEB

Deepnet, web invisível, undernet ou web oculta são alguns nomes que se dão a deep web. De forma mais simples, a deep web é definida como um conjunto de páginas e serviços em um ambiente de navegação que não contém nenhuma regulamentação ou controle. Essa parte da web é composta por sistemas que

trabalham com redes anônimas, fornecedoras de conteúdos escondidos. Segundo (Santos e Marchi, 2013) “A aparência dos sites na deep web geralmente nunca são bem feitos e sim feios, pois ninguém que navega por lá está preocupado com o layout mais sim com o conteúdo.”. Dessa forma, vemos layouts e suas cores sem harmonia, telas extensas e diversos links listados.

Muitos usuários não indicam a utilização de navegadores convencionais. (Blasechi e Marques, 2016) afirmam que “para acessar esse meio, muitos usuários indicam a não utilização de navegadores convencionais, como o internet explorer ou google chrome, por eles exporem o ip do usuário, fazendo com que outros usuários com má índole[..]”.

Essas redes anônimas não possuem qualquer tipo de ligação com a internet aberta, isto é, com a surface web. Conforme (Vignoli e Monteiro, 2013) nos falam a “Web Visível da Superfície visto que para acessar a dark web são necessários softwares intermediadores, pois os buscadores comuns não conseguem recuperar seus sítios”. Dentre essas redes, que foram criadas com o claro objetivo de tornar seus usuários irrastreáveis mascarando o número de IP, isto é, a identificação de cada computador, através de encriptação, a mais simples de acessar é a tor.

Segundo (Martins e Silva) “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”. A Deep Web, portanto fica “inexistente” para os mecanismos de busca comuns. Para manter as páginas ocultas, os endereços dos sites são compostos por letras e números sem sentido, que podem mudar ao longo do tempo, fazendo com que seus links não sejam facilmente passados de uma pessoa para outra, além de evitar, com isso o rastreamento.

> A Deep Web começa quando uma pessoa repassa para outra um conteúdo que não pode ser encontrado nos grandes sites de pesquisa. Ninguém terá acesso, nem que procure. Será preciso, antes, buscar outros conteúdos possivelmente relacionados, e conhecer pessoas que conhecem outras pessoas (ROHR apud LOPES)

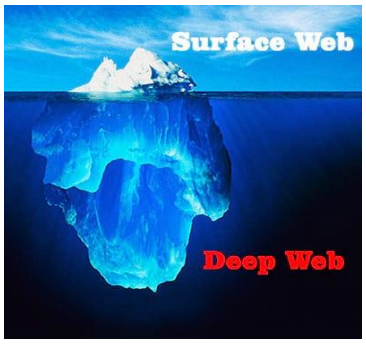
Dessa forma, ter acesso a um site oculto depende, às vezes, de um link direto de outro usuário. Podem ser grupos, fóruns ou páginas na surface web que falam sobre o assunto. Dentre a questão de como se da o repasse de links na deep

web, outra questão importante é sua dimensão em comparação a surface web ou web 2.0. Bergman afirma que

> [...] informações públicas na Deep Web são comumente de 400 a 500 vezes maior que as definidas da World Wide Web. A Deep Web contém 7.500 terabytes de informações comparadas a 19 terabytes de informação da Surface Web. A Deep Web contém aproximadamente 550 bilhões de documentos individuais comparados com 1 bilhão da Surface Web. Existem mais de duzentos mil sites atualmente na Deep Web. Seis das maiores enciclopédias da Deep Web contém cerca de 750 terabytes de informação, suficiente para exceder o tamanho da Surface Web quatro vezes. Em média, os sites da Deep Web recebem 50% mais tráfego mensal, ainda que não sejam conhecidos pelo público em geral. A Deep Web é a categoria que mais cresce no número de novas informações sobre a Internet. Deep Web tende a ser mais estrita, com conteúdo mais profundo, do que sites convencionais. A profundidade de conteúdo de qualidade total da Deep Web é de 1.000 a 2.000 mil vezes maior que a da superfície. O conteúdo da Deep Web é altamente relevante para todas as necessidades de informação, mercado e domínio. Mais da metade do conteúdo da Deep Web reside em tópicos específicos em bancos de dados. Um total de 95% da Deep Web é informação acessível ao público não sujeita a taxas ou assinaturas [...] (BERGMAN apud POMPÉO; SEEFELDT, 2013, p. 441).

Existem algumas analogias que melhor explicam como se da a deep web nesse mar de informação que temos hoje no ciberespaço. Segundo Pompéo e Seefeldt (2013) a primeira delas é a do iceberg.

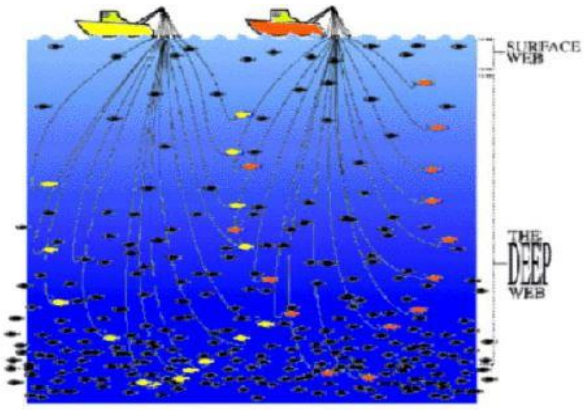
Figura 1 – Analogia de dimensão da Surface Web em comparação com a Deep Web.



Fonte: https://www.oficinadanet.com.br/post/10182-um-universo-chamado-deep-web

Aqui, surface web é representada pelo topo, pela parte visível. Já a deep web é representada como sendo a base, e, apesar de sabermos da sua existência, desconhecemos o seu tamanho.

Figura 2 – Analogia de dimensão da Surface Web
em comparação com a Deep Web.



Fonte: Bergman, 2012.

Outra analogia é a de um grupo de pescadores em um barco. (Figura 2). Quando estes jogam uma rede de pesca na parte superficial do mar a probabilidade de pescarem peixes é muito menor se comparada com a mesma rede jogada em maior profundidade. Sendo assim, quanto mais fundo o alcance, maior o retorno.

Diante do fluxo informacional da deep web, como também na surface web, Vemos que há uma grande demanda de temas diversos. São livros, monografias, documentos sigilosos, raros ou, por alguma razão, proibidos. Alguns sites famosos como Anonymous e do Wikeleaks vieram de lá da deep web.

Segundo Kohn (2013), “[...] um dos buscadores da Deep Web 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 [...]”. Além de acervos das mais variadas mídias, contudo, todos sem procedência. Por este motivo ressalta-se a necessidade de ter muito cuidado e atenção redobrada com determinados links listados nos resultados de busca.

É possível também encontrar fóruns de discussões dos mais variados tipos de temas. Porém, em alguns casos precisam de um cadastro. Conforme Agripino (2013) “A Deep Web possui diversas vantagens. Por não existir a necessidade de respeitar direitos autorais, a reprodução de obras completas é livre”. Esse é um dos motivos que leva o conteúdo de qualidade e relevante ser maior que a Surface Web. Existem alguns mecanismos de busca, no qual apresentam

especificações sobre determinado temas. Sites sobre literatura, programação e projetos científicos, por exemplo.

Existem várias bibliotecas virtuais que permitem o acesso a fontes cientificas. “A Deep Web também possui sistemas de busca, mas alguns sites só podem ser acessados se você souber a URL exata”. Agripino (2013) nos fala os mais conhecidos.

> 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 Complet 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. (AGRIPINO, 2013)

Isso significa que existe realmente bastante coisa importante para ser analisada e que podemos ter uma bagagem de conhecimento amplo sobre diversos assuntos. Porém, existe também o lado negativo da deep web. Segundo Abreu e Nicolau (2013)

> Todavia, um dos pontos desfavoráveis desse universo é fato de que em grande parte da Deep Web encontram-se conteúdos ilegais. Diversos grupos beneficiam-se do anonimato para compartilhar conteúdo criminoso, carregando o espaço com páginas de pedofilia contendo imagens e vídeos explícitos, páginas de necrofilia, anúncios de assassinos de aluguel e suas tabelas de preços que variam de acordo com a importância social da vítima, zoonecrofilia, fóruns de canibalismo, além de uma espécie de Mercado Livre.

Infelizmente existe esse outro lado. O anonimato chama atenção de criminosos pelo fato de não poderem ser rastreados, destacando-se a facilidade de encontrar informações de diversas formas.

Kohn (2013) nos explica melhor sobre a existência de sites bizarros, no qual você pode encontrar conteúdos bem agressivos.

> “A 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 venda 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.

Essa parte da Deep Web é bem ruim para os usuários. O usuário tem que se preocupar com a segurança, visto que está propenso a todo tipo de ação, desde a infecção do computador, até invasões hackers, além da possibilidade de acessar conteúdos indesejados. Existem formas de entrar na Deep Web de forma segura, sendo uma delas pela rede tor. Uma ferramenta para quem quer se proteger contra malwares e garantir uma navegação segura.

3.1 Tor project

A tecnologia utilizada para ter acesso a deep web é o Tor. Uma ferramenta de rede com formato de túnel que ajuda as pessoas e organizações a aumentarem a sua segurança e privacidade na Internet. Segundo (TOR PROJECT, 2017) Tor é um software livre e uma rede aberta que ajuda você a se defender contra uma forma de vigilância que ameaça a liberdade e privacidade, negócios confidenciais e relacionamentos, e a segurança do estado conhecida como análise de tráfego.

O navegador protege o usuário saltando suas comunicações em rede distribuída. Segundo (TOR PROJECT, 2017):

> A rede Tor é um grupo de servidores voluntários que permite que as pessoas melhorem sua privacidade e segurança na Internet. Os usuários de Tor utilizam esta rede conectando-se através de uma série de túneis virtuais, em vez de fazer uma conexão direta, permitindo que organizações e indivíduos compartilhem informações sobre redes públicas sem comprometer sua privacidade. Na mesma linha, a Tor é uma ferramenta efetiva de evasão de censura, permitindo que seus usuários alcancem destinos ou conteúdo de outra forma bloqueados. Tor também pode ser usado como um bloco de construção para desenvolvedores de software para criar ferramentas de comunicação com recursos internos de privacidade.

Além de ser um navegador que camufla seu IP, ele possibilita que as pessoas e as organizações possam aumentar a sua segurança e privacidade na internet, tendo em vista novas formas de comunicação com recursos de privacidades internas com aplicações para a troca de informações através da rede sem a preocupação de ter sua identidade revelada.

O Tor ajuda os jornalistas a se comunicar de forma mais segura. Eles usam o Tor para se comunicarem com suas fontes. As organizações não governamentais utilizam-no para que colaboradores de outros países possam se

conectar e trabalhar a distância sem que mais ninguém saiba que essas pessoas prestam serviços a elas. Grupos de ativistas, como a Electronic Frontier Foundation (EFF) usam-no como um mecanismo para manter as liberdades civis online asseguradas. (TOR PROJECT, 2017).

Diante da análise de tráfego, ela pode ser usada para inferir quem está falando com quem em uma rede pública. Segundo Sérgio Amadeu da Silveira é “uma forma de vigilância que ameaça a liberdade e a privacidade na rede”. Além da forma de vigilância e privacidade dentro da rede, a análise de tráfego permite que outros rastreiem seus comportamentos e interesses.

Isso pode afetar seu talão de cheques se, por exemplo, um site de comércio eletrônico use discriminação de preços com base em seu país ou instituição de origem. Pode até ameaçar seu trabalho e segurança física, revelando quem e onde você está. Por exemplo, se você estiver viajando para o exterior e se conectar aos computadores do seu empregador para verificar ou enviar o correio, você pode inadvertidamente revelar sua origem nacional e afiliação profissional a qualquer pessoa que esteja observando a rede, mesmo que a conexão seja criptografada.

A troca de informação, como e-mails, áudios ou outro tipo de mensagem, mesmo você criptografando cada uma delas, a análise de trafego ainda pode revelar muito sobre o que você está fazendo. Isso, porque suas informações se concentram nos cabeçalhos, no qual revela origem, destino, tamanho, tempo e assim por diante.

Um problema básico para dar privacidade é que o destinatário de suas comunicações pode ver que você enviou olhando cabeçalhos. Assim, podem ser intermediários autorizados, como provedores de serviços de internet e, por vezes, intermediários não autorizados.

O site oficial do tor usa uma analogia que explica: Segundo (TOR PROJECT, 2017):

> Tor ajuda a reduzir os riscos de análise de tráfego simples e sofisticada distribuindo suas transações em vários lugares na Internet, portanto nenhum ponto pode conectá-lo ao seu destino. A ideia é semelhante ao uso de uma rota tortuosa, difícil de seguir, a fim de eliminar alguém que o está atirando - e depois apagando periodicamente suas pegadas. Em vez de tomar uma rota direta de origem para destino, os pacotes de dados na rede Tor tomam uma via aleatória através de vários relés que cobrem suas faixas para que nenhum observador em um único ponto possa saber de onde os dados vieram ou para onde ele está indo.

Logo, diante da analogia deve-se entender que o Tor se torna um navegador lento, pelo fato de ele ter uma rota diferente dos outros navegadores como Internet Explorer, Mozilla Firefox ou Google Chrome, pois ele faz um caminho aleatório através de diversos servidores distribuídos de modo que ninguém, em qualquer ponto, poderá dizer de onde vêm os dados nem para onde vão. Possibilitar uma rede segura e anônima, sem vigilância, que seja viável a quem não tem certos conhecimentos em relação a informática, logo, o Tor segue garantindo o anonimato de forma segura.

3.2 Vigilância

Antes de falarmos sobre anonimato em rede, devemos entender um pouco sobre algumas questões em relação à vigilância e suas práticas. Segundo Foucault (apud ARAÚJO, 2013), nas sociedades soberanas da era clássica, o controle existia através da violência e da coerção. Já nas sociedades disciplinares (século XVIII a XIX), há uma mudança de paradigma e o ato de vigiar prevalece como mais eficaz que o de punir.

Hospitais, prisões, escolas e fábricas passam pelo confinamento da prática panóptica do indivíduo nessas instituições, mas conforme Deleuze (1992) ele nos fala que há um novo modelo social que trata as instituições com uma forma diferente de disciplina: trata-se do controle das formas de comunicação por meio das tecnologias da informação e de computadores (apud ARAÚJO, 2013).

A vigilância é assim analisada em sua forma histórica e social, visando a sua atualidade. Segundo Fernanda Bruno (2013),

> [...] as atuais práticas de vigilância contam com uma imensa e crescente diversidade de tecnologias, discursos, medidas legais e administrativas, instituições e corporações, enunciados e empreendimentos científicos, midiáticos, comerciais, políticos etc. (BRUNO, 2013, p. 19).

Ultrapassando os limites do panoptismo, explorando as formas das dinâmicas atuais recorrentes as práticas da vigilância, ela nos fala que as atividades de vigilância envolvem três elementos primordiais: observação, conhecimento e intervenção. A primeira, a observação, pode ser efetuada de modo visual, mecânico, eletrônico ou digital, e “[...] implica a inspeção regular, sistemática e focalizada de

indivíduos, populações, informações ou processos comportamentais, corporais, psíquicos, sociais, entre outros.” (BRUNO, 2013, p. 18).

A autora fala que a observação permite a produção de conhecimento sobre quem é vigiado, para extrair padrões, regularidades ou cadeias causais a respeito dos indivíduos, permitindo, assim, que se aja sobre suas escolhas e comportamentos.

Fernanda Bruno propõe que a noção de vigilância distribuída. “[...] não se trata de uma tecnologia ou atividade particular, mas o modo de funcionamento das redes que constituem a vigilância como dispositivo nas sociedades contemporâneas.” (BRUNO, 2013, p. 28).

A autora apresenta ainda uma lista que define o modo de funcionamento das redes que constituem a vigilância como dispositivos contemporâneos. O primeiro diz que vigilância tende a se tornar cada vez mais ubíqua e incorporada aos diversos dispositivos tecnológicos, serviços e ambientes que usamos cotidianamente, mas que se exerce de modo descentralizado, sem hierarquias estáveis e com uma diversidade de propósitos, funções e significações nos mais diferentes setores. Tendo em vista a coordenação de informação e pessoas nas estratégias de marketing e nos meios de comunicação.

A segunda é a diversidade de tecnologias, práticas, propósitos e objetos da vigilância. Tem o propósito de vigiar não só os suspeitos de algum delito ou ato criminoso, mas também consumidores, cidadãos comuns e internautas por meio de vigilância por tipos de interesse, transações eletrônicas e entre outras formas.

O terceiro nos fala que o padrão de vigilância, diferentemente dos dispositivos modernos de inspeção contemporâneos, atua tratando potencialmente vítimas em suspeitos e suspeitos em vítimas. Sem distinção

A quarta característica da vigilância distribuída considera que dispositivos podem atuar como vigilantes, ainda que não tenham sido projetados com essa finalidade. Como afirma Bruno, (2013, p.32).

> O caráter distribuído da vigilância consiste, aqui, no fato de que a sua ação, além de envolver uma rede de múltiplos agentes heterogêneos, supõe que estes muitas vezes deslocam as ações uns dos outros, produzindo sentidos, experiências que não podem ser previstos de antemão, mas que são decisivos para os efeitos que se produzem.

O quinto trata da gênese da vigilância. Ela não apenas se distribui entre indivíduos e instituições, como entre agentes humanos e não humanos. Sistemas técnicos automatizados que permitem a vigilância nos trabalhos desenvolvidos pelo homem, como por exemplo, a identificação dada por um robô para identificar alguém por meio de base de dados.

A sexta trata da forma de vigilância por meio do entretenimento e prazer. Reality shows, os sites de compartilhamento de vídeo e imagem e as redes sociais que exploram como você se sente em determinada situação analisando seu auto monitoramento.

Por fim, a Sétima vigilância distribuída convivem modelos mais hierarquizados e unilaterais com modelos colaborativos, no qual o individuo adota um olhar de vigilância sobre o outro individuo. Diante desses conceitos de vigilância diante do mundo contemporâneo, nota-se que, se necessário, uma forma de burlar o sistema de segurança, seria o uso do anonimato e a criptografia.

3.3 Anonimato e criptografia

Diante da evolução da internet em âmbito global, vemos que sua importância cresce diante de atividades sociais, culturais e econômicas. Anonimato quer dizer que o autor de uma mensagem não é conhecido e logo ele fica irreconhecível na rede. Segundo Carvalho (2010) “Anonimato quer dizer indistinguibilidade dentro de um conjunto de anonimato”. O anonimato serve a diferentes interesses, por diferentes grupos de pessoas.

Pessoas estas que não querem ser observadas e não querem ter divulgadas suas informações como nome, endereço, idade, amigos, interesses, opiniões pessoas, e outros; empresas que querem guardar segredos comerciais e usuários com acesso bloqueado por razões geográficas ou políticas. Colaborando com isso, (Abreu, Gomide, Vieira, et al) “Quando o usuário conecta seu dispositivo eletrônico na internet, automaticamente os sites vão fazendo uma biografia de buscas não autorizadas para oferecer produtos e serviços, isso seria ótimo se não fosse tão preocupante e invasivo”

Existem alguns tipos de usuários que utilizam o anonimato em rede. Segundo Carvalho (2010) esses usuários usam a "Pseudoidentidade: um indivíduo é identificado por um certo pseudônimo; Identidade irrastreável: um indivíduo não é

conhecido por nenhum nome, nem mesmo pseudônimos e o anonimato com um pseudo-endereço".

Além da forma de evitar a vigilância em rede e forma como o usuário se porta com as formas de anonimato, existem propósitos bons e ruins do anonimato que conforme Carvalho (2010) explica:

> Bons propósitos incluem denunciar um crime sem pôr a vida em ameaça; denunciar más práticas de sua empresa sem correr o risco de perder o emprego; Evitar perseguição política em países com governo repressivo; discutir problemas pessoais potencialmente embaraçosos, como problemas sexuais; obter avaliações mais objetivas de suas mensagens em discussões isentas de fatores sociais, de gênero, ou outros fatores que sejam afetados pelo conhecimento do nome dos participantes. Maus propósitos incluem: Proteger um criminoso; comunicação ofensiva; encontrar contatos para promover atos ilegais.

A questão do anonimato faz parte dessa evolução tecnológica também. Segundo Silveira (2009) o anonimato se dá na condição de comunicação não identificada, ou seja, da interação entre diversos usuários no ciberespaço que possuem uma identidade explicita ou que a ocultam. Diante disto Silveira, (2009, p.115) destaca:

> A ideia de anonimato remete-nos a uma série de relações sociais que dizem respeito à identidade, à subjetividade, ao controle, à segurança e aos direitos civis. Exemplificando, é possível destacar que a arquitetura da Internet e seus principais protocolos de conexão, ao assegurarem a comunicação distribuída sem a necessidade de identificação, dificulta o controle, e, ao assegurar a navegação de quem oculta um nome, também garante a navegação daqueles que construíram múltiplas identidades. Para problematizar essas relações a Internet é analisada como portadora de tecnologias do anonimato.

A criptografia já é uma tecnologia bem antiga, aproximadamente datam de 2.000 a.C., no Egito. Segundo Ulrich (2014, p.45), historicamente a criptografia foi utilizada por Estados em assuntos ligados a guerras e a questões diplomáticas com o objetivo de interceptar mensagens e de desvendar comunicações encriptadas. Hoffmann (2014, p.35) explica que a criptografia:

> [...] se preocupava principalmente com padrões linguísticos e com a análise de mensagens, como o próprio nome diz (criptografia, do grego kryptós, "escondido", e gráphein, "escrita"). Porém, é com a difusão e com a popularização da computação que ela atinge seu ápice. Atualmente, a criptografia é uma ramificação do campo da matemática. Na contemporaneidade, ela é usada principalmente em telecomunicações, em

> sites de comércio online e em sites e sistemas bancários, oferecendo um alto nível de segurança para os mesmos.

Diante desse contexto, vale ressaltar que a internet se deu na guerra fria, tendo em vista interesses militares e acadêmicos para melhorar as formas de comunicação entre seus usuários que, na maioria, bem no começo, eram mais usadas por hackers. Segundo (ASSANGE et. al., 2013), nosso “universo físico” proporciona a um indivíduo ou a um grupo de indivíduos que algo seja codificado com segurança e confiabilidade.

A criptografia diante do contexto de guerra se dá como arma para poder dificultar o roubo de informações e segurar que ela esteja segura diante do contexto de guerra ou não. Julian Assange escreveu um livro chamado Cypherpunks: liberdade e o futuro da internet e explica que os Cypherpunks defendem a utilização da criptografia e de métodos similares como meio para provocar mudanças sociais e políticas.

Segundo Assange (2013) apud Hoffmann (2014, p.36):

> Os cypherpunks são libertários: são pessoas que buscam proteger a liberdade individual da tirania do Estado tendo como “arma secreta” essa poderosa ferramenta. Até a década de 1990 essa ideia era bastante subversiva, afinal a criptografia era propriedade exclusiva dos Estados. Quando os primeiros ativistas da criptografia começaram a distribuir ferramentas criptográficas na forma de software livre, o governo estadunidense tomou medidas para impedir sua utilização, como, por exemplo, classificando-a como munição e restringindo a sua exportação.

Diante da liberdade individual para nos proteger da vigilância que existe na internet, a criptografia é uma grande ferramenta que impulsiona a forma de se comunicar em rede de forma segura. Segundo Assange (2013)

> Temos as soluções técnicas – serviços descentralizados, cada um hospedando seus próprios dados, criptografia, usuários confiando nos provedores próximos a eles, que os ajudam com serviços de dados criptografados e assim por diante. E temos as opções políticas, sobre as quais já falamos. [...] Precisamos de um software livre que todo mundo possa entender, que todo mundo possa modificar e que todo mundo possa examinar para verificar o que ele está fazendo. Acho que o software livre constitui uma das bases para uma sociedade online livre, para termos o potencial de sempre controlar a máquina, não permitindo que ela nos controle. [...] Precisamos de ferramentas de comunicação como o Tor [...] para ser possível nos comunicar só com as pessoas com as quais queremos nos comunicar.

Logo, diante das evoluções sociais, culturais e econômicas que a internet nos proporciona, não deixando de lado as possibilidades libertarias de comportamento na internet, na questão do anonimato e criptografia, vamos falar sobre alguns usuários que usam isso de forma positiva para uma determinada cultura que existe no ciberespaço: A cultura hacker.

3.4 Cultura hacker

Diante dos dados apresentados, voltados para história da internet, no qual Castells (2003) explora bem a questão sobre o desenvolvimento da internet, vemos que complementando isso, a cultura hacker faz parte desse nascimento da sociedade informacional.

Segundo Castells (2003) a cultura hacker desempenha um papel axial na construção da internet por duas razões: por um ambiente de inovação tecnológica e faz ponte com conhecimento originado da cultura tecnomeritocrática e seus subprodutos empresariais.

Os hackers sofrem um estereótipo ainda mal visto pela sociedade, pois a maioria não sabe que existem outros tipos de “hackers”. Diante da fala de Castells (2003):

> Os hackers não são o que a mídia diz que são. Não são uns irresponsáveis viciados em computadores empenhados em quebrar códigos, penetrar em sistemas ilegalmente, ou criar o caos no tráfego dos computadores. Os que comportam assim são chamados “crackres”, e em geral são rejeitados pela cultura hacker, embora eu pessoalmente considere que, em termos analíticos, os crackers e outros cibertipos são subculturas de um universo hacker muito mais vasto, e via de regra, não destrutivos.

Contracultura é claramente encontrada no desenvolvimento da internet, no contexto de Guerra Fria, no qual Castells (2003) explica. Pierre Levy (1999, p. 31) também constatou que é um movimento social nascido na Califórnia na efervescência da ‘contracultura’ tomou conta das novas possibilidades técnicas e inventou o computador pessoal.

Segundo (Silveira, 2010, p. 34) “O movimento social inspirado pela contracultura, que pregava distribuir o poder e emancipar as pessoas pelo acesso às

informações tem nos hackers a sua principal representação". O Hacker é aplicado para aqueles indivíduos que possuem um conhecimento superior aos outros em determinada área e utilizam essa isso para ajudar e não para destruir, conforme as mídias algumas vezes cometem esse erro terminológico. A definição original de hacker, segundo (Silveira, 2010, p. 34)

> Era a de "um programador de computador talentoso que poderia resolver qualquer problema muito rapidamente, de modo inovador e utilizando meios não convencionais"12. Entretanto, esse termo foi colocado em disputa quanto mais as redes informacionais adquiriram importância econômica e social. Em um primeiro momento, porque os compromissos dos hackers com a liberdade de informação e com o compartilhamento de códigos eram vistos como negativos para a acumulação.

Levy avalia os pontos centrais que observou na subcultura e quais são os elementos que formam uma ética construída nas comunidades hackers:

> Acesso aos computadores… deve ser ilimitado e total...Todas as informações deveriam ser livres...Hackers desconfiam das autoridades e promovem a descentralização...Hackers devem ser julgados por seus 'hackeamentos' e não por outros critérios, tais como escolaridade, idade, raça ou posição social... Você pode criar arte e beleza em um computador... Os computadores podem mudar sua vida para melhor (Levy, 2001, pp. 27-33).

Em geral tenta-se explicar que o pensamento hacker em si tem a ideia de que todo tipo de informação deve ser disseminada e não escondida, inclusive o conhecimento, não devem ser propriedade de ninguém e deve ser livre.

Himanen (2001, p. 18) nos fala que ao estudar a ética hacker em torno da plataforma Linux, constatou que o primeiro valor a guiar a vida de um hacker é a paixão ou algum objetivo interessante que gere alegria e realização.

Himanen (2001, apud Silveira, 2010) explicam que o hacker diante de uma paixão ou forma de resolver novos problemas e desafios, compartilham seus conhecimentos com a comunidade adquirem reputação combinando paixão com liberdade de para superar desafios.

Nota-se que a comunidade hacker age de forma libertária diante do desenvolvimento do conhecimento e sua própria disseminação para interação entre outros hackers da comunidade. Segundo (Castells 2003 , p.43)

> Há na cultura hacker um sentimento comunitário, baseado na integração ativa a uma comunidade, que se estrutura em torno de costumes e princípios de organização social informal. As culturas não são feitas de valores nebulosos. São enraizadas em instituições e organizações. Há uma

> organização desse tipo na cultura hacker, mas ela é informal; isto é, não é imposta pelas instituições da sociedade.

Por esses motivos dados antes diante da liberdade de expressão, liberdade informacional, vigilância, anonimato e que para que o conhecimento chegue a todos, num contexto de inovação tecnológica e interação entre os usuários, entraremos no método utilizado pelo estudo diante da problemática, tendo em vista quais fatores exercem mais influência na decisão dos usuários para uso da deep web?

4 METODOLOGIA

Este capítulo se divide em quatro subtópicos que explica de forma mais detalhada, o tipo de pesquisa que foi abordada, o local, no qual será aplicada a entrevista, os sujeitos que participaram e como foi feita a análise dos dados.

4.1 Tipo de pesquisa

De modo a atingir os objetivos propostos, achou-se pertinente a utilização de uma abordagem metodológica de cunho exploratório do tipo qualitativo. Sobre a pesquisa exploratória, na visão de Gil (1999, p.43) é desenvolvida,

> com o objetivo de proporcionar uma visão geral, de tipo aproximativo, acerca de determinado fato. Este tipo de pesquisa é realizado especialmente quando o tema escolhido é pouco explorado e torna-se difícil sobre ele formular hipóteses precisas e operacionalizáveis.

Diante disso, a proximidade do tipo de pesquisa permitiu analisarmos além de bibliografias, entrevistas com pessoas que tenham domínio do assunto estudado. Conforme Gil (1999, p. 109).

> A pesquisa bibliográfica é desenvolvida a partir do material já elaborado constituído principalmente de livros e artigos científicos. Embora em quase todos os estudos seja exigido algum tipo de trabalho desta natureza, há pesquisas desenvolvidas exclusivamente a partir de fontes bibliográficas.

Fez-se, então, conforme citado acima, um levantamento bibliográfico para a fundamentação teórica, a partir de pesquisa em livros, artigos e periódicos encontrados em bibliotecas e sites.

Colaborando com isto, diante do tipo de abordagem, Gerhardt e Silveira (2009, p. 31) utiliza-se da argumentação que:

> a pesquisa qualitativa não se preocupa com representatividade numérica, mas, sim, com o aprofundamento da compreensão de um grupo social, de uma organização, etc. Os pesquisadores que adotam a abordagem qualitativa opõem-se ao pressuposto que defende um modelo único de pesquisa para todas as ciências, já que as ciências sociais têm sua especificidade, o que pressupõe uma metodologia própria.

Com isso, apresentam-se os resultados através de percepções e análises, descrevendo a complexidade do problema e a interação de variáveis. Tendo em vista produzir dados a partir de observações extraídas de pessoas e lugares para interação com fenômeno estudado.

4.2 Local da pesquisa

O local escolhido para o estudo foi Grupo da Deep Web Brasil, no telegram[1] que é um mensageiro instantâneo simples, rápido, seguro e sincronizado entre todos os dispositivos. Segundo o Google play (2018) “O Telegram é o mensageiro instantâneo mais rápido do mercado, conectando pessoas de maneira única, distribuída entre diversos servidores ao redor do mundo”. Colaborando com isso, Canaltech (2018)

> Telegram é um aplicativo para troca de mensagens, considerado um dos principais concorrentes do WhatsApp. Ele apresenta funções semelhantes às dos demais nomes do gênero, permitindo envio e recebimento de conteúdos em texto, vídeo, áudio e imagem por meio de um pacote de dados ou de uma conexão Wi-Fi.

Figura 3 – Logo do Telegram

Fonte: https://logodownload.org/telegram-logo/telegram-logo-0/

[1] Informações do Telegram no Googleplay onde se faz o download do aplicativo - https://play.google.com/store/apps/details?id=org.telegram.messenger

Além disso, diante da questão de segurança o Telegram afirma que é mais seguro do que os mensageiros do mercado de massa como o Whatsapp e o Line. Para o Canaltech (2018) “O Telegram conta com alguns recursos mais específicos que envolvem a segurança e a privacidade das mensagens. Um deles é a possibilidade de iniciar conversas secretas”. Assim, com qualquer usuário em sua lista de contatos, as mensagens de áudio, vídeo, foto ou texto são automaticamente excluídos depois de tempo determinado pelo criador do chat.

De acordo com Junior (2009, p.97) as plataformas de mídias sociais “permitem aos usuários espaços ilimitados para armazenar ferramentas para organizar, promover e transmitir os seus pensamentos, opiniões, comportamentos e mídias para os outros”.

Logo, vemos o telegram, em especial o Grupo da Deep Web Brasil, como uma ferramenta que impulsiona as forma de interação entre os usuários para o mesmo objetivo, sendo esse o interesse pela deep web e áreas afins relacionadas à tecnologia.

O grupo Deep Web Brasil apresenta algumas regras feitas pelos seus administradores para manter a boa civilização dentro do grupo e para manter o foco. Com o comando/regras o Bot do grupo, que se chama, Robô ED, lista as regras: Proibições: CP; Pornografia de todo tipo; Gore; Perguntar como hackear algo/alguém; Divulgação indevida; Desrespeito aos membros; Pedidos esdrúxulos; Assuntos aleatórios diferentes dos interesses do grupo; Brincadeiras em excesso; Discussões de religião; EHI = BAN; Stickers que possivelmente ofendam alguém. Se não entende sobre o assunto, esteja aqui para aprender. Não partilhe desinformação, veja suas fontes; se não sabe do que algo se trata, deixe quem sabe falar. Qualquer dúvida contate um ADM com o questionamento. Detalhe: não é proibido falar de hacking. Apenas pedir de mão beijada.

4.3 Sujeitos da pesquisa

Foram entrevistadas pessoas que utilizam a deep web, periodicamente, até que haja uma saturação de dados que, conforme Glaser e Strauss (1967) explicam que “[...] a um momento no trabalho de campo em que a coleta de novos dados não traria mais esclarecimentos para o objeto estudado.”.

Acrescentando-se também que os entrevistados são maiores de 18 anos, contemplando diversas cidades do Brasil, que fazem parte do grupo deep web Brasil no telegram e que são ativos no grupo.

Para analisar e conhecer melhor como os usuários usam a deep web e assim alcançar respostas para os objetivos foi utilizada a técnica de entrevista que aconteceu via Telegram, pois foi a melhor forma de se comunicar com grupo que é composto por pessoas de diversos estados do Brasil.

A pesquisa foi dada por entrevista e com um guia previamente elaborado. Construir uma entrevista requer cuidado, para que as perguntas não fujam do assunto e nem influenciem as respostas dos entrevistados. Segundo Bogdan & Biklen (2010),

> "uma entrevista é utilizada para recolher dados descritivos na linguagem do próprio sujeito, permitindo ao investigador desenvolver intuitivamente uma ideia sobre a maneira como os sujeitos interpretam aspetos do mundo." Anderson & Kanuka (2003) consideram a entrevista com um método único na recolha de dados, por meio do qual o investigador reúne dados, através da comunicação entre indivíduos.

Dentre as diversas formas de entrevistas na literatura, foi utilizada a entrevista do tipo padronizada ou estruturada. Este tipo segundo Marconi e Lakatos, (2011, p. 281) é "quando o pesquisador segue um roteiro previamente estabelecido. As perguntas feitas ao indivíduo são pré-determinadas". A opção por esta modalidade se dá pelo fato de possibilitar uma aproximação aos entrevistados, contribuindo para analisar e conhecer melhor como os usuários usam a Deep Web, como se dá o anonimato em rede e analisar o caráter informacional em relação à sua dualidade informacional.

Dessa maneira, foi elaborado um guia de entrevista que contém 10 (dez) questões abertas, onde o entrevistado terá a liberdade de expressar suas experiências e opiniões. Sendo assim, essas questões serão organizadas em 04 (quatro) categorias: anonimato e criptografia; vigilância; deep web, comunidades virtuais e cultura hacker. As entrevistas foram marcadas, tendo em vista os horários e demais conveniências para os entrevistados, onde os mesmos foram esclarecidos sobre do que se trata a entrevista e se aceitam ser entrevistados ou não, sem nenhuma cobrança. As entrevistas não tiveram uma duração exata, pois cada candidato respondeu de acordo com seu tempo e aconteceram de forma virtual, à distância, pela plataforma de mensagens instantâneas Telegram.

Diante da entrevista, como um método de recolher os dados obtidos, foi usado um espaço amostral de fechamento por saturação. Corroborando com isso Fontanella, Ricas e Turato (2008, p.17).

> O fechamento amostral por saturação teórica é operacionalmente definido como a suspensão de inclusão de novos participantes quando os dados obtidos passam a apresentar, na avaliação do pesquisador, uma certa redundância ou repetição, não sendo considerado relevante persistir na coleta de dados.

Dessa forma, as entrevistas foram feitas com cada entrevistado de acordo com temas abordados no guia de entrevistas até que as respostas comecem a se repetir ou parecerem iguais, dando por fim as entrevistas.

4.4 Técnicas de análise dos dados

A técnica utilizada para análise dos dados foi análise de conteúdo que conforme Campos (2004, p.611) é "[...] compreendida como um conjunto de técnicas de pesquisa cujo objetivo é a busca do sentido ou dos sentidos de um documento."

Assim, análise de conteúdo é uma técnica que aponta uma descrição do conteúdo manifesto de comunicação de maneira objetiva. Para Bardin (2009),

> a análise de conteúdo temática deve ter como ponto de partida uma organização. As diferentes fases da análise de conteúdo organizam-se em torno de três polos: 1. a pré-análise; 2. a exploração do material; e, por fim, 3. A tratamento dos resultados: a inferência e a interpretação.

Inicialmente, foi feita uma transcrição de todas as entrevistas tiradas das conversas do Telegram com todos os entrevistados para um documento no World. Posteriormente foi realizada uma leitura de todas as informações (entrevistas) objetivando identificar de forma geral as respostas que tiveram mais relevância para comtemplar os objetivos propostos.

E por último, interpretação dos dados selecionados relevantes, divididos em suas respectivas categorias, permitindo, então, alcançar os objetivos que são: analisar os fatores que exercem mais influência na decisão dos usuários para uso da deep web, sendo o geral. E os específicos sendo: descrever como se dá o anonimato em rede na deep web e analisar o caráter informacional em relação à sua dualidade: lado positivo versus lado negativo.

5 ANALISE DE DADOS

Diante das entrevistas feitas pelos participantes do grupo Deep Web Brasil, no telegram, tendo em vista os dados levantados na realidade em que se deu a pesquisa, a análise dos dados foi dividida pelo seguinte agrupamento contendo em: Anonimato e Criptografia; Vigilância; Deep Web; Comunidades Virtuais e Cultura Hacker.

5.1 Anonimato e criptografia

Perante a primeira categoria, foi realizada a seguinte pergunta: Quais meios você usa para se tornar um anônimo na rede?

Nesse caso, a maioria dos entrevistados usa o anonimato para burlar ao máximo a captura de informação do seu computador e navegador. O Tor é a ferramenta no qual mais foi usada diante da forma de anonimato em rede. Como pode se observar nas respostas a seguir:

R.1: “Tô aprendendo ainda. Eu uso o navegador TOR, e vendo qual a melhor VPN”.

A VPN é uma rede privada que fica dentro da própria internet. Ela funciona como um túnel que dá acesso ao fluxo de informação, por meio de criptografia.

R.2: “Linux. Passando por uma rede anônima, como a onion/I2P, ou utilizando um conjunto de proxies (Proxychains)”.

O Linux possui diversas distribuições de características diferentes, dependendo da necessidade do usuário. Segundo (Castells, 2013.p,41) “O Linux é amplamente reconhecido como um dos sistemas operacionais mais confiáveis, em particular para computadores que trabalham na internet.” A função deste pacote proxychains é executar outros programas usando servidores proxy, criando assim uma camada de anonimato.

R.3: “Cara, existe vários meios: VPN, TOR, proxys e etc. Há uns tempos atrás eu usava o proxychains com o TOR para navegar”.

R.4: “sendo assim já usei alguns, mas como foi a rede onion a q mais acessei tinha o tor bem configurado e usava apenas ele.”

R.5: “Não faço muita questão de manter um anonimato na rede, até por que o sites que frequento não são nada de mais, porem uso de uma vpn simples.”
R.6: “Não tenho redes sociais. Nem fake. Meu número de celular é estritamente restrito a minha família. Meu telegram é emulado com um número gerado virtualmente. Não uso meu nome para nada na rede, meus e-mails são utilizados apenas para fins privados. Uso configurações e ferramentas para burlar ao máximo a captura de informação do meu computador e navegador. Não uso proxy ou VPN, mas faço uso do Tor também. Basicamente isso.”

Vemos aqui que além do uso do Tor para manter o anonimato, o R6 vive de forma anônima com seus comportamentos diariamente. Não usa redes sociais, limita seu número de celular somente para familiares, não usa seu nome verdadeiro na rede, ou seja, usa um nickname para se comunicar e, para uso do Telegram, ele emula um número virtual para ter acesso aos serviços de mensagens instantâneas.

R.7: “Não exponho meus dados pessoais hoje em redes sociais, não uso Windows, e não pago nada em cartão! Cadastro em sites ou algo do tipo coloco nome fictício, encomendas coloco pra entregar no trampo e assim por diante E sempre mudando de smartphone ou número de telefone.”

Temos outro exemplo de viver em forma anônima. O R7 não expõe seus dados em redes sociais, não usa o sistema operacional Windows, não paga nada em cartão, usa nickname para cadastro na rede, usa outro local para suas compras e, sempre troca de celular e número.

R.8: “no meu caso em especifico eu utilizo a rede Tor, que significa "the onion router". Darei um exemplo de como funciona: um usuário que acessar um site, mas ele nao quer revelar seu endereço IP, a marca que identifica seu computador. quando eles enviam um pedido, três camadas de encriptação são colocados em volta dele como as camadas de uma cebola. A mensagem é então enviada por uma serie de computadores que foram voluntários para agir como pontos de retransmissão. Conforme a mensagem passa de computador para computador, uma camada de encriptação é removida. Cada vez que é removida, tudo que o computador retransmissor pode ver é uma ordem que diz a ele para passar a

mensagem adiante. O ultimo computador retransmissor decripta a camada de encriptação mais interna, revelando o conteúdo da comunicação. Entretanto, o mais importante, a identidade do usuário é oculta.”

R.9:”Eu uso basicamente uso Tor e VPN”

R.10: “Usando proxy do tor , como por exemplo, no telegram tem suporte para usar proxy, e usar navegadores como tor browser , ou usar distro linux voltada para privacidade e anonimato como o tails e qubesOS.”

O Tails é um sistema operacional que pode ser usado em qualquer computador a partir de um pendrive, DVD ou emulado em uma maquina virtual. Ele tem como objetivo preservar a privacidade e o anonimato, e te auxilia a: usar a Internet de forma anônima e sem censura; contém conexões feitas à Internet que passam pela rede Tor; não deixa rastros no computador que o usuário utiliza; usa ferramentas de criptografia para seus arquivos, e-mails e mensagens.

O qubesOS é um sistema operacional voltado para a segurança, permitindo compartimentar as várias coisas que você faz isolando-as com segurança. Ele vai separar em qube, por exemplo, para uso de seus serviços bancários, outro qube para entrar somente em redes sociais e etc. Dependendo do que o usuário faça, ele pode isolar o modo de uso e navegação em rede.

Colaborando com isso (TOR PROJECT, 2017) nos fala que “[...] é um software livre e uma rede aberta que ajuda você a se defender contra uma forma de vigilância que ameaça a liberdade e privacidade [...]”. Outros entrevistados afirmam usar um conjunto de proxies, VPN ou até mesmo sistema operacional Linux, com distribuição em Tails e quebesOS voltadas para privacidade e o anonimato em si. Mas diante do objetivo, que é descrever como se dá o anonimato em rede na Deep Web, nota-se que, em grande parte, os entrevistados usam a rede TOR como algo primordial para ter acesso à Deep Web.

A segunda pergunta foi: Quais relações você acha pertinente para o uso do anonimato? Há como burlar a vigilância?

Neste aspecto, notou-se que os entrevistados afirmaram que o uso do anonimato é pertinente em alguns casos, por exemplo, no caso dos jornalistas e ativistas políticos que são perseguidos em alguns países em que a falta de informação e a vigilância é frequente. O acesso livre à informação, suas formas de compartilhamento e a forma de expressão também é mais uma forma positiva para o

uso do anonimato, entretanto, notou-se outro aspecto voltado para a dualidade do anonimato, no qual pode ser usado de forma maldosa, no caso de crimes cibernéticos, uso de sites ilícitos e roubo de informações partindo de alguns órgãos governamentais como a NSA. Conforme Carvalho (2010) explica: “denunciar um crime sem pôr a vida em ameaça; denunciar más práticas de sua empresa sem correr o risco de perder o emprego; Evitar perseguição política em países com governo repressivo”.

R.1: “Eu penso assim, nada é 100% anônimo, se tem como burlar a vigilância, a pessoa tem que ser muito boa, como eu entro na Deep Web só pra procurar livros e documentos sobre temas paranormais, eu não me preocupo tanto com privacidade”.

No caso do R1, para burlar a vigilância, o usuário não precisa ser muito bom (saber muito sobre anonimato em rede). Existem ferramentas de fácil acesso na internet que auxiliam o usuário a navegar de forma segura em rede. Como citado a cima, os próprios sistemas operacionais como, o Tails, QubeOS. Além do próprio navegador Tor, no qual o R2 fala logo abaixo.

R.2: “Privacidade e em partes segurança. Aquilo que você faz na web, por vezes, dependendo do país, pode te colocar em sérios apuros. O anonimato surge como uma forma de você ter o livre acesso à informação que deseja aceder ou compartilhar (comumente um vazamento de dados, ou um relato de jornalistas etc). A vigilância não pode ser 100% burlada, mas existem meios de amenizar seus efeitos. Mesmo utilizando uma rede como a TOR, o tráfego é conhecidamente anônimo pelo provedor, sabe-se que é a rede TOR. Por isso, existem meios de acessar à rede por nós pouco conhecidos, ou personalizados.”

R.3: “Sabemos que o anonimato é usado para o bem e para o mal, acredito que isso vai da mente de cada usuário. Sobre burlar a vigilância, claro que pode ser burlado! Exemplo: Outro dia eu tinha acabado de acordar, quando fui acessar o whatsapp, não estava conseguindo, o governo brasileiro barrou as conexões, logo usei um programa aqui, mudei a rota do tráfego e pimba, acessei o whatsapp.”.

R.4: “se eu entendi sua pergunta, acredito que deve se ter anonimato em tudo, pois ninguém precisa saber o que cada um acessa, mas existe um porém, pois muitos usam isso pra cometer crimes e manter-se em segredo, sendo assim não é algo q

deve ser disponível a todos, claro, todo tipo de informação passa por algum lugar... é só saber interceptar kkkkkk”

Nas respostas do R3 e R4, vemos que há um uso indevido do anonimato para fins ilícitos, muitos usam isso pra cometer crimes e manter-se em segredo.

R.5: “Depende muito do site/fórum que você frequenta. alguns fóruns de vazamentos de documentos (por exemplo) sempre tem chance de conter pessoas de órgãos públicos e tals. Ah, se você frequenta sites ilícitos talvez seja bom você usar ferramentas de anonimato kkkkkkk. Outra situação boa de usar anonimato são em países muito proibitivos (venezuela, china, koreia do norte) enfim, informações são barradas para essas pessoas e podem ser presas por simplesmente saber a verdade. Uma coisa muito obvia é: você nunca vai estar 100% anonimo, é algo extremamente complicado, mas vendo do outro lado, nenhuma vigilancia é 100% "acertiva", então, há sempre meios de burla-las.”

Sobre a resposta do R5, vemos que o anonimato não é 100% eficaz e que há formas de aumentá-la com as ferramentas citadas acima, porém também não há uma vigilância 100% sendo, assim, sempre havendo meios de burlá-las.

R.6: “Acho que o anonimato é mais importante para quem pode ser alvo de algo ruim. Por exemplo: pessoas que denunciam grupos criminosos ou políticos pode ter consequências. Para pessoas comuns que não gostam de ter informações capturadas que mais tarde são usadas para gerar algum tipo de vantagem sobre a pessoa, como induzir ela a uma compra, também é uma boa. Existem outros fatores mais e menos importantes. Sobre burlar a vigilância, 100%, acredito ser impossível, porque já nos termos de aplicativos, telefones celulares, computadores e afins cita-se muito sobre ter acesso a fotos, SMS, desempenho, navegação etc.”

R.7: “Rapaz eu trabalho na área de Tecnologia, então quanto mais as pessoas não souberem sobre mim mais longe eu Vou! Ô se tem... hoje em dia é muito fácil você passar por mim ou saber alguma coisa secreta, o uso do anonimato é mais para aquelas pessoas que trabalham com hackers não confunda hackers com crakers! Eu uso minha experiência para ajudar empresas a achar vulnerabilidades.”

No caso do R7, vemos que ele ajuda empresas a achar vulnerabilidades em sistemas, trabalhando, assim, com segurança da informação, que é uma área que trata diretamente com as falhas encontradas nos sistemas, para evitar que aconteçam ataques. Ele é considerado um 'Hacker ético' ou Pentester que atua com testes de intrusão que a própria empresa que o contrata permite que ele invada e encontre determinadas falhas para depois repará-las dentro do sistema. Ou seja, ele defende a empresa contra futuros ataques e roubo de informação.

R.8: “Para o uso do anonimato vou citar outro exemplo. Um lugar que o Tor ficou importante é o oriente médio. Durante a primavera Árabe, conforme os distúrbios se espalhavam pela região, ele se tornou uma ferramenta vital para os dissidentes... especialmente em lugares como a Síria. Um daqueles que a usaram desde o começo foi a ativista de oposição Reem al Assil. Palavras da própria "A vigilância na Síria é um problema muito sério para os ativistas ou para qualquer um, porque o regime sírio tenta o tempo todo entrar nos e-mails e FaceBook das pessoas para ver o que estão tramando, o que estão fazendo." Reem teve uma experiência pessoal da proteção oferecida pela Tor quando ela foi presa pela policia secreta. ela negou ter qualquer relação com qualquer ato de oposição, ou qualquer coisa e eles intimidar ela e disseram: "bem, veja, sabemos tudo sobre você agora, só precisamos que você nos diga." Mas ela sabia que eles não sabiam de nada. ao usar o Tor, ela era uma usuária anônima, então não puderam dizer que Reem estava fazendo isso e aquilo, esta vendo isso e aquilo. Então esse é um caso dos motivos pelo qual se usa o anonimato, especificamente na rede Tor.”

R.9: “O uso do anonimato ajuda para que a pessoa possa se expressar sem precisar se expor, para que ela ache um meio de ser ela mesma, de outro modo. (engraçado que esse comentário vale pro sentido bom e ruim rs) Burlar no modo exato, talvez não seria o certo, porém dificulta achar a pessoa rs.”

R.10: “O uso do anonimato não é só para praticar crimes, atualmente virou filosofia de vida, muitos jornalista utilizam do anonimato para se manter seguro na suas pesquisas , outro são perseguidos pelo estado e precisam de segurança. Sem falar que governos chineses ou NSA estão coletando diariamente nossos dados e se torna mais um motivo do uso do anonimato.
Burlar a segurança?, acredito que sim , mas não por muito tempo , sempre deve estar mudando táticas e formas mais seguras de anonimato.”

Sobre a vigilância, notou-se que há como burlá-la, mas somente em partes, no caso do exemplo dado pela R.8, vemos que a Reem teve sua experiência pessoal de proteção contra a vigilância da Síria usando o TOR quando ela foi presa pela policia secreta. O TOR seria um exemplo de amenizar a forma de vigilância que também não é 100%. De acordo com isso, (BRUNO, 2013, p. 28) nos fala da diversidade de tecnologias, práticas, propósitos e objetos da vigilância no contexto de consumo e interesses das pessoas. “Tem o propósito de vigiar não só os suspeitos de algum delito ou ato criminoso, mas também consumidores cidadãos comuns e internautas por meio de vigilância por tipos de interesse, transações eletrônicas [..]”.

Terceira pergunta: A criptografia é uma grande ferramenta que impulsiona a forma de se comunicar em rede de forma segura, você concorda com isso? Por quê?

Notou-se que a maioria das repostas sobre criptografia foram positivas por ser uma peça chave para uso do anonimato em rede. Hoffmann (2014, p.35) explica que a criptografia: “[...] se preocupava principalmente com padrões linguísticos e com a análise de mensagens, como o próprio nome diz (criptografia, do grego kryptós, “escondido”, e gráphein, “escrita”).”. Diante disso, vemos a criptografia como algo muito importante, como por exemplo, na troca de mensagens entre A e B (criptografia P2P), contra ataques de crackers, roubo de informações e para um bom funcionamento do TOR quando estiver navegando pela internet.

R.1: “Não concordo com isso, porque conheço muitas pessoas que tiveram conversas roubadas no Whatsapp, Facebook as as pessoas que conheço. Que foram hakeadas, clicaram em links maliciosos, a criptografia não acho que é 100% seguros, porque já vi falar que hackers invadiram empresas que investe alto em segurança e criptografia.”

R.2: “Concordo. A criptografia é peça chave dentro do contexto do anonimato, é ela quem inviabiliza para um interceptador, descobrir o conteúdo dos seus dados que trafegam. Como tudo hoje passa, em algum momento, pela internet, a criptografia é essencial para o anonimato ser minimamente possível.”.

Diante da resposta do R2, vemos que a criptografia codifica uma informação, de tal forma que somente o seu destinatário e o emissor da mensagem consigam acessá-la. “A criptografia é a tecnologia fundamental para a proteção da privacidade da mensagem (embora não do seu emissor, já que o computador de origem será identificado por seu ponto de entrada na rede eletrônica)” (Castells, 2013 apud Levy, 2001)

R.3: “Cara, esta pergunta é bem complexa, mas tentarei te responder de uma forma concisa e direta. A criptografia é algo muito importante, isso nem se discute, mas temos que ter em mente que tudo o que se faz, um dia é quebrado, essa é a lei da internet! Em outras palavras, criam uma nova criptografia, daí aparece uns camaradas mais doentes e acabam com a festa.”
R.4: “ahh sim, a criptografia já desbanca o meu ultimo argumento, pois com ela apenas quem tem a chave consegue entender a mensagem, apesar de nao manjar muito como funciona, o principio básico parece ser bom.”
R.5: “Com certeza, há diversos tipos de criptografias, das mais complexas as mais simples. Para conversas pessoais e sensíveis é SEMPRE importante usar algum meio que usa criptografia. Podemos ver o exemplo do telegram, ele tem uma criptografia centralizada (usada nos servidores dele) que até essa resposta nunca foi quebrada e o próprio telegram promete um prêmio pra quem conseguir, e alem disso, tem opção de criptografia P2P para uma segurança maior. Em diversos outros casos é necessário também como: login e senhas, inscrições em coisas publicas, armazenamento de dados, etc”
R.6: “Concordo em termos. A criptografia não é 100%, tampouco é usada 100% para o bem. Quero dizer: se por um lado ela estabelece uma conexão segura entre A e B conversarem sobre algo particular de cunho importantíssimo como, não sei, talvez uma denúncia também, por outro, pessoas más intencionadas fazem exatamente o mesmo com um propósito oposto, é o caso dos pedófilos na rede. É isso. Ela não é 100% segura e da margem para ambos os extremos.”

Na resposta do R6, vemos a dualidade da criptografia, pois ela pode servir para denunciar alguém sobre algo ilícito em rede, como também pode ser a chave para manter os segredos desses usuários que procuram por esse tipo de informação.

R.7: “Sim, concordo! Porque nunca se sabe quem tá por trás das redes sociais né... ou quem sabe um cracker invada sua rede por algum provedor de internet! Sempre é bom ter suas criptografias em dia é boa para sua segurança particular.”.
R.8: “sim, como falei lá na primeira pergunta, ela é fundamental pra o funcionamento da rede Tor.”
R.9: “Concordo, pois existem informações valiosas que precisam estar totalmente seguras contra possíveis roubos, nunca se sabe qual a consequência de um roubo de informação.”
R.10: “Concordo, pq quanto mais complexa a cripto , melhor , ou seja mais difícil se torna para descriptograr.”

Tivemos também, uma resposta negativa diante de uma das respostas sobre a quebra de criptografia em que, em alguns casos, pode acontecer por descuido do usuário (click em páginas maliciosas) ou erro de empresas no contexto de atualização de políticas de segurança da informação. Notou-se também, mais uma vez, a questão da dualidade diante da má intensão do uso da criptografia no contexto informação ilícita na rede.

Devemos notar que a internet muda constantemente. Sendo ainda importante frisar que houve uma potencialização tanto da comunicação, quanto dos fatores sociais dentro da rede. Surgiram novas necessidades de discussões para lidar com esse avanço na sociedade e debater o anonimato dentro da rede é essencial.

Qual o significado dessa busca pelo anonimato dentro da rede? Qual seu real sentido? O anonimato se tornou um fator social dentro da rede podendo ser desejável ou indesejável para alguns, sendo assim, é importante deixar claro que devemos da prioridade para a liberdade de expressão de forma legal sem ferir os direitos humanos.

A partir desse pensamento (Abreu, Gomide, Vieira, et al) dizem que,

> O anonimato garante uma forma de expressão, assegura o direito de defender a liberdade de informação, de enfrentar o poder instituído e a mídia. Estão livres os ideais políticos e sociais, as várias possibilidades de ser, sentir e agir, entre eles, ajudar um jornalista internacional, em um país aliado à censura, a se comunicar com sua respectiva redação.

Vemos o discurso dos autores com um viés voltado para o direito de defender a liberdade de expressão da informação indo contra os padrões que a mídia nos impõe, além da característica de criticar ideais políticos e sociais partindo dentro de um país aliado a censura.

> É natural que um governo instigue sua população, tornando-a alienada, e através de seu discurso demonstra a notícia de seu interesse distorcida. Tornar informações confidenciais públicas é perigoso. Porém, é necessário considerar aí o papel fundamental do jornalista: informar e servir à população, mesmo que isso vá contra o sistema político vigente. (Abreu, Gomide, Vieira, et al)

Isso não é somente para os jornalistas, mas também para a população como um todo. Mas sabemos que o anonimato dentro da rede também favorece e beneficia quem vive e procura por coisas ilegais.

Diante dessa dualidade do uso do anonimato na rede, vemos um embate diante das considerações de (Abreu e Nicolau) sobre o outro lado do anonimato.

> Diversos grupos beneficiam-se do anonimato para compartilhar conteúdo criminoso carregando o espaço com páginas de pedofilia contendo imagens e vídeos explícitos, páginas de necrofilia, anúncios de assassinos de aluguel e suas tabelas de preços que variam de acordo com a importância social da vítima, zoonecrofilia, fóruns de canibalismo, além de uma espécie de Mercado Livre onde se pode encontrar desde drogas até armas e órgãos.

Logo, vemos que a Deep Web serve também para publicar conteúdo polêmico ou ilegal, usando o anonimato como forma de proteger a identidade dos usuários.

Sobre os dois discursos citados acima, devemos entender que realmente há uma dualidade diante da deep web sobre o anonimato e que isso é bom por um lado e ruim por outro. A liberdade na internet é fundamental dentro da rede, para ambos os lado, porém depende somente de cada usuário a forma de como usar esse anonimato dentro da rede. Não tem como impedir o lado negativo do anonimato para sempre, pois sempre existirão pessoas com esses propósitos em qualquer lugar do mundo. Mesmo antes de existir a internet havia esse tipo de procura por determinados serviços e materiais ilícitos. Esse lado negativo do anonimato é que prejudica o modo de como as pessoas veem a deep web.

Os entrevistados buscam o anonimato como forma de burlar a vigilância dada pelo governo e como forma de se expressar dentro da rede sobre os diversos temas encontrados lá e se sentindo mais seguros. Esse é o sentido que os usuários buscam e o porquê de se tornarem invisíveis dentro da rede. Conforme (Abreu e Nicolau) afirmam:

> A identidade oculta remete à ideia de segurança, assim como um recinto próprio, separado do ambiente público e da intromissão alheia por paredes sólidas e portas fechadas. O anonimato é a condição ideal para deixar aflorar pensamentos e sentimentos privados, que sob tal status podem ser convertidos em ações livres dos pudores e censuras que cerceiam uma identidade revelada. Todavia, esse refúgio no anonimato não exprime apenas uma preocupação com as histórias e objetivos particulares que movem cada ator. Além de revelar as escolhas fundamentais que o sujeito faz sobre si mesmo, entram em pauta questões coletivas que envolvem política, economia, valores éticos e morais, ideais libertários e, muito frequentemente, até, práticas criminosas.

O anonimato minimiza o olhar social de quem tenta controlar, manipular e armazenar o que você faz dentro da rede. É a condição para deixar seus pensamentos, criticas e emoções que são somente seus, diante dos status anônimo, convertidos em ações livres de se expressar. A criptografia funciona somente como ferramenta para auxiliar o anonimato em si. Sendo a prática para os princípios e técnicas de comunicação segura na troca das informações dentro da rede

5.2 Vigilância

Quarta pergunta: você acredita que toda informação disseminada na Surface Web é controlada por governos e/ou corporações?

Nota-se nessa categoria a maioria das respostas dos entrevistados dizem que toda a informação não é controlada por governos ou corporações, mas em alguns casos, sim. Há um controle sobre o que estamos fazendo, e nossas escolhas diante das pesquisas feitas nos mostram propagandas sobre determinado produto ao qual pesquisamos. Canais, blogs, grupos de Facebook são apagados, dependendo do assunto que é proposto. Em determinados países pode a haver sim um “certo” controle. Corroborando com isso, (ASSANGE, 2013, p.36)

> A vigilância é muito mais óbvia atualmente do que quando o grosso dela era feito apenas pelos Estados norte-americano, britânico, russo e alguns

> outros, como o suíço e o francês. Hoje isso é feito por todo mundo e por praticamente todos os Estados, em consequência da comercialização da vigilância em massa. E ela tem sido muito mais totalizadora agora, porque as pessoas divulgam suas ideias políticas, suas comunicações familiares e suas amizades na internet.

Em alguns países mais repressores, como Arábia Saudita e Coreia do Norte, acham que a internet afeta a capacidade da população de definir a realidade, usando, assim, a vigilância em altíssimo nível por medo que a internet pudesse afetar seus métodos de governança.

R.1: “Acredito sim, na surface o governo tenta controlar o máximo possível, creio que eles veem o que estamos fazendo, porque hoje fui pesquisar. No Wal-Mart sobre telefone e uma geladeira, e advinha, entrei lá no Facebook eles estavam fazendo propaganda da mesma geladeira que procurei e o mesmo modelo de celular.”

Diante da resposta do R1, vemos a existência de ferramentas de controle que, segundo (Castells, 2013.p, 141). “Uma variedade de tecnologias de controle emergiu dos interesses entrelaçados do comércio e dos governos”. Assim vemos na resposta acima.

R.2: “Não controlada diretamente, mas pode ser. Um website com um conteúdo considerado ilegal pode – e vai – rapidamente ser banido da rede, ou de seu provedor, ao menos, e por vezes os seus mantenedores serão presos. Por vezes, uma causa legítima, como o Wikileaks também cai sobre esse véu do ilegal, e é onde o anonimato da rede auxilia na livre expressão do indivíduo e direito à informação.”

R.3: “Acredito que a maioria, o simples fato é de canais, blogs, grupos de Facebook de conservadores por exemplo, são apagados. Falo isso independente da orientação política das pessoas. Apesar que tenho minha visão sobre o mundo, é claro.”

R.4: “claro q não, mas com certeza existe muita coisa q é manipulada.”

R.5: “Toda não, até porque não tem como, é igual o pessoal que diz que quer "regulamentar" a bitcoin. É impossível e provável”

R.6: “Não acredito nisso. As informações propagadas na Surface podem partir de qualquer indivíduo. É uma rede livre. Cada um fala o que quiser. O que muda é o alcance.”

R.7: “Eu acredito até onde eu sei são vários provedores espalhados ao mundo a fora... Sei que começou com os britânicos depois daí eles fecharam e eu não sei como foi parar depois que o CEO da deep web foi preso só sei que eles ficam ocultos a vários países creio que não é controlada por governos, mas nunca se sabe o dia de amanhã!”

R.8: “não toda informação, mas uma boa parte sim.”

R.9: “Eu não diria toda, existem aqueles que conseguem resistir a pressão e abrir os olhos de quem ainda não consegue. Mas enorme parte é sim manipulada, direta ou indiretamente.”

R.10: “Acredito que não toda a informação, mas os principais meios e conhecidos, como redes sociais, são um exemplo de controle de dados pessoais.”.

Um exemplo de controle de dados pessoais que aconteceu recentemente foi a da Cambridge Analytics, no qual a empresa coletou bilhões de dados pessoais de norte americanos, pelo Facebook para montar perfis em função ao da candidatura de Donald Trump.

Diante disso, Bruno (2013, p.123) nos diz que informações pessoais e publicações em redes sociais que divulgamos podem ser sim capturadas para determinados fins.

> Num estrato mais superficial e explícito, há as informações pessoais e publicações que divulgamos voluntariamente na web (postagens em blogs, dados de perfil e conversações nas redes sociais). Mas além e aquém desse nível declarativo e sua respectiva inscrição, uma série de outras ações – navegação, busca simples cliques em links, downloads, produz ação ou reprodução de conteúdo – deixam vestígios mais ou menos explícitos, suscetíveis de serem capturados.

Assim, podemos dizer que há uma mineração que permite a extração de dados pessoais para diversos fins, um deles, por exemplo, seria para uso comercial para induzir a compra de algum produto como foi citado acima na resposta do R1. Sites da web e redes sociais, convertendo-os em informação estruturada para análise. E vemos que nossos entrevistados acham que certa parcela do conteúdo é manipulada por governos e instituições.

Quinta pergunta: Como você enxerga, de forma geral, a privacidade das pessoas hoje em dia?

Diante das respostas sobre privacidade nota-se a falta de esperança sobre o comportamento dentro da rede. A maioria das pessoas que acessam a internet não se importa nem com segurança, nem com privacidade. Fazem questão de se mostrarem e ainda mostrar os outros. A falta de informação sobre a importância e o valor de informações pessoais é deixada de lado, dando espaço ao exibicionismo.

R.1: "Tem pessoas que não ligam. Para privacidade, porque pelo que eu vejo nos pcs que formato. As pessoas não instalam nem um antivírus. E os pcs que eu peguei pra mexer tava cheio de vírus, na minha Opinião 70% da pessoas que tem seus. Dados vazados, são um pouco leigas. Com tecnologia."

R.2: "Um resto de esperança de uma minoria de pessoas que lutam por esse direito. A maioria das pessoas que acessam a internet não se importam nem com segurança, nem com privacidade. Num ponto mais específico, elas preferem ainda abrir mão disso, para obterem "segurança" por parte de seus governos, que controlam e manipulam tudo, com, ou mais comumente sem essa permissão."

R.3: "Hoje em dia não se tem mais privacidade, pois as pessoas fazem questão de se mostrarem e ainda mostrar os outros, confesso a você que ultimamente ando me privando mais de me mostrar, a não ser que seja para algo produtivo para a sociedade. Tenho em mente em não expor futuramente minha esposa, meus filhos e etc (quando eu achar a mulher que irei casar ainda KKKK."

R.4: "De forma geral ninguém liga pra isso, as pessoas só querem saber q as coisas q elas usam funcionem, não importa a maneira q ela funcione kkk".

R.5: "Falta de informação/raciocínio define. Tem pessoas que não se atentam que os serviços que elas utilizam, usam as informações dela. Em certo ponto chega a ser crime, mas muitas vezes não. A privacidade é dada quando assinamos os termos da própria, o bom é que pelo menos o Facebook não é obrigatório, já as informações que estão com o governo.".

"As tecnologias de investigação referem-se à construção de bancos de dados a partir dos resultados da vigilância e do armazenamento de informações rotineiramente necessárias.". (Castells, 2013 apud Garfinkel, 2000). Diante da

resposta do R5, vemos que a falta de informação define o descuido sobre a privacidade das informações em rede, assim tornando o usuário como alvo para pesquisa de mercado e para uso da politica.

R.6: “Vejo com absurdamente pouca. E não somente pelo problema citado na questão 2, mas também porque as pessoas se expõe muito em suas redes sociais sem tomar os devidos cuidados, isto é, elas se exibem para o público.”.
R.7: “Kkkkkk Muito aberto... Eles não ligam para as suas privacidades expõe suas senhas na mesa, falam para amigos ou colegas de trabalho As pessoas tem que entender nos dias de hoje que a tecnologia avançou muito Precisamos muito de pessoas como "Nos" para ensinar a estes ser humanos o que é privacidade Eles não tem noção nenhuma do que os Anônimos são capazes de fazer Nem precisa ser um hacker pra saber que a privacidade da pessoa é importante uma pessoa estudada com ensino médio completa ela já deve saber.”
R.8: “Bom, acho que todos temos direito a privacidade, mas nos dias de hoje com os escândalos da NSA esse direito está ameaçado, sendo uma alternativa o uso de redes anônimas.”

A NSA (Agência de Segurança Nacional dos EUA) contém todos os meios necessários para transitar e ter acesso às informações bancárias, correios ou documentos, por exemplo. Tudo pode ser lido pela NSA, segundo Edward Snowden, que é analista de sistemas e trabalhou como ex-administrador de sistemas da CIA e na própria agência de segurança nacional.

R.9: “Se eu pudesse resumir em uma palavra, escolheria" comprometida", a td momento, em todo lugar, tem alguém buscando dados seus, sabendo onde vc está ou oq vc fez.”

De acordo com a resposta do R9, o grande corpo de informações coletadas tanto individual como coletiva é gravada e processada para possível uso no futuro.

> [...] contido em seus registros eletrônicos, de pagamentos por cartão de crédito a visitas de websites, correios eletrônicos e chamadas telefônicas. No ambiente tecnológico atual, toda informação eletronicamente transmitida é gravada, podendo vir a ser processada, identificada e combinada numa unidade de análise coletiva ou individual. (Castells,2013.p,142)

Logo, em outros casos, os governos e instituições, visam indivíduos, já que dada pessoa pode ser caracterizada por um grande corpo de informação. Nossos usuários acham a privacidade hoje em dia uma preocupação diante de alguns comportamentos na rede.

R.10: “Estão cada vez mais expostos, e as pessoas estão cada vez menos preocupados com isso.”

5.3 Deep web

Sexta questão: Qual é a importância da Deep Web para as sociedades da atualidade?

Sobre as respostas de qual a importância da Deep Web na sociedade, notou-se que a maioria dos entrevistados apresentou o livre acesso à informação como algo fundamental para os usuários, servindo como um canal para fluir a informação sem censura. Incluindo assim, também, a privacidade, forma de expressão e o conhecimento, mas também depende muito da pessoa. Corroborando com isso, (Santos e Marchi, 2013)

> A DW pode ser usada de forma positiva ou negativa, isso depende do caráter de cada um que a usa, se a busca for relacionada a conteúdo acadêmico e livros, por exemplo, será encontrado, entretanto se a busca for por pedofilia, tráfico de drogas ou até mesmo assassinato de aluguel também será encontrado.

Se a pessoa procurar por algo ilícito, ela vai encontrar também. Infelizmente, existe o lado negativo, ou seja, sua dualidade diante do conteúdo encontrado lá.

R.1: “não sei se a deep web é importante, mas na minha opinião e um mundo novo, cheio de descoberta ,cabe a cada um de nós usar ela para o mal ou para o bem.”
R.2: “Essencialmente, servir de livre canal para a informação fluir, seja qual for o seu intuito, o direito à informação é, a meu ver, o direito fundamental do ser. Claro que, acaba servindo para fins ilegítimos, mas ao criar um ambiente seguro para todos,

esse tipo de oportunidade se abre para criminosos – que hora ou outra são presos, com frequência.”

R.3: “Cara, isso depende muito do país de origem da pessoa, pois quando é tranquilo eu não vejo tanta necessidade assim, MAS no caso de ser fechado (Coréia do Norte por exemplo..) eu acredito que seja bem válido. Daí é muito importante, uma pessoa lá de dentro poderá informar ao resto do mundo o que se passa no seu país.”

R.4: “ela é um meio de distribuir informação secundaria, onde cada um pode postar oque acredita ser útil. Claro existe os casos que a deep web é um meio único de informação confiável, mas são casos raros”

R.5: “divulgação de informação sem censura”

R.6: “Depende do local. Existem países em que a internet não é livre, por tanto, não permitem que a população acessem determinados sites, inclusive os de notícias. Para evitar um alienamento e para se ter o estudo livre, acredito que seja necessário o uso da Deep Web. Mas, para países como o Brasil, onde a internet é basicamente livre e muito grande, o uso dela fica banal e comumente os criminosos a utilizam, também os curiosos em busca de atrocidades que se quer existem por lá.”

O R6 nos fala que em alguns países a internet não é livre e não permitem que a população tenha acesso a informação e controlando seu fluxo, assim alienando a sociedade. A deep web seria a forma de burlar isso.

R.7 “A importância hoje na DW "PARA mim" é livros de estudos de programação e linhas de código que eu não acho no provedor da google! Agora para a sociedade seria importante eles saberem que tem muitos remédios para doenças raras e estudos que comprovam o que eles querem que são pagos na internet no dia de hoje. Enfim para pessoas comuns como eu falei ... tem muita coisa boa que na internet não tem de graça que o governo corrupto coloca imposto a tudo! Lá você encontra o que você procura sem taxas !”

R.8: “As importâncias são varias, isso inclui a privacidade, conhecimento. Muitas pessoas vão la em busca de aprender mais sobre algum assunto, por isso existem diversas bibliotecas por lá, também é importante pelo ativismo politico como citei no caso da Reem.”

R.9: “eu acho mt importante, não pq "é uma rede descentralizada q vc pode fazer oque quiser e ser anônimo"... mas pq lá vc pode acha o seu espaço, achar documentos, livros, filmes e oq mais quiser, q tenha "desaparecido " na surface... se vc mora em um país em q é proibida a navegação em um certo tipo de site, vc encontra na deep web... e lá vc literalmente acha o q procurar, por isso, se deve o cuidado.”

R.10: “Digo na minha opinião que a deep web não irá atender a todos , mas atenderá para aqueles que querem algo especifico, como por exemplo. seria muito importante para aqueles que gostariam de expressar suas opiniões em um mundo livre.”

Sétima questão: você acha que a Deep Web só tem conteúdo informacional ilícito? Pedofilia, necrofilia e zoofilia, dentre outros, por exemplo.

Sobre a existência de somente conteúdo ilícito na deep web, nota-se nas respostas que, além dos conteúdos ilícitos, também existem os conteúdos bons, que servem como fonte de informação para muitos usuários que a acessam. Livros, filmes, jogos, artigos, blogs e fóruns dos mais variados temas, como politica e liberdade de expressão. Como já falado acima sobre a dualidade em diversos outros aspectos, sobre o anonimato, por exemplo, que pode ser usado de forma positiva ou negativa, vemos aqui também uma dualidade informacional diante do conteúdo dentro da deep web. Em algumas respostas, como a do R4, vemos que esses conteúdos ilícitos não estão somente na deep web, mas também na própria surface web, como por exemplo, o whatsapp, telegram e facebook.

R.1: “não é só isso. tem muita coisa boa lá, já achei livros, filmes que não conseguia baixar na nossa camada tem ótimos fóruns de debate sobre vários temas.”

R.2: “Não. A informação flui na Deep Web da mesma forma que flui na Surface Web. A Deep Web é, essencialmente, uma surface anônima e segura. Grande exemplo de informação é o Wikileaks, ou mesmo grandes blogs ou fóruns, onde as pessoas simplesmente gostam da informação, e de compartilhá-la livremente.”

R.3: “Na verdade tem de tudo, vai do cara procurar o que quer.”

R.4: “nao, mas eles existem la como qualquer outra rede. "redes" como whatsapp, telegram, ate fecebook , kkkkkk essa bostas existe em tudo q é canto”

R.5: “obviamente não, algumas mídias tentam nos vender que deep web são exatamente essas coisas que você citou. Mas com deep ou sem deep, elas existem. Fraudes existem em ambos os ambientes e virus igualmente. Resumindo: Deep Web é uma surface sem censura.”
R.6: “Com toda certeza e experiência própria, a Darknet, em todas as suas redes, não abriga somente conteúdo ilícito. Contudo, infelizmente, acredito que o conteúdo ilícito seja o mais buscado. Eu prefiro dar ênfase aos livros, artigos, transparência política e liberdade de informação que os povos trocam entre si dentro das comunidades voltadas para determinados assuntos, tipo política.”

Na resposta do R6, vemos que o conteúdo ilícito, ele acredita, é o mais buscado como Martins e Silva nos dizem: “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 [...]”. Mas também existem as trocas de informações diante das informações de cunho politico.

R.7: “N como eu falei eu uso para outros fins. Citado a cima. Livros de estudos de programação e linhas de código que eu não acho no provedor da google.”
R.8: “kkkk essa é a maior definição errada sobre a Deep Web que vemos rolando por ai, como já falei anteriormente um dos motivos pela criação do Tor foi para que pessoas que sofressem algum tipo de repressão pudessem usufruir do anonimato dessa rede e pudesse se expressar. Também tem o caso do WikiLeaks, que foi muito importante pelos seus vazamentos e dentre outros casos, existem diversos. mas.. junto com o uso correto da rede, veio o uso errado, ou ilícito com você citou, de acordo com a resposta da primeira pergunta, fica quase impossível descobrir a verdadeira identidade dos usuários do Tor, sendo assim varias pessoas mal intencionadas começaram a criar sites ilicitos/criminosos. Dentre eles estão: Contrato de serviços (hackers, Hitman e etc), mercados negros (venda de drogas, cartões clonados, dinheiro falso e etc.), sites de pedofilia, necrofilia, estupro, venda de documentos falsos e dentre outros serviços ilegais.”

Corroborando com as respostas do R6 e R8, vemos que diante da expansão tecnológica e econômica, veio também à criminalidade.

> as mais diversas relações sociais e econômicas se expandiram com o avanço das tecnologias de comunicações e transportes, os crimes também ultrapassaram fronteiras, eis que intimamente ligados à vida em sociedade, não se tratando de patologia, mas fato social normal. Dito isto, imperioso destacar, então, que, com o advento da globalização, surgiu um novo fenômeno: o crime global. (Pompéo e Seefeldt, 2013, p. 443)

Assim, vemos que o armazenamento de dados ilegais, sites de pedofilia, necrofilia, estupro, venda de documentos falsos e dentre outros serviços ilegais fazem parte desse fenômeno global que acontece na internet.

R.9: “não, de forma alguma é exclusivamente algo ilícito ou maldoso, oq você procura, vc acha, seja bom ou ruim, mas o mais importante é nunca acreditar em td o q ve”

R.10: “Não, é mundo de dois lados , existem tanto esses casos horriveis ,quanto tbm tem grupos ou organizaçoes anti-cp (contra pedofilia) Sem falar dos inumeros acervos de livros espalhados , fóruns de debates politicos e assuntos de conhecimentos gerais , blogs , e downloads e jogos.”

Santos e Marchi (2013) nos falam que “Mesmo sendo perigosa a DW tem muito a nos oferecer para quem sabe usar, é uma experiência enriquecedora, uma biblioteca inacabável de conteúdos de todos os tipos livros, filmes, jogos e demais interesses.“. Como o R8 nos responde, vemos que junto com o uso correto da rede, veio o uso errado também, ou seja, quem faz a Deep Web é seu próprio usuário. Depende somente dele o que ele deseja procurar.

Nossos entrevistados acham que não existe somente esse tipo de conteúdo dentro da Deep Web. Existem também as coisas boas, citadas várias vezes acima.

Oitava questão: o que te leva a buscar informações na Deep Web ao invés da Surface Web?

Podemos analisar que nessa pergunta os entrevistados já apresentam algumas características da sétima questão tendo vista sempre a forma de liberdade dentro da Deep Web por meio das diversas fontes de informação, assim já saturando bem as respostas dadas.

R.1: “Eu fui por curiosidade, vi vídeos no youtube de como entrar, e fiquei feliz em achar as coisas que eu queria, porque eu gosto de ler livros e relatos sobrenaturais, e lá tem muitos fóruns sobre temas paranormais, e podemos falar de politica e outras opiniões sem preocupar muito”

R.2: “Como citado anteriormente, a privacidade é fator fundamental para a necessidade do uso da Deep Web. Pensar que meus dados não serão vendidos ou rastreados me dão um mínimo de felicidade ao navegar nessa imensidão de informação que é a Internet.”

R.3: “Então, tem certas informações que na surface não tem ou passa a ter depois de um tempo, como o tempo é ouro, o cara tem que se informar e não perder tempo.”

R.4: “Já parei de participar em tudo q fazia lá, não lembro nem a ultima vez q acessei algo diferente de youtube kkkkk, mas falando serio acho q não tem muita diferença no geral”

R.5: “No meu caso particular, a falta dela da surface. Artigos, livros. Algumas redes da deep eu ja usei por pura curiosidade. Como por exemplo, a ZeroNet, me encantei pelo modo como eles fazem os sites, é até mais simples do que hospedar um site na surface, fora os blogs e fóruns criados la. É uma aventura para desenvolvedores web”

R.6: “Eu prefiro dar ênfase aos livros, artigos, transparência política e liberdade de informação que os povos trocam entre si dentro das comunidades voltadas para determinados assuntos, tipo política. essas aí são as coisas que eu busco, agora, o que me leva a buscar é realmente a liberdade em relação ao conteúdo. Aqui se tem muito problema com direitos autorais, por exemplo, por lá não. Mas basicamente tudo que se tem lá se encontra aqui, a diferença é o tempo em que permanecem o online. Aqui na Surface as coisas somem facilmente. Lá não.”

Segundo Kohn (2012), pode-se encontrar livros sobre religião, psicologia entre outros e outros assuntos curiosos, além de acervos audiovisuais e de músicas. Existem vários fóruns de perguntas e respostas, onde os usuários trocam informações e interagem de forma anônima.

R.7: “livros de estudos de programação e linhas de código que eu não acho no provedor da Google! Agora para a sociedade seria importante eles saberem que tem muitos remédios para doenças raras e estudos que comprovam o que eles querem que são pagos na internet no dia de hoje. Enfim para pessoas comuns como eu falei ... tem muita coisa boa que na internet não tem de graça que o governo corrupto coloca imposto a tudo! Lá você encontra o que você procura sem taxas !”
R.8: “O anonimato e a disponibilidade do conteúdo, na maioria das vezes você encontra tais conteúdos na surface, mas alguns são mais acessíveis na Deep. Serviço de e-mail anônimo, é um que uso bastante. Bibliotecas, politica, hacktivismo, e tutoriais.”
R.9: “Na Deep existem mais fontes específicas sobre certos assuntos, existem fóruns, o q permite buscar as informações com pessoas e n apenas em sites de jornais.”
R.10: “Normalmente busco na Deep Web porque tem documentos, arquivos e informações mais verídicas em certos casos. Na Surface Web, encontramos muitas informações falsas e alteradas.”.

De um modo geral, vemos que a deep web possui uma dualidade, assim como o próprio status do anonimato. O conteúdo que existente é vasto e consegue atender diversos temas e gostos pela rede. Ela atrai pessoas bem intencionadas, que buscam informações preciosas e escondidas dentro da rede, como também atende um público mal intencionado. Mas qual o sentido de procurar informação dentro da deep web ao invés da surface web?

> A DW pode ser usada de forma positiva ou negativa, isso depende do caráter de cada um que a usa, se a busca for relacionada a conteúdo acadêmico e livros, por exemplo, será encontrado, entretanto se a busca for por pedofilia, tráfico de drogas ou até mesmo assassinato de aluguel também será encontrado. (Santos,2013)

Os entrevistados buscam informação na deep web, principalmente pelas fontes especificas sobre alguns assuntos. Os fóruns de discussões também fazem parte de suas fontes de informação. Podem-se encontrar conteúdos na surface, mas alguns são mais acessíveis na deep web, serviço de e-mail anônimo, bibliotecas, politica, hacktivismo e tutoriais.

Entretanto também existe o lado negativo da informação dentro da deep web. Diante do anonimato, usuários se beneficiam da invisibilidade da rede para contribuir de forma negativa, assim vemos um embate que, é normal por conta da dualidade existente dentro da rede. Reforçando o lado negativo e as respostas dos entrevistados sobre o lado negativo da deep web. Vignoli e Monteiro (2016) dizem que “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”[..]. A Hidden Wiki tem uma coleção de links para outros sites .onion, e artigos de enciclopédia.

> **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; intercepção 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 crendices**: 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. (Vignoli e Monteiro, 2016)

Infelizmente, a maioria dos conteúdos da deep web é de baixa qualidade e existe público para isso, porém para vê-los, depende somente do usuário. Os

entrevistados sabem exatamente o que se passa dentro da deep web, mas como dito em suas respostas, na maioria das vezes, eles buscam somente sobre o lado positivo dentro da rede.

5.4 Comunidades virtuais e cultura hacker

Nona questão: você contribui de alguma forma para alguma comunidade, fórum, grupo na surface Web ou na deep web no contexto de cultura hacker?

Os entrevistados, em alguns casos, não sabem muito bem como é a atividade hacker dentro da deep web. Alguns não contribuem, entretanto outros participam ativamente na surface web ao compartilhar informações à respeito do tema em fóruns, páginas no Facebook e no Telegram. Tendo o R6 como o único com uma filosofia cyberativista.

R.1: “da cultura hacker não entendo nada, sobre esse tema não sei de nada, mas em relação a fóruns de sobrenatural e óvnis estou sempre estou conversando.”
R.2: “Não. Ainda que por muitas vezes legitimo e necessário, o viés hackativista da Deep Web é turvo, não se tem muita certeza do que ocorre, também por não saber de quem se trata, e não conseguir ter certeza das reais intenções dos indivíduos envolvidos.”
R.3: “Oficialmente não, mas ajudo no que eu posso, em outros momentos me convidaram para escrever artigos, mas não aceitei.”
R.4: “não sei dizer se contribui, mas tentava ficar sempre a par do q acontecia”
R.5: “Não querendo divulgar mas ja divulgando, faço parte do blog online ctrlzeta.com.br onde um conjunto de estudantes criam artigos e postagem sobre diversos aspectos mas principalmente sobre tecnologia (por que hacker não é aquele que sabe invadir facebook né). Também ajudo no grupo do Deep Web Brasil no telegram, divulgando informações desse tema, acredito são comunidades voluntariamente unidas que enriquecem o conhecimento”
R.6: “Contribuí em relação a cyberativismo, tanto quanto contra políticos corruptos e grandes empresários, mas também contra alguns tipos de crimes digitais.”

Diante da resposta do R6, vemos cyberativismo, no qual ele já fez parte, como um movimento voltado para a luta contra crimes digitais em rede, política, socioambiental e sociotecnológica.

R.7: “Não Jack só pessoalmente, como falei eu entro procuro o que eu quero é saio, tenho um Notebook só para isto é não pesquiso em casa ou no trabalho só quando estou na biblioteca da faculdade.”
R.8: “Sou editor da maior pagina do facebook no mundo sobre DeepWeb, maior grupo no Telegram, faço artigos para o blog https://blog.deepwebbrasil.com e ate uns tempos tinha meu próprio site na rede Tor, que no momento está Off, mas logo irá voltar.”
R.9: “Ja participei de fóruns sobre assuntos relacionados a tecnologia, e sou editor na page da Deep web Brasil e escrevo, na maioria das vezes sobre Segurança da Informação, oq tem tornado essa experiência mais interessante, tiros dúvidas e mostro a bastante pessoas o real propósito de comunidades, separando os mitos da realidade.”
R.10: “Ss, tenho um canal que fala a respeito de deep web e o submundo darknet, alem de participar de alguns foruns surface e grupos aki no telegram a respeito disso.”

Diante do pensamento de Carvalho (2007, p.66), “agrupamentos de pessoas que se reúnem em função de suas afinidades e utilizam o ciberespaço como meio para intercambiar e difundir suas ideias, estabelecer relações sociais, realizar atividades conjuntas e lograr objetivos [...]”.

Assim, foi visto essa questão sobre as formas de compartilhamento de informação dentro da rede. Os entrevistados já participaram alguma vez, ou participam e contribuem no contexto de comunidade virtual.

Décima questão: como você enxerga o movimento hacker dentro da Deep Web?

Nesse ponto, nota-se mais uma vez a dualidade dentro do movimento hacker. Vemos um o movimento com bons olhos, que luta contra a pedofilia e outras coisas bizarras que acontecem na rede. Algumas vezes confundidos com os “crakers” que são os que praticam a quebra e a invasão dos sistemas, que visam o lucro por meio de roubo e venda informações. Com base em (Castells, 2013, p. 38):

> Os hackers não são o que a mídia diz que são. Não são uns irresponsáveis viciados em computador empenhados em quebrar códigos, penetrar em sistemas ilegalmente, ou criar caos no tráfego dos computadores. Os que se comportam assim são chamados de “crakers”, e em geral são rejeitados pela cultura hacker[..].

Logo, vemos que muitas vezes a figura do hacker é confundida com a do cracker, no qual ambos têm habilidades avançadas sobre informática, porém objetivos específicos diferentes.

R.1: “sim eles existem? Eu, enxergo com bons olhos, quero que eles continuem com o trabalho, por ajudas deles essas porcarias de doentes pedófilos, são presos, graças aos hackers estão fazendo a deep web um lugar melhor, eles estão fazendo um ótimo trabalho acabando com a pedofilia na rede.”

> Além de acervos de bibliotecas e fóruns dos mais diversos tipos de debates, a Deep Web é amplamente utilizada em países onde a comunicação da internet convencional é censurada, fazendo com que as pessoas se interajam com outros países sem que haja nenhuma intervenção do governo. Graças a ela também, um grupo bem famoso atualmente denominados de Anonymous conseguiu divulgar uma rede de pedofilia com cerca de 200 pedófilos no ano de 2011. (Blasechi e Marques, 2016)

Nota-se na resposta do R.1 que os hackers lutam contra o conteúdo ilícito dentro da rede fazendo seu trabalho na divulgação de usuários mal intencionados

R.2: “Um movimento misto, com o viés hackativista e o viés ilegal, que visa lucros próprios de forma individualista. “As chaves para os portões do anonimato são abertas e livres para todos, porém, nem todos merecem possuir estas chaves.” ~Jesus”

R.3: “Este termo "movimento hacker" é bem relativo, na verdade o que é ser um hacker? Nada mais do que ser um especialista que cria as coisas e não as destrói, não vou dizer todos, mas a maioria se dizem ser hackers, mas não passam de carders, script kiddies(maioria..) e acessam a Deep Web pensando que são melhores que os outros. Já vi várias coisas legais lá, como falei na pergunta anterior, o cara tem que garimpar...”

R.4: “em outro países... são bons, aqui no brasil diria q é bem fraquinho kkkk mas tem muitos q se esforçam e fazem funcionar.”
R.5: “Brasil ele é muito mal visto ainda. A maioria vê como uma forma de invadir a privacidade alheia ou adquirir coisas ilícitas. Mas vejo também gente de bem com objetivos ótimos tanto pra conhecimento próprio quanto pra comunidade. É lindo ver ativistas dando a cara pra mudar esses conceitos mal vistos pelo que vemos no fantástico e companhia.”.

Infelizmente o Brasil ainda tem esse preconceito diante do movimento hacker dentro da rede. Muitas vezes rotulados de forma errada e visto como um cracker. A Comunidade hacker além do cyberativismo, também leva em consideração as formas de conhecimento dentro da própria rede. Como a disseminação da informação, crítica contra o governo e habilidades avançadas em computação.

R.6: “O movimento hacker dentro da darknet é amplo e ativo, mas difícil de se encontrar. No entanto se encontra hackers bons e ruins, ou seja, aqueles que estão preocupados em se manifestar contra más elementos e na busca de criminosos, mas existem aqueles que vendem informações, cartões e afins. Para ambos os lados a procura é grande, mas para o segundo o mercado é maior. Existe muito tráfico digital. Acho legal a ideia de manter grupos unidos dentro da internet, mas em um canto que poucos conhecem. É um meio de se ter privacidade.”
R.7: “Muito importante! quanto mais hackers para ajudar outras pessoas a entender sobre a DW melhor ainda Ele a colocam conteúdos bons e ensinam além da DW ...Falando de "Hackers" o movimento dentro da DW tem mais crackers do que hackers.”
R.8: “Acho que tem dois lados. existem pessoas que querem ensinar e aprender, através de fóruns por exemplo. E existem os que ganham com isso, com os famosos serviços hackers. Resumindo tem uma parte boa e ruim de tudo lá.”
R.9: “Existem dois lados... o bom, da glr q tem um propósito, luta por um ideal e cria espaços de discussão sobre oq podem fzr, e o ruim, que é a galera que as vezes nem sabe o tamanho do prejuízo que pode dar, o mal que podem fazer e usam seu talento pra coisas fúteis, como roubar identidade, invasão de sites, mas mts das

vezes, essa galera nem sabe o q faz, muitos são imaturos e acham que a vida é ser um "anêmona" rs”

A resposta do R.9 nos fala mais uma vez da dualidade no movimento hacker dentro da rede. Ambos possuem conhecimento para mudar alguma causa de modo significativo, porém outros usam esse conhecimento para coisas fúteis e muitas vezes não sabem nem as proporções e consequências de onde podem chegar.

R.10: “movimento hacker na deep web, acontece muitas vezes para não ficar expostos na surface. E procuram lugares como esses na deep web para se manterem mais seguros.”

Vemos na resposta do R10 que os hackers não ficam na Surface por conta da segurança, se sentindo mais seguros dentro da Deep Web. Uma forma de comportamento diante da repressão de governos e instituições além da própria forma de compartilhar informações.

Existe apoio dos entrevistados sobre essa questão. E afirmam que realmente existe um movimento que busca lutar contra esse lado negativo dentro da rede.

Sendo assim, concluídas as entrevistas, diante das quatro categorias, nota-se que nenhum dos discursos é igual ao outro, no entanto todos apresentam elementos comuns sobre os temas. Assim, a forma de expressão se mostra saturada quando, na prática, o fechamento amostral se da pela exaustão. Passaremos para as considerações finais, tendo em vista o alcance dos objetivos.

6 CONSIDERAÇÕES FINAIS

O presente estudo teve como objetivo: Analisar os fatores preponderantes na decisão dos usuários para uso da Deep Web, considerando o anonimato em rede e o caráter informacional em relação à sua dualidade, de modo a assinalar alguns dos seus aspectos positivos e negativos.

A partir da análise dos dados feita, conclui-se que a deep web e o anonimato em rede, possuem dois lados, o lado positivo e o lado negativo. Assim,

dependendo somente do usuário como ele usará da melhor forma possível o status de anônimo e como ele se beneficiará dos conteúdos da rede.

Nesse caso, o objetivo geral e os específicos foram atingidos, pois os fatores que são preponderantes para os usuários diante do uso da deep web são exatamente o anonimato como forma de se proteger contra a vigilância e os perigos da rede durante a navegação e, também, o conteúdo encontrado lá que, muitas vezes não é encontrado na surface web.

A maioria dos entrevistados usa o anonimato para burlar ao máximo a captura de informação do seu computador e navegador com as ferramentas próprias para se manter seguros na rede e, diante do conteúdo informacional, conclui-se que a procura de informação é baseada somente para lado positivo e reforçando a ideia de que existe um lado negativo e ilícito da deep web, no qual os hackers lutam contra.

Navegar anonimamente na rede, discutir sobre assuntos entre milhares de pessoas de todos os lugares do mundo e não ser alvo de propagandas e vigilância são os benefícios em navegar nessa rede, além de seus vários conteúdos que despertam curiosidade diante deste fasto mundo que é a deep web.

REFERÊNCIAS

ASSANGE, Julian et. al. **Cypherpunks**: liberdade e o futuro da internet. São Paulo: Boitempo, 2013.

AGRIPINO, Caroline. **Deep web, a internet que o Google não vê**. 2012. Disponível em:< https://www.agenciaenlink.com.br/blog/deep-web-a-internet-que-o-google-nao-ve/>. Acesso em: maio/2018.

BERGMAN, Michael K. ***The Deep Web:*** *Surfacing Hidden Value*. Disponível em: <http://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf> Acesso em: 11 abr. 2018.

BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. (Coleção Cibercultura).

BARDIN, Laurence. **Análise de conteúdo**. Lisboa: Edições 70, 2009. Disponível em: <http://pt.*slideshare.net/alasiasantos*/analise-de-conteudo-laurence-bardin>. Acesso em 22 mai. 2018

BLATTMANN, Ursula; SILVA, Fabiano Corrêa da. Colaboração e interação na Web 2.0. **Revista ACB**: Biblioteconomia em Santa Catarina, Florianópolis, v. 2, n.e, p. 1919 – 215, jul./dez., 2007.

Bogdan, R. e Biklen, S. **Investigação Qualitativa em Educação**: Uma Introdução à Teoria e aos Métodos. Porto: Porto Editora. 2010.

CASTELLS, Manuel. **A galáxia da Internet**: reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: J. Zahar, 2003.

CAMPOS, Claudinei José Gomes. Método de análise de conteúdo: ferramenta para a análise de dados qualitativos no campo da saúde. **Rev bras enferm**, Brasilia, set./out. 2014.

CARVALHO, Andréa Vasconcelos. Comunidades virtuales y producción de inteligencia económica y competitiva. Inteligencia y Seguridad**: revista de análisis y prospectiva**, v. 3, p. 13-45, 2007.

CARVALHO, Andréa Vasconcelos; ALCOFORADO, Acilégna Cristina Duarte; SANTOS, Alexandre José**.** A Web 2.0 e o comportamento informacional dos estudantes de Biblioteconomia da UFRN. **Biblionline**, João Pessoa, v. 9, n. 2, p. 63-78, 2013.

CURTY, Renata G. **Web 2.0: Plataforma para o conhecimento coletivo**. In: TOMAÉL, Maria Inês (Org.). Fontes de Informação na Internet. Londrina, EDUEL, 2008. p. 53-78.

DELEUZE, G. ***Conversações*****.** Rio de Janeiro: Ed. 34, 1992.

FIGUEIREDO, Nice Menezes de. **Estudos de uso e usuários da informação**. Brasília: IBICT, 1994.

FONTANELLA, Bruno José Barcellos; RICAS, Janete; TURATO, Egberto Ribeiro. Amostragem por saturação em pesquisas qualitativas em saúde: contribuições teóricas. **Cad. saúde pública**, Rio de janeiro, v. 1, n. 24, p. 17-27, jan. 2008.

FOUCAULT, M. ***Vigiar e Punir***. Petrópolis: Vozes, 1983.

G1. Conheça a deep web e a 'internet invisível'. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/conheca-a-deep-web-e-a-internet-invisivel.html >. Acesso em: 07 jun. 2018.

GASQUE, Kelley Cristine Gonçalves Dias; COSTA, Sely Maria de Souza. Evolução teórico-metodológica dos estudos de comportamento informacional de usuários. **Ci. Inf**., Brasília, DF, v. 39 n.1 p. 21-32, jan./abr. 2010. Disponível em: <http://www.scielo.br/pdf/ci/v39n1/v39n1a02>. Acesso em: 20 fev. 2018.

GIL, Antônio Carlos. ***Métodos e técnicas de pesquisa social***. São Paulo: Atlas, 1999.

MINAYO, M. C.S. Análise qualitativa: teoria, passos e fidedignidade. **Ciência &Saúde Coletiva**, Rio de Janeiro, v. 17, n. 3, p. 621-626, 2012.

GOOGLEPLAY. Telegram. Disponível em: <https://play.google.com/store/apps/details?id=org.telegram.messenger>. Ace sso em: 07 jun. 2018.

HIMANEN, Pekka. **A ética dos hackers e o espírito da era da informação**. Rio de Janeiro: Editora Campus, 2001. Disponivel em: https://is2006.wordpress.com/2006/12/03/a-etica-dos-hackers-e-o-espirito-da-era-da-informacao/ Acesso em: 22 mar. 2018

HOOFFMANN, Thayse Vasconcelos. **Silk Road anonymous market: um estudo de caso sobre o comércio anônimo na deep web**. Porto Alegre:UFRGs. 2014. Disponivel em: <http://www.lume.ufrgs.br/handle/10183/110220>.Acesso em: 13 fev. 2018.

KOHN, Stephanie. OLHAR DIGITAL – Twitter, livros e música: o lado ‘cult’ da deep web. Dez/2012. Disponível em: Acesso em: maio/2018.

LEVY.Pierre. **Ciberdemocracia**. Lisboa: Instituto Piaget, 2002.

LEVY, Steven. **Hackers: heroes of the computer revolution**. New York: Penguin Books, 2001.

LIMA JUNIOR, Walter Teixeira. Mídia social conectada: produção colaborativa de informação de relevância social em ambiente tecnológico digital. **Revista de pós-graduação da Faculdade Cásper Líbero**. v.12, n.24, p. 95-106, dez 2009.

LOPES, Amanda**. Por trás das cortinas do computador: Quando a internet livre cedeu espaço à construção de regras para a promoção de direitos e liberdades**. Disponível em: http://www.oestadorj.com.br/mundo/por-tras-das-cortinas-docomputador/#sthash.m1Xjk2uM.dpuf. Acesso em: 10 jun.2018

MARCONI, M. de A. LAKATOS, E. M. **Metodologia Científica**. 5ª ed. São Paulo: Atlas, 2011.

MARTINS, Caio Arthur Lopes da Silva; SILVA, Maria Helena Barriviera e. **A dualidade da *Deep Web***. E-f@tec, Garça, v. 3, n. 2, p.1-7, 2013. Disponível em:<http://www.fatecgarca.edu.br/revista/Volume3/artigos_vol3/Artigo_16.pdf>. Acesso em: 05 abr. 2018.

MEIRELLES, Junia Cristina; MOURA, Mônica. Web 2.0: novos paradigmas projetuais e informacionais. **Revista Brasileira de Design da Informação**, [s. l.], n. 4, p.12-18, 2007. Disponível em: <https://bibliotecabauru.files.wordpress.com/2010/01/web-2-0-a.pdf>. Acesso em: 27 mai. 2018.

NIELSEN, Jacob. **Participation Inequality: Encouraging More User to Contribute**. 2006. Disponível em:< http://www.nngroup.com/articles/participation-inequality/> Acesso em: 24 fev. 2018.

PISANI, F.; PIOTET, D. **Como a web transforma o mundo: a alquimia das muldidões**. Tradução de Gian Bruno Grosso. São Paulo: Editora Senac São Paulo, 2010.

POMPÉO, Wagner Augusto; SEEFELDT, João Pedro. Nem tudo está no Google: deep web e o perigo da invisibilidade. In: Congresso Internacional de Direito e Contemporaneidade. **Anais**..., Santa Maria: UFSM, 2013. Disponível em: <http://coral.ufsm.br/congressodireito/anais/2013/3-11.pdf>. Acesso em: 16 nov. 2013. Acesso em: 10 jun. 2018.

RECUERO, Raquel. **Redes Sociais na Internet**. Porto Alegre: Sulima, 2009.

SILVEIRA, Sérgio Amadeu Da**. Ciberativismo, cultura hacker e o individualismo colaborativo**. 2010.

SILVEIRA, Sérgio Amadeu . Redes cibernéticas e tecnologias do anonimato. **Comunicação & Sociedade**, v. 1, p. 113-134, 2009.

SILVEIRA, Sérgio Amadeu . Hackers, monopólios e instituições panópticas: elementos para uma teoria da cidadania Digital. **Líbero** FACASPER, v. 1, p. 73-81, 2006.

Sistemas de anonimato. Disponível em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/rodolfo/index.html>. Acesso em: 07 jun. 2018.

SOUZA, Juliana Lopes De Almeida; ARAÚJO, Daniel Costa De; PAULA, Diego Alves De. Mídia social whatsapp: uma análise sobre as interações sociais. **Revista alterjor**, São Paulo, v. 1, n. 06, p. 132-165, jan. 2015.

TEIXEIRA FILHO, Jayme. **Comunidades Virtuais: como as comunidades de práticas na internet estão mudando os negócios**. Rio de Janeiro: Senac, 2002.

TOR Project: anonymity online. Disponível em:< https://www.torproject.org/>. Acesso em : 20 mar. 2018.

ULRICH, F. **Bitcoin** - a moeda na era digital. 1. ed. São Paulo: Mises Brasil, 2014.

WILSON, T.D. Models **in information behaviour research**. Journal of documentation, v. 55, n. 3, p. 249-270, 1999. Disponível em: Acesso em: 20 jan. 2018.

APÊNDICE A – ROTEIRO DE ENTREVISTA APLICADA AOS USUÁRIOS DO GRUPO TELEGRAM DEEP WEB BRASIL

1 Quais os meios você usa para se tornar um anônimo na rede?

2 Quais relações você acha pertinente para o uso do anonimato? Há como burlar a vigilância?

3 A criptografia é uma grande ferramenta que impulsiona a forma de se comunicar em rede de forma segura, você concorda com isso? Por quê?

4 Você acredita que toda informação disseminada na Surface Web é controlada por governos e/ou corporações?

5 Como você enxerga, de forma geral, a privacidade das pessoas hoje em dia?

6 Qual é a importância da Deep Web para as sociedades da atualidade?

7 Você acha que a Deep Web só tem conteúdo informacional ilícito? Pedofilia, necrofilia e zoofilia, dentre outros, por exemplo.

8 O que te leva a buscar informações na Deep Web ao invés da Surface Web?

9 Você contribui de alguma forma para alguma comunidade, fórum, grupo na *Surface Web* ou na *Deep Web* no contexto de cultura hacker?

10 Como você enxerga o movimento hacker dentro da Deep Web?