UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE BIBLIOTECONOMIA E COMUNICAÇÃO
DEPARTAMENTO DE COMUNICAÇÃO SOCIAL
HABILITAÇÃO RELAÇÕES PÚBLICAS

THAYSE VASCONCELOS HOFFMANN

SILK ROAD ANONYMOUS MARKET: um estudo de caso sobre o comércio anônimo na deep web

Porto Alegre

2014

THAYSE VASCONCELOS HOFFMANN

SILK ROAD ANONYMOUS MARKET: um estudo de caso sobre o comércio anônimo na deep web

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Relações Públicas, pela Faculdade de Biblioteconomia e Comunicação, da Universidade Federal do Rio Grande do Sul.

Orientador: Prof. Dr. Alex Fernando Teixeira Primo

Coorientador: Prof. Me. Willian Fernandes Araújo

Porto Alegre

2014

H699s Hoffmann, Thayse Vasconcelos

Silk Road anonymous market: um estudo de caso sobre o comércio anônimo na deep web /Thayse Vasconcelos Hoffmann ; orientador Alex Fernando Teixeira Primo ; coorientador Willian Fernandes Araújo. – 2014.

f.94 : il.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal do Rio Grande do Sul, Faculdade de Biblioteconomia e Comunicação, Departamento de Comunicação Social, Porto Alegre, 2014.

Departamento de Comunicação Social
Rua Ramiro Barcelos, 2705 Campus Saúde
Bairro Santana
Porto Alegre-RS
Cep: 90035-007
Telefone: (51) 3308-5146
E-mail: fabico@ufrgs.br

Thayse Vasconcelos Hoffmann

SILK ROAD ANONYMOUS MARKET: um estudo de caso sobre o comércio anônimo na deep web

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Relações Públicas, pela Faculdade de Biblioteconomia e Comunicação, da Universidade Federal do Rio Grande do Sul.

Aprovado em:__ de _____ de 2014.

BANCA EXAMINADORA

_____

Prof. Dr. Alex Fernando Teixeira Primo (orientador)

_____

Prof. Me. Willian Fernandes Araújo (coorientador)

_____

Me. Camila Cornutti Barbosa (examinador)

_____

Me. Leonardo Feltrin Foletto (examinador)

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE BIBLIOTECONOMIA E COMUNICAÇÃO

AUTORIZAÇÃO

Autorizo o encaminhamento para avaliação e defesa pública do TCC (Trabalho de Conclusão de Cursos) intitulado **SILK ROAD ANONYMOUS MARKET**: um estudo de caso sobre o comércio anônimo na deep web.
de autoria de THAYSE VASCONCELOS HOFFMANN, estudante do curso de COMUNICAÇÃO SOCIAL/RELAÇÕES PÚBLICAS, desenvolvida sob minha orientação.

Porto Alegre, ... de ..... de 20.....

Assinatura:

Nome completo do **orientador**: Prof. Dr. Alex Fernando Teixeira Primo

AGRADECIMENTOS

Agradeço ao meu pai, César, que sempre estimulou o meu lado crítico, questionador e inquieto. Obrigada por nunca medir esforços em me ajudar. Obrigada por ter dado todo o suporte necessário para a conclusão deste trabalho.

À minha mãe, Valeska, que sempre contribuiu para que eu desenvolvesse o meu lado mais afetivo, carinhoso e solidário. Obrigada, mãe, por toda a tua generosidade em sempre zelar por mim e sem esperar nada em troca.

Aos meus amigos (e foram vários!) que me estimularam a seguir em frente com a escolha do assunto desse trabalho. Obrigada por terem sido pacientes e compreensivos nos momentos em que tive de fazer concessões.

À Lisi, por todo o apoio emocional dado na reta final desse período da minha vida. Com certeza serás uma grande profissional na área que escolhestes.

Aos amigos da Bistrô, que foram compreensivos e solidários no momento em que eu mais precisei. A convivência diária com vocês me faz ter certeza da profissão que escolhi.

Ao meu orientador, Willian, por nunca ter duvidado da importância do meu tema de pesquisa e por construir um trabalho junto comigo ao longo de três semestres. Obrigada por respeitar e compreender o meu tempo de escrita e de reflexão.

Por fim, agradeço à UFRGS por abrir a minha mente para realidades que eu desconhecia há cinco anos e por me tornar uma pessoa mais interessante.

RESUMO

Esta pesquisa monográfica tem como objetivo principal o estudo da construção das práticas comunicacionais que se dão entre os interagentes do Silk Road, tendo em vista suas condições de anonimato e de ilegalidade. Faz-se a revisão bibliográfica que abarca conceitos relativos à história da internet, aos protocolos da internet e à vigilância e anonimato na rede. Além disso, são trazidas discussões sobre as tecnologias do anonimato, como criptografia, *Tor Project* e Bitcoins, aplicadas à comunicação e ao objeto de pesquisa. Em relação à construção metodológica, desenvolve-se um trabalho que tem como inspiração a etnografia virtual, a partir da observação não-participante e com uma postura silenciosa (*lurking*). Por fim, a partir da descrição crítica de dois vendedores do site (Blackhand e The Scurvy Crew), conclui-se que o anonimato não necessariamente dissocia identidade e reputação das práticas comunicacionais.

Palavras-chave: Comunicação. Anonimato. Ilegalidade. Deep web. Silk Road.

ABSTRACT

This paper main objective is to study the construction of communication practices that take place among the agents of Silk Road, considering their conditions of anonymity and illegality. A literature review that includes concepts related to the history of the Internet, internet protocols and monitoring and anonymity on the network has been carried out. In addition, discussions about the technologies of anonymity, such as encryption, Tor Project and Bitcoins, applied to communication and to the research object have been brought about. Regarding the methodological construction, a study that is inspired by the virtual ethnography has been developed, from a non-participant observation and a silent posture (lurking). Finally, from a critical description of two website vendors (Blackhand and The Scurvy Crew), it has been concluded that anonymity does not necessarily dissociate identity and reputation from communication practices.

Keywords: Communication. Anonymity. Illegality. Deep web. Silk Road.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O Silk Road Anonymous Market é um mercado anônimo online que está localizado na parte não indexada pelos motores de busca da internet, a chamada *deep web*. O site iniciou suas operações em fevereiro de 2011 e passou a ganhar maior visibilidade após a publicação de um artigo[1] no portal Gawker no dia 01 de junho de 2011. O Silk Road não é, em si, uma loja. Em vez disso, ele fornece a infraestrutura para que os vendedores e compradores realizem transações em um ambiente online que preza pelo anonimato dos interagentes. O acesso à página só é possível através do navegador Tor e o único meio de pagamento aceito pelo site é o Bitcoin.

O site permaneceu no ar por mais de dois anos, até que no dia 02 de outubro de 2013 o site foi fechado[2] pelo FBI. O fundador do Silk Road, Ross Ulbricht, conhecido como *Dread Pirate Roberts*, foi preso em São Francisco e responde pelas acusações de lavagem de dinheiro, tráfico de drogas e invasão a computadores. Todavia, o site foi reaberto[3] cerca de um mês após o acontecido, no dia 06 de novembro de 2013, estando sob novo comando e oferecendo algumas melhorias, sobretudo nos sistemas de reputação de vendas. A página permaneceu em funcionamento até que no dia 06 de novembro de 2014 uma operação conjunta do FBI, da Fiscalização de Imigração, Alfândega e Segurança Nacional dos EUA e agências europeias agindo através da Europol e Eurojust, localizaram o servidor que hospedava a página e a fecharam novamente[4]. Coincidência ou não, nas duas vezes em que o Silk Road foi fechado pelas forças repressoras, a data era 06 de novembro.

---

[1] The underground website where you can buy any drug imaginable. Disponível em: <http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160> Acesso em: 08 nov. 2014.

[2] Silk Road, maior mercado online de venda de drogas, é fechado pelo FBI e fundador vai preso. Disponível em: <http://info.abril.com.br/noticias/internet/2013/10/silk-road-maior-mercado-online-de-venda-de-drogas-e-fechado-pelo-fbi-e-fundador-vai-preso.shtml> Acesso em: 08 nov. 2014.

[3] Good News, drug users: Silk Road is Back. Disponível em: <http://www.vice.com/read/good-news-drug-users--silk-road-is-back> Acesso em: 08 nov. 2014.

[4] O sucessor do Silk Road acaba de ser fechado pelo FBI. Disponível em: <http://motherboard.vice.com/pt_br/read/o-sucessor-do-silk-road-acaba-de-ser-fechado-pelo-fbi> Acesso em: 06 nov. 2014.

Enquanto construíamos essa monografia, o site ainda estava em operação. Nosso texto introdutório foi escrito após o fechamento da página, por isso, neste ponto, nos referimos aos acontecimentos no passado. Já a nossa coleta de dados se encerrou no dia 02 de novembro, ou seja, quatro dias antes do encerramento do site. Portanto, há discrepâncias entre os tempos verbais ao longo desse trabalho e optamos por mantê-los assim na revisão final, justamente para pontuar que pesquisas relacionadas à internet não são estanques. Ao contrário, a velocidade dos acontecimentos na rede são experienciadas na prática pelo presente estudo.

Diante disso, nosso problema de pesquisa consiste em descobrir como se constroem as práticas comunicacionais no Silk Road tendo em vista suas condições de anonimato e de ilegalidade. Dessa forma, nosso objetivo geral é estudar as principais práticas comunicacionais que se dão entre os interagentes do Silk Road. Em relação aos objetivos específicos, buscamos discutir o anonimato como condicionante prática comunicacional específica; compreender a mecânica de funcionamento do site Silk Road com um olhar atento para suas especificidades e para o meio no qual está inserido; identificar e elucidar as principais tecnologias de anonimato na rede e que estejam ligadas ao Silk Road; problematizar e desconstruir algumas questões-tabu relacionadas ao Silk Road; fomentar os estudos científicos sobre a *deep web*, sobretudo no campo da Comunicação.

A relevância dessa pesquisa está relacionada principalmente com o ineditismo do assunto. Mercados negros online existem pelo menos desde 2011 e hoje, segundo o site Grams[5], há pelo menos 22 sites especializados em bens ilícitos, principalmente drogas entorpecentes, na *deep web*. Ou seja, existem milhares de práticas comunicacionais acontecendo em escala global nesses mercados e que não têm recebido o olhar crítico da comunicação, tampouco uma cobertura midiática para além do senso-comum quando o assunto é alusivo à *deep web*.

[5] O site Grams pode ser considerado o “Google” dos mercados negros na *deep web*. Ele tem por objetivo centralizar todas as informações relativas a itens ilícitos à venda nesses 22 *black markets* mapeados por ele. Disponível em: <http://grams7enufi7jmdl.onion/> Acesso em: 02 nov. 2014.

Como justificativa pessoal da autora, nunca houve dúvidas em relação à importância do presente estudo. A aproximação com o objeto empírico se deu em junho de 2013, através da leitura de uma matéria publicada pelo site Youpix[6], que faz referência à *deep web* como "o lugar mais assustador da internet". O subtítulo da chamada da matéria possui os dizeres "O Youpix não recomenda o acesso à *deep web*" (YOUPIX, 2014, online). Ou seja, a mídia parece ter instaurado um clima de terror em relação ao tema, passando a ignorar as possibilidades de abordagens mais isentas e menos preconceituosas.

Em 26 de julho 2013, o *Atlantis Marketplace*, um *black market* que atualmente não está mais operando, lançou um vídeo-comercial[7] nas redes sociais Youtube[8] e Vimeo[9]. O vídeo é uma animação feita, provavelmente, por profissionais de design gráfico, pois suas qualidades estéticas chamam a nossa atenção. Isso nos fez questionar sobre até que ponto a *deep web* era realmente um "local assustador" e se o seu acesso era mesmo não recomendável. Com isso, passamos a descobrir a existência desses mercados negros, conhecendo, então, o Silk Road, o mais notável dentre eles. Essa pesquisa é, acima de tudo, um desafio pessoal da autora na tentativa de sair do lugar-comum das pesquisas monográficas ao buscar um assunto pouco explorado. Mesmo com o desconforto sentido no início do trabalho – afinal, estamos imbuídos de preconceitos em relação à temática – resolvemos sair da zona de conforto e produzir algo no qual pudéssemos nos orgulhar.

Em um levantamento de estado da arte em relação a trabalhos acadêmicos que contemplem assuntos relacionados ao nosso objeto no Brasil, destacamos a escassez de pesquisas que pudessem servir como base para o presente estudo. Dentre os principais repositórios digitais do Brasil – Lume UFRGS, Banco de Teses da Capes, Biblioteca Digital da USP e Scielo – através de buscas por palavras-chave relacionadas

[6] Um passeio pela deep web, o lugar mais assustador da internet. Disponível em: <http://youpix.virgula.uol.com.br/comportamento/um-passeio-pela-deep-web-o-lugar-mais-assustador-da-internet/> Acesso em: 17 nov. 2014.
[7] Welcome to Atlantis Anonymous Marketplace. Disponível em: <http://vimeo.com/73064012> Acesso em: 17 nov. 2014.
[8] Disponível em: <https://www.youtube.com/> Acesso em: 17 nov. 2014.
[9] Disponível em: <https://vimeo.com/> Acesso em: 17 nov. 2014.

ao tema (“*deep web*”, “*dark web*”, “*darknet*”, “*hidden web*”, “web invisível”, “*black market*”, “Silk Road”) não foram encontrados resultados específicos, apenas algumas breves citações em artigos acadêmicos que não focavam diretamente em nenhum desses tópicos. Diante disso, torna-se ainda mais evidente a importância e o pioneirismo do nosso estudo ao se debruçar em questões ainda não contempladas cientificamente, sobretudo na área da comunicação. Ao mesmo tempo, é um enorme desafio partir de escassos recursos num trabalho monográfico e construir uma metodologia capaz de responder ao problema e aos objetivos de pesquisa num recorte temporal bastante restrito.

Estudos relacionados podem ser encontrados fora do Brasil. Destaca-se o trabalho do pesquisador estadunidense da Carnegie Mellon University, Nicolas Christin (2012). Ele realizou uma análise de medição sobre a primeira versão do *Silk Road*, problematizando o funcionamento do site sob o viés das ciências exatas. Ainda que a maioria de seus resultados não sirva como referência para essa monografia, é interessante notar a preocupação de Nicolas com questões políticas e sociais envolvidas no Silk Road, ainda que esse não seja o foco de sua análise. Ademais, é o único estudo de caso direcionado aos *black markets* que pudemos encontrar, o que reafirma mais uma vez a relevância do nosso estudo.

Metodologicamente, destacamos o artigo do pesquisador estadunidense Robert W. Gehl, que é professor do Departamento de Comunicação da *University of Utah*. Recentemente ele publicou um trabalho[10] sobre a *Dark Web Social Network*, um site de rede social da *deep web*. O autor faz uso da etnografia virtual adaptada às especificidades do seu objeto empírico, sendo um dos primeiros pesquisadores a pensarem na *deep web* como um universo com grande potencial para pesquisas acadêmicas. Trabalhos sob esse contexto quase sempre se deparam com questões simbolicamente associadas à *deep web*, como atividades ilícitas e/ou tabus, as relações entre anonimato e cibercrime, o uso de pseudônimos específicos e etc. Ainda que a pesquisa de Robert W. Gehl compartilhe o mesmo cenário que o nosso estudo,

[10] GEHL, Robert W. **Power/Freedom on the Dark Web**: A Digital Ethnography of the Dark Web Social Network, New Media and Society: Forth coming, 2014. Disponível em: <http://ssrn.com/abstract=2498629>. Acesso em: 14 de out. 2014.

ela trata de um site de rede social não diretamente ligado a atividades ilegais, portanto sua análise não difere tanto de uma análise centrada em uma rede social da *surface web.*

Diante das dificuldades de construir uma metodologia que fosse capaz de responder o problema e os objetivos da presente monografia, optamos por realizar uma pesquisa qualitativa. Para Bauer e Gaskell (2008), a pesquisa qualitativa lida com interpretações e realidades sociais, sendo utilizada, na maior parte das vezes, quando não se tem como objetivo encontrar resultados mensuráveis. Esse trabalho é, portanto, um estudo de caso, que se caracteriza por ser um estudo profundo de um ou de poucos objetos, de modo a permitir o seu conhecimento amplo e detalhado (GIL, 2008). Segundo Yin, o estudo de caso

> [...] é um estudo empírico que investiga um fenômeno atual dentro do seu contexto de realidade, quando as fronteiras entre o fenômeno e o contexto não são claramente definidas e no qual são utilizadas várias fontes de evidência. (YIN *apud* GIL, 2008, p.58)

Para o autor, ele é ideal para descrever a situação do contexto em que está sendo feita determinada investigação. Em se tratando de *deep web*, o ambiente em que se encontra o objeto faz parte da análise como um todo, não sendo possível analisar o *Silk Road* sem considerar as especificidades do meio.

Esse estudo está organizado em cinco capítulos. Após esta seção introdutória, no capítulo dois buscamos realizar um aprofundamento teórico sobre as origens da internet através de Castells (2003); sobre os protocolos da internet recorrendo a Castells (2003), Silveira (2006, 2009), Galloway (2004), Araújo (2013) e Lessig (1999); e sobre vigilância e anonimato na rede, referenciando Bruno (2013), Silveira (2009) e Castells (2003) novamente.

No terceiro capítulo discorremos sobre questões referentes às tecnologias do anonimato sob o viés da comunicação. Trazemos conceitos sobre criptografia utilizando Silveira (2009), Assange et. al. (2013), Castells (2003); conceitos e definições buscando diferenciar a *surface web* da *deep web* ao utilizarmos Pompéo e Seefeldt

(2013) e Monteiro e Fidencio (2013); explanação acerca do *Tor Project* citando Monteiro e Fidencio (2013) e Silveira (2009); e, finalmente, versamos sobre as criptomoedas, considerando a história das moedas tradicionais ao falarmos mais especificamente sobre Bitcoins, a partir das ideias de Ulrich (2014) e Assange et. al. (2013).

No capítulo quatro detalhamos os procedimentos metodológicos de nossa pesquisa a partir de Hine (2000), Fragoso, Recuero e Amaral (2011) e Kozinets (2002), trazendo conceitos sobre etnografia virtual e observação não-participante (*lurking*). A seguir, partimos para a análise do objeto, procurando trazer dados a respeito da estrutura e funcionamento do site Silk Road. Após, desenvolvemos uma descrição crítica dos perfis de dois vendedores do site: Blackhand e The Scurvy Crew.

Finalmente, no quinto e último capítulo, encontram-se as considerações finais em relação ao nosso estudo. Nesse ponto, fazemos um fechamento de nossa análise, procurando relacionar os dois vendedores descritos com os conceitos apreendidos em nossa base teórica. Respondemos o nosso problema e nossos objetivos de pesquisa e apontamos algumas perspectivas futuras em relação a novas produções científicas que possam abordar a mesma temática deste trabalho monográfico.

2 INTERNET

Quando estudamos a história da internet, logo percebemos que um conjunto de felizes coincidências colaboraram para a formação da rede que conhecemos e que tece as nossas vidas hoje. Se alguma dessas coincidências não estivesse presente, o rumo da internet poderia ter sido outro completamente diferente. Tudo parece ter acontecido na hora e nos lugares mais propícios para que se firmasse um meio de comunicação de muitos para muitos, inédito na história da humanidade e que reconfigurou a cultura da comunicação de massa já fortemente estabelecida. Estudar as origens e o processo evolutivo da internet se mostra fundamental para que, mais adiante, consigamos compreender as diversas questões que permeiam este trabalho: sociedade de controle *versus* anonimato, arquitetura de rede e protocolos, criptografia e monetização da rede.

2.1 ORIGENS DA INTERNET

Os processos que marcaram as diretrizes da internet já são bastante difundidos por quem inicia seus estudos na cibercultura, e estão situados num espaço temporal bastante restrito se compararmos a outros acontecimentos revolucionários ao longo da história da comunicação humana. A internet originou-se num contexto de Guerra Fria, em plena corrida armamentista vivida pelos Estados Unidos e pela União Soviética. Em setembro de 1969 surgiu a Arpanet, arquitetada pela ARPA (*Advanced Research Projects Agency*), instituída pelo Departamento de Defesa dos Estados Unidos. Conforme conceitua 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 e flexível.

Os primeiros nós da rede se concentravam em centros universitários de pesquisa e foram fundamentais para seu rápido aprimoramento. Com o passar dos anos, foi se instituindo uma rede de redes que, para que pudessem se comunicar umas com as outras, precisavam de protocolos de comunicação padronizados. Em 1973 surgiu, então, o protocolo de controle de transmissão (TCP), sendo acrescido pelo protocolo intrarrede (IP), conhecido por nós até hoje como o padrão TCP/IP. Na década de 1980, o Departamento de Defesa estimulava a comercialização da tecnologia da internet e financiava fabricantes de computadores estadunidenses a incluírem o TCP/IP em seus protocolos. “Na altura da década de 1990, a maioria dos computadores nos EUA tinha capacidade de entrar em rede, o que lançou os alicerces para a difusão da interconexão de redes.” (CASTELLS, 2003, p. 15). Em 1974 surgiu o sistema operacional UNIX, e logo foi liberado para as universidades, inclusive seu código-fonte, tornando-se a língua franca da maioria dos departamentos de ciência da computação dos EUA. Isso mostra que, desde os primórdios, a rede alicerçava-se na tradição da fonte aberta, cujo objetivo deliberado era manter o acesso a toda informação relativa a sistemas de softwares disponíveis aos usuários. Castells (2003) comenta que esse movimento de fonte aberta e a cultura dos primeiros hackers foram cruciais na configuração técnica e social da internet, conforme retomaremos diversas vezes ao longo do presente estudo.

Um ponto decisivo na popularização da internet foi o desenvolvimento 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 chamou esse sistema de hipertexto de *world wide web*, a rede mundial. Diversos *softwares* de navegação foram sendo lançados, mas o mais orientado para o produto foi o Mosaic, que possuía uma avançada capacidade gráfica. Pouco após, por questões legais, tiveram de trocar o nome para *Netscape Communications*, e, em 1994, era lançado o primeiro navegador comercial, *o Netscape Navigator*. Finalmente, em 1995 a Microsoft descobriu o potencial da internet e lançou seu próprio navegador, o Internet Explorer, acoplado ao software Windows 95.

Sendo assim, na metade da década de 1990, a internet já estava bastante delineada e pronta para chegar ao grande público. Segundo Castells, a internet “[...] estava privatizada e dotada de uma arquitetura técnica aberta, que permitia a interconexão de todas as redes de computadores em qualquer lugar do mundo; [...] e vários navegadores de uso fácil estavam à disposição do público”. (CASTELLS, 2003, p. 19). Conforme iniciamos nossa fala no início deste capítulo, o nascimento da internet é fruto de felizes e improváveis coincidências: a intersecção entre a *big science*, a pesquisa militar e a cultura libertária. As aplicações militares acabaram sendo secundárias no projeto da Arpanet, ainda que o projeto original de Paul Baran tivesse realmente orientação militar. Da mesma forma, o projeto não teria sido financiado pelo governo estadunidense se não fosse pelo contexto de Guerra Fria, em que havia forte apoio popular e de órgãos governamentais para que se investissem em tecnologias de ponta. É importante frisar que a ARPA gozava de considerável autonomia “[...] na avaliação das formas de estimular a pesquisa tecnológica em áreas decisivas, sem sufocar a criatividade e a independência [...]” (CASTELLS, 2003, p. 21), tendo sido essa autonomia o seu grande trunfo. O autor ainda destaca que a Arpanet não foi uma consequência fortuita e ingênua de uma pesquisa que ocorria paralelamente. Ela “[...] foi prefigurada, deliberadamente projetada e subsequentemente administrada por um grupo determinado de cientistas da computação que compartilhavam uma missão que pouco tinha a ver com estratégia militar.” (CASTELLS, 2003, p. 21).

Vale deixar claro que a internet não teve origem no mundo dos negócios, sobretudo por ser uma tecnologia cara e arriscada demais para ser assumida por empresários preocupados com retornos a curto prazo. Felizmente e para benefício do mundo, “[...] a internet se desenvolveu num ambiente seguro, propiciado por recursos públicos e pesquisa orientada para missão, mas que não sufocava a liberdade de pensamento e inovação.” (CASTELLS, 2003, p. 24). Este trabalho monográfico tratará em diferentes momentos sobre a economia e sobre os negócios que vêm se firmando na internet depois de sua popularização em meados da década de 1990. Sendo assim, é fundamental que demarquemos as origens, os interesses e a cultura libertária desde os seus primórdios para que possamos compreender as diferenças entre políticas *da*

internet e políticas *na* internet (SILVEIRA, 2009) que veremos com mais clareza adiante.

2.2 PROTOCOLOS DA INTERNET

Os primeiros programadores trabalharam fortemente na ampliação do alcance da rede, compartilhando conhecimentos e melhorando a acessibilidade das tecnologias que iam surgindo. Eles foram os primeiros hackers – o termo é, ainda hoje, erroneamente tratado de forma pejorativa – e exerceram um papel fundamental na cultura da internet. Eles desenvolveram protocolos da rede que asseguram a liberdade da comunicação, valor primordial dentro da cultura hacker. “A ideia era proteger a livre expressão de quaisquer tipos de pressão política, religiosa, ideológica, profissional, corporativa, pública ou privada.” (SILVEIRA, 2009, p. 111). A partir de suas diversas contribuições, surgiu uma internet “[...] cuja feição mais característica era a abertura, tanto em sua arquitetura técnica quanto em sua organização social/institucional.” (CASTELLS, 2003, p. 26). Tecnicamente falando, a flexibilidade dos protocolos de comunicação lançou bases para o fornecimento de padrões compatíveis para diferentes sistemas de interconexão de computadores. Um dos desafios em relação à expansão e à globalização da internet residia na difícil concordância quanto a um padrão protocolar internacional. Em 1976, a Europa defendia o padrão x.25, que era incomunicável com o TCP/IP, e acreditava que o controle e a responsabilidade pela rede deveriam ficar a cargo de provedores de rede públicos. Após uma intensa discussão entre governos, fabricantes de computadores e operadoras de telecomunicações, acabaram prevalecendo os protocolos da Arpanet, que eram flexíveis o suficiente para integrar diferentes sistemas em rede e, portanto, os TCP/IP se estabeleceram como padrões para a internet global. Conforme pontua Araújo (2013), a responsabilidade sobre a coordenação dos protocolos da internet ficou a cargo de organizações sem fins lucrativos como a *Internet Society* e a *Internet*

Engineering Task Force (IETF). Essa última trabalha publicando os *Request For Comments* (RFC), que são documentos que detalham os padrões utilizados na rede.

A partir deste ponto, passaremos a discutir sobre protocolos sob uma perspectiva crítica, instaurada por Alexander Galloway com a publicação *"Protocol: how control exists after decentralization"*. O autor compreende a internet como uma rede distribuída (padrão de conexão todos-com-todos) de computadores que se dá em escala global. Para ele, trata-se de uma gigante teia em que cada nó representa um agente autônomo, capaz de se conectar com qualquer outro ponto da rede. Se comparada às redes centralizadas (padrão um-com-todos) e às redes descentralizadas, ela é menos hierárquica (GALLOWAY, 2004). Esse aspecto distribuído da rede contrasta com o que se tinha até antes do advento da internet em termos de meios de comunicação de massa. Os meios tradicionais eram extremamente centralizadores, ao passo que a internet propicia um ambiente de comunicação muito mais horizontalizado, ou seja, os indivíduos, os computadores e os servidores são os nós e podem se comunicar todos com todos. Conforme Galloway (2004), os protocolos são os responsáveis por determinar as possibilidades de atuação de um computador em rede, ditando as regras de funcionamento de todo o sistema. Os protocolos são, antes de qualquer coisa, um tipo de controle lógico que dá suporte à dimensão distribuída da internet.

Conforme vimos, a estrutura da rede está em contraposição à estrutura centralizada dos meios de comunicação tradicionais – como a televisão, ainda que esta venha se redefinindo ao longo dos últimos anos e venha pegando emprestadas algumas das qualidades da internet. Apesar de distribuída e por fora dos poderes institucionais, governamentais e corporativos (GALLOWAY, 2004), a internet não está livre de controles. O senso comum aponta para ela como um sistema que libertará a sociedade do exercício de poder vertical por parte dos Estados, mas a noção primordial que norteia a cibernética diz que as tecnologias digitais são baseadas em códigos que delimitam o nosso comportamento (LESSIG, 1999, *apud* SILVEIRA, 2009). Para Lawrence Lessig (1999), no ciberespaço, o código é a lei. Por cibernética, entende-se que, de acordo com Wiener (1998, *apud* SILVEIRA, 2009, p. 3), o termo "tem a ver com

processos de controle e de comunicação de animais, homens e máquinas, ou seja, de como a informação é processada e controlada em sistemas vivos ou artificiais". Sendo assim, Silveira (2009) destaca que uma rede cibernética construída artificialmente é uma rede de controle e não apenas de comunicação.

Na comunicação em rede, as possibilidades, os limites e o controle estão nas suas arquiteturas, códigos e protocolos. Castells (2003) caracteriza a chamada cultura da internet. Para ele, ela é estruturada dentro de quatro camadas: a cultura tecnomeritocrática, a cultura hacker, a cultura comunitária virtual e a cultura empresarial. Juntas, elas são responsáveis pela construção de uma ideologia de liberdade que norteia a internet, fazendo com que ela não tenha um controle central – não existe um "dono da rede". A primeira delas, a cultura tecnomeritocrática, está ligada ao meio acadêmico e científico que proporcionou o surgimento da internet, e prima pela excelência tecnológica da mesma. A segunda, a cultura hacker, tem como valores fundamentais a liberdade e o compartilhamento de informações que visam ao aprimoramento da própria rede. Entretanto, segundo Galloway (2004) a subversão do ideal hierárquico não elimina as formas de controle na rede, muito pelo contrário. Segundo Araújo (2013), a dita ideologia de liberdade frisada por Manuel Castells não acaba com o controle, apenas muda-o de diagrama.

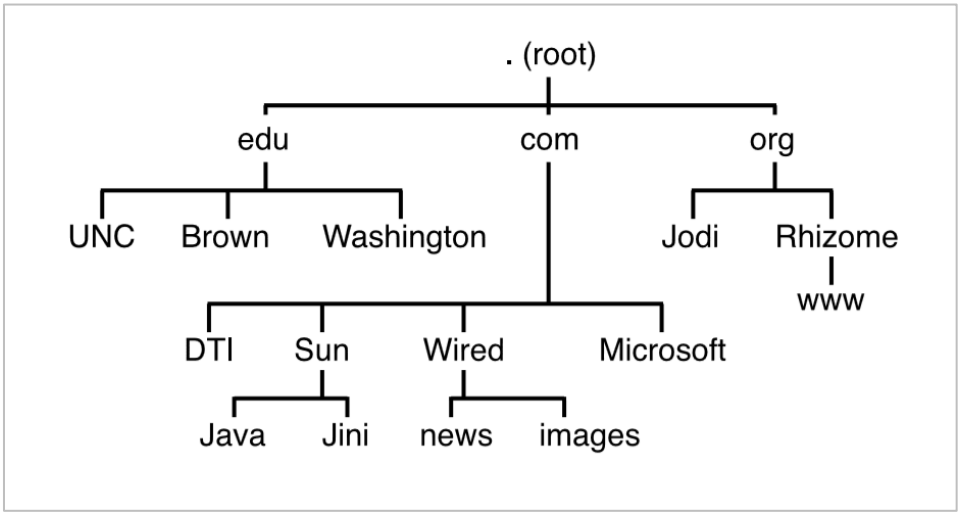
A comunicação entre computadores na internet só é possível através de um conjunto de recomendações e regras que descrevem normas técnicas específicas pelas quais os computadores irão interagir, os chamados protocolos (GALLOWAY, 2004). Segundo o autor, eles apresentam dois mecanismos que atuam de maneira oposta. Ao passo em que os protocolos distribuem a comunicação entre computadores, eles também submetem os fluxos informacionais a uma hierarquia extremamente vertical. Segundo Araújo (2013), que nos ajuda a compreender melhor as ideias de Galloway, o primeiro mecanismo que compõe a relação dialética da ambiguidade protocolar refere-se ao padrão TCP/IP. Da forma como foi estruturado, é possível que um computador em rede interaja com qualquer outro de maneira distribuída. Nesse tipo de organização lógica, cada nó da rede, cada computador da internet é igual a todos os

outros que a compartilham, formando, assim, uma estrutura sem hierarquias (ARAÚJO, 2013). Para Silveira,

> [...] ninguém pode se comunicar na Internet sem um IP, nem mesmo é possível abrir uma página da web sem um endereço IP. Mas, não existe nenhuma necessidade de vincular uma identidade civil a um número de IP para que a comunicação se estabeleça. (SILVEIRA, 2009, p.5).

Em contraposição, temos o segundo mecanismo, o DNS, que concentra o controle em hierarquias definidas de maneira bastante rígida. O autor Araújo conceitua o DNS como "[...] o grande banco de dados descentralizado que mapeia os nomes dos sítios que se pode visitar na web e os converte no endereço específico de rede em que as informações estão alocadas." (ARAÚJO, 2013, p. 52). Eles são os chamados endereços de IP. Neste ponto, uma rápida e ilustrada explicação a respeito do DNS nos ajudará a compreender de que maneira o controle se dá dentro desde mecanismo.

Figura 1 – Exemplo da estrutura de "árvore invertida" do DNS.



Fonte: Galloway, 2004, p. 49.

Galloway (2004) representa esse padrão como sendo uma árvore invertida (ver Figura 1). No topo estão os servidores-raízes, representados por um único ponto (“.”), que mantêm o controle de todas as informações do DNS. Eles têm autoridade sobre os domínios de primeiro nível (TLDs), como "com", "edu” e “org”. “Em DNS, cada *‘name server*’ só pode responder apenas com informações fidedignas sobre a zona imediatamente abaixo dela. É por isso que o sistema é hierárquico [...]” (GALLOWAY, 2004, p. 49, tradução nossa). Sendo assim, quase todo tráfego da web tem de se submeter a essa estrutura, composta por pouco mais de uma dúzia de servidores-raiz ao redor do mundo. (ARAÚJO, 2013). É importante frisar que esses servidores-raiz têm controle apenas sobre os processos, e não sobre os conteúdos. Porém, sem o apoio fundamental dos servidores-raiz, todos os ramos menores da rede DNS se tornam inutilizáveis. Isso vem a quebrar a imagem que temos da internet como uma grande rede (teia, malha) incontrolável (GALLOWAY, 2004).

> Se, hipoteticamente, alguma autoridade quiser proibir a China da Internet (por exemplo, durante um “surto de hostilidade”), eles poderiam fazê-lo muito facilmente através de uma simples modificação da informação contida nos servidores-raiz no topo da árvore invertida. Dentro de 24 horas, a China vai desaparecer da Internet. [...] Paul Garrin descreve: “Com o golpe de uma tecla delete, países inteiros podem ser apagados do resto da rede. [...] Controle o ‘.’ e você controla o acesso.” (GALLOWAY, 2004, p. 10, tradução nossa).

Ou seja, ainda que esta seja uma ação politicamente inviável, ela nos dá a dimensão do poder hierárquico que o DNS pode proporcionar, conforme problematiza Araújo (2013). O autor relembra o caso da exclusão do site WikiLeaks dos servidores da Amazon em 2010 como um exemplo concreto de como o DNS pode ser usado para exercer controle sobre a rede.

Todavia, o que tenciona essa mecânica protocolar é justamente sua ambivalência. Nesse episódio de exclusão da WikiLeaks, os conteúdos armazenados no site em questão não desapareceram da rede em função dos “sites espelhos”, que são réplicas do original que se encarregam apenas de repetir os conteúdos. A partir deles, torna-se inviável a eliminação total da maioria dos conteúdos da rede, pois eles se distribuem em diversos servidores espalhados pelo mundo e em grande velocidade.

(ARAÚJO, 2013). Ao mesmo tempo em que as atividades ciberativistas como a WikiLeaks se submetem ao controle do DNS, elas se beneficiam do caráter distribuído da rede.

Desta forma, o autor Galloway acredita que a resistência contra os tipos de controle que se dão na rede não deve ser contra o protocolo em si, e sim por dentro das instâncias que o definem, como os órgãos responsáveis pela determinação de protocolos, como a *Internet Engineering Task Force* (IETF) (ARAÚJO, 2013). Sobre essa questão, Sergio Amadeu (2006) diz que:

> Decisões sobre a arquitetura das redes e seus protocolos estão sendo tomadas por engenheiros, mas têm grande impacto social e podem limitar ou ampliar a liberdade da comunicação entre as pessoas. São decisões de grande impacto público e, portanto, adquirem relevância política, mesmo que tenham sido tomadas por comitês técnicos. (SILVEIRA, 2006, p. 78).

Sendo assim, decisões aparentemente técnicas estão sendo debatidas sem que os cidadãos tenham conhecimento e possibilidade de recusá-las. Decisões estas que podem afetar a privacidade e o anonimato dos internautas na rede. Silveira expõe que

> Se for definido que o protocolo de comunicação básico entre as milhares de redes deverá ter como padrão o fim do anonimato na comunicação, isso afetará completamente a forma como conhecemos a Internet hoje.” (SILVEIRA, 2006, p.74).

É preciso que estejamos conscientes da existência do controle técnico se quisermos utilizá-lo de outro modo. O indivíduo preocupado com o anonimato na web pode evitar que seu fluxo de informação seja rastreado utilizando um *proxy* anônimo capaz de ocultar a informação de identificação do computador de origem. Porém, sem as técnicas de ocultamento, praticamente todas as conexões podem ser vigiadas por aqueles que detêm a técnica: Estado, crackers e empresas privadas. O que vem se observando é que a cultura de liberdade que sempre fez parte da rede mundial de computadores vem assumindo uma nova forma.

> As novas articulações tentam retirar da internet as qualidades que a fizeram mais democrática do que as demais mídias de massa. A cultura da liberdade que caracteriza a rede mundial incomoda esses segmentos e os lança em uma jornada de combate à atual dinâmica da internet." (SILVEIRA, 2011, p. 4).

Diante disso, passamos agora a entrar mais especificamente no que tange o anonimato na rede. Sergio Amadeu destaca que a internet está em constante desenvolvimento, o que desagrada diversos segmentos, tanto econômicos quanto políticos (SILVEIRA, 2009). Segundo ele, "a tendência é que a disputa pela alteração da arquitetura da rede intensifique-se quanto mais importante a rede torne-se para as corporações e para o capitalismo." (SILVEIRA, 2009, p. 107). Os *backbones* da internet, isto é, a infraestrutura da rede por onde passam as correntes elétricas que são compreendidas como sinais (CASTELLS, 2003), estão sob o domínio de grandes operadoras de telecomunicação. É diante do enorme poder concedido a essas empresas que reside uma preocupação crescente entre vários segmentos que atuam em defesa da liberdade da internet para que ela seja mantida como um espaço livre. A partir disso, trazemos o conceito de neutralidade da rede (*net neutralit*), tão discutido atualmente, que diz que nenhuma camada da rede, nenhum pacote de informação "deve ser tratado de modo diferenciado pelos controladores da rede física, independentemente do endereço IP de origem ou de destino e da aplicação a que pertence." (SILVEIRA, 2009, p. 106). Sendo assim, tanto um grande portal de notícias quanto um modesto blog devem ser tratados do mesmo modo, sem distinção. Da mesma forma, conforme veremos a seguir, o anonimato na rede é amplamente defendido por quem acredita que a internet seja a maior expressão do período histórico em que vivemos, representante de uma mudança de paradigma das comunicações.

2.3 VIGILÂNCIA E ANONIMATO

Antes de falarmos sobre as implicações do anonimato na rede, precisamos entender brevemente algumas questões anteriores, como a história das práticas de

vigilância em nossa sociedade. Segundo detalha Foucault (2007, *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. Assim, o confinamento dos indivíduos em instituições panópticas, como hospitais, prisões, escolas e fábricas passa a imperar na sociedade. Após a Segunda Guerra Mundial, conforme apontou Deleuze (1992) um novo modelo social toma o lugar das instituições disciplinares: trata-se do controle contínuo da comunicação, através das tecnologias da informação e de computadores (*apud* ARAÚJO, 2013). Sendo assim, conforme aponta a pesquisadora 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).

A vigilância moderna se complexificou em relação aos modelos anteriores, ganhando novos sentidos e ultrapassando os limites disciplinares e panópticos. Para ela, 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). Segundo a autora, a observação deve permitir a produção de conhecimento sobre quem é vigiado, de modo a se extraírem padrões, regularidades ou cadeias causais a respeito dos mesmos, permitindo, assim, que se aja sobre suas escolhas e comportamentos. Contudo, só podemos falar em vigilância se sobre esses dois elementos, observação e produção de conhecimento, houver a intenção de intervir sobre os indivíduos em foco e governar as suas condutas.

Em sua análise, Fernanda Bruno propõe a noção de vigilância distribuída. Segundo ela, “[...] 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). Aqui, enumeraremos de maneira breve os sete principais atributos que a descrevem. O **primeiro** atributo diz que a vigilância tende a se tornar cada vez mais incorporada aos diversos dispositivos tecnológicos e aos serviços que usamos cotidianamente. O **segundo** é a diversidade de tecnologias, de práticas e, sobretudo, de propósitos e de objetos da vigilância. Os focos atuais não mais se restringem nem se justificam por grupos suspeitos e perigosos, mas atingem todos – consumidores, cidadãos comuns, internautas, criminosos etc. É importante frisar que não se monitoram apenas indivíduos ou grupos, mas informações, transações eletrônicas e demais rastros deixados no ciberespaço. O **terceiro** diz que, diferentemente dos dispositivos modernos de inspeção, no modelo contemporâneo todos podem ser potencialmente vítimas ou suspeitos. A **quarta** característica da vigilância distribuída considera que dispositivos podem atuar como vigilantes, ainda que não tenham sido projetados com essa finalidade.

> 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 (BRUNO, 2013, p. 32).

O **quinto** atributo trata da mudança de natureza da vigilância. Ela não mais se distribui apenas entre indivíduos e instituições, mas entre sistemas técnicos automatizados que permitem que ela se exerça a distância, com um baixo custo e em extensões antes impensáveis para os limites do homem. A **sexta** propriedade considera que a vigilância se faz presente também nos circuitos de entretenimento e prazer, como exemplo, as redes sociais da internet. Segundo Fernanda Bruno,

> [...] a sua distribuição por inúmeros contextos sociais e o seu caráter cotidiano vão de par com uma tonalidade afetiva plural que se distancia do aspecto preponderantemente sombrio de outrora. (BRUNO, 2013, p. 34).

A autora destaca, ainda, que são crescentes os dispositivos voltados para o automonitoramento, ou seja, dispositivos que aliam vigilância, cuidado de si e

otimização de desempenho, seja em relação ao trabalho, à saúde ou à produtividade. Por fim, o **sétimo** e último atributo diz que a colaboratividade é incentivada não apenas na produção de conteúdos, mas também nas práticas de vigilância, sendo associadas ao exercício de cidadania. Diante disso, conclui-se que o modelo de vigilância distribuída não é apenas uma expansão dos modelos modernos citados anteriormente, e sim uma reconfiguração que produz novos sentidos e novas práticas.

Seguindo na discussão, passamos a tratar agora da legitimação das práticas e das tecnologias de vigilância, sendo próprios a cada época e sociedade. Ao longo da história, os regimes de legitimação são fundamentais para a sua difusão e consolidação, tornando as práticas de vigilância toleráveis e até mesmo requeridas dentro da sociedade. Contemporaneamente, é possível identificar três grandes vias de legitimação. A primeira é a da segurança, e o seu vínculo com a vigilância se dá hoje de maneira renovada. “Um de seus elementos mais determinantes consiste na noção de risco, que confere um estatuto particular à vigilância como meio de garantir segurança.” (BRUNO, 2013, p. 37). Essa noção de risco atualmente direciona grande parte das políticas e das tecnologias de segurança e vigilância. No campo da segurança, o discurso e a lógica do risco autorizam uma série de dispositivos de vigilância de caráter preventivo. A vigilância se torna, então, uma resposta que se pretende autoevidente diante de riscos sociais. Sendo assim, “[...] quando a segurança é entendida como redução de risco de ocorrência de males futuros, ela legitima todo um aparato de vigilância que deve supostamente conjurar este futuro projetado.” (BRUNO, 2013, p. 39). Como exemplo, vemos a expansão da videovigilância como instrumento de combate ao crime, respaldado por governos e populações. Essa lógica do risco, aliada à ampliação do sentimento de inseguranças nos grandes centros urbanos e após os ataques terroristas em 11 de setembro de 2001, a videovigilância, não apenas nos espaços públicos, mas também nos privados, torna-se autoevidente e autolegitimada. (BRUNO, 2013). Mesmo com isso, é curioso notar que o aumento da videovigilância não gera a redução da criminalidade esperada, segundo a autora, e isso parece não ser suficiente para que se reveja ou se descarte essa medida securitária. (BRUNO, 2013).

Após o episódio do 11 de setembro nos Estados Unidos, as relações entre segurança e vigilância passam a não mais focalizar apenas indivíduos e populações classificados como perigosas – todos estão sob suspeita. As informações que circulam no ciberespaço passam a ser monitoradas por diversos setores e sob diferentes pretextos. “Ações e comunicações cotidianas no ciberespaço se tornam cada vez mais sujeitas a coleta, registro e classificação.” (BRUNO, 2013, p. 8). Com isso, uma complexa rede de saberes vem se constituindo a partir desse processo, passando a ter efeitos de poder que intervêm nas escolhas e nas ações dos indivíduos. Como bem aponta Silveira (2009), o medo em relação ao anonimato na rede se intensifica e políticos conservadores e detentores das velhas mídias passam a superdimensionar crimes hediondos para conseguir apoio público visando à restringir algumas liberdades no ciberespaço. O autor também traz as ideias de liberdade de Benjamin Constant para compor a discussão:

> O pretexto de prevenção do crime tem as maiores e mais incalculáveis consequências. A criminalidade potencial é inseparável da liberdade de todos, das vidas de todas as classes, do crescimento de todas as faculdades humanas. Os que detêm a autoridade, alegando interminavelmente o receio de que um crime possa ser cometido, podem tecer uma vasta teia que envolva todos os inocentes. (CONSTANT, 2007, p.146, *apud* SILVEIRA, 2009, p. 7-8).

Para os liberais, como Benjamin Constant, a ideia de liberdade incorpora a esfera privada e os direitos dos indivíduos diante das maiorias, não cabendo ao Estado legislar sobre comportamentos, crenças e inclinações dos indivíduos. Constant foi um dos primeiros a refletir e a valorizar questões como privacidade e anonimato. Para ele, tratavam-se de valores imprescindíveis à liberdade dos modernos, além de serem fundamentais para distinguir as esferas pública e privada. (SILVEIRA, 2009). Já os utilitaristas, em contraposição aos liberais, tinham Jeremy Bentham o seu maior expoente e defendiam a supressão de qualquer incerteza quanto às identidades pessoais, “uma vez que isso obscurecia a classificação e o correspondente cálculo geral necessário a estruturar o bem-estar social. Para ele [Bentham], era necessário o reconhecimento total dos indivíduos, bem como era preciso uma polícia geral das identidades.” (SILVEIRA, 2009, p. 8). Como apontou Bauman,

> [...] a modernidade tinha um especial horror à indefinição, à incerteza e à ausência de controle. Nesse contexto, o anonimato foi considerado um fator de incerteza em um mundo que clamava por identidades precisas e centradas. (BAUMAN, *apud* SILVEIRA, 2009, p. 7).

Essa visão é sustentada até hoje sob o pretexto de que a ausência de responsabilidade sobre certas ações pode trazer consequências negativas à sociedade. Silveira (2009) retoma Habermas, que diz que um dos efeitos negativos do argumento anônimo irresponsável e inverídico, mas tratado como verdadeiro, é o de gerar injustiças e danos irreparáveis. É inegável, portanto, que o anonimato traz consigo dificuldades ao ser usado para fins ilícitos e ilegítimos. Todavia, como bem descreveu a ex-presidente do ICANN, Esther Dyson (1998), precisamos aprender a lidar com esse lado sombrio do anonimato em vez de colocá-lo por inteiro à margem da lei:

> É melhor para nós viver na atual situação de liberdade com riscos que estimula a liberdade com certas compensações. Qualquer tentativa de automatizar o processo de conceder o anonimato poderia torná-lo mais rastreável... e certamente chamaria atenção para seus usuários. Se o anonimato desenfreado se torna um problema, haverá tempo suficiente para lidar com ele. De fato, o perigo está mais provavelmente em outra direção -- excesso de vigilância do governo e muito pouca privacidade. (DYSON, 1998, p. 254, *apud* SILVEIRA, 2009, p. 12).

Enquanto combates contra o anonimato se dão no plano dos códigos, dos protocolos e, sobretudo, entre os Estados, a iniciativa privada também quer se beneficiar com o não-anonimato na rede. Tecnologias amigáveis e facilitadoras vão se tornando peças-chave na consolidação da sociedade de controle. As inúmeras funcionalidades e as interfaces amigáveis passam a ter a mesma importância social que o direito ao íntimo, à autonomia e a não-intromissão na vida dos cidadãos. (SILVEIRA, 2009). Vive-se um tempo em que empresas e governos vêm se aprimorando na tarefa de monitorar e coletar rastros digitais a partir da navegação dos usuários da rede. Constroem-se enormes bancos de dados compostos de perfis que orientam a economia, a publicidade, a política e as administrações públicas e privadas. O monitoramento assume formas mais ou menos evidentes, que vão desde

rastreadores como *cookies* e *beacons*, pouco visíveis, mas eficientes na coleta de dados gerados a partir das ações dos usuários em sites e em aplicativos até a lei francesa Hadopi que criminaliza o compartilhamento de arquivos que violem direitos autorais. Nota-se que a França, mesmo sendo um país democrático, adota medidas como essa que, em outrora, eram exclusivas de Estados autoritários. O exemplo mais emblemático de como as técnicas de rastreamento no ciberespaço podem ser eficazes e por vezes imperceptíveis é a Corporação Google. Um usuário do Gmail, uma vez tendo feito *login* em sua conta, terá seu IP automaticamente vinculado a ela. Dessa forma, através do cruzamento de dados, o interagente estará conectado aos demais serviços do Google sem precisar de novas identificações. Toda e qualquer pesquisa que ele fizer no buscador ficarão armazenadas nos bancos de dados da empresa e servirão como base para análises de perfis de comportamento futuras. De acordo com Fernanda Bruno (2013), os processos de *dataveillance* (vigilância de dados), *data mining* (mineração de dados) e *profiling* (perfilagem) sustentam a vigilância contemporânea sobre indivíduos e populações, construindo saberes e interferindo em suas condutas.

Em face do exposto, a autora propõe que sejam repensadas as noções de privacidade e informações pessoais nos dias de hoje tendo em vista essas novas modalidades de coleta, registro e classificação de informações sobre os indivíduos. Para ela, não significa que mesmo sem identificação em termos jurídicos, os hábitos e ações monitorados com a finalidade de construir perfis psicológicos não violem a privacidade dos sujeitos. Como bem aponta,

> [...] em nossa cultura, a privacidade não é simplesmente um direito civil, mas também uma propriedade, logo algo que se pode conceber como mercadoria e que se pode “trocar” ou “vender” como bem quiser. Em suma, trata-se de repensar a noção de privacidade no seio das novas práticas de coleta, classificação e uso de informações sobre indivíduos, e que essa questão não seja apenas pensada no âmbito do direito ou da propriedade, mas também no horizonte das práticas de liberdade. (BRUNO, 2013, p. 147-148).

Paralelamente, existe uma porção expressiva de usuários que se preocupam com a privacidade e com o anonimato na rede. O ativismo político e a guerrilha

informacional baseados no anonimato vêm ganhando visibilidade, como é o caso do grupo *Anonymous* e do site *4Chan*, este último focado no compartilhamento de imagens sem a necessária identificação dos interagentes. Ao passo que as possibilidades de expressão pessoal e coletiva são potencializadas ao longo do desenvolvimento da internet, aumentam também as formas de resistência às liberdades, sobretudo advindas do campo político, contra a cultura estabelecida da internet, conforme viemos tratando neste trabalho até o momento. Para burlar o controle e a vigilância, usuários lançam mão de tecnologias específicas. De acordo com Castells “há uma poderosa contra-medida que poderia reforçar a segurança por todo o sistema: a difusão de tecnologia avançada de criptografia para organizações e as pessoas em geral.” (CASTELLS, 2003, p. 131). Se, através da criptografia, todos os usuários pudessem se proteger de ações mal-intencionadas, não haveria motivos para os Estados vigiarem cidadãos sem qualquer indício de ligação com atividades criminosas. Todavia, ao longo das duas últimas décadas, travou-se uma batalha para que a criptografia fosse deslegitimada e criminalizada, sendo esse um recurso extremo dos Estados para manter algum nível de controle sobre os fluxos de informação. Portanto, esse é o assunto do próximo capítulo, em que iremos tratar mais especificamente das tecnologias do anonimato, seus usos e justificativas, fazendo uma aproximação maior com o objeto de estudo do presente trabalho monográfico.

3 TECNOLOGIAS DO ANONIMATO

3.1 CRIPTOGRAFIA

A criptografia não é uma tecnologia nova. Os primeiros registros da arte de cifrar mensagens datam de 2.000 a.C., no Egito. Segundo Ulrich (2014), 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. Até o século XX, ela 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.

Conforme vimos no início do capítulo anterior, a Internet foi construída a partir da Arpanet, uma rede formada no contexto da Guerra Fria e com objetivos militares e acadêmicos. Sua evolução, desde o início, sofreu influências da cultura hacker que, por sua vez, carregava valores da contracultura norte-americana da década de 1960. Nessa época não existia uma instituição proprietária da rede, pois, a partir da década de 1970, ela era vista como um experimento coletivo, conforme explica o pesquisador Sérgio Amadeu Silveira (2009). Segundo Julian Assange (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. Para Jacob Appelbaum (ASSANGE et. al., 2013), a força de praticamente todas as autoridades modernas provém da violência ou da ameaça de violência. Porém, com a popularização da criptografia, “[...] nem toda a violência do mundo poderá resolver uma equação matemática.” (ASSANGE et. al., 2013, p. 80). Dado o poder que ela proporciona aos indivíduos, a criptografia é vista como ferramenta de libertação pelos chamados *cypherpunks*. No capítulo de apresentação do livro “*Cypherpunk*s: liberdade e o futuro

da internet" há uma breve explicação acerca do termo. Os *cypherpunks* defendem a utilização da criptografia e de métodos similares como meio para provocar mudanças sociais e políticas. "Criado no início dos anos 1990, o movimento atingiu seu auge durante as 'criptoguerras' e após a censura da internet em 2011, na Primavera Árabe [...]" (ASSANGE et. al., 2013, p. 2).

Segundo Assange (2013), 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. Como aponta Castells,

> [...] o rápido desenvolvimento de tecnologias de proteção da privacidade é exatamente o que preocupa os governos, estimulando suas tentativas de proibir o uso privado de tecnologias de criptografia e de declarar seu uso e venda ilegais. (CASTELLS, 2003, p. 151).

O governo estadunidense tentou, inclusive, introduzir tecnologias concorrentes com falhas propositalmente incorporadas para que os órgãos de manutenção da ordem pública pudessem sempre decriptar as informações. A divisão dos lados nessa 'criptoguerra' é bastante complexa. De um lado, temos uma rede de governos e corporações que espionam tudo que fazemos na rede. De outro, os *cypherpunks* e demais ativistas que trabalham para desenvolver novas tecnologias e códigos que possam influenciar as políticas públicas.

Essa divisão de lados e a noção de que mesmo Estados democráticos possam ser tiranos não é uma ideia infundada se pensarmos no caso WikiLeaks. Quando tivemos o episódio do "bloqueio bancário" em 2010, ficou bem claro que o Estado estava disposto a exercer seu poder e a sua influência, em suas mais variadas instâncias, para derrubar o site e impedir que documentos confidenciais continuassem a vazar e a comprometer órgãos governamentais. Como a WikiLeaks foi projetada para

ser um canal totalmente seguro para o envio de documentos e fazendo uso de uma criptografia poderosa, os governos tiveram de encontrar outras formas de prejudicá-lo. As ações da WikiLeaks representam uma prova do poder da criptografia, sobretudo em relação ao papel que ela pode exercer em nosso tempo e em como ela poderá redefinir alguns jogos de poder ao longo do século XXI. Jérémie Zimmermann, defensor dos direitos de anonimato online, traz uma interessante reflexão que pode ser pensada como uma diretriz para usuários individuais da criptografia e para a sociedade como um todo.

> 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. (ASSANGE et. al., 2013, p. 79).

Sendo assim, passaremos a discutir ao longo deste capítulo as principais características e aplicações das tecnologias que são fundamentais para a existência e manutenção do objeto empírico deste trabalho, o site Silk Road. O comércio de drogas ilícitas na internet só é possível graças a recentes tecnologias como o Tor e o Bitcoin, pois, juntos, eles garantem o anonimato de vendedores e de compradores, tornando bastante difícil para as forças repressoras a missão de erradicar as atividades do Silk Road. Iniciaremos o próximo tópico definindo o que é *deep web*, que se constitui como o espaço anonimizado em que se encontra o objeto de pesquisa em questão.

3.2 *DEEP WEB*

A *World Wide Web*, ou apenas Web, como é comumente chamada, contém dados e informações que, armazenadas em determinados servidores, podem ser exibidos por meio de hipertextos, vídeos, sons e imagens. Através de navegadores e provedores de busca, a internet direciona os usuários a determinadas páginas. Conforme explicam Pompéo e Seefeldt, a busca na web se dá mediante duas categorias "[...] a) a primeira delas é a conhecida como *surface web* (podendo ser chamada também de *clearnet*) b) enquanto a segunda é o que especialistas de sistemas de informação chamam de *deep web*." (POMPÉO; SEEFELDT, 2013, p. 439). Enquanto a *surface web* refere-se a páginas facilmente encontradas por mecanismos de busca, como o Google, por exemplo, a *deep web* é um compilado de páginas que, por alguma razão, não está presente nos resultados desses mecanismos, mesmo que contenham a expressão ou as palavras-chave pesquisadas pelo usuário. Cada página da rede possui padrões que a registram em servidores. Caso não sigam os padrões definidos, as mesmas ficam à margem da listagem dos resultados da pesquisa. Aqui, cabe destacar a definição de web invisível proposta por Sherman e Price. Trata-se de

> [...] páginas de textos, arquivos, muitas vezes de alta qualidade e com autoridade informacional disponíveis na *World Wide Web* cujos motores de buscas gerais não podem, devido a limitações técnicas, ou não querem, por escolha deliberada, adicionar aos seus índices de páginas Web. Às vezes, também é referida como 'Web Profunda' ou 'material escuro'" (*apud* MONTEIRO; FIDENCIO, 2013, p. 38).

De acordo com Pompéo e Seefeldt, "a expressão *deep web* foi criada por Michael K. Bergman, fundador do programa *Bright Planet*, software especializado em coletar, classificar e procurar conteúdo nessa esfera da web." (POMPÉO; SEEFELDT, 2013, p. 440). A expressão faz alusão à profundeza, enquanto a *surface web* se restringe àquilo que é superficial – não necessariamente àquilo que é raso, simplista ou genérico, e sim que está na superfície, que pode ser visualizado e encontrado. Não existe uma

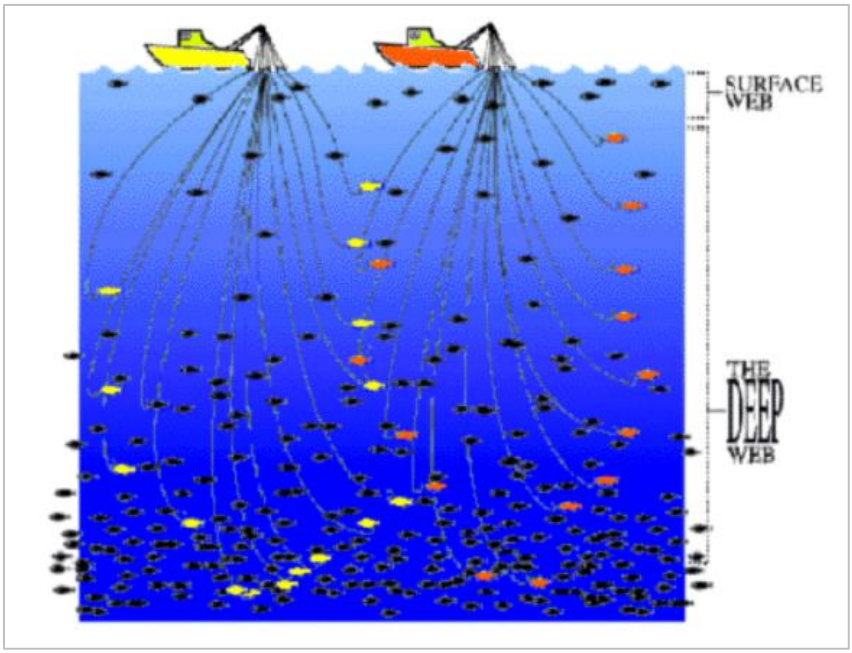
estimativa que seja consenso entre os pesquisadores a respeito da dimensão do tamanho da *deep web* em comparação com a *surface web*. Bergman afirma que

> [...] 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).

Para tanto, existem algumas analogias que, segundo Pompéo e Seefeldt (2013), nos ajudam a entender melhor essa relação de comparação. A primeira delas é a do *iceberg*. Aqui, a *surface web* é representada pelo topo, ou seja, pela parte visível. Já a *deep web* é representada como sendo a base, e, apesar de sabermos da sua existência, desconhecemos a medida exata de seu tamanho. Há também uma analogia feita com o mar, em que se faz menção a uma pessoa que, nadando, consegue visualizar apenas uma parte da água, mas que, com os devidos equipamentos de mergulho, pode imergir mais e descobrir um mundo que antes era invisível. O mesmo acontece com a web: com poucos recursos o usuário acessa a superfície, porém sem os instrumentos necessários jamais alcançará a profundeza. Finalmente, existe outra relação que faz alusão a um grupo de pescadores em um barco. Quando esses jogam uma rede de pesca na parte superficial de um rio, 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 que se obtém. A figura a

seguir (ver Figura 2) representa graficamente essa analogia do grupo de pescadores em um barco.

Figura 2 – Analogia da dimensão da *surface web* em comparação com a *deep web*.



Fonte: Bergman, 2012.

Apesar da definição técnica acerca do que é a *deep web*, aos pesquisadores da comunicação interessa o seu estudo no plano simbólico, ou seja, no que ela representa para a internet e para a sociedade como um todo. Nesse sentido, ela é vista como o "submundo" da internet, conhecida, sobretudo, por abrigar inúmeros cibercrimes, dentre os quais contrabando de mercadorias e de materiais radioativos, tráfico de órgãos humanos, prostituição, pornografia, pedofilia, organização de jogos de azar, sequestros, compra e venda de assassinatos, falsificações e comércio de drogas ilícitas[11]. Ainda que a *deep web* seja um espaço usado para criar relações seguras e confiáveis entre ativistas, organizações e entidades, são pelos crimes que se dão

[11] Os 8 piores casos da deep web que foram descobertos por internautas da surface. Disponível em: <http://ahduvido.com.br/os-8-piores-casos-da-deepweb-que-foram-descobertos-por-internautas-da-surface>. Acesso em: 17 nov. 2014.

nesse espaço que ela é reconhecida no imaginário popular. Em um dos poucos estudos que tratam sobre o mercado de drogas que se instaurou na *deep web,* especificamente sobre o site Silk Road, o pesquisador norte-americano Nicolas Christin (2012) diz que existe certo nervosismo entre os líderes políticos quando se trata de redes anônimas. O recente desenvolvimento de interfaces como o navegador Tor faz com que seja extremamente fácil para qualquer um navegar na internet anonimamente, independentemente do seu conhecimento técnico. É através do Tor que a *deep web* passou a ganhar maior visibilidade e alcance, principalmente porque ele facilita imensamente o acesso de pessoas leigas a esse espaço para além-Google.

3.2.1 Tor Project

Uma das principais tecnologias para se ter acesso à *deep web* é uma aplicação chamada Tor (*The Onion Router*), que possibilita que os usuários naveguem de maneira anônima. De acordo com Beckett, “o desenvolvimento inicial do Tor era para o Laboratório de Pesquisa Naval Americano, para proteger a comunicação governamental.” (*apud* MONTEIRO; FIDENCIO, 2013, p. 43). Hoje, ele é usado todos os dias com uma grande variedade de propósitos por “pessoas normais”, militares, jornalistas, policiais, ativistas entre outros. Segundo definição do site [12] oficial do projeto, o Tor é uma “rede de túneis virtuais” que possibilita que as pessoas e as organizações possam aumentar a sua segurança e privacidade na internet. Ele permite que desenvolvedores de softwares possam criar novas ferramentas de comunicação com recursos de privacidade internas. Além disso, o Tor fornece a base para uma série de aplicações que possibilitam que organizações e indivíduos partilhem informações através de redes públicas sem a preocupação de terem suas identidades reveladas.

Suas aplicações são diversas entre os setores e as classes da sociedade. A variedade de pessoas que o utilizam é, na verdade, parte do que o torna tão seguro. O

[12] **Tor Project**: Anonymity Online. Disponível em: <https://www.torproject.org/>. Acesso em: 20 ago. 2014.

Tor esconde o usuário por entre os outros usuários da rede, de modo que, quanto maior e mais diversificada é a base de pessoas que o utilizam, mais o anonimato será protegido. Silveira explica que “[...] o Tor distribui a comunicação através de uma rede de voluntários transmissores ao redor do mundo, impedindo o monitoramento da conexão, dos sites acessados e evitando que se descubra a localização física dos interagentes.” (SILVEIRA, 2009, p. 6). Alguns jornalistas usam o Tor para se comunicarem de forma mais segura 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, 2014).

O Tor dificulta a chamada análise de tráfego que, segundo Sérgio Amadeu da Silveira é “uma forma de vigilância que ameaça a liberdade e a privacidade na rede” (SILVEIRA, 2009, p. 6). A Análise de tráfego pode ser usada para inferir quem está falando com quem em uma rede pública. Conhecer a origem e o destino do seu tráfego de internet permite que outras pessoas possam acompanhar o seu comportamento e os seus interesses na rede. Pacotes de dados da internet são constituídos por duas partes: um bloco de dados e um cabeçalho. O bloco de dados é o que está sendo enviado – um e-mail, uma página ou um arquivo de áudio. Mesmo que o usuário encripte a carga de dados das suas comunicações, a análise de tráfego ainda é capaz de revelar muitas informações sobre o que ele está fazendo, isso porque ela se concentra no cabeçalho, que é onde está contida a origem, o destino, o tamanho e o tempo dos dados. Portanto, a criptografia não protege contra possíveis ataques e violações de privacidade na rede, pois ela apenas esconde o conteúdo do tráfego na internet, mas não os cabeçalhos.

A solução, portanto, está em uma rede anônima distribuída, como o Tor. Ele distribui as transações por vários lugares na internet, de forma que nenhum único ponto pode ligá-lo ao seu destino. O site oficial do Tor (TOR PROJECT, 2014) usa uma analogia que explica que a ideia é semelhante a usar um caminho sinuoso, com uma

rota de difícil acompanhamento, a fim de livrar-se de alguém que esteja seguindo-o e, em seguida, apagar as próprias pegadas deixadas ao longo da trajetória. Em vez de optar por uma rota direta entre a origem e o destino, os pacotes de dados na rede Tor seguem um caminho aleatório através de diversos servidores distribuídos de modo que nenhum observador, em qualquer ponto, poderá dizer de onde vêm os dados nem para onde vão. É por isso que a navegação pelo Tor se dá de maneira muito mais lenta do que em um navegador comum, causando estranhamento em um usuário acostumado com o Internet Explorer, Mozilla Firefox ou Google Chrome. Proporcionar uma rede de anonimato que seja viável mesmo para quem não tem conhecimentos técnicos em relação à criptografia é um desafio bastante grande. Nesse sentido, o Tor é bastante feliz em sua tentativa de garantir o anonimato na rede do maior número de pessoas possível.

3.3 CRIPTOMOEDAS

Em “*Cypherpunks*: liberdade e o futuro da internet”, os autores remontam uma parte da história das moedas virtuais. A primeira delas foi o *eCash*, criada em 1994 pelo cientista da computação e estudioso de criptografia David Chaum em oposição à Visa e à MasterCard – empresas que detêm boa parte das informações relativas a transações monetárias entre os indivíduos ao redor do globo. Apesar de se basearem em uma autoridade central, as moedas *chaumianas*, como ficaram conhecidas, usam protocolos criptográficos concebidos por Chaum para garantir o anonimato das transações na rede. Ainda que não tenha caído no gosto popular, o *eCash* representou a primeira tentativa de criar uma moeda virtual e anônima. De acordo com Julian Assange, é de extrema importância que se tenham moedas digitais anônimas justamente porque o controle dos meios de pagamento constitui um dos três ingredientes do Estado. No momento em que se retira o monopólio estatal dos meios de interação econômica remove-se um desses três principais ingredientes. Para ele, a liberdade de interação econômica ou a privacidade nessas interações é, talvez, mais

importante do que a própria liberdade de expressão, uma vez que as interações econômicas são o que de fato fundamentam toda a estrutura da sociedade. (ASSANGE et. al., 2013).

Seguindo na linha do tempo do desenvolvimento das criptomoedas, foi só em 2009 que prosperou a primeira moeda digital realmente eficaz, segundo Jacob Appelbaum (ASSANGE et. al., 2013). Ninguém sabe ao certo quem é o inventor – ou se existe um grupo de inventores – responsável pela moeda chamada Bitcoin. Sob o pseudônimo de Satoshi Nakamoto, lançou-se, em 2008, num fórum online aberto sobre criptografia, um documento que detalhava o funcionamento da nova moeda. A ideia em si e os preceitos não eram novos. Em 1998, eles já haviam sido explicitados numa lista de discussão *cypherpunk* pelo membro Wei Dai, que "[...] expunha as principais características do protocolo de uma criptomoeda e como ela poderia funcionar na prática." (ULRICH, 2014, p. 42). Sendo assim, o Bitcoin não surgiu de repente. Segundo Ulrich, ele é, na realidade, resultado de mais de duas décadas de intensa pesquisa e desenvolvimento por pesquisadores praticamente anônimos. O sistema representa um avanço importante na ciência da computação, "[...] cujo desenvolvimento foi possibilitado por vinte anos de pesquisa em moedas criptográficas e quarenta anos de pesquisa em criptografia por milhares de pesquisadores ao redor do mundo." (ULRICH, 2014, p. 44).

Há pouco mais de cem anos, segundo Ulrich (2014), o desenvolvimento da moeda foi retirado das forças de mercado e posto nas mãos dos governos. As consequências disso foram instabilidade econômica e explosão do poder dos estados e dos bancos centrais ao redor do mundo. No paradigma atual, temos a crescente perda de privacidade financeira sob a justificativa das ameaças terroristas intensificadas após o 11 de setembro. É nesse contexto que as criptomoedas, sobretudo o Bitcoin, surgem na tentativa de reverter essas tendências e de construir um mundo mais livre, não apenas no âmbito econômico, mas principalmente no social (ULRICH, 2014). É o que veremos mais detalhadamente nos tópicos a seguir ao explicarmos a evolução das moedas e o funcionamento da rede Bitcoin.

3.3.1 História das moedas

A história do dinheiro nos últimos cem anos nos ajuda a compreender questões políticas, sociais e econômicas presentes em nossa sociedade na atualidade, bem como o contexto que propiciou o surgimento das criptomoedas. O economista Fernando Ulrich (2014), autor de “Bitcoin: a moeda na era digital”, explica de maneira simples como se deu a história do dinheiro na Idade Contemporânea. Até o século XIX, metais preciosos, sobretudo o ouro, eram as moedas em circulação. Nessa época, os bancos centrais começaram a ganhar ainda mais força e autonomia, passando a exercer poder sobre a economia, algo sem precedentes na história, e com o respaldo dos governos. Com o desenvolvimento e a intensificação da divisão do trabalho, o crescimento econômico exigiu um aperfeiçoamento do dinheiro utilizado nos intercâmbios no mercado, fazendo surgir o serviço de custódia do ouro oferecido pelos bancos. Os depositantes entregavam seu ouro aos banqueiros e recebiam certificados de armazenagem. Devido à praticidade, os certificados passaram, então, a circular e a valer como se fossem o metal precioso e, na medida em que o uso do papel físico ampliou-se, o número de transações com o ouro diminuiu.

Até então, os substitutos do ouro tinham 100% de lastro, ou seja, ainda que a moeda circulante fosse em papel, havia nos cofres dos bancos o equivalente em metal precioso. Porém, assim que os bancos se deram conta que a maioria dos depositantes não exigia o resgate dos depósitos em espécie, passaram a operar com reservas fracionárias, ou seja, mantendo em custódia apenas uma fração do dinheiro físico que lhes foi depositado e emprestando o restante. Com isso, tendo ganhado a confiança dos clientes, não era mais necessário nem que houvesse papel-moeda. Ordens de movimentação e depósitos bancários eram concedidas e o dinheiro passava de uma conta a outra de maneira intangível, constituindo, assim, o que chamamos de moeda bancária ou escritural. Como explica Fernando Ulrich (2014), a função monetária desempenhada pelos metais preciosos nos últimos séculos foi a de servir como âncora de valor, de forma a disciplinar as tentativas de inflacionar os papéis-moedas. O ouro serviu como lastro apenas para que tivéssemos a segurança de que a oferta monetária

não seria inflada pela emissão excessiva de substitutos do metal precioso – cédulas ou moedas bancárias. Na opinião de Ulrich, não tardou para que governos e bancos se valessem desse sistema, passando a emitir papéis-moedas a bel-prazer e gerando hiperinflações.

Em 1971 o presidente estadunidense Richard Nixon instituiu o fim da conversibilidade do dólar – e consequentemente de qualquer outro papel-moeda nacional – em ouro, deixando os bancos centrais livres das restrições impostas pelo lastro no metal precioso. Passamos, então, a viver na era do papel-moeda fiduciário, ou seja, as moedas emitidas hoje pelos governos não têm lastro algum, apenas a confiança dos governos e dos cidadãos nesse sistema. A partir disso, lançamos as bases que nos permitirão discutir especificamente sobre Bitcoins, entendendo a sua razão de ser, seus objetivos e seus mecanismos de funcionamento, bem como compreendendo e desmistificando as várias críticas feitas à moeda digital.

3.3.2 Bitcoins

Primeiramente, é difícil compreender e explicar os mecanismos de funcionamento e a lógica por trás do experimento Bitcoin, uma vez que ele traz consigo conceitos dos mais variados campos do conhecimento, muitos deles distantes da Comunicação Social e das Ciências Humanas. Aqui, cabe ressaltar que ao longo deste trabalho trataremos Bitcoin como um experimento, sobretudo porque se trata de uma tecnologia bastante nova e que não se sabe ao certo se perdurará. De qualquer forma, o experimento Bitcoin abre caminho para que novas moedas digitais mais aprimoradas e eficazes surjam no futuro. Há uma enorme dificuldade em encontrarmos fontes fidedignas a respeito do tema, muito em função de seu curto tempo de existência e da complexidade em torno de seu entendimento. Nesse sentido, o economista Fernando Ulrich é bastante feliz em sua obra ao trazer informações e discussões construtivas a respeito dos Bitcoins, sem cair em falácias e no senso-comum.

Podemos conceitualizar o Bitcoin como uma moeda digital *peer-to-peer* (par a par, de ponto a ponto), de código aberto e que não depende de uma autoridade central encarregada de criar unidades monetárias e de verificar e controlar transações. Uma rede *peer-to-peer* é considerada descentralizada, ou seja, a força computacional é distribuída e não há um servidor centralizado. Dessa forma, a rede é global e composta de milhares de usuários que atuam como seus próprios intermediários. Todas as transações que ocorrem na economia Bitcoin são registradas em uma espécie de livro público e distribuído chamado de *blockchain*[13], o que nada mais é do que um grande banco de dados público, contendo o histórico de todas as transações realizadas desde o seu surgimento em 2009. Como bem explica Fernando Ulrich (2014), no caso do Bitcoin

> [...] a rede *peer-to-peer* desempenha uma função fundamental: a de garantir a distribuição do *blockchain* a todos os usuários, assegurando que todos os nós da rede detenham uma cópia atual e fidedigna do histórico de transações do Bitcoin a todo instante. (ULRICH, 2014, p. 45).

Ainda que não garanta totalmente o anonimato dos usuários, a rede Bitcoin permite o uso de pseudônimos. As chaves públicas de todas as transações, chamadas de "endereços Bitcoin", são registradas no *blockchain* e não estão vinculadas à identidade de ninguém. Todavia, o endereço IP do usuário pode ser facilmente registrado quando alguém realiza uma transação usando Bitcoins. Para aumentar as chances de manter o anonimato, faz-se necessário o uso de softwares como o Tor, conforme já discutimos anteriormente. Por isso, a combinação de criptomoedas com a tecnologia Tor permite que os usuários do Silk Road efetuem compras e vendas sem a preocupação de serem descobertos e punidos legalmente.

A economia Bitcoin depende dos usuários que proveem a força computacional para realizar os registros das transações. A eles damos o nome de "mineradores", que são recompensados pelo seu trabalho com novos Bitcoins recém-criados. Segundo Ulrich (2014), "Bitcoins são criados ou 'minerados' à medida que milhares de

[13] Explorador de Blocos Bitcoin. Disponível em: <https://blockchain.info/>. Acesso em: 20 ago. 2014.

computadores dispersos resolvem problemas matemáticos complexos que verificam as transações no *blockchain*.” (ULRICH, 2014, p. 19). Ou seja, cada “minerador” contribui com a força de processamento de seu computador visando à sustentação da infraestrutura que mantém e valida o sistema. O processo de mineração não se dará infinitamente, tendo a rede Bitcoin sido projetada para imitar a escassez do ouro na Terra. Somente poderão existir 21 milhões de unidades da moeda, número esse previamente conhecido pelos usuários de Bitcoin.

A criptografia, cuja importância já discutimos anteriormente, desempenha especificamente três funções essenciais na economia Bitcoin. Primeiramente, ela impossibilita que um usuário gaste os Bitcoins da “carteira” de outro usuário. Em segundo lugar, impede que o *blockchain* seja violado e corrompido e, por fim, pode ser usada para encriptar uma “carteira”, de modo que somente o proprietário possa utilizá-la através de uma senha definida por ele próprio. Aliada ao software Tor, a rede Bitcoin constitui um sistema de pagamentos extremamente seguro e confiável para quem o utiliza.

Há vantagens expressivas que podem ser atribuídas ao sistema Bitcoin. Ele pode ser muito benéfico ao facilitar o acesso ao capital por grupos controlados ou censurados por governos tiranos, possibilitando a privacidade financeira dos mesmos. Além disso, uma das maiores vantagens do Bitcoin está na redução dos custos das transações. Segundo Ulrich (2014), não há fronteiras políticas à moeda digital:

> Você pode enviar e receber Bitcoins de qualquer lugar a qualquer pessoa, esteja ela onde estiver, sem ter que ligar ao gerente do banco, assinar qualquer papel, comparecer a alguma agência bancária ou ATM. Nem mesmo precisa usar VISA ou PayPal. Você pode ter domicílio no Brasil, estar de férias em Xangai e enviar dinheiro a uma empresa na Islândia com a mesma facilidade com que envia um e-mail pelo seu iPhone.” (ULRICH, 2014, p. 63).

Em dezembro de 2010 tivemos o que ficou conhecido como “bloqueio bancário” ao site WikiLeaks. Grandes instituições financeiras como Visa, Mastercard, PayPal e Bank of America cederam à pressão estadunidense e passaram a bloquear transferências bancárias de doações realizadas ao site. Até o momento, a WikiLeaks

enfrenta a interrupção de boa parte de seu fluxo de renda e, uma das alternativas para continuar recebendo donativos de apoiadores, consiste em aceitar pagamentos em Bitcoin. Nesse sentido, o bloqueio bancário constitui uma afirmação do poder de controlar as transações financeiras e minar a liberdade econômica dos indivíduos. Como Ulrich (2014) bem nos traz, “Bitcoin não é apenas uma forma de realizar transações globais com baixo ou nenhum custo. Bitcoin é, em realidade, uma forma de impedir a tirania monetária. Essa é a sua verdadeira razão de ser.” (ULRICH, 2014, p. 105).

Apesar dos benefícios que ele traz consigo, algumas possíveis desvantagens merecem a nossa atenção. Existe um questionamento sobre até que ponto crackers podem comprometer a economia Bitcoin através de tentativas de desestabilizar o sistema, corrompendo algoritmos, alterando saldos e falsificando Bitcoins. Sobre isso, Fernando Ulrich (2014) destaca que não há registro de qualquer tipo de ataque ao *blockchain*, apenas sites de casas de câmbio foram hackeados de 2009 para cá. Ou seja, a moeda Bitcoin jamais esteve sob ataque. Sobre a possibilidade de falsificação, o autor explica:

> O Bitcoin é, então, durável e perfeitamente divisível, embora incorpóreo. Ademais, um Bitcoin é insuperavelmente uniforme, porque sua homogeneidade é matemática (por definição) e não física (não depende de medições empíricas relativas a um padrão), sendo tecnicamente impossível falsificá-lo. O ouro, ao contrário, depende de verificações e comprovações quanto a sua pureza e massa. Já o papel-moeda, embora seja bastante homogêneo, pode ser mais facilmente falsificado, dificultando a distinção de unidades monetárias genuínas das ilegítimas. (ULRICH, 2014, p. 66).

É importante ressaltar que muitas das ditas desvantagens e riscos de segurança enfrentados pelo Bitcoin são similares àqueles que o dinheiro tradicional também sofre. Notas de papel-moeda podem ser roubadas, destruídas e perdidas. Da mesma forma, informações financeiras podem ser interceptadas e utilizadas por criminosos, e sites e sistemas de bancos podem ser alvos de ataques *DDoS*, afinal, a maior parte do arranjo monetário atual constitui-se de dígitos eletrônicos no ciberespaço. Sobre isso, é interessante pontuarmos que, após a substituição do metal precioso em espécie por

papel-moeda e moedas bancárias não lastreadas, passamos a viver numa realidade em que o cerne do nosso sistema monetário já é digital e intangível, tal qual o sistema Bitcoin é. Grande parte das críticas ao Bitcoin deriva da concepção de que um dinheiro não pode depender de outras tecnologias – como a internet e a eletricidade – e que por isso o Bitcoin jamais atingiria o nível de universalidade e flexibilidade que o dinheiro físico permite. Não podemos nos esquecer, contudo, que o ouro e o papel-moeda também são dependentes de outras tecnologias. O ouro precisa ser minerado, cunhado e transportado. O papel-moeda, da mesma forma que o Bitcoin, depende da eletricidade para que seja impresso.

O sistema Bitcoin está frequentemente associado a atividades criminosas, principalmente por ser bastante difícil associar transações registradas no *blockchain* a identidades pessoais. O “dinheiro-vivo”, historicamente, é o mais utilizado por lavadores de dinheiro no intuito de não deixar rastros de suas movimentações. (ULRICH, 2014). Apesar de seu uso em atividades ilícitas, jamais se considerou banir o papel-moeda tal qual alguns governos consideram fazer a respeito da rede Bitcoin. Uma das maiores marcas na sua reputação, segundo Ulrich (2014), vem da ligação entre ele e o Silk Road. Ainda que o Silk Road trabalhe apenas com pagamentos em Bitcoin, as transações efetuadas no site representam uma parcela quase insignificante do total da economia Bitcoin. Em seu estudo, Nicolas Christin (2012) aponta que, em junho de 2013, o total de transações mensais no Silk Road alcançou aproximadamente 1,2 milhão de dólares, ao passo que o mercado de Bitcoin acumulou 770 milhões de dólares em transações no mesmo período. Isso nos faz refletir que, enquanto tecnologia, Bitcoin não é necessariamente boa ou má. Acreditamos que eventuais crimes relacionados ao Bitcoin estão atrelados a diversas outras questões, sobretudo no uso que os usuários fazem do sistema, e não na tecnologia em si.

É especialmente no âmbito legal e regulatório que se encontram as maiores incertezas quanto à ação dos governos diante do crescimento do Bitcoin. Alguns deles já se pronunciaram a respeito do assunto, outros, como o brasileiro, seguem em silêncio. Se a rede Bitcoin continuar a crescer e a prosperar, isso poderá levar a sérias ações repressivas. Segundo Julian Assange, não será possível destruir o Bitcoin,

sobretudo “[...] porque a criptografia impede ataques simples por parte das forças repressoras, mas os serviços de câmbio internacional para a conversão do Bitcoin podem ser vigiados com muito mais facilidade.” (ASSANGE et. al., 2013, p. 110). Ou seja, no momento em que ele for percebido como um concorrente genuíno às moedas estatais e às autoridades bancárias, o tratamento legal despendido poderá ser no sentido de minar e dificultar o acesso dos usuários à rede Bitcoin. Conforme os entusiastas do Bitcoin, o lado positivo do experimento Bitcoin consiste no que ele representa para a sociedade em termos de liberdade econômica e nas portas que ele abre para que novas criptomoedas, mais avançadas e aprimoradas, surjam no futuro. Uma boa alternativa para o futuro do Bitcoin, segundo Assange (2013), é tentar ser adotado pelos provedores de internet e pela indústria de serviços na internet. Sendo aceito por uma variedade de indústrias, formar-se-á um *lobby* para impedir que ele seja banido de alguma forma, tal como aconteceu com a criptografia. Esta foi, por vários anos, classificada como comércio de armas, mas, uma vez que a criptografia foi incorporada aos navegadores-padrão e aos sistemas bancários, sobretudo por proporcionar segurança e proteção aos usuários, formou-se um *lobby* poderoso o suficiente para impedir que ela fosse banida. Portanto, sejam quais forem os empecilhos que o Bitcoin enfrentará daqui para frente, certamente ele deixa marcas expressivas e duradouras no ambiente financeiro global.

4 SILK ROAD ANONYMOUS MARKET

Nesse capítulo serão apresentados os procedimentos metodológicos empregados nesta monografia. Em seguida, será feita a análise da estrutura e do funcionamento do Silk Road, bem como uma descrição crítica a respeito dos perfis de dois vendedores do site: Blackhand e The Scurvy Crew.

4.1 PROCEDIMENTOS METODOLÓGICOS

A metodologia utilizada na pesquisa empírica se dá, primeiramente, numa pesquisa de caráter exploratório a fim de validar a proposta de estudo e de efetuar uma aproximação com o objeto em questão. Segundo Gil (2008), pesquisas exploratórias têm como objetivo principal proporcionar visão geral, de tipo aproximativo, acerca de determinado fato, principalmente quando o tema escolhido é pouco explorado, tornando difícil a tarefa de formular hipóteses precisas e viáveis. Como pontua o autor, muitas vezes as pesquisas exploratórias constituem a primeira etapa de uma investigação mais ampla e o produto final desse processo passa a ser um problema mais esclarecido e passível de investigação através de procedimentos melhor sistematizados. Nesse sentido, nosso objeto de estudo enfrenta a problemática do ineditismo. Logo, diante dessa condição que o presente estudo enfrenta, a pesquisa exploratória parece ser adequada na medida em que possibilita uma abordagem inicial a um objeto empírico novo ao campo de estudos da comunicação.

Seguindo na descrição metodológica, acreditamos que a etnografia virtual (também chamada de etnografia digital ou netnografia) serve como inspiração para alcançarmos os objetivos dessa pesquisa. O curto prazo para a realização de um trabalho monográfico não nos permitiria aplicar a etnografia virtual tal como ela é descrita por alguns autores, por isso optamos por realizar uma pesquisa qualitativa de inspiração etnográfica. Cristine Hine (2000) foi uma das primeiras pesquisadoras a

analisar interações sociais em comunidades virtuais utilizando o método etnográfico. Para ela, na etnografia virtual a internet pode ser entendida sob duas perspectivas: a internet enquanto cultura e a internet enquanto artefato cultural. O primeiro viés compreende a internet como um espaço distinto do *off-line*, tendo como foco "[...] o contexto cultural dos fenômenos que ocorrem nas comunidades e/ou mundos virtuais." (FRAGOSO, RECUERO e AMARAL, 2011, p. 41). Já na segunda ótica a internet é vista como [...] "um produto da cultura, uma tecnologia que foi produzida por pessoas particulares com objetivos e prioridades situadas contextualmente." (HINE, 2000, p. 9). Aqui, a rede é percebida como um elemento da cultura e não como uma entidade à parte, integrando os âmbitos *online* e *off-line*. (FRAGOSO; RECUERO; AMARAL, 2011). A ênfase é dada nos diversos usos e apropriações que os atores sociais fazem da internet. Kozinets defende a etnografia virtual como

> [...] uma nova metodologia de pesquisa qualitativa que adapta técnicas da pesquisa etnográfica para o estudo de culturas e comunidades emergindo através das comunicações mediadas por computador." (KOZINETS, 2002, p. 2).

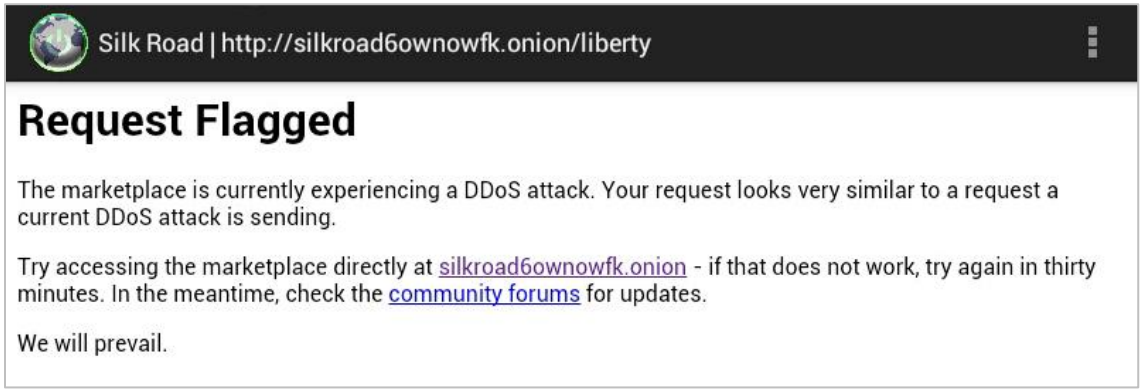
Para o autor, a etnografia virtual se diferencia em relação a três aspectos da abordagem etnográfica tradicional: 1) o *entrée* do pesquisador na comunidade online; 2) a obtenção e análise dos dados, afetando as ideias de inscrição no campo de pesquisa e anotações de campo e 3) a questões éticas da pesquisa feita em ambientes online, em que os limites entre quais dados os informantes consentem em disponibilizar para o pesquisador são mais dificilmente demarcados.

De acordo com Fragoso, Recuero e Amaral (2011), há dois tipos de pesquisadores na rede, classificados de acordo com seus graus de inserção: o silencioso (*lurker*) e o ativo (*insider*). Kozinets diz que as "[...] netnografias podem variar ao longo de um espectro que vai desde ser intensamente participativa até ser completamente não obstrusiva e observacional." (KOZINETS, 2007, *apud* AMARAL, 2008, p. 8). A etnografia tradicional tem como foco a observação participante, afinal é impossível que se faça uma abordagem não participante em situações face a face. Em se tratando de ambientes virtuais, é possível que o pesquisador esteja invisível e

apenas observe e descreva os aspectos que lhe cabem sobre determinada comunidade e/ou cultura.

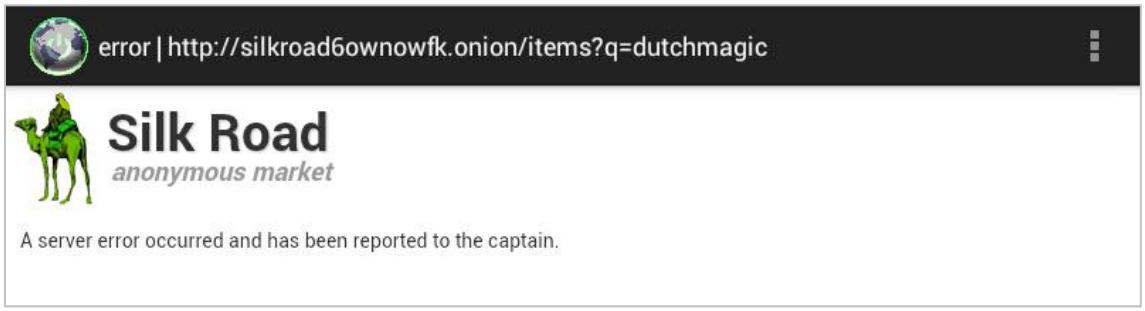
No presente estudo, optamos pela postura de pesquisa silenciosa (*lurking*) por diversas razões. No primeiro contato com o objeto empírico, durante o primeiro movimento exploratório, pudemos perceber a instabilidade do Silk Road, conforme exemplificamos através das figuras abaixo (ver Figuras 3 e 4):

Figura 3 – Aviso de que o site provavelmente está sob ataque *DDoS*.



Fonte: Silk Road, 2014.

Figura 4 – Aviso de problemas com o servidor.



Fonte: Silk Road, 2014.

Ataques de crackers não são incomuns e ele está constantemente na mira das forças regulatórias, o que faz com que não consigamos prever quando o site estará fora do ar. Acompanhar e interagir em fóruns de discussão e em postagens dentro do site pode ser uma tarefa árdua e incerta, podendo comprometer o cronograma, as análises e os resultados da nossa pesquisa. Como não objetivamos entrevistar vendedores e consumidores, tampouco conhecer a fundo suas motivações pessoais, cremos não ser necessária a interação direta entre pesquisador e pesquisado. Ademais, entendemos que o anonimato é a base do bom funcionamento do Silk Road. As compras e as vendas só acontecem quando ambos os lados sentem-se seguros nessa relação. Se algum observador resolver participar ativamente desse ambiente ele poderá gerar desconfiança entre os usuários. Ainda na fase de pesquisa exploratória, em abril de 2014, pudemos perceber, principalmente através dos fóruns de discussão, um clima de paranoia que faz parte do cotidiano dos usuários do site. Por se tratar de um site envolvido com atividades ilícitas, é de se esperar que ele seja pouco amigável a práticas relacionais, sobretudo com pesquisadores que não pertençam à "comunidade" e desconheçam alguns de seus códigos.

Em face do exposto, faremos uma observação não-participante a fim de encontrarmos as respostas para o nosso problema de pesquisa inicial. Objetivamos, portanto, não interferir nas práticas cotidianas do site, e nosso foco estará voltado para as informações que forem públicas e visíveis. Optamos por não preservar a identidade de nenhum interagente do site, afinal, não entramos em contato com nenhum vendedor ou comprador, portanto todos os dados coletados são públicos. Ademais, as identidades pessoais já estão preservadas pelos próprios usuários ao fazerem uso de tecnologias do anonimato, como conexão via Tor e uso de programas de encriptação de mensagens através de chaves criptográficas pessoais (as chamadas PGP *keys*), e por optarem por não revelarem seus nomes reais ao utilizarem nicknames.

Analisaremos de forma sucinta a estrutura básica do site – interface, tipos de produtos vendidos, informações fornecidas pela equipe do SR e sistemas reputação de vendas –, com um olhar atento para três questões fundamentais: anonimato, confiabilidade e ilegalidade. Durante a pesquisa exploratória, observamos vários

vendedores do site e três deles chamaram a nossa atenção. Sendo assim, compondo o escopo da análise, faremos uma descrição crítica dos perfis dos vendedores Blackhand e The Scurvy Crew. O Blackhand foi escolhido por ter, aparentemente, uma ótima reputação no Silk Road e por estar sempre entre os primeiros colocados nos rankings das categorias de produtos nos quais se encontra. Esse vendedor é também um dos poucos a possuir uma clara preocupação com a necessidade de se construir uma identidade visual através de um logotipo marcante (o seu representa uma mão preta, em alusão ao seu nome de usuário dentro do site). Mesmo em um mercado-negro, onde a comunicação visual parece estar em segundo plano, o vendedor se mostra consciência da importância disso. Já o The Scurvy Crew foi escolhido em função da pesquisa exploratória que realizamos em abril. Nesse período, pudemos perceber que ele era um dos vendedores mais bem cotados no site, assim como o Blackhand. Ele ganhou, inclusive, uma matéria no portal norte-americano VICE[14], o que fez sua visibilidade aumentar consideravelmente. Porém, durante o período de nossa coleta de dados, o The Scurvy Crew estava sob investigação pela equipe técnica do Silk Road, tendo sido acusado de "*scamm*" (fraude) por vários de seus compradores. Então, em função dessa notável "ascensão e decadência" que pudemos acompanhar é que escolhemos analisar o *profile* desse vendedor.

Avaliaremos os textos que compõem a página de cada um deles, buscando menções e referências a anonimato – incluindo as tecnologias do anonimato –, confiança, relacionamento, comunicação com os clientes e construção identitária. O período de análise se concentra de 26 de outubro a 02 de novembro de 2014. Contudo, devemos ressaltar que alguns dados a respeito dos vendedores datam do final de abril (21/04/2014) e do final de setembro (30/09/14). Conforme detalharemos melhor no momento de cada análise, ambos encontravam-se em modo de suspensão no período de nossa coleta de dados – ainda que cada um deles por razões diferentes.

A coleta de dados se deu da forma mais prudente possível. Conforme explicamos anteriormente, o site sempre foi muito instável, o que, para uma pesquisa

[14] My top-secret meeting with one of Silk Road's biggest drug lords". Disponível em: <http://www.vice.com/read/the-scurvy-crew-silk-road-interview>. Acesso em: 30 de set. de 2014.

científica, constitui-se como um problema de ordem prática. Dessa forma, para não perdermos nenhum dado relevante para a nossa análise, sempre que adentrávamos na página dávamos o maior número possível de "*screenshots*", mesmo em conteúdos que depois foram descartados do escopo analítico final. Sendo assim, conseguimos coletar um grande volume de dados que, mesmo com o fechamento do site no dia 06 de novembro de 2014, não nos impediu de escrever toda a nossa análise. Todas essas informações excedentes estão organizadas e sob a posse da autora desse trabalho.

O acesso aos dados se deu através de um *tablet* com o sistema operacional *Android*. Fizemos o download de dois aplicativos (*Orbot* e *Orweb*) que, combinados, nos deram acesso à rede Tor e, portanto, ao site Silk Road. Algumas configurações básicas no *Orbot* foram necessárias, mas pudemos encontrar, com relativa facilidade, tutoriais em fóruns de informática que nos ajudaram no passo a passo desse processo.

4.3 ESTRUTURA E FUNCIONAMENTO

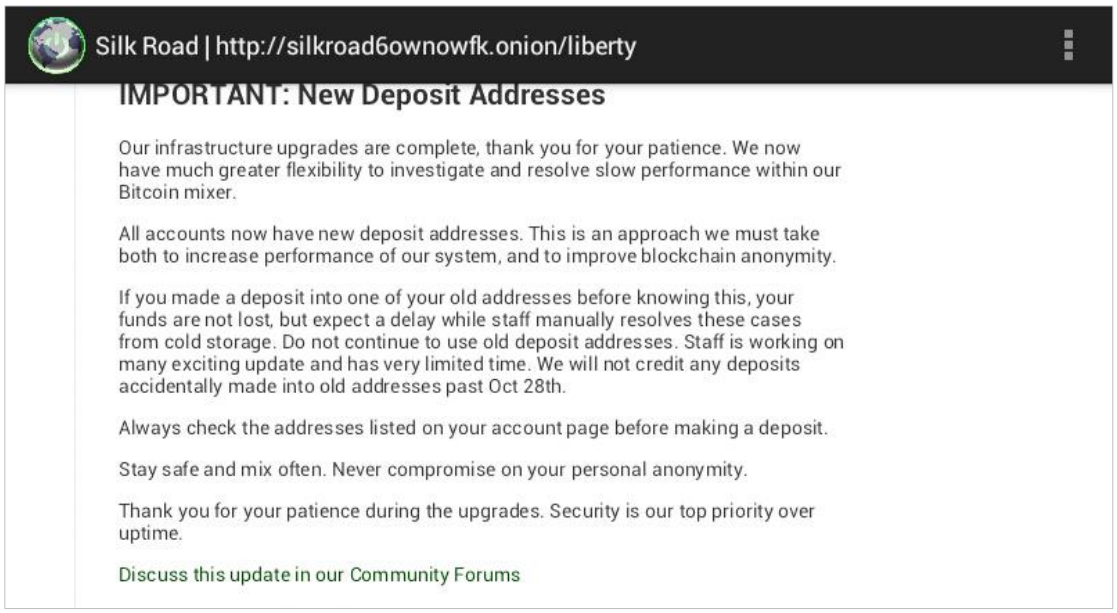
O Silk Road (SR) possui uma interface simples e com boa usabilidade. Diferentemente de alguns sites da web comum, o SR opta por não utilizar grandes recursos visuais e de programação, como *flash*, em função da lenta conexão através do Tor. Ao digitarmos a URL do site, vemos uma tela branca com o logotipo do SR e com um espaço para preenchermos o nome de usuário e senha. Por motivos de segurança, assim como em outros *black markets*, o acesso é restrito a usuários previamente cadastrados.

Assim que o acesso é validado, passamos para a tela principal da página. É interessante notar que a URL inicial não possui o sufixo "/*home*" como a grande maioria dos sites, e sim "/*liberty*". Nesse ponto, há um mural de avisos e uma espécie de manifesto escrito pelos administradores da página. O primeiro aviso se refere às atualizações na infraestrutura do site, como novos endereços de depósitos de Bitcoins visando à melhoria no anonimato no *blockchain* (ver figura 5). Os dizeres

> Fique seguro e mude com frequência **senhas e chaves criptográficas** [grifo nosso]. Nunca comprometa o seu anonimato pessoal. Obrigado pela sua paciência durante o período de atualizações. A segurança é a nossa prioridade no tempo em que estamos no ar operando [...]. (SILK ROAD, 2014, tradução nossa),

já trazem a ideia de que segurança, confiabilidade e anonimato são os valores mais estimados para a equipe técnica do site.

Figura 5 – Comunicados do *Silk Road Team* na página inicial do site.

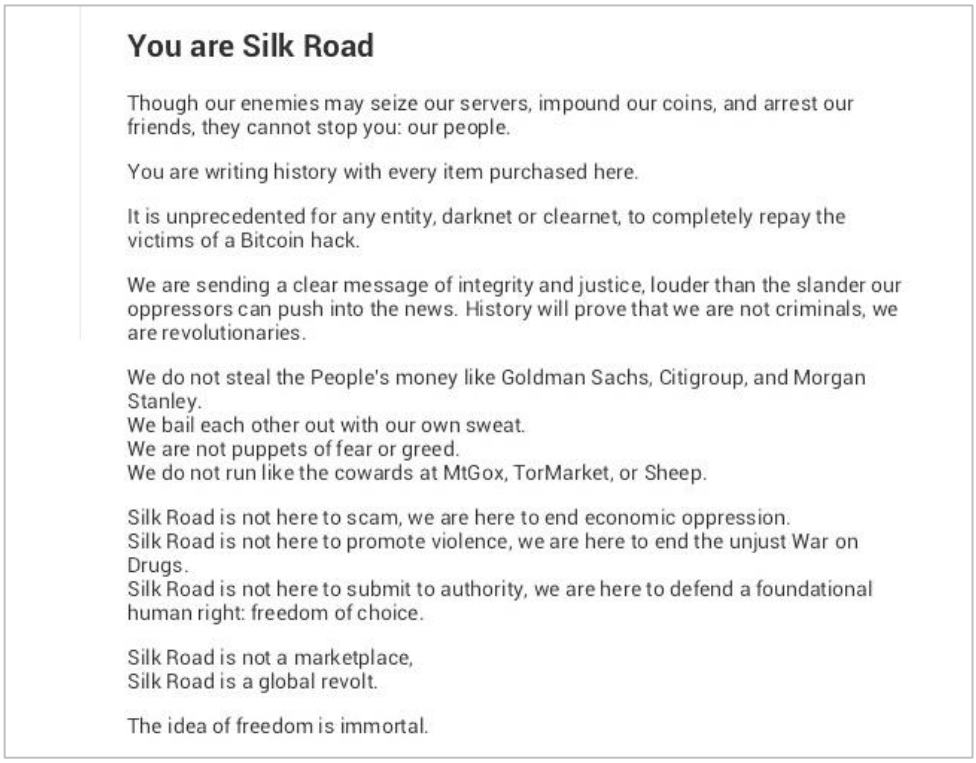


Fonte: Silk Road, 2014.

Em seguida temos um texto-manifesto que expressa, em poucas palavras, a visão que a equipe administradora do site tem em relação a várias questões que permeiam a *deep web* e os *black markets*. Para o *Silk Road Team,* mesmo diante de adversidades e de represálias – como comprometimento de servidores, roubos de moedas e prisões – não há como impedir o funcionamento do site – ou de mercados-negros em geral –, tampouco conter o ímpeto dos atores envolvidos nesse processo.

Em referência ao ataque sofrido em fevereiro de 2014, eles dizem que é sem precedentes na história – tanto na *darknet* quanto na *clearnet* – que uma entidade consiga reparar totalmente as vítimas de um *Bitcoin Hack*, algo que eles se orgulham de ter conseguido fazer. "Estamos enviando uma mensagem clara de integridade e de justiça, muito maior do que a calúnia de nossos opressores nos noticiários. A história vai provar que não somos criminosos, somos revolucionários." (SILK ROAD, 2014, tradução nossa).

Figura 6 – Texto-manifesto do *Silk Road Team* na página inicial do site.



You are Silk Road

Though our enemies may seize our servers, impound our coins, and arrest our friends, they cannot stop you: our people.

You are writing history with every item purchased here.

It is unprecedented for any entity, darknet or clearnet, to completely repay the victims of a Bitcoin hack.

We are sending a clear message of integrity and justice, louder than the slander our oppressors can push into the news. History will prove that we are not criminals, we are revolutionaries.

We do not steal the People's money like Goldman Sachs, Citigroup, and Morgan Stanley.
We bail each other out with our own sweat.
We are not puppets of fear or greed.
We do not run like the cowards at MtGox, TorMarket, or Sheep.

Silk Road is not here to scam, we are here to end economic oppression.
Silk Road is not here to promote violence, we are here to end the unjust War on Drugs.
Silk Road is not here to submit to authority, we are here to defend a foundational human right: freedom of choice.

Silk Road is not a marketplace,
Silk Road is a global revolt.

The idea of freedom is immortal.

Fonte: Silk Road, 2014.

Com a afirmação de que com isso estão enviando uma mensagem de integridade e de justiça, trazemos, aqui, uma reflexão bastante importante para o presente estudo. Em primeiro lugar, mesmo um mercado-negro especializado em itens

ilícitos precisa ter relações de confiança bem estabelecidas entre os interagentes. A associação entre o comércio de bens ilegais com condutas mal intencionadas e desonestas faz parte do senso-comum, mas que logicamente não se sustenta, como veremos ao longo desta análise.

Se não houvessem regras previamente estabelecidas e um código de conduta mínimo, o Silk Road simplesmente não funcionaria e as transações entre vendedores e compradores não se efetivariam. Um mercado livre, portanto, como se propõe o Silk Road, não é sinônimo de um mercado descontrolado, sem normas e fraudulento. O Silk Road é um mercado livre principalmente no sentido econômico. É bastante enfatizado no texto-manifesto que os grandes “ladrões” da sociedade são as instituições financeiras, como Goldman Sachs, Citigroup e Morgan Stanley. O trecho

> [...] Silk Road não está aqui parapraticar fraudes, estamos aqui para acabar com a opressão econômica. [...] Silk Road não está aqui para se submeter à autoridade, estamos aqui para defender um direito humano fundamental: liberdade de escolha" (SILK ROAD, 2014, tradução nossa).

corrobora com essa discussão. A liberdade de escolha promovida pelo SR consiste em permitir que vendedores e compradores negociem itens proibidos pela maioria das autoridades legais ao redor do mundo (principalmente substâncias entorpecentes), sem a necessidade do intermédio de instituições bancárias que, como vimos no capítulo anterior, exercem controle e vigilância na sociedade.

Seguindo na descrição da estrutura e do funcionamento do site, concentramo-nos em identificar os itens que são comercializados na página. À esquerda do texto-manifesto, temos um menu com 23 categorias que organiza os produtos disponíveis entre os vendedores, conforme podemos ver na figura 7:

Figura 7 – Menu lateral que categoriza todos os itens à venda no site.

Fonte: Silk Road, 2014.

O primeiro item refere-se às drogas, estando subdividido de acordo com o tipo: estimulantes, psicodélicos, prescrições, precursores (substâncias utilizadas na síntese de novas drogas), outros, *cannabis* e esteroides. Em seguida, temos álcool, vestuário, arte, livros, colecionadores, equipamentos de computador, encomendas

personalizadas, *digital goods* (contas de serviços online, contas *premium*), parafernálias de drogas (equipamentos necessários para o preparo e/ou uso de algum tipo de droga), eletrônicos, eróticos, falsificações, *hardware*, ervas e suplementos, joias, materiais de laboratório, jogos e loterias, medicamentos, *money* (livros, documentos ou serviços para ganhar dinheiro), embalagens, serviços e documentos. No dia 26 de outubro, contabilizamos um total de 16.294 itens à venda, dentre os quais 13.961 referentes a drogas entorpecentes e medicamentos. Ainda que o *Silk Road* se posicione como um *Anonymous Market* (mercado anônimo), a reputação do site está diretamente associada à venda de drogas ilícitas, tanto entre os usuários quanto na mídia. O anonimato, aqui, está intimamente ligado à ilegalidade.

Conforme vimos no capítulo anterior, a *deep web* é simbolicamente associada à pedofilia, contudo não encontramos nenhum material dessa natureza em negociação. O posicionamento frente a essa questão por parte da equipe mantenedora do Silk Road não foi mencionado no texto-manifesto da página inicial e em nenhum outro comunicado da equipe dentro do site. Ainda que não possamos afirmar a existência de um texto que expresse claramente o que pode ou não ser vendido no site, acreditamos que existam *guidelines* que regulem a não existência de conteúdos de pedofilia e de armamentos bélicos. Portanto, mais uma vez podemos dizer que o Silk Road não está livre de normas que regulem suas práticas e alguns limites, inclusive morais e éticos, são dados.

Ao ganhar notoriedade midiática após o fechamento da versão 1.0, o Silk Road chamou também a atenção de fraudadores, conhecidos como "*scammers*" dentro da comunidade. Um dos principais desafios do *Silk Road Team* está em evitar que vendedores e compradores mal intencionados prejudiquem o funcionamento do site. Para ajudar a evitar situações como a de fevereiro de 2014, o site aprimorou o sistema de reputação dos vendedores. Entre o final de abril e o final de setembro de 2014 – não sendo possível precisar exatamente a data – foi acrescentado um índice numérico que mede o "*score*" de cada vendedor (ver Figura 8).

Figura 8 – Comparativo que demonstra que a equipe técnica do site implantou um sistema de reputação dos vendedores.

Fonte: produção da autora.

Não foi encontrado nenhum detalhamento a respeito desse índice, mas pudemos observar algumas características sobre ele. Ele vai até o número 100 – portanto 100 é o melhor que se pode alcançar –, porém não conseguimos identificar se ele parte de zero. Não encontramos, durante o período de observação descrito, algum vendedor que atingisse a pontuação máxima, o que nos leva a crer que trata-se de um sistema reputacional bastante criterioso. Além de ser numérico, ele ajuda o comprador a identificar os melhores vendedores também por um sistema de cores: verde (bom), amarelo (regular), vermelho (ruim) e cinza (novo vendedor que ainda está em período de observação).

Além disso, há também o *vendor feedback* (ver Figura 9), que fica exposto no perfil de cada vendedor. Ele vai de zero a cinco estrelas, sendo atribuído pelo comprador após a negociação com determinado vendedor. Esse *feedback* é mostrado também em formato numérico, não ficando claro como essa contagem é feita – apenas podemos concluir que 5 é o valor máximo atingível. Abaixo do *vendor feedback* há um detalhamento desse *feedback*, ficando visíveis os comentários dos compradores, o número de estrelas atribuídas, o link para o produto que foi comprado e a data do comentário (sem especificação de horário).

Figura 9 – *Vendor feedback*, com um índice dos últimos 30 dias, dos últimos 60 dias e um índice total.

Fonte: Silk Road, 2014.

4.4 ANÁLISE DE VENDEDORES DO SITE

Conforme descrevemos nos procedimentos metodológicos, teremos como foco a análise dos *profiles* de cada vendedor, não fazendo parte do escopo analítico a descrição de cada produto à venda, tampouco questões referentes a *layout* do site e comentários de *feedbacks* dos compradores – ainda que alguns desses dados possam aparecer em momentos pontuais. Nosso objetivo é dar ênfase aos momentos em que o anonimato e a ilegalidade são invocados pelos vendedores nesses perfis escritos por eles próprios. É importante destacarmos que o site não padroniza os conteúdos que devem constar em cada *profile* – eles são organizados por cada vendedor de acordo com suas próprias necessidades e regras. O Silk Road apenas regula informações básicas, como quantidade de itens à venda, *vendor score* e *vendor feedback*, há quanto o tempo o vendedor comercializa no site, a última vez em que ele adentrou em sua conta, o país de origem dos produtos e para onde o vendedor realiza a entrega. Quaisquer outras informações ficam a cargo de cada vendedor.

4.4.1 Vendedor 1: Blackhand

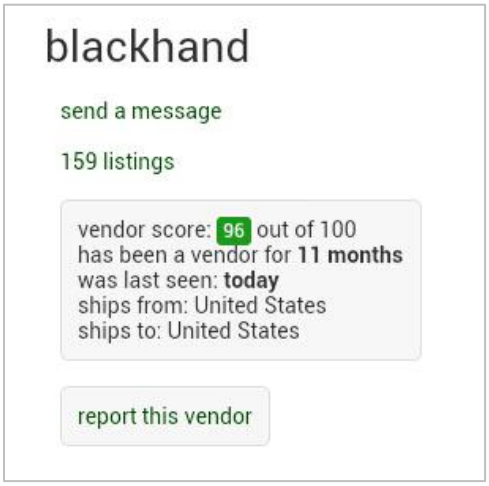
Blackhand é, provavelmente, um dos vendedores mais interessantes de serem observados no Silk Road. Possui uma enorme variedade de produtos à venda, não estando restrito somente a drogas entorpecentes. Além de alguns tipos de drogas, como *ayahuasca*, nicotina e cogumelos alucinógenos, o Blackhand também comercializa livros (com temáticas bastante variadas, como técnicas de roubos, técnicas *hackers*, astrologia, misticismo, satanismo, pirataria e *fitness*), documentos falsificados, serviço de criação de identidades visuais, videogames raros, seringas, removedores de *tags* e de etiquetas, kit de chaves universais e etc.

Figura 10 – Compilado de alguns itens comercializados pelo Blackhand.

Fonte: produção da autora.

Desde a pesquisa exploratória feita em abril de 2014, pudemos perceber sua relevância dentro do site, estando sempre entre os primeiros resultados de busca nas suas categorias de atuação. Seu *score* de reputação era 96 de 100 em 01 de novembro de 2014, um número que podemos considerar como sendo muito bom, sobretudo porque ele é um dos vendedores com mais produtos à venda (159 itens) e provavelmente realiza um grande número de transações, estando constantemente sob avaliação e crítica dos compradores. Quanto maior o número de vendas, maior a responsabilidade do vendedor em responder as mensagens de todos os clientes, de manter o controle sobre seu estoque, de despachar os produtos com segurança e de cumprir com os prazos assumidos. Quanto maior a visibilidade de um vendedor, maiores tornam-se os riscos também, que vão desde ter suas encomendas interceptadas pelas forças repressoras até a negociação com compradores mal intencionados ou infiltrados no site. Podemos aferir, portanto, que Blackhand é um bom vendedor, que consegue lidar com um grande volume de produtos e de clientes, sendo capaz de estabelecer relações de confiança com seus compradores tanto no pré-venda quanto no pós-venda, mantendo seu *vendor score* (figura 11) seu *vendor feedback* (figura 12) sempre bem cotados.

Figura 11 – Informações fornecidas pelo site a respeito do Blackhand.



Fonte: Silk Road, 2014.

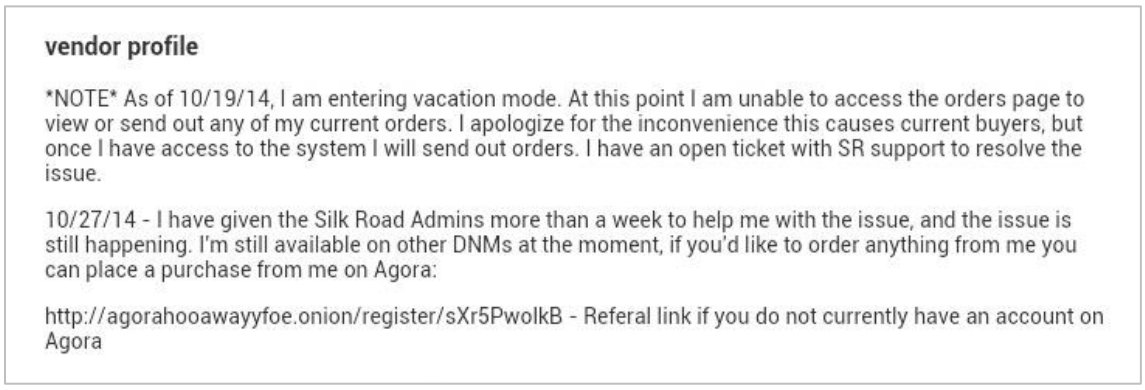
Figura 12 – *Vendor feedback* do Blackhand.

Fonte: Silk Road, 2014.

A partir daqui, analisaremos ponto a ponto o perfil do Blackhand, descrito por ele próprio. O *profile* desse vendedor é divido em tópicos que organizam o conteúdo postado por ele, já que o site não oferece um *layout* que organize e padronize os perfis de todos os vendedores. Na parte superior temos os avisos mais recentes (ver Figura 13) e de máxima importância, que merecem a atenção dos visitantes da página. Ele explica que desde o dia 19 de outubro entrou em "*vacation mode"* (pelo contexto, podemos entender que se trata de uma espécie de suspensão conferida pelo SR ao vendedor), o que o deixa incapaz de acessar a página de encomendas para visualizar ou enviar qualquer um dos seus pedidos. No período de observação de nossa análise, como a página estava suspensa, não era possível encontrá-la através do campo de buscas do site. Somente digitando "*/users/blackhand*" ao final da URL do site é que conseguimos encontrar o perfil do vendedor. Conforme o próprio Blackhand relata em 27 de outubro, ele está há mais de uma semana tentando resolver seu problema[15] de acesso junto à equipe de suporte do Silk Road e que, portanto, só está conseguindo vender em outros *black markets*, como o Agora[16].

[15] Em 02 de novembro de 2014, no último dia de nossa coleta de dados, a página do Blackhand continuava suspensa pela equipe do site.
[16] O Agora segue em funcionamento mesmo após o fechamento do Silk Road. Disponível em: <http://agorahooawayyfoe.onion> Acesso em: 16 de nov. de 2014.

Figura 13 – *Vendor profile* do Blackhand.



Fonte: Silk Road, 2014.

A seguir, temos uma descrição dos conteúdos que podem ser encontrados no perfil, organizados na forma de nove tópicos: 0) comunicados; 1) sobre mim; 2) política de reembolso; 3) política de "finalização precoce[17]"; 4) política de tempo de entrega; 5) política de transporte; 6) formatação de endereço; 7) pedidos em grande quantidade; 8) não sabe como usar PGP? Veja aqui.

Figura 14 – Organização dos conteúdos disponíveis em seu perfil descritos pelo próprio Blackhand.

Fonte: Silk Road, 2014.

[17] "Finalização precoce" (*FE: finalize early*) é quando o comprador paga em Bitcoins ao vendedor antes mesmo de ter recebido o produto.

Com o intuito de trazermos material consistente para a análise e evitando o excesso de informações, analisaremos apenas os pontos que consideramos fundamentais para nos ajudar a responder o nosso problema de pesquisa, ou seja, pontos que nos ajudem a entender como se constroem as práticas comunicacionais no Silk Road tendo em vista suas condições de anonimato e de ilegalidade. Primeiramente, no item **“Comunicados”** (*announcements*), destacamos três comentários do Blackhand. O primeiro deles é do dia 04 de janeiro de 2014:

> Hoje eu recebi o maior elogio da minha carreira em meu *feedback*: "Blackhand é, talvez o criminoso mais exageradamente sofisticado e profissional que eu já tive o prazer de encontrar". Não há nada realmente digno de nota a dizer, isso só fez eu me sentir bem. Eu decidi, quando eu comecei a vender no Atlantis seis meses atrás que, se eu ia ser um criminoso, eu decidi ser quase palavra por palavra que o usuário disse sobre mim: exageradamente sofisticado e profissional. (SILK ROAD, 2014, tradução nossa).

Aqui o vendedor se mostra bastante feliz com um *feedback* positivo deixado por um comprador em seu perfil. As qualidades atribuídas pelo cliente são justamente aquelas com as quais ele sempre buscou ser reconhecido desde que entrou para a “vida no crime”: sofisticação e profissionalismo. Portanto, mesmo que o Blackhand se intitule como criminoso e comercialize bens ilícitos em mercados negros, ele preza pelo profissionalismo e busca manter boas práticas comunicacionais com seus consumidores, construindo uma boa reputação nos ambientes em que atua. Seguindo na análise dos comentários, temos um que data do dia 02 de abril de 2014 e que merece nossa atenção:

> Eu ia anunciar isso ontem, mas não queria que ninguém pensasse que era uma piada do dia primeiro de abril, por qualquer motivo insano. Meu anúncio é este: eu não vou responder a mensagens me pedindo para envios internacionais. Eu sei que isso soa muito rude e pouco profissional da minha parte, mas meu tempo é precioso para mim, e responder a todas as mensagens que recebo em todos os mercados toma o meu tempo, e quando cada um dos meus anúncios tem "apenas EUA" claramente escrito na seção de transporte, é um pouco frustrante quando me perguntarem se eu faço envios internacionais. Eu estou em processo de investigar como faço para fazer envios internacionais anonimamente, mas é um processo lento e eu não vou estar disposto a

> fazê-lo até que eu esteja absolutamente certo de que não há risco para mim. (SILK ROAD, 2014, tradução nossa).

De forma bem humorada, o Blackhand reforça entre seus compradores que ele não realiza envios internacionais. O próprio Silk Road, como já mencionamos anteriormente, padroniza esse tipo de informação – de onde o vendedor é e para onde ele realiza entregas. Mesmo assim, os clientes do Blackhand parecem insistir para que ele envie para outras regiões além dos EUA. O vendedor diz que, como tem uma grande cartela de clientes em vários *black markets*, não vai mais perder tempo respondendo a uma pergunta que já está respondida através da padronização oferecida pelo SR. Blackhand diz, ainda, que está tentando formular uma estratégia para envios internacionais, mas que, por razões de segurança, ainda não está preparado para essa tarefa. Isso nos mostra, mais uma vez, o profissionalismo desse vendedor. Ele reconhece suas limitações práticas e técnicas e prefere não arriscar ter sua identidade revelada pelas forças repressoras, tampouco colocar seus consumidores em situações igualmente inseguras. Por fim, o terceiro e último comentário é do dia 08 de setembro de 2014:

> Além disso, tem havido um recente fluxo de usuários deixando *feedbacks* negativos sobre as vendas de livros eletrônicos, sem entrar em contato comigo em primeiro lugar. Se há um problema com sua compra, entre em contato comigo para resolução. Se você deixar um *feedback* negativo sem qualquer explicação ou mesmo a tentativa de me dar a chance de fazer o certo, o nosso negócio será permanentemente terminado. (SILK ROAD, 2014, tradução nossa).

Aqui, o vendedor pede para que ele tenha a chance de resolver qualquer problema com algum cliente insatisfeito antes de receber um *feedback* negativo. Como no SR o sistema de *feedback* é referência para os consumidores escolherem os melhores vendedores, o Blackhand se preocupa em manter seus índices em alta, pois suas vendas e seu reconhecimento como bom vendedor dependem disso. Seu objetivo maior, portanto, parece ser bem claro: garantir a satisfação do comprador e fazer da

relação vendedor-comprador mutuamente benéfica, sem, é claro, comprometer o anonimato de nenhuma das partes.

Seguindo na análise dos tópicos de conteúdos do perfil do vendedor, no item **“Sobre mim”** (*about me*) temos uma descrição do Blackhand sobre quem ele é e a que ele se propõe:

> Simplesmente dizendo, "eu sou A Mão Negra", e eu decidi há muito tempo que, se eu vou ser um criminoso, então eu vou ser o criminoso mais sofisticado e profissional que já se encontrou. Atualmente tenho uma boa seleção de *Ayahuasca* [www.ayahuasca-info.com/pt/introduction/], San Pedro cactos seco (mescalina), ferramentas utilizadas por ladrões e bens digitais. Estou sempre à procura de novos produtos para vender. Eu era vendedor no *Atlantis*, no *Sheepmarket* e no *Black Market Reloaded* e em cada um deles eu realizei mais de 1000 vendas e nunca recebi uma classificação negativa. Estou sempre disposto a trabalhar com um cliente insatisfeito para fazer com que uma experiência negativa se transforme em uma experiência positiva. (SILK ROAD, 2014, tradução nossa).

Aqui, como já discorremos anteriormente, o Blackhand constrói sua identidade como sendo a de um criminoso extremamente profissional, que cumpre com seus compromissos e busca realizar um bom trabalho, buscando novos produtos para incrementar seu negócio. Ele conta que já vendeu no *Atlantis Market Place*, no *Sheepmarket* e no *Black Market Reloaded* e que em todos eles nunca recebeu uma classificação negativa. Não podemos comprovar se esses dados são realmente verdadeiros, afinal não tivemos acesso às informações desses outros mercados, apenas podemos aferir que no Silk Road o Blackhand se estabeleceu como um vendedor confiável, que preza por uma boa relação com seus clientes. Como ele próprio descreve no trecho acima, ele se mostra sempre disposto a reverter o quadro de insatisfação de algum comprador.

No tópico **“Política de reembolso”** (*refund policy*) podemos perceber uma preocupação do vendedor em estabelecer regras prévias em relação a possíveis devoluções de dinheiro (Bitcoins) a seus compradores. Ele diferencia a política de reembolso entre bens digitais e entre bens físicos. Em relação aos bens digitais, o

Blackhand se propõe a ajudar o comprador caso haja algum problema técnico e, em casos raros onde não há solução, ele restitui o comprador (não sabemos detalhes de como esse reembolso é feito). Já em relação aos bens físicos, o Blackhand deixa claro que se o cliente forneceu um endereço incorreto não haverá reembolso nem reenvio de mercadoria. Se a falha for do próprio Blackhand ao embalar o produto, o reembolso é de 50%. Em situações hipotéticas como essa, o comprador poderia solicitar a intervenção da equipe técnica do Silk Road pedindo uma mediação de conflito. Não sabemos como o *Silk Road Team* se comporta em casos como esse – nem se esses casos realmente chegam até ele – mas acreditamos que, no momento em que o site dá liberdade para seus vendedores estabelecerem a maioria de suas regras, são estas que devem valer, afinal de contas. Por fim, o vendedor deixa claro que se diversas reclamações relativas a falhas são feitas pelo mesmo comprador ele entenderá que existe uma má intenção e uma desonestidade por parte do mesmo. Nesse ponto, podemos entender que os vendedores também podem ser prejudicados pelos clientes e que quebras de confiança podem ocorrer de ambas as partes.

Em seguida, temos a **"Política de finalização precoce"** (*finalize early policy*), em que o Blackhand deixa claro que jamais pedirá ao comprador que lhe pague antes de ter recebido o produto, pois entende que isso é um risco tanto para ele quanto para o comprador. O site disponibiliza o *escrow service*[18] (algo como "serviço de custódia"), em que o comprador deposita o valor da compra para a equipe mantenedora do site. Quando o produto é dado como recebido, o Silk Road libera a quantia correspondente para o vendedor. Isso torna, mais uma vez, evidente a preocupação tanto do SR quando do Blackhand em evitar golpes e atitudes desonestas mesmo em um ambiente de anonimato e de ilegalidade.

No item **"Política de tempo de entrega"** *(turnaround time policy)* percebemos que há uma preocupação por parte do vendedor em relação a possíveis demoras na entrega de mercadorias:

[18] O *escrow service* do Silk Road é bastante semelhante ao "Mercado Pago" do site Mercado Livre. As diretrizes do "Mercado Pago" podem ser acessadas em: https://www.mercadopago.com.br/ajuda/termos-epoliticas_194?dejavu=component%3Dfooter%26action%3Dtyc%26caller%3D%252F%253Fgclid%253DCNbjhuzI_8ECFeLm7Aod7wcAuQ%26page_id%3DCOMPONENTS

> Eu verifico e atualizo as minhas ordens de pedidos com a maior frequência que eu posso (várias vezes ao dia, geralmente) e pelo menos uma vez por dia aos finais de semana. É possível (especialmente nos fins de semana) que eu não consiga verificar ou cumprir ordens de 48-72 horas, sobretudo se eu for preso ou se estiver com um grande número de encomendas. Eu não costumo ter de lidar frequentemente com tempos de espera prolongados, mas se eu sentir que eu vou fazer você esperar um tempo incrivelmente longo, vamos discutir uma compensação justa para os seus problemas. Em todos os casos de compensação eu vou lhe fornecer um item diferente, mas semelhante, além de sua compra. Eu cuido bem dos meus clientes e, com isso, crio fãs leais. (SILK ROAD, 2014, tradução nossa).

O vendedor revela a regularidade com que acessa o seu perfil e verifica suas encomendas, buscando sempre não deixar nenhum cliente esperando tempo demais por uma resposta. Ele deixa claras as suas limitações de tempo, não sendo possível atender imediatamente as solicitações de todos os seus compradores. Mais uma vez, de forma bastante sarcástica, ele diz que se o tempo de espera estiver sendo muito longo é porque ele pode estar preso. Ou seja, sua identidade de “criminoso” é novamente invocada. É preciso lembrar os compradores de que, apesar das similaridades com outros mercados online da *surface web*, o Silk Road lida principalmente com mercadorias ilícitas e que, portanto, crimes estão sendo praticados cotidianamente. A possibilidade de o vendedor ser preso é real, e os consumidores devem estar cientes dessa adversidade tão característica e tão latente de um ambiente *underground* como a *deep web*. Finalmente, o Blackhand explica que se ele perceber que o tempo de entrega realmente está sendo maior que o habitual, ele se compromete a enviar uma espécie de “brinde” ao cliente prejudicado. Ao afirmar que cuida bem de seus clientes e que, com isso, cria fãs leais, o vendedor demonstra saber se relacionar com seus consumidores, recorrendo até mesmo a estratégias relacionadas à área do marketing e da propaganda. O mais interessante nisso tudo é que todas essas práticas parecem funcionar muito bem e sem a necessidade de os interagentes conhecerem as identidades reais um do outro.

Em **“Formatação de endereço”** (*address formatting*) o Blackhand explica que o cliente deve fornecer um endereço real e vinculado a uma pessoa que possa, de fato,

receber a encomenda. Esse é, provavelmente, um dos pontos mais críticos dessa íntima relação entre anonimato e ilegalidade. Até o momento da entrega da mercadoria, todas as interações entre os envolvidos se dão através de ambientes protegidos por tecnologias do anonimato. Já no momento da entrega da mercadoria física, as desconfianças por parte dos clientes tendem a aparecer mais, principalmente por suas localizações físicas reais estarem em jogo. Consequentemente, isso evoca o medo da descoberta das identidades reais dos compradores por parte dos órgãos repressores, por isso alguns clientes costumam fornecer endereços falsos ou que não lhes pertencem. Acreditamos que, nesse ponto, a relação de confiança entre comprador e vendedor precisa ser ainda mais forte do que em um mercado comum da *surface web*, afinal, eles estão lidando com riscos reais de intervenção policial.

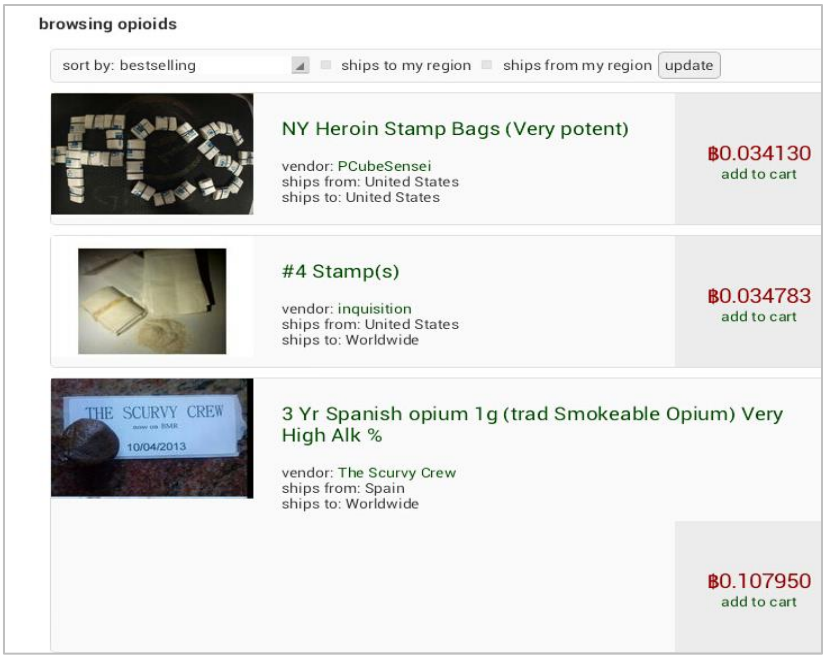
Por fim, no item **“Não sabe como usar PGP? Veja aqui”** *(don’t know how to use PGP? Look here)* o vendedor ensina o passo a passo de como criar uma chave criptográfica e de como encriptar conteúdos. A troca de mensagens entre vendedores e compradores se dá, exclusivamente, através de um programa que utiliza endereços criptografados com PGP, o que garante a não identificação dos interagentes e dos conteúdos trocados entre si. Como o Silk Road não oferece uma tecnologia própria e realmente segura de troca de mensagens, cada comprador define as regras sobre qual software irá utilizar para se comunicar com seus clientes. Para evitar indagações referentes à comunicação PGP, o Blackhand explica bem didaticamente – considerando, inclusive, que o usuário é totalmente leigo no assunto – em seu *profile*, e essa parte técnica do passo a passo não nos é relevante nessa pesquisa, por isso optamos por não descrevê-la.

Dito isso, podemos afirmar que esse vendedor organiza muito bem as regras e as condições com as quais trabalha, a fim de evitar dúvidas e possíveis desgastes com seus consumidores. No tópico em que discutiremos os resultados de nossa análise como um todo, aprofundaremos mais as nossas percepções em relação ao Blackhand.

4.4.2 Vendedor 2: The Scurvy Crew

O The Scurvy Crew (TSC) é um vendedor igualmente interessante de ser analisado porque pudemos acompanhar sua ascensão e seu declínio dentro do Silk Road entre o final de abril e o início de novembro de 2014. Conforme podemos perceber nas figuras abaixo (ver Figuras 15 e 16), ao contrário do Blackhand, seus índices reputacionais (*vendor score* e *vendor feedback*) não se mantiveram estáveis ao longo do tempo. Em 21 de abril de 2014, o The Scurvy Crew era o terceiro colocado no ranking da categoria na qual ele é especializado, opioides, conforme podemos ver na figura abaixo:

Figura 15 – The Scurvy Crew era bem cotado no Silk Road em 21 de abril de 2014.

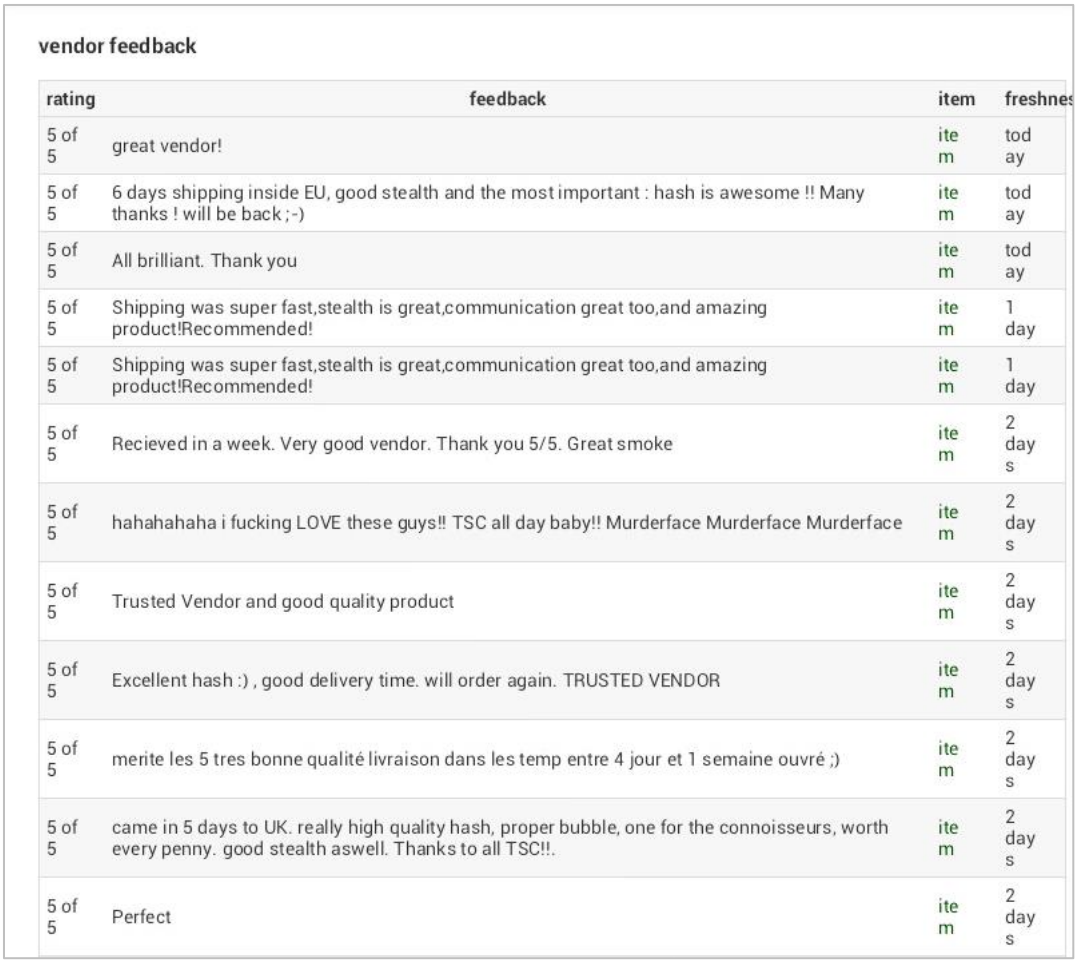


Fonte: Silk Road, 2014.

Nessa mesma data (21/04) o site ainda não possuía o *vendor feedback* organizado sob forma numérica, mas, através da figura 16, podemos notar que os comentários dos compradores são, em sua totalidade, positivos. O número de

“estrelas” atribuídas pelos compradores é o máximo alcançável por um vendedor dentro do Silk Road (5 estrelas).

Figura 16 – Imagem que demonstra que o The Scurvy Crew era considerado, pelos seus clientes, um bom vendedor.



vendor feedback

rating	feedback	item	freshnes
5 of 5	great vendor!	item	today
5 of 5	6 days shipping inside EU, good stealth and the most important : hash is awesome !! Many thanks ! will be back ;-)	item	today
5 of 5	All brilliant. Thank you	item	today
5 of 5	Shipping was super fast,stealth is great,communication great too,and amazing product!Recommended!	item	1 day
5 of 5	Shipping was super fast,stealth is great,communication great too,and amazing product!Recommended!	item	1 day
5 of 5	Recieved in a week. Very good vendor. Thank you 5/5. Great smoke	item	2 days
5 of 5	hahahahaha i fucking LOVE these guys!! TSC all day baby!! Murderface Murderface Murderface	item	2 days
5 of 5	Trusted Vendor and good quality product	item	2 days
5 of 5	Excellent hash :) , good delivery time. will order again. TRUSTED VENDOR	item	2 days
5 of 5	merite les 5 tres bonne qualité livraison dans les temp entre 4 jour et 1 semaine ouvré ;)	item	2 days
5 of 5	came in 5 days to UK. really high quality hash, proper bubble, one for the connoisseurs, worth every penny. good stealth aswell. Thanks to all TSC!!.	item	2 days
5 of 5	Perfect	item	2 days

Fonte: Silk Road, 2014.

Seguindo nessa rápida reconstrução histórica da reputação do TSC no Silk Road, a partir do dia 30 de setembro de 2014, seu *score* reputacional já estava em 65 de 100, um número bastante ruim e que fica grifado em vermelho, como que indicando uma situação de alerta aos compradores em potencial. Depois, no dia 01 de novembro de 2014, quando ele já estava com suas vendas suspensas e sob investigação pela equipe do site, o seu *score* era 47 de 100, como podemos ver na figura logo abaixo

(ver Figura 17). Vendedores com *vendor score* muito baixo tendem a gerar desconfiança por parte dos compradores, tal como acontece num mercado online da *surface web*, como *Ebay*[19], *Etsy*[20] e Mercado Livre[21].

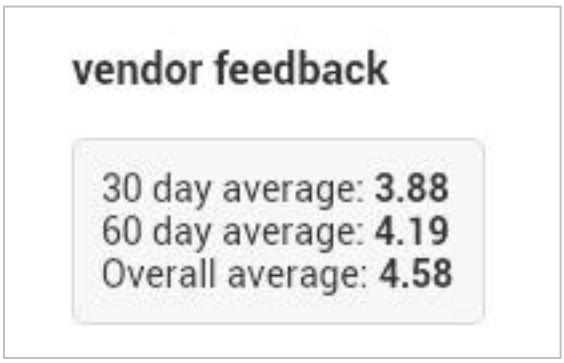
Figura 17 – Declínio do *vendor score* ao longo do tempo.

Fonte: produção da autora.

Da mesma forma, seu *vendor feedback* era considerado bom até 60 dias antes do período em que os dados de nossa pesquisa foram coletados (01 de novembro de 2014). Já nos 30 dias anteriores ao dia 01 de novembro, o seu *vendor feedback* numérico já havia caído consideravelmente, conforme podemos perceber na figura a seguir:

[19] Disponível em <http://www.ebay.com/> Acesso em 14 de novembro de 2014.
[20] Disponível em <https://www.etsy.com/pt/?ref=hdr> Acesso em 14 de novembro de 2014.
[21] Disponível em <http://www.mercadolivre.com.br/> Acesso em 14 de novembro de 2014.

Figura 18 – Declínio do *vendor feedback* numérico ao longo de um período de 60 dias.



Fonte: Silk Road, 2014.

Essa decadência visível do TSC – apesar de não sabermos exatamente o porquê de ele não estar cumprindo com seus compromissos com seus compradores e, portanto, recebendo tantas qualificações negativas – nos faz pensar na hipótese de que esse vendedor não conseguiu construir tão bem e de maneira tão sólida as relações com os seus clientes tal como o Blackhand conseguiu fazer – e de maneira bastante notável.

Em face do exposto, a partir daqui passaremos a analisar o texto que compõe o perfil desse vendedor, afinal esse é o foco de nossa análise. Antes de chegarmos ao *vendor profile* propriamente dito, vale destacarmos os tipos de produtos que o The Scurvy Crew comercializa. Ele possui uma quantidade menor de mercadorias (44 itens), se comparado ao Blackhand, e é especializado apenas em drogas entorpecentes, como haxixe, maconha, cocaína, heroína, LSD, ópio, *Spanish Bayer Opium* (um tipo especial de ópio) e diversos tipos de pílulas, conforme podemos ver abaixo (figura 19):

Figura 19 - Compilado de alguns itens comercializados pelo The Scurvy Crew.

Fonte: produção da autora.

Os conteúdos de seu perfil são bastante desorganizados, tanto na forma de texto quanto na forma visual, o que torna a nossa análise bem mais dificultosa do que a do vendedor anterior. Na parte superior temos os avisos mais recentes e de máxima importância. Há uma nota dos administradores do Silk Road dizendo que a conta do The Scurvy Crew foi desativada enquanto eles analisam um *scam report* (denúncia de fraude apontada pelos usuários do site). Em seguida, temos uma série de avisos do TSC a seus clientes:

> IMPORTANTE !!!!!!!!! *[sic]* Eu estive no hospital nas últimas 2 semanas, temos um grande lote de encomendas que estão saindo para entrega agora, esperamos entregar todas que estiverem atrasadas dentro da próxima semana. [...] Estamos agora com um estoque completo e remetendo a pilha de encomendas acumuladas. Espere para fazer comentários, se possível, o que nos permitirá lidar melhor com todos os problemas decorrentes de ordens de atraso. [...] Por favor, fique conosco enquanto elevamos a nossa pontuação de reputação ao nível que era antes da minha ida ao hospital. (SILK ROAD, 2014, tradução nossa).

Aqui, notamos que o The Scurvy Crew é, na verdade, uma equipe de vendedores. Em alguns momentos o TSC fala em primeira pessoa e em outros utiliza o termo “nós”. Optamos, portanto, a sempre nos referirmos a The Scurvy Crew como “ele”. Resumidamente, nos comentários acima, ele diz que os pedidos já estão saindo para entrega e pede que os compradores compreendam que ele esteve hospitalizado por duas semanas. Ele pede, ainda, que os clientes não desistam de comprar dele em função dos baixos índices reputacionais que vem enfrentando.

A seguir, temos um tópico que, fazendo uma analogia com o perfil do Blackhand, corresponderia ao item “Sobre mim”. Nesse ponto, o The Scurvy Crew afirma ser um dos melhores vendedores do *Sheepmarket* e do *Black Market Reloaded*, além de ter sido um dos melhores no Silk Road “original”. Por fim, ele agradece ao portal Vice pela entrevista publicada sobre eles.

Depois disso, temos o tópico **“Missão”** que explica, de maneira bastante confusa e longa, a que o The Scurvy Crew se propõe. Não pretendemos transcrever e traduzir todo esse texto, apenas destacaremos alguns pontos-chave que se relacionam com o nosso problema e nossos objetivos de pesquisa.

> O The Scurvy Crew acredita que todos os seres humanos têm o direito de escolher o que fazem com seus corpos. A busca para satisfazer a curiosidade, para curar doenças ou a busca pela iluminação espiritual através do uso de drogas já existe há milênios. [...] O TSC não acredita que qualquer organização tenha o direito de tirar essa escolha do povo, ou limitar o seu alcance a alguns poucos escolhidos. [...] Procuramos tornar os medicamentos disponíveis que são remédios naturais, como haxixe, ópio, ou ferramentas espirituais como o LSD, independentemente das leis em seus países de origem. [...] Fazemos isso porque acreditamos que nenhum homem tem o direito de tirar o que a natureza cria, e teremos o maior prazer em jogar com a nossa liberdade para lhe fornecer essas coisas. O que nos fez bem sucedidos e que nos torna diferente de outros fornecedores é que tomamos uma posição política nesta luta, em vez de ser um vendedor 100% impulsionado pelo lucro. (SILK ROAD, 2014, tradução nossa).

O TSC se apresenta de forma recorrente e libertária em relação às políticas públicas defendendo o anonimato e o uso de substâncias entorpecentes. Ele acredita que os seres humanos devem ter autonomia sobre seus corpos e que o uso de drogas,

sobretudo as “naturais” e “espirituais” às quais ele se refere, sempre fez parte da história das civilizações ao longo do tempo. Nesse ponto, chegamos a uma reflexão extremamente importante de nossa análise, que contrapõe os dois vendedores analisados. Ao contrário do Blackhand, que constrói deliberadamente a sua identidade de criminoso profissional, o The Scurvy Crew constrói o seu discurso tendo como base a crença de que seu trabalho é, acima de tudo, um trabalho social, um trabalho de alguém que defende uma causa e se sacrifica por ela. Para ele, ao menos na forma como ele se posiciona em seu *profile*, esse sacrifício é a sua liberdade individual.

A seguir, o vendedor discorre de maneira bastante extremista sobre as injustiças e incongruências do “sistema” no qual vivemos:

> [...] O estado escraviza seu povo através da supressão econômica, favoritismo político e legislação injusta. É um novo tipo de escravidão, que tenta nos enganar em uma ilusão de liberdade. [...] Este mundo está sendo conduzido por pessoas incrivelmente doentes. O abismo entre o que você acha que está acontecendo e o que está realmente acontecendo é absolutamente enorme. A ganância é o ponto que define a forma de como o sistema está doente. Por que um homem deve possuir bilhões e outro não ser capaz de alimentar seus filhos? (SILK ROAD, 2014, tradução nossa).

Logo em seguida ele se posiciona em relação a questões financeiras, dizendo que um mercado global não deve ser regulamentado pela moeda. Nesse sentido, conforme pontuamos em nosso referencial teórico, o Bitcoin (única moeda aceita no Silk Road) constitui uma alternativa ao sistema econômico tradicional controlado pelo Estado. Ainda que o TSC não mencione o Bitcoin no trecho a seguir, os ideais econômicos descritos por ele vão ao encontro daquilo que os entusiastas dessa criptomoeda postulam:

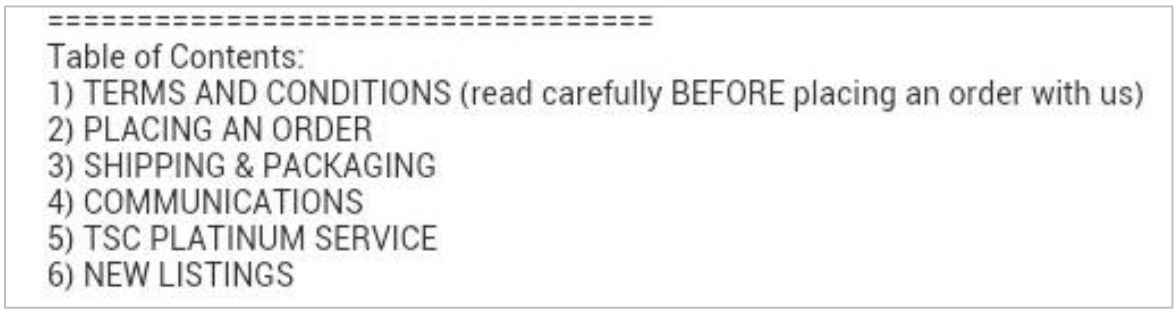
> [...] Acreditamos em um mercado global que não possa ser regulamentado pela moeda. Um que não se preste à manipulação e permita o livre comércio e a automoderação. Nós acreditamos em um futuro de verdadeira liberdade. Liberdade em que os nossos telefonemas não possam ser ouvidos e nossas escritas permaneçam como sendo nossas.” (SILK ROAD, 2014, tradução nossa).

Por fim, o vendedor pontua que, na sua concepção, a verdadeira liberdade está diretamente relacionada ao anonimato das comunicações, como telefonemas e mensagens escritas.

Avançando na descrição do *profile* e tendo destacado os principais tópicos de sua “Missão”, temos o item **“Feedback”**. Aqui, o vendedor destaca alguns comentários positivos deixados pelos seus compradores no seu *vendor feedback*. Isso nos faz refletir que, como esses comentários foram previamente selecionados pelo TSC, não há nenhum deles que seja negativo. Ademais, não podemos comprovar a veracidade dessas informações, tampouco sabermos a data desses comentários que, possivelmente, são relativos aos “tempos áureos” do The Scurvy Crew, em abril de 2014.

Logo após vemos uma espécie de índice (ver Figura 20) que categoriza os conteúdos que devem ser lidos pelos compradores antes de efetuarem uma compra: 1) termos e condições; 2) fazendo um pedido; 3) envio e embalagem; 4) comunicações; 5) TSC serviço platinum; 6) novos anúncios. Novamente, ao contrário do Blackhand que é bastante sucinto e objetivo, o TSC possui um menu desorganizado tanto visualmente quanto na distinção dos conteúdos de cada seção.

Figura 20 – Organização dos conteúdos disponíveis em seu perfil pelo próprio The Scurvy Crew.



Fonte: Silk Road, 2014.

Em **"Termos e Condições"** (*terms and conditions*) o vendedor pontua que o The Scurvy Crew é um grupo honesto e que todas as regras estabelecidas no *profile* têm por objetivo proteger não só a eles como a toda a comunidade do Silk Road. Sendo assim, conforme dissemos na análise da estrutura e do funcionamento do SR, mesmo em um *black market* especializado em itens ilícitos é necessário que hajam normas que sejam suficientes para construir relações de confiança entre os interagentes.

> A satisfação do cliente é o nosso objetivo número um. Se algo der errado, vamos fazer tudo o que pudermos para fazer tudo certo. Qualquer membro do fórum que comprou de nós e teve algum problema pode atestar isso. [...] Somos um grupo honesto e quando lidamos com você esperamos o mesmo. Com isso em mente, por favor, entenda que o que se segue é para proteger não só TSC, mas você e toda a comunidade SR também. [...] Infelizmente, como muitos outros fornecedores, nós tivemos problemas com compradores tentando nos enganar. (SILK ROAD, 2014, tradução nossa).

A seguir, o vendedor traz uma informação importante que não tínhamos tido acesso até então: a existência de uma espécie de *blacklist* (lista negra) de compradores não confiáveis. Ou seja, da mesma forma que os compradores recorrem ao *vendor score* e ao *vendor feedback* a fim de encontrar os melhores fornecedores, os

vendedores trocam entre si (ou em algum fórum privado) informações que podem ajudar a protegê-los de clientes mal intencionados e golpistas.

> Compradores na lista negra de fornecedores, favor NÃO tentar fazer uma compra. Nós verificamos cada comprador, antes de aceitar uma encomenda. Se você não cumprir este requisito, por favor, não envie uma mensagem para nós pedindo uma exceção. Nós não iremos vender para você. (SILK ROAD, 2014, tradução nossa)

Logo após, o TSC afirma que faz "muitas coisas" para manter sua reputação no Silk Road. Essa informação não se confirma se considerarmos a rápida reconstrução reputacional que fizemos anteriormente em relação a esse vendedor. Seus índices caíram vertiginosamente de abril de 2014 para cá, e as explicações sobre os motivos disso estar acontecendo não estão disponíveis em seu perfil. Ao contrário, temos dados que provavelmente são datados da época em que o The Scurvy Crew era considerado um dos principais vendedores do SR, conforme podemos perceber no trecho abaixo:

> Fazemos muitas coisas para manter nossa reputação. [...] Você vai ter seu pedido de forma rápida e com segurança em 99,9% das vezes. [...] A partir de agora, os reenvios vão ser uma ocorrência rara. [...] Somos um grupo de pessoas inteligentes, por favor, não tente tirar proveito da nossa bondade tentando dobrar seus pedidos pedindo um reenvio. [...] Todo o objetivo do TSC é fazer chegar o produto nas mãos de nossos clientes e isso é o que fazemos de melhor! (SILK ROAD, 2014, tradução nossa).

Concluído o tópico "Termos e condições", passamos para a análise de **"Fazendo um pedido"** (*placing an order*). Aqui, tal como o Blackhand, o TSC enfatiza que seus compradores devem fornecer dados reais para que as entregas sejam possíveis. Ele reforça, ainda, que o cliente deve usar criptografia PGP para fazer suas encomendas, sobretudo porque o site pode estar comprometido – principalmente por órgãos como o FBI, que realizam investigações bastante complexas na tentativa de derrubar os diversos *black markets* existentes na *deep web*. Afinal, como ele mesmo pontua, "segurança é fundamental neste jogo" – o jogo de disputas, tensionamentos e construções simbólicas e discursivas do Silk Road.

> [...] Por favor, use algum nome verdadeiro ou o nome de alguém conhecido que viva no endereço de entrega. Além disso, certifique-se de incluir um nome. Se você não incluir um nome e não receber o seu pedido, você terá negado um reenvio. [...] O site pode ser comprometido, portanto, nós sugerimos que você use a criptografia PGP quando fizer a sua encomenda. Não é obrigatório, mas é para o seu benefício. [...] Segurança é fundamental neste jogo, por isso, certifique-se de não estar pegando nenhum atalho. (SILK ROAD, 2014, tradução nossa).

Em **"Envio e embalagem"** (*shipping & packaging*) o TSC explica brevemente como se dá o processo de despacho de suas encomendas. Ele discorre também sobre o meticuloso trabalho de embalagem e ocultação de suas mercadorias e sobre como isso está relacionado ao seu sucesso enquanto vendedor. Ele diz estar sempre um passo à frente dos vigilantes (as forças repressoras) ao estar sempre aprimorando suas técnicas de embalo. Nesse quesito, o The Scurvy Crew demonstra maior preocupação do que o Blackhand, que não chega a detalhar esse item.

> Nós enviamos de segunda a sexta, duas vezes por dia. [...] Quando recebemos um grande número de encomendas, só podemos enviar certo número de pacotes por dia por razões de segurança [...] Todos os nossos pacotes são duplamente selados a vácuo! Usando as mais recentes técnicas de ocultação da *dark web*, temos um dos mais baixos percentuais de não-entrega devido ao meticuloso cuidado que tomamos no planejamento e preparo dos pacotes. Mudamos a embalagem, os estilos e os formatos regularmente para nos manter um passo à frente dos vigilantes. (SILK ROAD, 2014, online, tradução nossa).

Finalmente, no tópico **"Comunicações"** (*communications*) o vendedor procura se mostrar disponível para tirar as dúvidas de seus compradores. Da mesma forma que o Blackhand (porém de maneira menos enfática), ele diz que não irá responder às perguntas que já foram respondidas em seu *profile vendor*. Porém, como ele não organiza seus conteúdos de forma clara e organizada, provavelmente seus consumidores devem fazer perguntas "óbvias" com frequência e não devem obter respostas do vendedor.

> The Scurvy Crew está aqui para você! Sinta-se livre para enviar mensagem com todas as perguntas. NÃO tenha medo de usar a linha de assunto. Colocar o que quiser lá dentro, só não deixe em branco. As únicas perguntas que ignoradas são as que já foram respondidas aqui (por exemplo, "quando vai chegar o meu pacote?") (SILK ROAD, 2014, online, tradução nossa).

Sendo assim, concluídas as descrições dos perfis do Blackhand e do The Scurvy Crew, faremos, nas considerações finais, uma discussão geral da análise. Buscaremos relacionar os dois vendedores entre si, trazendo alguns apontamentos no que diz respeito à estrutura, ao funcionamento e ao posicionamento discursivo do site Silk Road, considerando sempre o nosso problema e nossos objetivos de pesquisa.

5 CONSIDERAÇÕES FINAIS

O presente trabalho buscou responder o problema e os objetivos de pesquisa da melhor forma possível, considerando o pouco tempo para a realização de uma monografia e levando em conta também as dificuldades enfrentadas, que vão desde a bibliografia escassa sobre tecnologias do anonimato, *deep web* e mercados negros até as dificuldades de acesso e coleta de dados em um ambiente pouco explorado pela autora. A seguir, procuramos descrever alguns apontamentos que nos ajudam a fazer um fechamento em relação à análise dos vendedores Blackhand e The Scurvy Crew, sempre buscando fazer ligações com os dados levantados no que tange a estrutura e o funcionamento do Silk Road.

Antes de analisarmos os dois vendedores mais profundamente já trabalhávamos com a hipótese de que cada um deles construía suas práticas comunicacionais de maneiras bastante distintas entre si. Após a análise, pudemos comprovar isso de modo ainda mais acentuado do que supúnhamos inicialmente. A forma que cada um deles encontrou para se comunicar em um ambiente de anonimato e de ilegalidade é bastante demarcada. Enquanto o Blackhand constrói sua identidade como a de um criminoso profissional e consciente de cada etapa de seu trabalho enquanto comerciante, o The Scurvy Crew busca se firmar como um libertário, tanto no sentido econômico como no social, em que sua posição política justifica sua atuação – e não a possibilidade de lucro.

Podemos afirmar que ambos são criminosos, afinal os dois vendem itens considerados ilícitos pela maioria das autoridades globais. Porém, entre eles é notável a diferença de percepção sobre esse fato. O Blackhand se entende como criminoso – inclusive vende itens específicos para serem usados por outros criminosos – e busca atingir um alto nível de sofisticação em todos os seus processos e práticas. Antes da realização desse trabalho, sequer imaginávamos que poderíamos nos deparar com um vendedor tão bem estruturado quanto o Blackhand. Um dos objetivos de nossa pesquisa é problematizar e desconstruir algumas questões-tabu relacionadas ao Silk

Road e, de certa forma, aos *black markets* em geral. Nesse sentido, ao nos debruçarmos sobre esse vendedor, podemos afirmar que a *deep web*, recorrendo ao sentido simbólico do termo, não é construída *apenas* por pessoas em relações fraudulentas, apesar de o senso-comum apontar para a *deep web* como um “local” onde toda a sorte de bizarrices e crimes escabrosos se encontram. Dessa forma, cumprimos de maneira bastante feliz com esse objetivo inicial ao colocarmos em perspectiva alguns desses tabus.

Entre os dois vendedores fica bastante clara a ideia do anonimato em contraposição a uma noção específica de “poderosos”. Em relação ao The Scurvy Crew, isso é construído como sendo parte indissociável de sua identidade. Enquanto o Blackhand se autodenomina como criminoso, o TSC não usa estes termos ao longo de seu *profile*. Ao contrário, ele se coloca na posição de um benfeitor que arrisca sua liberdade individual ao lutar pelo direito dos seres humanos em governar seus próprios corpos, ao lutar contra a opressão dos governos e contra a opressão econômica. A escolha aparentemente deliberada em dedicar mais espaço de fala a sua missão do que às suas políticas de venda nos dá indícios de que ele acredita que sua contribuição ao Silk Road é, acima de tudo, a de um trabalho social. O The Scurvy Crew, sobretudo quando menciona em sua missão que a verdadeira liberdade está em “nossos telefonemas não serem ouvidos e nossas escritas permanecerem como sendo nossas” (SILK ROAD, 2014, tradução nossa), mostra-se bastante ciente da relação entre liberdade e anonimato. A primeira, portanto, é evocada em seu discurso como justificativa para o anonimato.

Ambos reconhecem a importância de uma boa reputação dentro do Silk Road, tendo sido recorrentes as menções ao *vendor score* e ao *vendor feedback* ao longo dos perfis dos dois vendedores. Porém, num comparativo, podemos aferir que o Blackhand é o que melhor constrói sua reputação ao longo do tempo, estabelecendo relações de confiança mais sólidas e duradouras do que o The Scurvy Crew. Esse último parece não ter obtido melhor resultado ao gerenciar seus processos e, mesmo a notória visibilidade conquistada com a matéria no portal Vice não foi o suficiente para que ele se mantivesse como um dos mais notáveis vendedores do Silk Road.

Um de nossos objetivos específicos buscava compreender a mecânica de funcionamento do Silk Road com um olhar atento para suas especificidades e para o meio no qual está inserido. Sob uma perspectiva mais ampla, percebemos que o Silk Road enquanto um espaço anonimizado que propicia a existência de um comércio de bens ilícitos na *deep web*, preocupa-se em oferecer as bases para que outras pessoas negociem e criem suas próprias regras. O seu papel é oferecer segurança técnica, estabilidade da página e garantir os anonimatos, além de atuar como moderador em situações de desonestidade ou de fraude.

Numa analogia bastante interessante, o discurso da equipe do site parece mesclar as falas do Blackhand e do The Scurvy Crew. O *Silk Road Team* descreve alguns ideais libertários em seu texto-manifesto na página inicial que vão ao encontro do que o TSC descreve em seu perfil. Da mesma forma, a equipe do Silk Road demonstra o seu profissionalismo em diversos momentos. Ela estabelece índices de reputação entre seus vendedores, oferece canais de comunicação e de suporte aos usuários e disponibiliza mecanismos de segurança como o *escrow service*. Além do mais, a equipe alega ter conseguido ressarcir a maioria das vítimas do *Bitcoin Hack* acontecido em fevereiro de 2014, num trabalho longo e árduo. Por tudo isso é que o *Silk Road Team* mostra-se tão sofisticado e profissional quanto o Blackhand.

Nosso estudo buscou manter-se focado desde o início na questão do anonimato, fazendo apontamentos teóricos sobre as origens, os protocolos e a vigilância na internet, bem como trazendo a criptografia, a *deep web* e as criptomoedas através de um viés menos técnico e mais direcionado à comunicação social. Cremos termos conseguido identificar e elucidar as principais tecnologias do anonimato na rede e que têm ligação com o Silk Road, tal como objetivávamos desde o início.

O nosso problema de pesquisa consistia em descobrir como se constroem as práticas comunicacionais no Silk Road tendo em vista suas condições de anonimato e de ilegalidade. Nesse sentido, conseguimos responder essa questão de maneira bastante satisfatória. Em um contexto anônimo, a reputação e a construção de uma identidade forte são talvez ainda mais importantes na medida em que os consumidores e os administradores do site valorizam isso. Cada vendedor busca se legitimar como

sendo alguém reconhecível e tendo uma reputação – e o anonimato não necessariamente dissocia identidade e reputação das práticas comunicacionais. O anonimato aparece nas construções discursivas do Silk Road em uma perspectiva que o coloca como inversamente proporcional às autoridades, às grandes empresas e aos "poderosos". Outro de nossos objetivos de pesquisa pretendia discutir o anonimato como condicionante prática comunicacional específica, o que acreditamos termos conseguido fazer ao longo da análise de nosso objeto empírico.

Finalmente, chegamos ao ponto de fazermos um balanço geral de nosso trabalho. A instabilidade do site e a conexão lenta via Tor foi um dos principais apontamentos negativos que identificamos. Com isso, fomos extremamente prudentes na coleta dos dados de nossa pesquisa, o que acabou revelando-se um de nossos grandes trunfos. Na medida em que a comunicação trabalha na construção dos registros da história humana, nosso trabalho contribui para o campo pelo simples fato de termos registrado e produzido conhecimentos sobre algo que já faz parte do passado. Apesar de uma enorme quantidade de dados ter sido perdida com o fechamento do Silk Road, nos orgulhamos de, ainda que de maneira modesta, termos conseguido documentar uma parte de sua história.

Nosso estudo encontrou algumas limitações que merecem ser discutidas. Antes de definirmos o escopo de nossa análise, avaliamos a possibilidade de realizarmos uma observação participante no Silk Road. Contudo, concluímos que isso seria inviável por diversas razões, principalmente por que nos demandaria mais tempo e mais conhecimentos técnicos do que dispúnhamos naquele momento. Ademais, a nossa interação com usuários do site poderia esbarrar em questões éticas, principalmente pela possibilidade de termos de lidar com pessoas usuárias de drogas, portanto em situação de vulnerabilidade social.

Em face do exposto, acreditamos verdadeiramente que esse trabalho monográfico constitui um passo inicial importante nos estudos relacionados a um assunto com grande potencial e ainda tão pouco explorado, sobretudo pelos acadêmicos brasileiros: a *deep web*. Desde o início, um de nossos principais objetivos consistia em fomentar os estudos científicos sobre a *deep web*, principalmente no

campo da comunicação. Esperamos conseguir inspirar estudos ainda mais ricos sobre o assunto no futuro.

As perspectivas são bastante amplas. Há outros *black markets* em funcionamento, cada um com suas especificidades, que merecem ser analisados. Por fim, procedimentos metodológicos diferentes dos utilizados por nós também podem ser explorados por outros pesquisadores, gerando resultados e percepções que possam vir a complementar o nosso estudo.

REFERÊNCIAS

AGORA Market. Disponível em: <http://agorahooawayyfoe.onion>. Acesso em: 16 nov. 2014.

AMARAL, A. **Autonetnografia e inserção online.** O papel do pesquisador-insider nas subculturas da web. In: Anais do GT Comunicação e Sociabilidade do XVII Encontro Anual da Compós. São Paulo, 2008. Disponível em: <http://www.compos.org.br/data/biblioteca_315.pdf> Acesso em: 10 out. 2014.

ARAÚJO, W.F. . ***We open governments***: Análise de discurso do ciberativismo praticado pela organização WikiLeaks. 2013. 207 f. Dissertação (mestrado)- Universidade Feevale, Novo Hamburgo, 2013. Disponível em:< http://www.academia.edu/7046139/We_open_governments_An%C3%A1lise_de_discurso_do_ciberativismo_praticado_pela_organiza%C3%A7%C3%A3o_WikiLeaks >. Acesso em: 19 nov. 2014.

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

BAUER, Martin W.; GASKELL, George; ALLUM, Nicholas C. Qualidade, quantidade e interesses do conhecimento: evitando confusões. In: BAUER, Martin; GASKELL, George (org) **Pesquisa Qualitativa com Texto, Imagem e Som – um manual prático.** 7ed. Petrópolis: Vozes, 2008, p. 17-27.

BERGMAN, Michael K. ***The Deep Web:*** *Surfacing Hidden Value*. Disponível em: <http://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf> Acesso em: 21 abr. 2014.

BITCOIN: *open source p2p money*. Disponível em: <https://bitcoin.org/en>. Acesso em: 20 ago. 2014.

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

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

CHRISTIN, Nicolas**.** ***Traveling the Silk Road:*** *a measurement analysis of a large anonymous online marketplace.* Disponível em: <http://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf> Acesso em: 02 nov. 2014.

FRAGOSO, Suely. **Métodos de pesquisa para internet**. Porto Alegre: Sulina, 2011.

GALLOWAY, A. ***Protocol*: *How control exists after decentralization***. Boston: MIT, 2004.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. – 6 ed. – São Paulo: Atlas, 2008.

HINE, Christine. **Virtual Ethnography**. Londres: Sage Publications, 2000.

KOZINETS, R. ***The field behind the screen:*** *using netnography for marketing research in online communities. Journal of marketing Research*, n.39, p.61-72, 2002.

MONTEIRO, Silvana Drumond; FIDENCIO, Marcos Vinicius. **A web invisível:** um olhar sobre a parcela de informação no ciberespaço que os mecanismos de busca não conseguem indexar. Disponível em <http://www.uel.br/grupo-pesquisa/ciberespaco/doc/web_invisivel_enaic.pdf>. Acesso em: 01 set. 2013.

MONTEIRO, Silvana Drumond; FIDENCIO, Marcos Vinicius. As dobras semióticas do ciberespaço: da web visível à invisível. **TransInformação**, v. 25, n.1, p. 35-46, jan./abr. 2013. Disponível em: <http://www.scielo.br/pdf/tinf/v25n1/a04v25n1.pdf>. Acesso em: 20 maio 2014.

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.

SILK Road 2.0. Forums. Disponível em: <http://silkroad5v7dywlc.onion>. Acesso em: 01 nov. 2014.

SILK Road 2.0: Disponível em: <http://silkroad6ownowfk.onion>. Acesso em: 02 nov. 2014.

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

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

SILVEIRA, Sérgio Amadeu . Novas dimensões da política: protocolos e códigos na esfera pública interconectada. **Revista de Sociologia e Política UFPR**, Paraná, v. 17,

p. 103-113, 2009.

SILVEIRA, Sergio Amadeu. A Internet e o novo Cavalo de Tróia. **PoliTICs**, n. 10, p. 2-9, ago. 2011.

TOR Project: *anonymity online*. Disponível em:< https://www.torproject.org/>. Acesso em : 20 ago. 2014.

ULRICH, Fernando. **Bitcoin**: a moeda na era digital. São Paulo: Instituto Ludwig von Mises Brasil, 2014.