

UNIVERSIDADE FEDERAL DE SANTA CATARINA  
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS

BARBARA IDAERLA SANTOS CALDERON

**EM QUE MEDIDA A *DEEP WEB* AUMENTA A DIFUSÃO DE PODER**

Florianópolis, 2014

UNIVERSIDADE FEDERAL DE SANTA CATARINA  
CURSO DE GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

A Banca Examinadora resolveu atribuir nota 10 à aluna Barbara Idaerla Santos Calderon, na disciplina CNM7280 – Monografia, pela apresentação do trabalho EM QUE MEDIDA A *DEEP WEB* AUMENTA A DIFUSÃO DE PODER, em 04 de Dezembro de 2014.

Banca Examinadora:

---

Prof. Dr. Jaime César Coelho  
Orientador

---

Prof. Dr. Lucas Pereira Rezende

---

Prof. Dra. Adriane Nopes

*Aos meus pais.*

**BARBARA IDAERLA SANTOS CALDERON**

EM QUE MEDIDA A *DEEP WEB* AUMENTA A DIFUSÃO DE PODER

Trabalho de Monografia submetido ao curso de Relações Internacionais da Universidade Federal de Santa Catarina como parte dos requisitos obrigatórios para a obtenção do Grau de Bacharel em Relações Internacionais.

**Orientador:** Prof. Dr. Jaime César Coelho.

Florianópolis, 2014



## RESUMO

CALDERON, Barbara I. S. **Em que Medida a *Deep Web* Aumenta a Difusão de Poder.** 2014. 59f. TCC (Graduação) – Curso de Relações Internacionais, Departamento de Economia e Relações Internacionais, Universidade Federal de Santa Catarina, Florianópolis, 2014.

Este trabalho trata da difusão de poder para além do Estado em face da Deep Web, o "submundo" da *web*. Para isso, utilizou-se o conceito de poder segundo Susan Strange (1996). Foram discutidos casos provenientes da Deep Web e que obtiveram repercussão internacional como o *Wikileaks*, o grupo *Anonymous*, *Silk Road*, terrorismo islâmico *jihadista*. Procurou-se analisar, segundo a teoria, os resultados das ações desses agentes na dimensão real geográfico e suas consequências.

**Palavras-chave:** *Deep Web*, poder, difusão de poder

## ABSTRACT

This work regards the diffusion of power beyond the State concerning the Deep Web, the undergrounds of the digital web. To do so, the concept of power according to Susan Strange was used. The cases that gained most international repercussion, and whose origins is the Deep Web, were discussed such as the Wikileaks, the group Anonymous, Silk Road, the islamic jihadist terrorism. It was our intention to analyze, according to theory, the results of the actions of these agents in the real geographic dimension e its consequences.

**Key-words:** *Deep Web*, Power, diffusion of power

## SUMÁRIO

<b>INTRODUÇÃO</b> .....	9
<b>1. O CONCEITO DE PODER</b> .....	13
1.1 A razão de ser do Estado .....	13
1.2 A definição de poder.....	14
<b>2. BREVE HISTÓRICO DA DEEP WEB, FUNCIONAMENTO E CASOS ILUSTRES</b> .....	20
2.1 Desafios .....	20
2.2 A Sociedade em Rede.....	21
2.3 Breve História da Internet .....	22
2.4 A Indexação das Páginas .....	24
2.5 <i>The Onion Router (TOR)</i> .....	26
2.6 Freenet .....	26
2.7 I2P.....	27
2.8 <i>A Deep Web</i> .....	27
2.8.1 A Deep Web através do uso do <i>software TOR</i> .....	29
2.8.2 O potencial de informação da <i>Deep Web</i> .....	30
2.9 <i>Wikileaks e Anonymous: Organizações Políticas que Navegam nas Profundezas do Oceano das Informações</i> .....	31
2.10 O Lado Obscuro da <i>Deep Web</i> .....	35
2.10.1 Comércio de Bens Ilícitos .....	36
2.10.2 O Terrorismo.....	39
2.11 A Lavagem de Dinheiro e as Moedas Digitais .....	42
2.12 Conclusão .....	45
<b>3. DIFUSÃO DE PODER EM FACE DA DEEP WEB</b> .....	47
<b>CONSIDERAÇÕES FINAIS</b> .....	52
<b>REFERÊNCIAS BIBLIOGRÁFICAS</b> .....	54

## INTRODUÇÃO

Quando Maynard Keynes propôs uma nova rota de atuação para o Estado no período que sucedeu a crise de 1929, ficou entendido que o Estado teria de se impor às forças do mercado a fim de que se tomasse “as rédeas” da economia ou assumiria o risco de aprofundar e alongar a crise econômica, e conseqüentemente social. O Estado, portanto, teria utilizado de sua autoridade política para fazer os reajustes necessários que colocariam novamente a máquina de desenvolvimento “de volta aos trilhos”. Contudo, com o avanço trilhado pelos Estados capitalistas ao longo de todo o século XX, ficou subentendido a existência de uma autonomia cada vez mais crescente aos agentes econômicos. Estes pautavam seu crescimento por novas redes de integração de alcance global. Sendo assim, surgiram novos questionamentos concernentes à autoridade do Estado: estaria ela, dentro dessa nova perspectiva, declinando? Caso a resposta fosse afirmativa, de que modo a autoridade do Estado estaria entrando em declínio? Poderíamos assumir que este declínio é global, regional ou local? A tecnologia teria algum papel quanto a isso?

É fato que o avanço das tecnologias proporcionou ao ser humano um aumento da qualidade de vida e do bem-estar, bem como repercutiu em aumento das lacunas da desigualdade nas regiões periféricas do mundo, uma vez que nem todos estão incluídos em rede (Castells e Cardoso, 1999). A tecnologia, igualmente, trouxe questões referentes à ética, à moralidade e autoridade.

Nesse sentido, o desenvolvimento da Internet, pelos militares norte-americanos no início da década de 1980, surge como um marco tecnológico comparável à primeira revolução industrial. É inegável que a internet revolucionou os meios de comunicação, trouxe as sociedades mais próximas, alterou o comportamento em sociedade, encurtou o espaço e também encurtou tempo. Sendo assim, nada mais natural que tenha trazido questões fundamentais sobre o relacionamento do cidadão e do Estado ao qual ele pertence. Mas não apenas isso. A internet também nos questiona acerca do nosso próprio convívio em sociedade, acerca da censura, da liberdade, do fomento e propagação de ideologias, ao controle da *world wide web*<sup>1</sup> e, eventualmente, à autoridade em rede – se é que existe alguma autoridade.

---

<sup>1</sup> Segundo Michael Bergman (2001), apesar de ser usada como sinônimo de “Internet”, a *world wide web*

O presente estudo tem como objetivo analisar em que medida ocorre a difusão do poder na esfera da *Deep Web* - a internet profunda que nasceu em 1998 como uma alternativa à *Surface Web*, ou internet “rasa”, à qual é vigiada, e que o usuário médio acessa todos os dias por meio do computador, dos *smartphones*, dos *tablets*, ou demais dispositivos digitais. As perguntas trazidas anteriormente são necessárias para auxiliá-los na busca de respostas sobre o que é o poder, quais as responsabilidades do Estado e os contornos do seu campo de atuação. Todas essas indagações são fundamentais para se entender o novo fenômeno da inserção do Estado, da sociedade e dos novos agentes no campo da *Internet Profunda*<sup>2</sup>.

Os autores-base que nos auxiliaram no desenvolvimento do estudo foram Susan Strange, Manuel Castells e Gustavo Cardoso. Susan Strange foi a principal expoente da Economia Política Internacional da Escola Inglesa<sup>3</sup>. Seu livro intitulado *The Retreat of the State: the Diffusion of Power in The World Economy*, publicado em 1996 pela editora *Cambridge University Press*, discorre, como afirma o próprio título, sobre a retração do Estado e a difusão do poder na economia global. Para tanto, Strange se utiliza de fundamentos teóricos para basear a sua tese do declínio da autoridade do Estado, além de oferecer evidências empíricas para sustentar a sua proposição. Tais evidências dissertam sobre as autoridades existentes além do Estado, o controle das comunicações, o crime organizado, companhias de seguro, cartéis e protecionismo privado, e finalmente as organizações internacionais.

Manuel Castells realiza pesquisas sobre a sociedade da informação, sobre comunicação e também sobre globalização. Gustavo Cardoso é professor de Mídias, Tecnologia e Sociedade na Universidade Instituto de Lisboa. Ambos autores, em seu livro intitulado *The Network Society From Knowledge to Policy*, publicado em 2005 pela editora *Center for Transatlantic Relations*, tratam, sobretudo, da transição das sociedades para a chamada “sociedade em rede” na nova era da tecnologia - à qual estaríamos submetidos atualmente. Seus estudos envolvem assuntos acerca da economia mundial, tecnologia e inovação, produtividade, as reformas organizacionais e a modernização tecnológica no setor público, a reformulação do papel do Estado e sua relação com os cidadãos, a sociedade em rede, em termos globais e locais, além de suas políticas e perspectivas.

---

<sup>2</sup> Internet Profunda, tradução de “*Deep Web*”.

<sup>3</sup> Mais sobre a Escola Inglesa pode ser lida no livro de Benjamin Jerry Cohen, *International Political Economy: an Intellectual History*.

Os avanços tecnológicos da informação abriram oportunidades novas no que diz respeito à velocidade de comunicação, ao encurtamento do tempo e do espaço nas relações sociais humanas, potencializando a difusão do poder (Strange, 1996). Sendo assim, buscamos compreender de que modo a *Deep Web*, espaço da web não indexado por mecanismos de buscas da *Surface Web*, contribui para essa difusão de poder.

O presente estudo será pautado pela seguinte questão central: “*De que forma a Deep Web aumenta a difusão do poder para além do Estado?*” Dito de outra forma: em que sentido a autoridade do Estado é afetada pela *Deep Web*?

Cabe ressaltar que, certamente, o esforço feito para elucidar os pontos centrais dessa monografia serão pautados por estudos ainda recentes sobre o funcionamento e os efeitos da *Deep Web* no convívio social e o desafio imposto à autoridade do Estado. Por ser um tema recente, não temos a pretensão de dar uma resposta definitiva em relação ao assunto, muito menos restringir as respostas.

O objetivo geral, portanto, é investigar de que forma a *Deep Web* se apresenta como ferramenta que contribui para o aumento da difusão de poder. Sendo assim, os objetivos específicos são identificar o funcionamento da *Deep Web*; identificar as características diferenciais em relação à outros meios de comunicação; identificar de que forma grupos políticos, ao fazerem uso da *Deep Web*, aumentam as chances de sucesso de suas operações no plano real geográfico; compreender as consequências e os resultados advindos do uso da *Deep Web*.

A pesquisa apresentada neste trabalho foi desenvolvida segundo o modelo dedutivo. A justificativa para tal é que se partiu de um conceito abrangente de poder para compreender de que forma a *Deep Web* permite que grupos políticos tenham impacto em resultados concernentes à dimensão real geográfica.

Na primeira parte do trabalho, de cunho teórico, será realizada uma análise bibliográfica baseada em livros. A seguir, para uma observação da situação atual, a realidade prática, o estudo terá como principais fontes artigos acadêmicos, monografias, pesquisas e notícias, redigidos por estudiosos na área bem como organizações midiáticas e agências estatais. Por fim, a metodologia da pesquisa será feita de maneira cronológico-teórica para, posteriormente, chegar a conclusões práticas, a partir das repercussões internacionais dos casos e a influência nos resultados em meio à dinâmica da sociedade.

Como tentativa de resposta à pergunta de pesquisa, decidimos dividir a pesquisa em três partes. A primeira parte, discutida sob a forma do primeiro capítulo, tratará sobre o

conceito de poder. O segundo capítulo está incumbido de trazer um breve histórico da internet, do nascimento da *Deep Web* no final da década de 1990, e a consequente inserção da sociedade civil e do Estado nesse novo meio de comunicação e interação. Além disso, elencamos alguns casos famosos que transcenderam à barreira do “digital” e tiveram consequências no mundo real geográfico para embasar a hipótese de que a *Deep Web* é uma importante ferramenta de empoderamento de outros agentes que não o Estado. Finalmente, o terceiro capítulo discutirá a difusão do poder, em específico sob o viés da *Deep Web*, e versará sobre a concentração/difusão do poder do Estado nesse momento atual da história.

Finalmente, faz-se necessário esclarecer que a bibliografia utilizada para a realização dessa monografia encontra-se, em sua maioria, na língua inglesa e foi traduzida para a língua portuguesa segundo autoria própria. Julgou-se assim ter sido melhor.

## 1. O CONCEITO DE PODER

### 1.1 A razão de ser do Estado

A autoridade estatal tem entrado em declínio? O mundo vivencia uma retração do Estado? Para compreendermos um pouco sobre o significado de poder, de que forma este poder está incumbido no Estado e como isso afeta a sociedade civil, necessitamos primeiramente fazer algumas importantes ressalvas.

Muitos acadêmicos poderão esboçar alguma incredulidade frente à questão do aumento da difusão de poder para além da autoridade do Estado. (Strange, 1996). O Estado tem se colocado presente nas muitas esferas da prática social, inclusive se inserindo *online*. No entanto, quando se fala da difusão do poder, a autora não trata da questão apenas em termos quantitativos, mas em termos qualitativos. O fato de ocorrer uma retração na autoridade do Estado se relaciona com as falhas de governos em cumprir com muitas das funções básicas que lhe dão legitimidade e que são suas atribuições legais. Segundo Strange, tais funções seriam:

“[...] A manutenção da ordem e das leis civis, a defesa do território contra depredações de invasores estrangeiros, a garantia de moeda circulante na economia, a confiança da interpretação clara das regras acerca de trocas básicas de propriedade entre compradores e vendedores, credores e tomadores de empréstimo, arrendadores e inquilinos [...]” (STRANGE, 1996).

Em outras palavras, a própria garantia do funcionamento dos mercados que existem em uma economia é dada pelo Estado – pois o mesmo seria o “cimento” que assegura o direito à propriedade. Além disso, o Estado proporcionou a construção de sentimentos de identidade e lealdade que conferiu uma coesão social necessária. (Strange, 1996).

Ora, se um Estado é falho em determinada matéria a qual deveria prover um bom gerenciamento e funcionamento, de certo essa vácuo pode, e muitas vezes irá, ser preenchido por outros agentes. Assim nascem novas autoridades sobre determinada matéria que competem – muitas vezes ilegalmente – com o Estado de Direito. Este último perde um pedaço da sua área de atuação, ao qual foi destinado e tido como razão de ser criado. Fica evidente, portanto, que caso não tome atitudes em relação à essa

perda, pode-se dizer que o mesmo corre o risco de ver a sua autoridade enfraquecida (perda de legitimidade) - tornando o jogo muito mais perigoso do que se presumia em um primeiro momento.

Quanto a isso, Strange (1996) faz uma importante observação no que se refere à relação dos Estados e da economia. A autora argumenta que, na História, é possível observar que os Estados tiveram um papel de grande autoridade sobre os mercados mas que atualmente esse jogo está invertido em muitas áreas: os mercados têm tido uma frequente autoridade sobre os Estados. Esse declínio de autoridade sofrido pelos governos têm um efeito de transbordamento o qual atinge outras instituições.

## 1.2 A definição de poder

Para a definição de poder, utilizamos o trabalho realizado por Susan Strange no livro intitulado *The Retreat of the State: the Diffusion of Power in the World Economy*. Tal definição é mais abrangente, mais ampla e consegue precisar o elemento essencial ao poder. De certo, a própria definição de poder é exaustiva, árdua e poucos autores na literatura disponível das Relações Internacionais trouxeram um conceito *rigoroso*. Sendo assim, Strange (1996) também afirmar que o comum é encontrar menções sobre o poder, dar exemplos do que seria poder, de uma forma um tanto genérica. Assim, o conceito de poder foi sendo disseminado, compreendido, mas não rigorosamente definido, deixando espaço para dúvidas. Cientistas políticos utilizaram uma grande variedade de palavras para designar poder variando desde ações explícitas, como a coerção direta da violência, até as ações mais implícitas, quando o poder pode se tornar uma arte sutil de persuasão. Como afirma Strange (1996, p.17) poder foi mencionado por muitos autores da academia de Relações Internacionais como sendo uma espécie de influência ou autoridade sobre os demais.

Nesse sentido, Susan Strange aborda o tema do poder de forma abrangente, inclusiva e foi bem sucedida em sua definição para ilustrar o caso que pretendemos abordar. Segundo a autora, e para o presente estudo, o conceito de poder seria “a habilidade de uma pessoa, ou grupo de pessoas, a afetar o resultado de modo que suas preferências tenham prioridade sobre a preferência dos outros.” (STRANGE, 1996, p.17). Dessa forma, o conceito de poder estabelecido se livra da armadilha de estar sempre relacionado com a “busca de interesse”, seja esse interesse nacional, interesse de classe, interesse corporativo ou o que seja.

O problema quanto à essa definição é de cunho metodológico pois não há como quantificar o poder de forma a saber quem possui mais poder, quem é mais poderoso em uma determinada situação. Talvez por essa dificuldade de quantificar o poder é que o mesmo seja muitas vezes definido em termos de “capacidades” ou “recursos.” (Strange, 1996, p.18). É comum, por exemplo, ao analisarmos a política externa de um país termos em mente os recursos que este país têm disponível para sustentar a sua decisão, seja ela qual for. Quando uma decisão é tomada pela unidade de decisão de última instância de um Estado, isso significa que essa unidade dispõe dos meios necessários para comprometer os recursos que darão vazão à decisão. É até possível que se possa reverter tal decisão, porém não sem grandes custos para o Estado. (Hermann, 1989).

A definição de poder a qual utilizamos não trata dos recursos, sejam humanos ou materiais, mas sobre a habilidade que se possui para afetar o resultado de modo a favorecer a sua preferência em detrimento da preferência dos demais. Apesar de, metodologicamente, ser difícil quantificar o poder, é preciso admitir que existe também outra dificuldade quando se insere o elemento “vontade” nas estimações que fazemos sobre poder. No entanto, para a autora,

“[...] se, e quando, se é necessário adicionar “vontade” e “habilidade” para os recursos de homens (e mulheres) e materiais que podem ser considerados, então se tem adicionado dois fatores não quantificáveis e muitas vezes imprevisíveis para a questão”. (STRANGE, 1996).

Outra importante tentativa de explicar o poder seria a distinção de Joseph Nye entre *soft power* e *hard power*, que não possui uma precisão definida e nem muito menos se desenvolveu em uma teoria geral de poder na Economia Política Internacional. (Nye, 1990). O que Joseph Nye fez foi descrever dois tipos de poderes exercidos pelos Estados Unidos da América. Nesse sentido, Susan Strange (1996) argumenta que as duas distinções são, mais ou menos, equivalentes ao poder coercitivo, relacional (*soft power*) e o poder indireto, estrutural (*hard power*).

Stanley Hoffman e Kenneth Waltz, em 1968, observaram que “uma enorme capacidade nem sempre era traduzida em poder sobre resultados”. (WALTZ apud STRANGE, 1996, p.19) Na época em que o mundo ainda vivenciava a Guerra Fria, Waltz foi firme ao afirmar que não se poderia confundir o uso de uma bomba nuclear com possuir a opção de utilizar a bomba nuclear. Apesar de a bomba nuclear estar disponível, seu uso não foi necessário para que se alcançassem os resultados almejados.

O fator principal era que se pudesse “ser visto” como Estado com a possibilidade de usar a bomba, caso a desejasse usar. Hoffman, mais tarde, argumentou que o poder era discernível do controle sobre os resultados, ao qual Waltz foi contrário. Para ele, “Estados poderosos nem sempre conseguiam prevalecer suas preferências sobre os resultados”. Então, de que forma eram eles poderosos? Na ocasião, Waltz deu o exemplo do final da Guerra do Golfo em que os Estados Unidos, apesar de belicamente superiores ao Iraque, não conseguiram alcançar um dos seus maiores objetivos no resultado da guerra: retirar Saddam Hussein do poder do Iraque. Em outras palavras, apesar de toda a capacidade disponível, não foi possível que uma das preferências norte-americana prevalecesse no resultado da guerra. Para finalizar, Waltz concluiu que “poder é apenas uma das causas entre outras, da qual não se pode se isolar.” (WALTZ apud STRANGE, 1996, p.19)

Por quais motivos a definição de poder foi negligenciada dos estudos das Relações Internacionais? Susan Strange elenca dois possíveis fatores para que o conceito de poder tenha sido pouco trabalhado.

A primeira das hipóteses se refere à dificuldade encontrada para se aplicar a economia na política. Como fazer uma ciência relativamente exata se aplicar em uma ciência social que lida com a inexatidão? A resposta foi encontrada no uso do elemento “racionalidade”, que é largamente utilizado quando se busca explicar o comportamento dos agentes econômicos. Nesse sentido, quando uma questão é imposta, o indivíduo se pauta pela racionalidade que se traduziria como o mesmo de buscar ganhos materiais ou recursos, e evitar custos. Essa racionalidade é inerente a um pensamento lógico econômico e foi aplicada à lógica política. Em termos de política, um Estado dentro do sistema internacional agiria de acordo com a lógica da racionalidade, ou seja, sua tendência seria a de buscar ganhos e evitar custos. Dessa lógica também deriva o dilema da segurança no sistema internacional. No entanto, a autora nos lembra que há uma problema no uso da racionalidade em termos políticos: é difícil incluir nessa lógica racional - busca de ganhos e desejo de evitar custos - ações que derivam da assimetria de poder pois o poder não é quantificável. Ou seja, como explicar determinadas ações dos Estados quando estas derivam da assimetria de poder existente no sistema internacional? Fica claro, portanto, que utilizar a racionalidade, presunção básica da análise econômica, em termos políticos é dificultoso porque o objetivo e o propósito de quem detém o poder não é único, mas apresenta-se em múltiplos. Não há apenas um

objetivo, ou um único propósito, porém são vários objetivos que se interpenetram e que não obedecem uma hierarquia racional. (Strange, 1996, p.20)

Herbert Simon, economista norte-americano, foi um pesquisador que ampliou o pensamento econômico ao introduzir a sua teoria da “racionalidade limitada”, em 1958. Essa teoria tem uma grande importância por derrubar o pensamento convencional admitido até então de que empresas agem com o objetivo de maximizar os lucros e de que consumidores agem com o objetivo de adquirir os produtos e serviços com os menores preços. Em outras palavras, que os indivíduos agem em busca da melhor alternativa dentro das alternativas possíveis. De acordo com Simon, isso não é verdade. O que se pôde inferir de suas pesquisas é que os indivíduos agem de acordo com uma aproximação satisfatória dos resultados, pois eles não têm o conhecimento de todas as alternativas e nem possuem um único objetivo, mas sim múltiplos. Esses indivíduos tomariam suas decisões baseando-se na alternativa que eles conhecem e que irá satisfazer um número maior de objetivos. Contudo, apesar de não ser necessariamente a melhor opção, é a mais satisfatória entre as apresentadas. Simon chamou esse indivíduo de “homem administrativo”, em contraposição ao “homem econômico” da teoria econômica, este sim com o conhecimento de qual seria a opção de maior otimização do resultado e sempre em busca dessa opção.

Disso podemos concluir que, em termos práticos, não existe a necessidade constante de se conseguir o melhor resultado possível, e sim a escolha dos resultados suficientes para atingir objetivos múltiplos. Tais objetivos (ou preferências), contudo, não são constantes. Pelas mais variadas razões, esses objetivos se modificam no tempo e isso requer um novo pensamento sobre qual decisão tomar, e quais opções disponíveis. O elemento estático é inexistente. Sendo assim, como uma ferramenta de análise do mundo real, é preciso ter algum cuidado com o uso do termo “racional” uma vez que os objetivos são múltiplos e sobretudo não são estáticos, sofrem mudanças ao longo do tempo.

A segunda hipótese para o conceito de poder ter sido negligenciado pela literatura das Relações Internacionais, segundo Strange, é a preocupação que a academia tem com a hegemonia. (Strange, 1996, p.21) Artigos, teses, e muitas outras publicações fazem referência à hegemonia, excluindo, por consequência, o estudo sobre a natureza e o uso do poder entre os Estados. Muito se busca explicar e compreender o

papel do *hegemon*<sup>4</sup> no sistema internacional, principalmente, com o crescimento da desordem - em especial em meados da década de 1970. Uma das explicações encontrava respaldo na perda de poder dos Estados Unidos como consequência de má escolhas políticas, porém era necessário encontrar evidências da perda desse poder, tornando a problemática muito mais árdua. A explicação alternativa, no entanto, encontrou apoio com os estudos de Kindleberger, de 1973, sobre a “Teoria da Estabilidade Hegemônica” (TEH). Em um sistema anárquico, pressupondo que o Estado é egoísta e está em constante busca pelos melhores resultados segundo seus interesses nacionais, convém uma situação propícia para o surgimento de “*free-riders*” – o que causaria instabilidade. O *hegemon* poderia conferir estabilidade ao sistema ao prover bens públicos, equilibrando-o novamente. Dessa forma, fica esclarecido que o *hegemon* para exercer esse papel deve ter capacidades econômicas, políticas e militares suficientes para prover e manter essa estabilidade – que não existiria se não fosse suas provisões. O *hegemon* pode ampliar as regras do sistema internacional, bem como prevenir a adoção de tantas outras, além de realizar um papel líder na produção de novas regras. (Ming-Te, Liu, 2011). Para Keohane (1984), como resultado, “as estruturas de poder hegemônico, dominados por um único país, são as que mais conduzem à construção de um forte regime cujas regras são relativamente precisas e bem-obedecidas”. Ele também afirma que “ao declínio das estruturas hegemônicas de poder pode-se esperar um declínio da força e dos regimes econômicos internacionais correspondentes.”

Susan Strange faz uma diferença entre poder relacional e poder estrutural no que se refere a assuntos de economia política internacional. O poder relacional seria a forma de poder mais clássica na literatura das Relações Internacionais, de cunho realista, em que poder é caracterizado como a habilidade de fazer com que os outros façam algo que não fariam na ausência do exercício desse poder. Já o poder estrutural, segundo Strange, é caracterizado por quatro estruturas que estão relacionadas entre si sem que haja a predominância de uma sobre as outras. São elas, portanto: a estrutura da produção, a estrutura da segurança, a estrutura das finanças e a estrutura do conhecimento<sup>5</sup>.

Resumindo, tanto a perspectiva Neoinstitucionalista como a perspectiva da Estabilidade Hegemônica, em suas versões liberal e realista, não tratam o poder como uma capacidade de influenciar resultados, tal qual a definição abrangente dada por Susan Strange. A autora argumenta que capacidades e recursos são “uma forma pobre

---

<sup>4</sup> Hegemon ou “líder financeiro”. (Kindleberger, 1973).

<sup>5</sup> Mais sobre esse assunto é discutido no livro “States and Markets” publicado em 1988 por Strange.

de julgar o ‘poder relativo’; é mais ‘poder sobre algo’ do que ‘poder derivado de algo’ que importa”. (STRANGE, 1996, p.26). Quando os estudiosos concentram-se na teoria da estabilidade hegemônica de forma superficial para responder as questões, eles também tenderiam a se concentrar em “capacidades baseadas em áreas geográficas que os levariam à conclusões equivocadas.” (STRANGE, 1996, p. 25)

A autora ainda destaca o modo como o poder pode ser exercido, ainda que inconscientemente, apenas estando presente no cenário. Essa na verdade é uma contribuição dos estudos de gênero. (Strange, 1996, p.26) Por exemplo, tais estudos elucidam a eficácia do poder em ser exercido nas relações entre homens e mulheres na sociedade - mesmo que o desejo de explorar o privilégio não exista. Ou seja, o poder pode ser exercido apenas “estando ali”. Susan enfatiza essa importante contribuição dos estudos de gênero que ilumina as distinções entre poder relativo e poder estrutural. Quando falamos em relacionamentos é difícil pensar no poder sendo exercido por um agente sobre o outro de forma inconsciente, porém quando se trata de poder em termos estruturais a compreensão se torna mais fácil ao percebermos que as relações dentro das estruturas são afetadas – mesmo de forma não intencional. (Strange, 1996, p.26)

Resumidamente, conclui-se que o fato do poder existir, de estar presente, naturalmente o coloca, em algumas situações, em exercício - se tornando um poder inconsciente.

A conclusão elencada por Strange é a de que não há como mensurar da mesma forma resultados políticos e econômicos uma vez que existe um alto grau de complexidade no estudo de causa e efeito dessas dimensões, assim sendo, não se pode transpor mecanicamente a teoria do *homo economicus* para a ciência política. Existe um grau de dificuldade acentuado quando se trata dessa temática dentro das sociedades e das relações entre duas ou mais sociedades - quanto mais quando se trata de Estados em um sistema internacional. Quando a literatura das Relações Internacionais coloca em foco o poder estrutural dos Estados Unidos nas últimas décadas do século XX, fica claro para a autora que as principais conclusões a que se pode chegar foi a mudança na balança de poder dos Estados para os Mercados. (Strange, 1996, p.29). Dessa forma, ressalta Strange, os formuladores de política norte-americanos não tinham, na verdade, como objetivo aumentar o poder dos mercados sobre os governos, nem muito menos aumentar o poder sobre o governo deles próprios – porém, se poderia dizer que o “tiro saiu pela culatra”.

## 2. BREVE HISTÓRICO DA DEEP WEB, FUNCIONAMENTO E CASOS ILUSTRES

### 2.1 Desafios

O mundo tem atravessado nas últimas três décadas um momento de transformação estrutural largamente atribuído às tecnologias de informação. No livro intitulado *The Network Society, from Knowledge to Policy*, Manuel Castells e Gustavo Cardoso (2005) versam sobre a transformação da sociedade como a conhecemos para uma nova configuração de sociedade apoiada nas tecnologias da informação.

O segundo capítulo desse estudo traz uma abordagem referente ao histórico da Internet, e em especial a “Internet Profunda” conhecida como *Deep Web*. Sendo assim, apresentamos o funcionamento e o espaço digital que oferece à alguns setores da sociedade uma ferramenta inovadora no que tange a propagação de conteúdos e atividades ilícitas.

Nosso mundo tem feito parte de um processo de transformação estrutural por mais de duas décadas. Esse processo é multidimensional, mas é associado com a emergência de um novo paradigma tecnológico baseado na informação e nas tecnologias de comunicação que tomaram forma nos anos 1970's e foi difundido de forma desigual ao redor do mundo. Nós sabemos que tecnologia não determina a sociedade: ela é a sociedade. Sociedade molda a tecnologia de acordo com as necessidades, valores, e o interesse de pessoas que a utilizam. [...] Apesar da tecnologia ser uma condição necessária para a emergência de uma nova forma de organização social baseada no networking, ela não é suficiente. [...] Eu conceituei como ‘sociedade em rede’ a estrutura social resultante da interação entre o novo paradigma tecnológico e a mais abrangente organização social. (CASTELLS E CARDOSO, 2005, p.3)

Castells e Cardoso (2005) têm uma interessante abordagem em relação às novas organizações sociais emergentes da era da tecnologia da informação. A sociedade em rede, ao qual atribuem o objetivo de suas pesquisas, é uma sociedade formada por indivíduos, negócios e os próprios Estados, que opera nas áreas locais, nacionais e internacionais. Para se compreender um pouco mais sobre essa nova organização social, faz-se necessário o entendimento sobre a revolução tecnológica realizada nas últimas décadas que proporcionou um aumento da produção econômica e uma vantagem no que diz respeito ao encurtamento do tempo e do espaço, além de ter trazido novos questionamentos e desafios no campo da autoridade estatal.

Os estudos de Susan Strange em relação à difusão de poder do Estado foram escritos em uma época em que ainda não se produzira uma abordagem sistemática sobre o novo meio de comunicação no mundo: a conexão entre redes de computadores. Hoje em dia, muito se discute sobre os contornos da nova sociedade em rede e como a Internet se encaixa nas linhas do Direito, principalmente em questões que afetam a liberdade de expressão, a honra e a privacidade - a exemplo do trabalho realizado por Nascimento (2009). Nesse sentido, é natural que questionemos como acontece a inserção do Estado nessa esfera virtual e, mais especificamente, em que medida a mesma contribui, se é que contribui, para o aumento da difusão desse poder. Sendo assim, trataremos especificamente a *Deep Web* por dois motivos: primeiramente, a caracterização principal da “Internet Profunda” se baseia no completo anonimato, motivo pelo qual a mesma foi criada; em segundo lugar, pela sua abrangência em termos de conteúdo e atividades ilícitas que, pela natureza abstrata e global da rede de computadores, se torna um meio onde práticas criminosas, que desconhecem fronteiras e desafiam os juristas e estadistas, se configuram. Na *Deep Web*, como veremos adiante, ocorrem transgressões que envolvem a própria soberania nacional e a segurança transnacional.

## 2.2 A Sociedade em Rede

Segundo Manuel Castells, o século XX brindou a vida humana com um salto em termos tecnológicos que é responsável pelas mudanças que vêm acontecendo no plano da sociedade e do indivíduo. Este período é conhecido como a “Era da Informação” ou da “Sociedade em Rede”. Castells e Cardoso definem “sociedade em rede” como sendo “a estrutura social que resulta da interação entre o novo paradigma tecnológico e a organização social como um todo.” (Castells e Cardoso, 2005, p.3) O início dessa “Era da Informação” se daria a partir da década de 1970 e é responsável por gerar efeitos tanto na esfera coletiva quanto na esfera individual. É comum muitas pessoas atribuírem à essa sociedade como principal característica o conhecimento, porém os autores enfatizam que o conhecimento sempre teve um papel central em todas as sociedades da história que são conhecidas. Sendo assim, o que é atribuído como algo inédito seria “a base microeletrônica da tecnologia em rede que provê novas capacidades para uma antiga forma de organização social: em rede” (Castells e Cardoso, 2005, p.4), e não o conhecimento em si. No entanto, existe uma grande diferença na forma que

utilizávamos as redes de ligação no passado, e como utilizamos as redes de ligação atualmente: o caráter digital de alcance global. A digitalização se configura, portanto, como o principal fator dessa era. Em outras palavras, a comunicação digital por ser capaz de sobrepor barreiras geográficas e fronteiriças, uma vez que a rede de comunicação tem um alcance global, possibilita que a sociedade em rede seja também global. (Castells e Cardoso, 2005, p.4) Cabe ressaltar ainda que esta sociedade em rede é difusa e apresenta um elemento de exclusão por não incluir a totalidade da humanidade.

A questão, contudo, não é sobre como alcançar tal estágio superior de desenvolvimento humano, mas sobretudo reconhecer que existe um terreno novo que não é abraçado pelo Direito, e se submete às margens do conhecimento e do alcance da lei - o que proporciona um aumento de atividades ilícitas que se propagam com velocidade e facilidade no campo digital e abstrato da *Deep Web*. Pelo seu alcance global, e seu uso digital, tais atividades criminosas configuram um desafio à segurança internacional e uma ameaça à própria soberania, vistos sob um novo prisma: o prisma tecnológico. A sociedade em rede, ainda segundo Castells e Cardoso (2005), hoje configura o núcleo da nossa sociedade. Sendo assim, se torna imperioso que novos estudos sejam realizados nesse campo, que se discuta mais sobre o assunto, para compreendermos o funcionamento da rede, e como as relações de poder se configuram no campo digital. Tais questionamentos são pontos centrais desse novo desafio.

Como pressupõe Castells e Cardoso:

Aceitar a democracia da comunicação é aceitar diretamente a democracia, algo que nenhum Estado aceitou no mundo. Aceitar o debate pra redefinir os direitos de propriedade acerta o coração da legitimidade do capitalismo. Aceitar que os usuários são os produtores da tecnologia desafia o poder do especialista. (Castells e Cardoso, 2005, p.20)

### 2.3 Breve História da Internet

A internet originou-se durante a Guerra Fria, no ano de 1969 nos Estados Unidos. Inicialmente tinha o nome de ARPAnet<sup>6</sup> e seu intuito era o de interligar laboratórios de pesquisas, constituindo-se em uma rede pertencente ao Departamento de Defesa Norte-Americano. Posteriormente, essa tecnologia teve uma maior abrangência e passou a

---

<sup>6</sup> *Advanced Research Project Agency*, ou “Agência de Investigação de Projetos Avançados dos Estados Unidos.”

integrar também as Universidades e Laboratórios, mantendo-se assim por cerca de duas décadas. (Oliveira, Totti e Souza, 2013, p.3)

O objetivo principal da rede de computadores era promover a troca de informações rápidas de uma forma segura, além de servir como uma possível alternativa aos meios de comunicação existentes se, por ventura, viesse a ocorrer uma guerra nuclear. Como meio de comunicação, seu grande diferencial é a linguagem específica a qual utiliza para funcionar: os chamados TCP/IP<sup>7</sup> (*Transfer Control Protocol/Internet Protocol*), que compõem um padrão utilizado por todo o sistema.

Segundo Nascimento, portanto:

[...] a Internet pode ser definida como uma rede mundial de computadores composta por redes menores, ou seja, como uma rede de redes. Uma rede de computadores é formada por, no mínimo, dois computadores individuais conectados fisicamente para compartilhar informações. Assim, quando o usuário se conecta ao seu provedor de internet, forma com ele uma rede. O provedor, por sua vez, se conecta a outro provedor maior, nacional ou internacional, formando com ele outra rede. Os grandes provedores fornecem a estrutura física da internet, de cabos e roteadores, chamada de *internet backbone*. Todos os provedores que estão no topo dessa hierarquia de redes se conectam, então, a Pontos de Troca de Tráfegos, ou PTTs, que são computadores ou redes centrais que viabilizam a troca de dados entre as redes diretamente conectadas ao PTT e, conseqüentemente, entre todos os computadores conectados a qualquer das redes interconectadas. [...] O compartilhamento de dados apenas terá sucesso se os computadores interconectados falarem a mesma linguagem de informática. (NASCIMENTO, 2009, p.25)

Cabe ressaltar que o que comumente chamamos de “Internet”, ou a *Surface Web*, ao qual o usuário médio acessa diariamente mediante um dispositivo conectado à rede, na verdade é um dos meios pelos quais é possível realizar a troca de informações, não constituindo, portanto, a totalidade da rede mundial de computadores. Esse meio específico da Internet, utiliza um protocolo também específico, chamado de “protocolo HTTP”<sup>8</sup>. (Pisarewicz, 2013, p.44) Em outras palavras, um dos protocolos utilizados pela internet de superfície, a qual possui facilidade de acesso e abrangência mundial, se configura como apenas uma das linguagens utilizadas pela rede para transferir dados.

Como consequência da sua natureza de fácil acesso, grande abrangência e alta velocidade da transmissão de dados, a Internet acaba por se constituir como uma fonte de criação e de recebimento da informação altamente democrática, inexistindo qualquer

---

<sup>7</sup> TCP, ou *Transfer Control Protocol*, têm a função de verificar se os dados são transmitidos de forma correta, na sequência apropriada e sem erros na rede. IP têm como objetivo marcar cada dispositivo conectado à rede com um endereço único. (Oliveira, Totti e Souza, 2013, p.3)

<sup>8</sup> Do Inglês *Hypertext Transfer Protocol*.

órgão ou instituição que controle a rede ou que a administre. Nas palavras de Nascimento (2009), “a rede mundial é, por sua própria construção, descentralizada, pois é uma união de diversos computadores e redes de computadores independentes que decidem se conectar e utilizar uma linguagem padronizada para a transferência de dados”.

Um dos elementos que reforça o parâmetro democrático da Internet é o fato de não haver um centro único de armazenamento de arquivos, sendo impossível a destruição de todos os dados contidos na esfera virtual. Além disso, a transmissão dos dados se mantém ativa mesmo que não haja um envolvimento humano direto: não existe um ponto central de controle da informação.

Sobretudo, podemos afirmar que a Internet constitui um âmbito de ampla divulgação de pensamentos e informações. Um campo vasto, abrangente, com ausência de um órgão ou instituição controladora e de fácil acesso pelo usuário. É de se esperar que nesse âmbito aconteça a frutificação de ideologias, filosofias, discussões e construção de pensamentos coletivos com percepções congruentes.

#### 2.4 A Indexação das Páginas

A natureza da Internet de Superfície e a Internet Profunda são distintas. Propomos uma explicação breve do funcionamento desses dois tipos de internet para elucidar as diferenças marcantes da Internet Profunda que constituem verdadeiros desafios ao Estado e ao Direito.

Na *World Wide Web* (WWW), ou simplesmente *web*, a transmissão e o armazenamento de dados ocorrem por meio de servidores e são exibidos em hipertextos. (Pompéo e Seefeldt, 2013, p.439). Hipertextos são os conhecidos *links*, que conectam uma determinada página à outra por meio do clique do *mouse*. Nesse ambiente é que existem os provedores de busca como o Google, o Yahoo e o Bing, por exemplo. A função do Google é direcionar o usuário à página que se pretende buscar a partir de palavras-chave. Estas páginas são mostradas ao usuário, através do *web browser*<sup>9</sup>.

É a maneira de indexação das páginas em mecanismos de busca que define se a mesma será ou não encontrada por esses serviços. Noutras palavras, cada página da rede possui padrões que a registram em servidores como ‘Google’ e ‘Yahoo!’. Caso não sigam os

---

<sup>9</sup> Também conhecido como navegador web. Os mais conhecidos são o Google Chrome, Mozilla Firefox e o Internet Explorer.

padrões definidos, as mesmas ficam à margem da listagem de seus resultados de pesquisa, mesmo que tenham o conteúdo que é pesquisado pelo usuário. (POMPÉO; SEEFELDT, 2013)

Estar indexado, portanto, significa que a página atende aos padrões definidos e, portanto, será mostrada na listagem de resultados.

A ordem que essas páginas se colocam no resultado da busca obedece a relevância do conteúdo da página e também ao número de referências à determinada página. Por exemplo, quanto mais alto o número de referências à uma página (através dos hipertextos, ou *links*), mais alto ela estará no índice de resultados da busca e, portanto, mais facilmente de ser visualizada, uma vez que se encontra no topo. O resultado disso é que a página cresce em popularidade, pois é muitas vezes visualizada e a informação alcança a visualização de um grande número de usuários.

A diferenciação básica entre *Surface Web* e *Deep Web* se dá pela forma como essas páginas são encontradas pelos mecanismos de busca. Discorrem Pompéo e Seefeldt (2013) sobre isso, dizendo que enquanto a primeira resume a coletânea de páginas facilmente encontradas por mecanismos de busca, a segunda resume páginas que, por algum motivo, ficam alheias a esses provedores, não podendo serem listadas como resultados. Ou seja, se tornam “invisíveis” ao usuário médio da *web*.

O termo *Deep Web* foi primeiramente cunhado por um pesquisador chamado Michael Bergman que escreveu o primeiro artigo sobre o assunto. Segundo Bergman (2001), a *Deep Web* nasceu em meados de 1996 como fruto do desenvolvimento de um esforço do Laboratório de Pesquisas da Marinha dos Estados Unidos. O objetivo principal era a primazia pelo anonimato absoluto e a impossibilidade de se rastrear os acessos do usuário. Esse lado “oculto” da *web* requer um navegador preciso para ser acessado.

Pesquisas em relação à *Deep Web*, como a realizada por Ciancaglini (2013), evidenciam os três principais redes de “acesso” à *Deep Web*, utilizados por usuários e que possuem como característica o anonimato utilizado tanto pelo consumidor do conteúdo quanto por aquele que provê o conteúdo. São elas: TOR, I2P e Freenet. As informações colhidas foram retiradas da pesquisa realizada por Ciancaglini (2013) para a TREND MICRO, empresa de *software* de segurança de conteúdo para a Internet cujo conteúdo é relacionado à *Deep Web* e o *Cybercrime*.

## 2.5 *The Onion Router* (TOR)

A rede *The Onion Router* (TOR) nasceu em 2002 e foi desenvolvida pela Marinha norte-americana. Como dito anteriormente, a rede TOR “permite comunicações anônimas através de ‘nódulos voluntários’ que são responsáveis por traçar uma rota de pedidos criptografados<sup>10</sup> para que o trânsito de dados possa passar despercebido pelas ferramentas de monitoramentos.” (CIANCAGLINI, 2013).

Para se ter acesso à região da *Deep Web*, o usuário deve realizar o *download* do *software* TOR. Uma vez que o usuário tenha instalado o programa no seu dispositivo de conexão à rede, o acesso se realiza através dessa rota de nódulos cujo monitoramento é impossibilitado. Assim, cada nódulo se torna incapaz de decifrar o conteúdo, pois só reconhece o nódulo imediatamente pós ou prévio, e não os nódulos iniciais e finais. Em outras palavras, o rastreamento da origem e do destino do circuito se torna muito difícil devido à complexidade da estrutura. O servidor que também receber um pedido da rede TOR visualizará o pedido como sendo ele proveniente do último nódulo anterior à este servidor, sendo incapacitado de descobrir a rota dentro do circuito que leva ao primeiro nódulo do pedido. (Ciancaglini, 2013).

A grande dificuldade do monitoramento, portanto, decorre do fato de que cada nódulo dentro do circuito apenas reconhece o nódulo anterior e o nódulo posterior.

## 2.6 Freenet

A rede *Freenet* existe desde os anos 2000 e opera também com o conceito de nódulos em um circuito. A diferença é que cada nódulo no circuito é responsável por um subconjunto de recursos disponíveis na rede que os alimenta colaborativamente quando um pedido é requisitado. (Ciancaglini, 2013, p.7). Sendo assim, cada nódulo mantém uma espécie de lista de nódulos vizinhos. Esse processo é reconhecido por Ciancaglini (2013) como o “princípio do mundo pequeno”.

Por trabalhar com o conhecimento dos nódulos vizinhos, a *Freenet* é mais utilizada para servir conteúdos estáticos<sup>11</sup>, e não dinâmicos<sup>12</sup> como é o caso do TOR. Também não trabalha com outros tipos de serviços da internet, como *e-mails*. Por esse

---

<sup>10</sup> Pedidos criptografados são pedidos cuja informação é difícil de ser lida por quem não detém a chave de criptografia.

<sup>11</sup> Por exemplo, páginas da rede que são estáticas possuem um endereço fixo na Internet.

<sup>12</sup> Por exemplo, páginas da rede cujo endereço é automaticamente gerado a partir de cada acesso à página.

motivo, pode-se dizer que a Freenet oferece menos flexibilidade, uma vez que está atrelada à conteúdos estáticos. (Ciancaglini, 2013, p.7)

## 2.7 I2P

A rede I2P foi desenvolvida em 2003 como um resultado possível da evolução da *Freenet*. Seu objetivo é prover “invisibilidade” para os usuários que desejam hospedar algum serviço, como um *e-mail*, *torrent*, etc. (Ciancaglini, 2013, p.6)

A forma como o I2P opera é por meio da criação de túneis. Cada nóculo em I2P funciona como sendo um roteador<sup>13</sup>. Dessa forma, se dois computadores estão em duas redes diferentes e têm a intenção de trocar dados entre si, elas necessitarão de um roteador que faça o encaminhamento dos pacotes de dados entre as duas redes.

O I2P possui o diferencial de ter sua comunicação criptografada<sup>14</sup> em múltiplas camadas (Ciancaglini, 2013, p.6): criptografia entre remetente e destinatário da informação; criptografia entre os roteadores na rede; e criptografia nos túneis de comunicação. Dessa forma, procura-se proteger em mais de uma camada o anonimato do usuário e do provedor do serviço.

## 2.8 A *Deep Web*

Como dito anteriormente, Michael K. Bergman cunhou o termo “Deep Web” em 2001 quando escreveu um artigo que foi publicado pela empresa *Bright Planet* que oferece serviços de inteligência nessa esfera da Internet. Seu tutorial é reconhecido por ter sido pioneiro na área e recebeu alguns prêmios. (Bergman, 2013).

Na sua pesquisa, Bergman (2001) faz um estudo sobre a *Deep Web* e provê uma estimativa quanto ao seu tamanho. A *Deep Web* abrangeria páginas da Internet que por algum motivo não são indexadas pelos mecanismos de buscas, pois não obedecem seus requerimentos. Um dos requerimentos, por exemplo é ter página estática. Comumente, as páginas da *Deep Web* possuem um caráter dinâmico e, sendo assim, para serem encontradas necessitam aparecer como resultado de uma busca específica.

Bergman (2001) sugere uma metáfora para o melhor entendimento em relação à

---

<sup>13</sup> Dispositivo que encaminha pacote de dados entre redes de computadores. (CAMPOS, 2014).

<sup>14</sup> Por criptografia entende-se a técnica em que uma determinada informação é codificada de forma que o entendimento do formato original só é possível quando o destinatário da mensagem possui a chave da criptografia, que decifra o código pela qual a mensagem está submetida. (PISA, 2012).

*Deep Web*. A busca na Internet pode ser comparada à ação de jogar uma rede pesqueira no mar e arrastá-la afim de que se encontre peixes, ou resultados. No entanto, apesar de uma boa parte desses peixes serem pegos por essa rede, é fato que nas profundezas do mar, por ter um alcance limitado, essa rede de pesca fica impossibilitada de obter os peixes que nadam ao fundo do oceano. A maior parte dos peixes, portanto, é deixada “de lado” porque não se consegue pegá-los.

Essa metáfora se aplica à *Deep Web* porque a maior parte das informações contidas na *web* está localizada bem abaixo da superfície, colocadas em *sites* cujo endereço é gerado de forma automática - ou seja, não são estáticos porque os endereços de forma a se acessar determinada página se alteram constantemente. Mecanismos de busca padrão, como o *Google*, por exemplo, são impossibilitados de encontrar esses *sites*. Bergman (2001) acredita ainda que a *Deep Web* possui cerca de 10 camadas, ou níveis, e a entrada do usuário em cada nível é feita de forma gradual.

Segundo a pesquisa realizada por Bergman (2001), apesar de não ser conhecida do público em geral, a *Deep Web* é altamente popular. Ou seja, detém muita atividade. No ano de 2001, a *Deep Web* era cerca de 500 vezes maior que a *Surface Web*, possuindo uma qualidade de “um mil a duas mil vezes” acima da mesma. Por “qualidade” o autor define como sendo o valor atribuído quando o resultado corresponde com precisão a expectativa, ou intenção, de uma busca desejada. (Bergman, 2001). Dito de outra forma, atribui-se qualidade ao resultado de uma busca quando o usuário obtém o resultado que esperava - se o usuário encontra o que se pretendeu buscar.

O pesquisador também elenca alguns dados resultantes de sua pesquisa:

A *Deep Web* contém aproximadamente 550 bilhões de documentos individuais comparados com 1 bilhão da *Surface 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. Ela também tende a ser mais restrita, com conteúdo mais profundo, do que sites convencionais. 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 taxas ou assinaturas. (BERGMAN, 2001, p.1)

Em relação à arquitetura da rede, Pompéo e Seefeldt (2013) afirmam que a

configuração das páginas da *Deep Web* pode se dar por inúmeros tipos de conteúdos, ou seja, podem ser de diferentes formas: por conteúdo dinâmico<sup>15</sup>, conteúdo isolado<sup>16</sup>, conteúdo de acesso limitado<sup>17</sup>, conteúdo de *script*<sup>18</sup>, conteúdo-não HTML/texto<sup>19</sup>, conteúdo antigo<sup>20</sup>, web contextual<sup>21</sup> e web privada<sup>22</sup>.

### 2.8.1 A Deep Web através do uso do *software* TOR

Os três sistemas de acesso citados acima, TOR, *Freenet* e I2P, compõem algumas das maneiras em que o usuário pode obter acesso às páginas que não são indexadas por mecanismos de busca existentes na *Surface Web*. No entanto, a rede TOR é aquela que mais atraiu usuários e, conseqüentemente, que mais oportunidade ofereceu para a criação de mercados “alternativos” de bens e serviços na esfera digital. A razão para esse fato, segundo Ciancaglini (2013), é que o TOR é um sistema mais antigo que os demais e, portanto, vem ganhando há mais tempo destaque nos meios de comunicação. Por também oferecer um relevante grau de anonimato, o TOR se tornou uma ferramenta anti-censura utilizada por muitos jornalistas e profissionais da informação.

Sendo assim, o presente estudo tem se limitado aos casos e estudos no âmbito de utilização do *software* TOR, por terem maior abrangência e cobertura midiática, além de possuírem maior número de artigos e pesquisas quando se referem às informações sigilosas que navegam pela *Deep Web*. É notória a quantidade de artigos que se limitam a investigar situações e problemas que ocorrem na *Deep Web* sob o uso do sistema TOR como principal ferramenta de “entrada” ao “submundo” da rede - apesar de existirem outras formas de acesso. As páginas que são “lidas” pelo TOR têm em sua URL<sup>23</sup> o

<sup>15</sup> “Páginas que necessitam de uma requisição do usuário ou do preenchimento de um formulário, os quais são analisados e, se suficientes, recebem a página para ser visualizada”. (POMPÉO; SEEFELDT, 2013).

<sup>16</sup> “Páginas que exigem do usuário o prévio conhecimento do endereço, uma vez que não possuem advindas de outros sites.” (POMPÉO; SEEFELDT, 2013).

<sup>17</sup> “Páginas que permitem o acesso de modo técnico, por meio de quebra-cabeças que garantam a identidade do usuário.” (POMPÉO; SEEFELDT, 2013).

<sup>18</sup> “Páginas que somente são acessíveis com mecanismos específicos, uma vez que são encriptadas.”

<sup>19</sup> “Páginas que foram codificadas em imagens, sons, palavras ou arquivos desconhecidos.” (POMPÉO; SEEFELDT, 2013).

<sup>20</sup> “Páginas anteriores à WWW, as quais os buscadores atuais não conseguem encontrar.” (POMPÉO; SEEFELDT, 2013).

<sup>21</sup> “Páginas que só são exibidas quando conferidos e aceitos o IP do usuário ou sequência de navegação prévia.” (POMPÉO; SEEFELDT, 2013).

<sup>22</sup> “Páginas que precisam de registro e senha previamente estabelecido.” (POMPÉO; SEEFELDT, 2013).

<sup>23</sup> *Uniform Resource Locator*, ou convenção padronizada de nomes para endereçar documentos acessíveis pela Internet ou por Intranets. (COMPUTER HOPE, 2014.)

sufixo “.onion”. Tais nomenclaturas de endereço específico se alteram constantemente para preservar o anonimato, portanto, se desejar voltar à essa mesma página no futuro, seu endereço ou nomenclatura terá igualmente mudado de forma.

A *Deep Web* oferece espaço para a prática de atividades legais, ilegais e atividades que ainda não detém um reconhecimento jurídico específico quanto a seu caso, a exemplo do *Wikileaks*. Segundo Oliveira (2012), um dos grandes legados do *Wikileaks* é a inovação representada no uso da informação enquanto arma política capaz de promover transformações, pois a mesma evidenciou o grau de despreparo da legislação de muitos países com relação ao advento da informatização do conhecimento na política internacional. Sendo assim, é a partir do caso da *Wikileaks* que testemunhamos o primeiro líder de Estado, Barack Obama, a alertar sobre as questões de cibersegurança, no ano de 2009 durante um discurso dirigido ao povo estadunidense. Não apenas isso, mas também reconheceu a dependência das redes de internet que os Estados Unidos enfrentam - além de também admitir o grau de vulnerabilidade dos sistemas utilizados. Contudo, o presidente dos Estados Unidos, para oferecer um contraponto, tornou a segurança cibernética um ponto essencial da estratégia de defesa norte-americana e criou um departamento na Casa Branca para tais fins. (Oliveira, 2012, p.40)

### 2.8.2 O potencial de informação da *Deep Web*

Apesar de a *Deep Web* estar muitas vezes ligada às ideias de atividades ilícitas que escapam às “garras” dos mecanismos de busca da *Surface Web*, não é verdade que toda a *Deep Web* se abasteça de atos criminosos. Como afirmam Martins e Silva (2013) fica a critério do usuário a seleção de assuntos ao qual se propõe buscar nessa esfera da rede. Se o usuário está interessado em encontrar arquivos legais que possuem difícil acesso na *Surface Web* - seja porque tais arquivos estão mais ao final da indexação dos mecanismos de busca, seja porque tais arquivos são pouco disseminados na rede - ele terá uma maior chance de encontrar os mesmos arquivos na *Deep Web* de uma forma mais rápida. Essa rapidez se traduz em qualidade, pois, conforme dito anteriormente, terá encontrado o que se propôs a buscar. Cabe ressaltar, no entanto, que por não haver a necessidade de se respeitar uma legislação em vigor no que diz respeito à esfera cibernética, muitos arquivos de livros com conteúdo integral também estão disponíveis nessa parte da web.

Martins e Silva (2013) nos explanam acerca das possibilidades de pesquisa de conteúdo legal disponíveis na *Deep Web*. Os autores também exemplificam algumas formas de se buscar conteúdo:

O *Infomine* é um mecanismo de busca específico para conteúdo de bibliotecas universitárias norte-americanas, entre elas a Universidade da Califórnia; o *Intute* permite acesso ao conteúdo de todas as universidades da Inglaterra; o *Complete Planet* dá acesso a assuntos diversos, como militares, comidas ou meteorologia para agricultores; o *IncyWincy* possui busca por imagens; o *DeepWebTech*, permite acesso a temas como medicina, negócios e ciências; o *Scirus* é direcionado para assuntos científicos, como jornais, homepages de cientistas, materiais didáticos e patentes; o *TechXtra* é direcionado para a área de exatas, como matemática, engenharia e computação. [...] Há aqueles que usam a Web Invisível para armazenar informações que precisam gerar tráfego, como por exemplo, resultados parciais de pesquisas, e o simples armazenamento de bases de dados organizacionais que não estão sendo utilizadas no momento. (MARTINS; SILVA, 2013)

Além de poder fazer buscas relacionadas à uma determinada matéria, a *Deep Web* oferece também um importante meio jornalístico de reunião e produção de informações que conta com o completo anonimato para dar voz à liberdade de expressão e imprensa, uma vez que a *Surface Web* é reconhecidamente um espaço que está sob constante monitoramento de instituições governamentais.

Teles et al (2014) discorrem sobre o poder da mídia:

[...] A mídia pode ser ferramenta de manipulação e afirmação das instituições estatais e daquelas mantenedoras do *status quo*. Nesse caso, ela falha em sua função social de promoção da democracia e formação da consciência pública, comprometendo, assim, a aplicabilidade do direito à liberdade de pensamento e livre escolha da sociedade por informações incompletas ou distorcidas. (TELES ET AL, 2014)

Sendo assim, a dificuldade de monitoramento no “submundo da internet” e o uso de criptografia capaz de blindar o anonimato do usuário oferecem importantes ferramentas para as práticas jornalísticas e da liberdade de imprensa, sendo o caso da *Wikileaks* notório.

## 2.9 *Wikileaks* e *Anonymous*: Organizações Políticas que Navegam nas Profundezas do Oceano das Informações

O mundo da difusão do poder une os novos agentes e os novos meios de comunicação e difusão da informação, de tal forma que a autoridade do Estado vê-se limitada e ameaçada. Estes são os exemplos eloquentes do *Wikileaks* e do *Anonymous*.

Segundo Pacheco (2011), o *Wikileaks* constitui-se em uma organização não-governamental sem fins lucrativos fundada em 2006 por Julian Assange, considerado também editor e porta-voz, que tem como objetivo principal trazer informações consideradas importantes e relevantes para o público em geral. A organização, portanto, se propõe a publicar informações cuja natureza seja de teor ético, político e histórico, e ao fazê-lo demonstra uma clara forma de combate à censura, uma vez que acredita na liberdade de imprensa como um dos pilares da democracia. O *Wikileaks* conta, ainda, com 5 funcionários de jornada integral e mais 800 voluntários que estão presentes nos cinco continentes do mundo, totalizando cerca de aproximadamente 180 países (Pacheco, 2011).

Porém como a organização consegue reunir tais informações sigilosas? Ainda segundo Pacheco (2011), são três formas de se reunir as informações: através do envio postal; pessoalmente; e por meio de pastas *onlines* que são protegidas por mecanismos criptográficos. No momento que a equipe do *Wikileaks* tem conhecimento de tais informações, logo se inicia um processo de verificação do material quanto à veracidade. Para tanto, a organização conta com uma equipe jornalística no seu corpo de membros que ficam responsáveis por redigir um resumo das informações reunidas. Assim que tal documento é redigido, ele é publicado juntamente com a informação em sua integridade para evitar qualquer tipo de censura.

É interessante notar que o *Wikileaks* vale-se do apoio de um grupo de juristas que estão presentes em diversas localidades do globo e têm como objetivo garantir que as ações realizadas pela organização estejam dentro da legalidade, obedecendo aos padrões legais a fim de que se possa resguardá-la de possíveis problemas com a justiça. (Pacheco, 2012).

A divulgação dessas informações acaba se tornando possível graças à ausência de restrições jurídicas quanto ao uso do ciberespaço pela maioria dos países. As exceções à regra seriam países como a China e o Irã – reconhecidos por manterem legislações específicas sobre esta matéria. (Pacheco, 2012).

Em outras palavras, a blindagem ao anonimato das fontes, por meio da criptografia, permite que a coleta de dados se dê em um âmbito mais abrangente e cujos usuários podem ter fácil acesso para reunir e enviar as informações sigilosas.

Mas como é realizada essa coleta de dados? Através do *crowdsourcing* (Teles et al, 2014). Como afirmam os autores:

Este seria um modelo na qual “o potencial interessado anuncia seu problema e determina um preço (ou não), atraindo um grupo de candidatos à resolução do mesmo (*crowd*). Neste grupo, ele analisa as propostas e escolhe a que melhor lhe convém. Além do *Wikileaks*, outras instituições como a *Mozilla Foundation*, *Wikipedia*, *Stockphoto* e *Threadless.com* utilizam-se do modelo virtual de *crowdsourcing* que já cooperou para o desenvolvimento de produtos famosos como o sistema operacional “Linux”, e o navegador para a Internet “Mozilla Firefox”. (TELES ET AL, 2014).

A seguir, listamos alguns dos casos pelos quais o *Wikileaks* se tornou famoso diante do conhecimento público, devido às notícias terem circulados nos meios tradicionais de comunicação.

Primeiramente, houve o caso da divulgação de um vídeo retratando um helicóptero do exército estadunidense durante a guerra do Iraque em que o mesmo disparava tiros contra à população civil de iraquianos em 2007. (Pacheco, 2012, p.50) O vídeo atraiu a atenção da opinião pública e colocou a organização sob os holofotes, pois a situação em questão se tratava de uma grave quebra do comportamento legal.

Em outra oportunidade, desta vez no ano de 2010, cerca de 391 mil documentos secretos referentes à guerra do Iraque e 77 mil referentes à atuação norte-americana no Afeganistão vieram à tona. (Pacheco, 2012, p.50)

Porém talvez o caso que mais tenha obtido atenção da mídia tradicional ao redor do mundo foi a divulgação, no dia 29 de Novembro de 2010, de 251.287 telegramas diplomáticos dos EUA que seriam trocados entre as embaixadas norte-americanas assentadas em mais de 180 países. (Pacheco, 2012, p.50)

Para a publicação do conteúdo desses telegramas, o fundador do *Wikileaks*, Julian Assange, realizou um trato com as cinco maiores publicações midiáticas do planeta: *The Guardian*, inglês; *El País*, espanhol; *The New York Times*, estadunidense; *Le Monde*, francês; e finalmente, *Der Spiegel*, alemão. (Pacheco, 2012, p.52) O trato consistia na publicação do conteúdo dos telegramas pelas publicações em uma data combinada. Discorre Pacheco (2012) sobre os jornais de maior circulação no mundo que “numa operação concertada, libertaram informações retiradas de telegramas confidenciais da diplomacia americana cedidos pelo *Wikileaks*, para que fosse feita a análise da informação pelos seus jornalistas reconhecidos e, posteriormente, publicada”.

A escolha por essas cinco grandes publicações teria sido o resultado da ponderação quanto à credibilidade.

Outro notório grupo que alcançou cobertura midiática nos últimos anos e provém do submundo da internet é o grupo *Anonymous*. Gabriella Coleman, portadora da *Wolfe Chair in Scientific and Technological Literacy* da Universidade McGill, é professora, pesquisadora e autora de livros e artigos sobre a cultura *hacker*<sup>24</sup>. Ela discorre sobre o fato de que enquanto o *Wikileaks* reflete sobre as mudanças em relação às faces do jornalismo na era da comunicação em rede, e tem na figura de Julian Assange como o líder, uma figura única, o grupo *Anonymous* discute se ataques provenientes da negação de serviços online é legítima como uma tática de protesto, além de ter uma premissa de anti-liderança<sup>25</sup>.

O *Anonymous* mantém suas operações abertas ao usuário interessado em contribuir para expressar a importância política do anonimato. Em suma, o *Anonymous* se configura em uma bandeira utilizada largamente por indivíduos e grupos que organizam formas coletivas de ação.

O início do grupo tem raízes em 2008, porém ao longo dos anos sofreu uma metamorfose em relação aos seus objetivos. Quando nascido, o *Anonymous* era conhecido na rede por ser um grupo que praticava o *trolling*<sup>26</sup>. A partir de 2010, no entanto, sua diretriz havia se alterado: o grupo adquiriu características de um ativismo estável e distinto por meio da mobilização de pessoas, da comunicação em rede de forma anônima, e nesse caso suas atividades frutificaram-se pela *Deep Web*, e pela sua abrangência global. (Coleman, 2013). O grupo *Anonymous*, por exemplo, contribuiu em grande medida para as conhecidas revoluções árabes e africanas deflagradas na primavera de 2011 - além de serem notáveis suas denúncias por meio da publicação de casos de estupro em cidades do Estado de Ohio, nos Estados Unidos, e Halifax, capital da província canadense da Nova Escócia.

---

<sup>24</sup> “Pela definição de Eric Raymond, um *hacker* é aquele que é reconhecido na cultura hacker enquanto tal. Pekka Hinamen sugere que há um mal-entendido na forma como a opinião pública entende o hacker: este seria apenas um programador informático e um conhecedor dos sistemas de redes, enquanto aqueles que se dedicam a furar redes de segurança são conhecidos como *crackers* e, normalmente, são banidos da própria comunidade. Um traço da cultura hacker é a crença na reinvenção da sociedade através do progresso tecnológico aberto e grátis.” (PACHECO, 2012).

<sup>25</sup> Não há uma única figura individual que seja atribuída ao grupo *Anonymous*.

<sup>26</sup> “Trolling”, na linguagem da Internet, significa “fazer traquinagem com uma pessoa, pessoas ou organizações, profanando a reputação e revelando informações humilhantes ou pessoais”. (COLEMAN, 2013, p.3)

Outra característica do grupo *Anonymous* é quanto à imprevisibilidade de suas ações que são orquestradas de forma a receber extensa atenção midiática. Tal imprevisibilidade decorre principalmente da mutação que o grupo frequentemente sofre, pois não há apenas uma categoria quanto ao discurso de suas investigações políticas. O resultado disso é que, como mencionado anteriormente, o grupo *Anonymous* alcança grande visibilidade perante a população no geral, além de ser marcado por uma estética própria que o diferencia dos demais grupos. (Coleman, 2013). Nesse sentido, segundo Coleman, são da mesma “família” que o *Wikileaks*, pois são dois grupos frutos da investigação e da intervenção política orquestrada por *hackers*.

Finalmente, Coleman (2013) explica que a preocupação e o interesse do grupo *Anonymous* em relação ao anonimato e a privacidade são de grande importância uma vez que, na concepção do próprio grupo, as sociedades passam por uma era em que tanto o anonimato e a privacidade estão se erodindo face à vida do cidadão; em contraposição, observamos um crescente aumento desses direitos concedidos aos governos, sobretudo evidente no aumento da vigilância sistemática e dos segredos de Estado resguardados pelos Estados Unidos.

## 2.10 O Lado Obscuro da *Deep Web*

Em se tratando de uma rede de computadores cujo anonimato é preservado segundo a configuração de funcionamento da própria rede, além de oferecer facilidade de acesso, é razoável que a criminalidade veja essa parte da *web* como uma ferramenta para inserir e expandir as suas atividades ilícitas.

Dentro desse contexto, a rede TOR em particular atraiu, e reuniu, usuários que buscam acesso ao conteúdo ilegal. A pesquisa realizada por Ciancaglini (2013) distingue duas formas principais em que tais práticas se dão no ambiente da *Deep Web* mediante o uso do programa TOR.

A primeira forma se dá por meio de ambientes denominados *marketplaces* ou “praças de mercado”, ou ainda “feiras digitais”. As *marketplaces* digitais comercializam todo o tipo de bens e serviços, seja ele de conteúdo legal ou ilegal.

A segunda forma se dá através de duas subcategorias que constituem as páginas privadas dessa esfera da rede – as *message boards*, local no qual todo tipo de “classificados”, sobre qualquer bem ou serviço, é postado; além das *message boards*,

existem ainda os *sites privados* que oferecem um tipo específico de produto. (Ciancaglini, 2013, p.14)

### 2.10.1 Comércio de Bens Ilícitos

Em se tratando das *marketplaces* mais conhecidas da *Deep Web*, se encontram a *Silk Road* e a *Atlantis* (Ciancaglini, 2013). Ambas as páginas não estão mais na ativa. Por uma questão de número de pesquisas e estudos realizados, iremos nos ater à *Silk Road* como um exemplo de *marketplace* que teve maior êxito no âmbito da Internet Profunda.

A *Silk Road* ganhou notoriedade, como dito anteriormente, por ter sido alvo da atenção midiática (Ciancaglini, 2013, p.10) Além disso, tornou-se objeto de pesquisa acadêmica, como os trabalhos realizados por autores como Christin (2013) sobre análise mensurável de um *marketplace* anônimo e *online*; Van Hout e Bingham (2013a) que realizaram um estudo das experiências dos usuários da *Silk Road* e, também, sobre o estudo que realizaram sobre a revolução no comércio de drogas realizada por vendedores e consumidores usuários da *Silk Road* (2013b).

Segundo Christin (2013), a *Silk Road* constituiu-se como um site de *e-commerce*<sup>27</sup>, nas quais os produtos eram divididos em categorias e seções definidas. Além disso, o *site* contava ainda com o uso de carrinhos de compra virtuais; administração de saída<sup>28</sup>; continha também um serviço de pagamento que se utilizava de moedas digitais criptografadas, como o *bitcoin* e o *litecoin* (Ciancaglini, 2013).

Nicolas Christin realizou em maio de 2013 uma extensa pesquisa no âmbito da *Silk Road* em que coletou dados durante 8 meses entre o final de 2011 e 2012. A partir de seus achados, o autor conseguiu descrever uma imagem detalhada do tipo de bens vendidos na *Silk Road*. Para isso, Christin analisou mais de 24 mil itens em separado e descobriu que o site é largamente utilizado como, principalmente, um mercado para substâncias controladas e narcóticos. No entanto, ainda oferece bens de conteúdo pornográfico, armamentos, bens digitais, e moedas virtuais – porém em menor escala.

Christin (2013) descobriu que a maioria dos itens para a compra ficam disponibilizados por cerca de 3 semanas e depois são retirados. A maioria dos

---

<sup>27</sup> E-commerce refere-se à realização de negócios entre vendedores e compradores utilizando-se da Internet.

<sup>28</sup> Operação de realizar *login* e *log out*.

vendedores, contudo, some, em média, depois de 3 meses contados a partir da sua chegada no *site* – evidenciando uma tática dinâmica da preservação da identidade. No período em que se dispôs a realizar a coleta de dados sobre o *Silk Road*, entretanto, o pesquisador contabilizou cerca de 112 vendedores que permaneceram durante todo o período de pesquisa de 8 meses.

O funcionamento das vendas e do recebimento do produto se dá pela seguinte forma: uma vez realizada a compra de um item, o produto deve ser enviado para o destinatário via correio. Com a finalidade de preservar o anonimato, o próprio *site* de *e-commerce* recomenda que se utilize um endereço físico diferente do endereço residencial do comprador, como uma caixa postal, por exemplo. Dessa forma, ativa-se mais uma camada de proteção que visa garantir o anonimato. Uma vez completada a transação – que acontece quando o usuário recebe o item no local físico de destino – é de obrigação do comprador avisar a *Silk Road* para que o mesmo possa liberar os fundos que estão sob seus cuidados<sup>29</sup> para o vendedor. Quando isso acontece, o endereço utilizado é apagado de todos os registros. (Christin, 2013).

A *Silk Road*, contudo, teve o encerramento de suas atividades em outubro de 2013 quando Ross William Ulbricht, suspeito de ser o dono e principal administrador da *Silk Road*, foi preso pelo FBI<sup>30</sup>. Ross Ulbricht enfrenta acusações de tráfico de narcóticos, *computer hacking*<sup>31</sup> e lavagem de dinheiro.

Ainda segundo a pesquisa realizada por Ciancagline (2013), de acordo com o FBI, em quase dois anos de existência, o montante gerado pelo comércio realizado na *Silk Road* totaliza cerca de 9 milhões e meios de *bitcoins*, além de colecionar cerca de 600 mil *bitcoins* provenientes da coleta de comissões em vendas. À época das acusações isso se traduziria em aproximadamente 12 bilhões de dólares em vendas e 80 milhões de dólares em comissões. (Ciancagline, 2013, p.11)

No que se refere aos sites privados e específicos, o conteúdo é colocado à disposição em páginas através de uma apresentação que contém preços, descrição dos serviços oferecidos e informações relativas ao contato para que se possa efetivar os pedidos. (Pompéo e Seefeldt, 2013) Em outras ocasiões, é confeccionado um sistema completo que abrange a administração de pagamentos para automatizar o pedido

---

<sup>29</sup> Operação também conhecida como “escrow”. (Christin, 2013, p.4)

<sup>30</sup> Federal Bureau of Investigation, principal braço investigativo do Departamento de Justiça dos Estados Unidos. <<http://www.fbi.gov/about-us/faqs>>

<sup>31</sup> Operação de tentar ilegalmente invadir o sistema de um computador para danificá-lo ou roubar informações. <<http://www.computerhope.com/jargon/h/hacker.htm>>

(Ciancagline, 2013, p.14). Nesse âmbito se frutificam, por exemplo, uma das práticas mais comuns nesse lado obscuro da rede: os assassinatos por encomenda (Pompéo e Seefeldt, 2013). Os que oferecem esse serviço em forma de anúncio exigem, no entanto, algumas condições prévias para que o pedido seja executado. Como afirmam os autores:

Os envolvidos geralmente moram no Leste Europeu e exigem diversas condições para executar o serviço a ser realizado, bem como o valor correspondentemente cobrado. Os parâmetros para a quantificação do serviço são dois: o mérito e o tipo de alvo. O primeiro significa o aumento do preço ao passar do tempo conforme o número de objetivos alcançados. O segundo considera a personalidade do alvo, ou seja, quanto maior a fama e o contato com o público ou a dificuldade de eliminar o alvo, maior o preço. Por exemplo, em se tratando de um militar, que, por essência, representa riscos ao assassino, o valor é mais caro. (POMPEO; SEEDFELDT, 2013, p.445)

Notadamente, outras atividades ilícitas que podem ser encontradas no âmbito da *Deep Web* também oferecem um alto grau de perigo à sociedade civil. Essas atividades, ao se utilizarem do anonimato, da privacidade, da criptografia e do uso de moedas digitais criptografadas, encontram um campo vasto a ser explorado na *Deep Web*. Tais atividades de alta periculosidade abrangem:

O contrabando de mercadorias e de materiais radioativos, órgãos humanos, lixos orgânicos e inorgânicos, prostituição adulta e infantil, organização de jogos de azar, sequestros, compra e venda de assassinatos, extorsão, falsificações das mais diversas espécies, inclusive a de moedas em curso ou cartões de crédito, de identidades civis ou seu tráfico de informações, de tecnologias, objetos de arte, estão entre as principais ações dessa rede criminosa que envolveu, de maneira global, o crime. (POMPÉO; SEEFELDT, 2013, p.444)

Em estudo realizado em março de 2014 pela International Centre for Missing & Exploited Children revela que “a pornografia infantil e a indústria da exploração sexual, em particular, estão saindo dos mecanismos econômicos tradicionais e se inserindo nas sombras do mundo digital”. A pesquisa cita ainda um quadro de anúncios *online* que, segundo a Secretária do Departamento de Segurança Interna, Janet Napolitano, e o Procurador-geral dos Estados Unidos, Eric Helder, é descrito como tendo sido criado e operado com o objetivo de “promover a pedofilia e encorajar o abuso sexual de menores”. (INTERNATIONAL CENTRE FOR MISSING & EXPLOITED CHILDREN, 2014, p.8)

Embora em grande número na *Deep Web*, estas não são o único tipo de práticas ilícitas encontradas no lado “escuro” da Internet. Outros usos incluem o financiamento

do terrorismo<sup>32</sup> e a lavagem de dinheiro. Esta última, em realidade, recebe uma especial atenção dos estudiosos uma vez que se revela como sendo a “raiz” pela qual os demais delitos são estabelecidos. (Pompéo e Seefeldt, 2013). Em outras palavras, as atividades ilícitas são sustentadas financeiramente a partir dessa prática, de difícil coibição.

Os autores ainda chamam a atenção para o tráfico internacional de entorpecentes, sobretudo porque é o primeiro crime a ser financiado pela lavagem de dinheiro. (Pompéo e Seefeldt, 2013, p.444) Ainda afirmam sobre os entorpecentes que:

Plantados, colhidos e produzidos sinteticamente em diferentes lugares do mundo, são internacionalmente comercializados, seguindo rotas que partem principalmente do Peru, Bolívia e da Colômbia, passando por toda a América Latina, Europa e Estados Unidos, fazendo, muitas vezes, o caminho inverso. (POMPÉO; SEEFELDT, 2013, p.444).

Mais sobre a lavagem de dinheiro e o financiamento das organizações criminosas transnacionais será discutido adiante.

### 2.10.2 O Terrorismo

É fato que muitos grupos terroristas encontram-se divididos em células que estão distribuídas nas mais distantes regiões do mundo. O uso da internet, e em especial a *Deep Web*, que possui como característica o anonimato, serve como uma forma de conectar essas células para que se seja possível a produção, o recebimento e o compartilhamento do conhecimento entre elas. Mais que isso, o fácil acesso à internet permite que se crie um espaço para reunião de mentes semelhantes e que se construa, por exemplo, fóruns de discussão sobre determinados assuntos, ou que sirva de instrumento para o recrutamento de apoiadores e simpatizantes. (Cohen-Almagor, 2012)

Nesse sentido, Cohen-Almagor (2012) fez um estudo em relação aos grupos terroristas radicais islâmicos do movimento *jihadista*<sup>33</sup> e encontrou algumas semelhanças com a própria internet: ambos são difusos e descentralizados, com a falta de uma estrutura coerente, porém detêm um alcance global e muitas vezes são

---

<sup>32</sup> Cohen-Almagor (2012) define terrorismo como sendo “a ameaça ou o emprego da violência contra alvos não-combatentes para propósitos políticos, religiosos ou ideológicos, realizados por grupos sub-nacionais e/ou indivíduos clandestinos que estão dispostos a justificar todos os meios para cumprir seus objetivos”.

<sup>33</sup> “A palavra árabe *jihad* não significa ‘guerra santa’ ou ‘guerra justa’. [...] *Jihad* tem o sentido específico de lutar pela causa de Deus – seja lá o que é entendido por esse significado.” (BONNER, 2006, p.2)

caracterizados como caóticos pela falta de uma hierarquia. Além disso, o autor ainda define termos como *e-jihad*<sup>34</sup> e *cyberterrorismo*<sup>35</sup>.

Propriamente dito, segundo Cohen-Almagor (2012) o *cyberterrorismo* é decorrente de motivação político-ideológica cujos ataques contra as infraestruturas da informação resultam em violência contra as agências governamentais e oficiais, tanto quanto resultam em violência contra alvos não-combatentes. Portanto:

É possível ainda que o *cyberterrorismo* tenha o potencial de enfraquecer a economia de um país ao atacar a infraestrutura crítica de grandes cidades como represas, reatores nucleares, abastecimentos de água e energia, uma vez que são coordenados *via* computadores. (COHEN-ALMAGOR, 2012)

Apesar de não se ter um número exato do número de organizações e grupos terroristas no mundo, Cohen-Almagor (2012) afirma que os Estados Unidos iniciaram um processo de identificação desses grupos que culminou na identificação de alguns dados em 2011. Esses dados identificam 48 organizações terroristas cujas atividades foram monitoradas pelo governo estadunidense.

Buscando mais a fundo sobre dados em relação ao uso da Internet por grupos terroristas foi possível encontrar um artigo da *Scientific American*<sup>36</sup>, cuja autoria é de Luis Miguel Ariza (2005) em que descreve a internet como uma das ferramentas de recrutamento e coordenação de planos de grupos terroristas<sup>37</sup>. O autor ainda destaca que em 1998 existiam na rede cerca de 12 *websites* terroristas, enquanto que em 2005, esse número já apontava para mais de 4.700 mil *websites*. Um evidente e estrondoso aumento de páginas cujo conteúdo destina-se ao recrutamento de jovens para a *jihad* e fomento da educação básica para aqueles que simpatizam com a causa terrorista. Mas não apenas isso: muitos *websites* oferecem seções religiosas e seções de contribuição. (Cohen-Almagor, 2012, p.41). Na seção de contribuição é possível discutir-se novas formas de levar o movimento *jihadista* adiante com usuários que estejam em diferentes

<sup>34</sup> “O termo se refere à maneira pela qual a tecnologia de informação é aplicada por grupos como Al-Qaeda de modo a organizar a logística para suas campanhas, através da aplicação de e-mail e arquivos criptografados, bem como uma forma de desenvolver sua própria inteligência estratégica.” (COHEN-ALMAGOR, 2012, p.40)

<sup>35</sup> “Quando o terrorismo é conduzido pela tecnologia de informação. É definido como sendo ataques de motivação ideológico-política contra estruturas da informação que resultam em violência contra oficiais e agências do governo, bem como alvos não-combatentes. Tais atos criminosos através do uso do computador são perpetrados por grupos sub-nacionais e agentes clandestinos e podem resultar em morte e/ou destruição, criando o terror para o propósito de coagir governos a alterarem suas políticas.” (COHEN-ALMAGOR, 2012, p.40)

<sup>36</sup> Revista estadunidense fundada em 1845 que reúne artigos sobre ciência, tecnologia da informação e política.

<sup>37</sup> Artigo intitulado de *Virtual Jihad* publicado em 2005 por Luis Miguel Ariza.

localidades. Na seção religião é costume ter a publicação de referências à *jihad* feitas pelo Alcorão, em que se discute o aspectos do martírio, a explicação sobre “quem” ou “o que” pode ser considerado um alvo legítimo, bem como consultas doutrinárias *online* com membros religiosos.

A explicação para que aconteça a multiplicação dos *websites* em tão pouco tempo se dá pelo *software* TOR cuja criação, como mencionada anteriormente, foi destinada a aumentar o anonimato e a privacidade na navegação em rede através da criptografia e do dinamismo das páginas *online*. Em um espaço seguro do monitoramento de instituições e agências de governo, torna-se mais viável a disseminação de conteúdo sem haver represálias. Muitas atividades realizadas por grupos terroristas abrangem um nível técnico como a descoberta de *code-names*<sup>38</sup>, a descoberta de frequências de radio utilizadas por serviços de segurança. (Cohen-Almagor, 2012, p.42)

O indivíduo interessado na causa *jihadista*, inicialmente não possui a informação sobre o acesso “obscuro” à *Deep Web*. Por vezes, também não se têm acesso à Surface Web, e assim a principal forma de recrutamento continua sendo via presencial. No entanto, no que tange à esfera digital de comunicação, não é incomum que muitos usuários novos e simpatizantes da causa terrorista iniciem seu contato com o movimento *jihadista* na *Surface Web*, em redes sociais como o *Facebook*, por exemplo. Conforme o interesse e o engajamento na causa aumentam, há um movimento em direção ao lado “invisível” dos mecanismos de busca da *Surface Web*, ou seja, à *Deep Web*.

Longe do monitoramento presente na Internet de Superfície, as organizações terroristas encontram um meio de desenvolver-se, planejarem e coordenarem atividades em uma escala global. Segundo dados da General Intelligence and Security Service (2012) é estimado que em 2012 existiam algumas centenas de fóruns *jihadistas*, que seriam a linha essencial do movimento *jihadista* virtual de alcance global. Além disso, a pesquisa destaca que existem cerca de 25 mil *jihadistas* originários de mais de 100 países – fala-se, inclusive, de uma “profissionalização do jihadismo”.

Talvez uma das maiores eficiências em se tratando de resultados seja o uso da *Deep Web* para dar cabo às instruções e planejamento de ataques, bem como coordenar e preparar operações violentas contra alvos específicos.

---

<sup>38</sup> Nome dado à um produto enquanto ainda está sob desenvolvimento e, portanto, não possui um nome oficial. (Computer Hope, 2014).

Sendo assim, o caso mais famoso é o ataque às torres gêmeas, *World Trade Centers*, em Nova York, nos Estados Unidos, pelo grupo terrorista Al-Qaeda que culminou na destruição dos arranha-céu e na morte de 2.977 pessoas (CNN Library, 2014). Após duas semanas decorrentes da destruição das torres, o FBI conseguiu localizar os e-mails trocados pelo grupo cujo conteúdo se referia à detalhes operacionais do plano de agressão terrorista. (Cohen-Almagor, 2012, p.49). Outras milhares de mensagens foram criptografadas e colocadas em *websites* protegido por senha e de uso do grupo. A polícia encontrou as mensagens porque tiveram acesso ao computador do terrorista-líder preso, Abu Zubaydah, membro sênior da Al-Qaeda. Sobre isso, escreve o autor:

As primeiras mensagens achadas no computador de Abu Zubaydah datam de Maio de 2011, e as últimas foram enviadas no dia 9 de Setembro, dois dias antes do ataque que dramaticamente mudaram os negócios do mundo. A frequência das mensagens foi mais alta em Agosto de 2011. (COHEN-ALMAGOR, 2012, p.49)

Esses achados confirmam a utilização da *Deep Web* pelo grupo terrorista Al-Qaeda para planejar e executar seus planos contra o alvo específico, localidades consideradas chave nos Estados Unidos.

Porém, como esses grupos que efetuam o *cyberterrorismo* e financiam suas atividades? Um dos métodos comuns utilizados para financiar o funcionamento dessas organizações e suas atividades é através do *fundraising*<sup>39</sup>. Estes podem ser realizados através de “apelo direto por e-mail ou website”; “venda de produtos”; “negócios não relacionados ao grupo”, como a lavagem de dinheiro, a venda de drogas, a corrupção, o crime econômico, e o tráfico de dinheiro; na forma de organizações *online* semelhantes às destinadas à eventos de caridade; além de fraudes e apostas. (Cohen-Almagor, 2012, p.45)

## 2.11 A Lavagem de Dinheiro e as Moedas Digitais

É certo que a lavagem de dinheiro representa um dos papéis principais nas atividades das organizações criminosas no mundo. Ter que administrar e manter uma rede de atividades ilícitas requer capital, pois são atividades onerosas. São questões referentes aos salários, logística, treinos, subornos e outros custos que demandam

---

<sup>39</sup> Ou angariação de fundos.

investimento dos grupos que operam às margens da lei. A lavagem de dinheiro<sup>40</sup> participa nesse processo como um procedimento secundário que precede uma atividade ilícita, sendo esta o meio pela qual se consegue o capital financeiro. (Thomson Reuters, 2013). A pesquisa afirma ainda que quase 95% de toda lavagem de dinheiro processada no mundo não é detectada pelos organismos do governo ou instituições financeiras, evidenciando a dificuldade de rastreamento.

Para transformar o dinheiro proveniente de atividades ilícitas em dinheiro “limpo”, os lavadores de dinheiro utilizam-se de instituições financeiras ou outras estruturas financeiras como: contas bancárias localizadas em territórios estrangeiros que possuem leis que protegem a identidade dos indivíduos ou corporações; o uso de *shell corporations*<sup>41</sup>; sistemas bancários paralelos; *trade-based laundering money*<sup>42</sup>, cartões pré-pagos, muitas vezes conhecidos como *gift cards*. (Thomson Reuters, 2013).

O uso das moedas digitais<sup>43</sup> também se afirma atualmente como uma das grandes formas de se obter dinheiro “limpo”, uma vez que é possível a troca da moeda real por moeda virtual. Um dos casos mais ilustrativos foi o que aconteceu nos Estados Unidos e ficou conhecido como o maior caso de lavagem de dinheiro já flagrado por oficiais do governo (Thomson Reuters, 2013). Em maio de 2013, promotores dos Estados Unidos indiciaram sete pessoas em uma operação *cybercriminosa* envolvendo um banco que supostamente controlou mais de 6 bilhões de dólares para traficantes de drogas, grupos de pornografia infantil, ladrões de identidade, *hackers*, e outros criminosos, todos conectados através da troca de moeda virtual.

Qual seria então o atrativo da moeda virtual? Algumas das moedas virtuais possuem elevado grau de anonimato, como o *Bitcoin*, que dificulta em larga medida o rastreamento de uma pessoa ou entidade. O anonimato se demonstra possível a partir do momento que o usuário torna anônimo o seu endereço de IP<sup>44</sup>. Caso o usuário não mascare o seu endereço de IP, então será possível identificar a localidade física do indivíduo, pois toda transação em *bitcoin* é publicada *online*. (FBI, 2012, p.5) Outra forma de se quebrar com o anonimato se refere aos serviços terceirizados que utilizam o

---

<sup>40</sup> “É a prática de se processar dinheiro e ativos ganhos por meios ilícitos em status legal (limpo).”

<sup>41</sup> Quando uma corporação opera sem possuir nenhum ativo ou operação relevantes.

<sup>42</sup> O processo de disfarçar a procedência de um crime e mover o valor através das transações de comércio em uma tentativa de legitimar as origens ilícitas.

<sup>43</sup> Conhecidas também como moedas virtuais. Alguns exemplos são Bitcoin, Litecoin, Zen, Namecoin, etc.

<sup>44</sup> *Internet Protocol*.

*bitcoin* e podem requisitar uma identificação válida ou até mesmo a informação bancária para completar a transação. (FBI, 2012, p.5)

Em se tratando do *bitcoin*, é necessário observar algumas características. De acordo com Fernando Ulrich (2014), não existe um governo ou agência central reguladora do valor do *bitcoin*, ou mesmo do seu uso. O valor de uma moeda de *bitcoin* vem da crença dos usuários de que irão poder trocar a moeda por bens, serviços ou até a mesmo por moeda física em uma data futura (FBI, 2012, p.4), uma vez que já existem prestadores de serviços, como hotéis, que aceitam o pagamento em *bitcoins*. O *bitcoin* é trocado livremente e de forma anônima em redes ao redor do mundo, sendo a principal moeda comercializada na *Deep Web*. O fato de ser largamente utilizada nessa esfera da rede tem explicação: o seu caráter de anonimato atrai usuários e *websites* da Internet Profunda que estão dispostos a negociar na moeda digital. Em outras palavras, seu uso é permitido e até preferível como uma forma de pagamento. É possível ainda realizar a compra de moedas virtuais em sites disponíveis na *Surface Web* como o E-bay e o Craigslist. (THOMSON REUTERS, 2013, p.8)

Para se utilizar a moeda é necessário instalar o *software* gratuito *Bitcoin*. (FBI, 2012). O programa utiliza uma criptografia pública denominada PKI<sup>45</sup>. Com essa criptografia o programa automaticamente gera um endereço único de *Bitcoin* por onde o usuário pode receber e transferir pagamentos. Cabe ressaltar que a criação de endereços é ilimitada dando ao usuário a possibilidade de criar quantos endereços *Bitcoins* desejar. Para enviar moedas, o usuário deve inserir no programa a quantidade desejada a ser enviada, tal qual o endereço de *Bitcoin* de destino. Uma vez realizada a operação de envio, não é possível reverter o comando. (FBI, 2012, p.14)

O relatório do FBI nos indica que os desenvolvedores do *Bitcoin* não detêm o poder e a autoridade sobre a moeda, e nem possuem uma base de dados centralizada (FBI, 2012, p.4) – fato este que dificulta muito a operação da polícia no controle, rastreamento e detenção da moeda. Eles mantêm, no entanto, páginas na internet que servem de guia à comunidade usuária do *Bitcoin*.

---

<sup>45</sup> Sigla para *Public Key Cryptography*.

## 2.12 Conclusão

A *Deep Web* como ferramenta de comunicação sigilosa entre grupos de indivíduos ao redor do mundo se prova muito eficaz. O anonimato, a dinâmica das páginas não-indexadas, o fácil acesso pelo *software* TOR, e a criptografia tornaram o ambiente da *Deep Web* menos suscetível ao monitoramento efetivo pelas instituições governamentais e demais agências. Além disso, a *Deep Web* oferece um espaço digital que se multiplica em tamanho de *websites*, conteúdo e informações, sendo superior em tamanho comparado com a *Surface Web* em 500 vezes (Bergman, 2001).

Portanto, quando se fala sobre anonimato em uma vasta rede global de informações, é compreensível que o espaço se torne atraente para indivíduos, organizações e grupos criminosos que desejam um meio privado para executar atividades ilícitas. Outros grupos, como jornalistas, por exemplo, utilizam essa esfera da *web* como ferramenta anti-censura com repercussões no cotidiano real. É nesse sentido que o funcionamento da *Deep Web* serve como uma ferramenta para que a informação seja recebida, enviada e compartilhada sem que sofra resistências ou censuras dos governos e Estados.

No entanto, é fato que as redes de crime internacional conseguiram obter vantagens das oportunidades resultantes de mudanças na política, nos negócios, na tecnologia e na comunicação – que tanto fortaleceram a democracia e os mercados livres. (Viano, 2010). Também é verdade que as redes criminosas e as atividades ilícitas existiam muito antes da Internet e da *Deep Web*. Porém, como afirma Viano (2010) o que ocorre é uma globalização de problemas que afetam um país, ou grupo de países, sem que haja uma internacionalização correspondente da autoridade do Estado. Enquanto antes o crime, muitas vezes, era considerado local, atualmente ele pode tomar aspectos globais tendo como um dos contribuidores para a teia criminosa, o indivíduo médio. Em outras palavras, a *Deep Web* proporciona ao indivíduo médio uma segurança física significativa, de modo que o mesmo possa contribuir com o aumento das atividades ilícitas do crime organizado ao averiguar a diminuição do risco e facilidade de acesso à essa rede criminosa através de ferramenta inovadora.

O autor ainda destaca que uma vez que a criminalidade tome proporções globais, com células espalhadas pelas mais variadas regiões do mundo, o controle do crime não dependerá de um Estado mas sim da cooperação em conjunto com os outros Estados em cujo território operam as outras células.

É compreensível, portanto, que a globalização imponha desafios às fronteiras geográficas que historicamente delineavam os limites da soberania, da cidadania e do próprio Estado-nação. (Viano, 2010). Mas, no entanto, o que seria o *ciberespaço*? E onde ele se encaixaria nisso tudo? Quem nos brinda com uma resposta é Guilherme Carvalho Silva (2013):

Uma nova geografia se delineia através do ciberespaço, uma geografia onde fronteiras são ressignificadas, são delimitadas, são diluídas. O ciberespaço reúne elementos que articulam novas formas de relações sociais, ou pelo menos, formas com outra matriz de complexidade do que as que se vislumbravam até então. [...] De um lado, o ciberespaço permite manifestações de liberdade, de outro, o fardo do controle total. Para os incluídos nos processos de entendimento técnico do mesmo – os arautos da criptografia – ele possibilita a liberdade de comunicação livre, para os prisioneiros do fetiche tecnológico, ele dá a *sensação* de liberdade. [...] Para que o ciberespaço possa ser além de uma distopia e de uma utopia, o mesmo deve ser vivenciado em seu componente de correlação indissociável com o espaço geográfico. O que ocorre no ciberespaço deve repercutir no espaço geográfico, necessariamente. Senão, vira um mundo de sem mundo, uma virtualidade apenas. As revoltas que hoje se espalham globalmente e que têm o componente de aglomeração ideológica e mobilização via ciberespaço, só conseguem ter algum peso e efetividade se aplicados no espaço geográfico. (SILVA, 2013, p.167)

O ciberespaço, e em especial a *Deep Web*, tem contribuído para aumentar o engajamento de pessoas nas mais diversas causas. Isso ocorre pela democratização da Internet, ou qualquer indivíduo mediante um dispositivo de acesso à rede, pode dela extrair conhecimento e se informar. O acesso a informação, de modo livre e não-censurado, permite que as pessoas detenham uma opinião sobre determinada matéria e estabelecessem discussões sobre assuntos que por ventura estejam interditados nos meios de comunicação tradicionais. Presenciamos um momento em que as opiniões são disseminadas instantaneamente na rede, abrindo espaço para o debate e a discussão sobre os mais diversos assuntos. O anonimato, e em especial a criptografia, permite que a rede dê vazão à vozes que de outra forma seriam perseguidas pela autoridade do Estado. Não se pretende aqui, contudo, discorrer acerca da moral, mas apenas estabelecer um nexos entre a ampliação da liberdade pela inovação tecnológica e as consequências disto sobre a autoridade estatal, por consequência sobre a relação entre sociedade civil e Estado.

No próximo capítulo, discutiremos em que medida a *Deep Web* aumenta a difusão de poder para além da autoridade do Estado.

### 3. DIFUSÃO DE PODER EM FACE DA *DEEP WEB*

Como bem lembra Susan Strange (1996), os limites geográficos não mais coincidem com a extensão dos limites da autoridade política sobre a economia e a sociedade. De acordo com as quatro estruturas de poder, descritas e analisadas pela autora no seu livro “States and Markets” (1994), as quais são segurança, produção, finanças e conhecimento, pode-se afirmar que o Estado é líder apenas em uma delas: segurança, e que mesmo assim, muitas das vezes, necessita recorrer em apoio aos demais Estados no sistema internacional. Esse fato ocorre porque nem todo poder estrutural sobre a segurança está embutido no escopo da autoridade estatal. Sendo assim, surgem outras autoridades não-estatais cujo poder é exercido na sociedade e entre as sociedades. (Strange, 1996).

A autora compreende a dificuldade de parte dos acadêmicos em acreditar no declínio da autoridade estatal. Mas cabe lembrar, no entanto, que Strange (1996) não crê que a autoridade declinou em termos de quantidade, mas sim de qualidade. Isso ocorre uma vez que a maioria dos governos de Estados territoriais tem operado de modo falho no que concerne às suas funções básicas e pelas quais foram instituídos. (Strange, 1996, p.xii) Tal declínio de autoridade estatal é refletido pela difusão de autoridade para outras instituições e associações, além de corpos locais e regionais. (Strange, 1996, p.4)

Para compreendermos em que medida a *Deep Web* aumenta a difusão de poder para além do Estado, primeiramente se torna interessante relembrar a definição de poder segundo Susan Strange, cuja abrangência é mais ampla que as demais definições sobre poder e política encontradas na literatura sobre o assunto. Sendo o poder descrito como “a habilidade de uma pessoa ou grupo de pessoas para afetar os resultados de forma que suas preferências tenham precedência sobre a preferência dos outros”. (Strange, 1996, p.17)

A maioria dos acadêmicos interessados em política internacional ao longo do século XX utiliza a unidade de análise primária: o Estado. O problema, segundo Strange, é que muitas vezes “primária” se torna “única”. Esse fato se traduz em um problema porque falha em observar outras autoridades que não sejam o Estado e que possuem e exercem o “poder sobre” os resultados. (Strange, 1996, p.34)

O que então seria política? Segundo David Easton, um grande influente em Ciência Política, a política poderia ser descrita como sendo “a alocação autoritária de

valores no sistema”. (Easton, 1953). Susan Strange traduz esses valores como sendo quatro: a riqueza criada; a segurança provida; a justiça distribuída; e a liberdade, ou autonomia, permitida. A seguir, afirma que, “toda sociedade provê alguma riqueza, alguma segurança, alguma justiça e algum grau de liberdade para escolher”. (STRANGE, 1996, p.34)

Seguindo essa linha de raciocínio parece claro que o Estado não é o único que possui a autoridade para alocar tais valores. (Strange, 1996, p.34). Política não é feita apenas por intelectuais, líderes de opinião, políticos ou pessoas que participam de partidos políticos, ou até mesmo movimentos sociais com objetivos políticos. (Strange, 1996, p.35) Segundo Bertrand de Jouvenel, filósofo político francês do pós-guerra, a definição de autoridade política se dá pela seguinte forma:

[...] De acordo com duas presunções básicas: primeiro, a ação se torna política quando a ajuda de outras pessoas é uma condição necessária para um indivíduo alcançar seu objetivo; e segundo, a política conseqüentemente ocorre quando um projeto requer o apoio da vontade dos outros. (De Jouvenel, 1957, apud STRANGE, 1996, p.35)

Ou seja, quem deseja ser político, necessita do apoio da vontade de outros para alcançar o seu objetivo. Strange ainda adiciona que “o estudo não deve compreender somente a o fluxo de vontades, mas também as conseqüências enquanto a associação durar e com quais resultados.” (STRANGE, 1996, p.36)

Como partimos da definição de poder de Strange (1996), nos parece lógico que analisemos a economia política internacional, focalizando a *Deep Web*, do ponto de vista estruturalista e funcional - a mesma utilizada por Strange. Essa metodologia tem como característica prover uma boa quantidade de flexibilidade uma vez que não se limita a intervenção da autoridade somente a Estados ou agências do Estado, mas abrange também qualquer tipo de autoridade. (Strange, 1996, p.42).

Nesse caso, essa metodologia aborda as várias funções da autoridade na política econômica e realiza questionamentos sobre quem ou o quê efetiva tais funções ou responsabilidades, e com quais efeitos sobre os resultados. Como afirma a autora:

A questão se inicia com ‘quem’, se é que alguém, está exercendo autoridade – e com qual propósito, com quais meios e com quais conseqüências. Minha hipótese é que muitos Estados perderam o controle sobre algumas funções da autoridade e, ou a estão dividindo com outros Estados ou com outras autoridades não-estatais. O resultado em muitos casos é que ninguém é responsável pelas funções da autoridade, embora se finja

que sim. Os resultados presumem um declínio geral do poder da maioria dos Estados e algum ganho na autoridade de mercados mundiais e empresas operando em tais mercados. [...] De forma alguma isso significa que a soberania está em risco ou que as corporações transnacionais estão deslocando o Estado [...] Pois seria um grosso exagero ao qual quer ninguém seriamente esperaria. (STRANGE, 1996, p.44)

Ressalta-se ainda que, como pouca atenção é dada às autoridades não-estatais na sociedade, não existe propriamente uma definição que abrangeria todas as formas desse tipo de autoridade. Mas ela pode ser determinada se levarmos em conta os resultados. É nesse sentido que Strange elenca a importância de duas categorias de poder para auxiliar a observação.

Primeiramente, o poder relacional - que pode ser exercido diretamente - e é exemplificado com o cargo de chefe de uma multinacional, ou o chefe da máfia, cuja autoridade sobre a relação social é exercida com os subalternos. Em segundo lugar, o poder estrutural - exercido indiretamente - é exemplificado com o cargo de banqueiro, ou um segurador que detém autoridade para diminuir as opções disponíveis. (Strange, 1996, p.91)

Em suma, enquanto o poder relacional é exercido diretamente a partir das relações entre os indivíduos ou grupos, o poder estrutural é exercido indiretamente, pois é capaz de afetar a escolha dos demais na sociedade. Cabe lembrar ainda que as autoridades podem fazer rivalidade à autoridade do Estado, ou podem ser autoridades toleradas pelo Estado e até bem-vindas. (Strange, 1996, p.96)

Portanto, partindo de uma visão estrutural e funcionalista do poder, observamos o declínio da autoridade estatal em face da *Deep Web* uma vez que, a partir do anonimato e da criptografia inerente a essa região do *ciberespaço*, propicia-se a multiplicação de organismos políticos - a exemplo dos citados, *Wikileaks*, *Anonymous*, mercado *Silkroad*, terrorismo islâmico - que possuem nesse ambiente espaço para a proliferação de ideologias, disseminação do conhecimento, planejamento e coordenação de atividades ilícitas, e que interagem de forma a ter consequências no plano real geográfico. Isso se deve à própria estrutura da *Deep Web*, diferente dos outros meios de comunicação que são passíveis de constante monitoramento e vigilância por terceiros, e que assim desafia ambos estadista e jurista. Não que seja completamente impossível rastrear dados ou informações na *Deep Web*, mas a sua estrutura torna tal ação muito ardorosa, de difícil, dispendiosa e complicada realização.

O caso da *Wikileaks* evidencia o uso da *Deep Web* de forma a reforçar o combate à censura e reafirmar o direito à liberdade de expressão, dando aos jornalistas e pesquisadores ferramentas para desafiar a autoridade dos que controlam a informação – e em muitos casos, o controle é diretamente, ou indiretamente, decorrente do próprio Estado. A *Deep Web*, assim, acaba por funcionar como um veículo blindado e que resguarda o anonimato necessário para a investigação e a delação de casos sem que o jornalista necessariamente sofra censura ou até mesmo riscos derivados de suas atividades jornalísticas.

Por outro lado, *websites* da *Deep Web*, como a *Silk Road*, oferecem a oportunidade de organizações criminosas expandirem suas atividades, pois contam com a dificuldade da vigilância por parte do Estado. Sendo assim, mercados locais podem ver um salto no alcance de suas atividades, tomando dimensões inclusive transnacionais. Não somente isso, fóruns e mercados negros na *Deep Web* veem na possibilidade de anonimato e na segurança da criptografia seus riscos diminuídos nas operações de contrabandos e serviços ilícitos, multiplicando seu número e suas atividades, interconectando o planeta sem, necessariamente, enfrentar o risco físico de investigação pela polícia. Observa-se, portanto, que apesar do crime organizado não ser um evento novo, a maneira como o indivíduo comum possui acesso fácil à teia do crime organizado – e nela contribuindo, seja com compra de pornografia infantil, pagando por serviços de imagem e áudio disponíveis nessa região da Internet, ou participando do comércio ilegal de bens – é que se demonstra inovador com o uso da *Deep Web*. Ressalta-se ainda que o risco é diminuído, porém não é eliminado.

Crimes organizados, planejados e coordenados por grupos terroristas da *jihad* islâmica gozam de segurança ao expor suas ideologias e efetivar suas comunicações pela *Deep Web*. Essa talvez seja uma das suposições para o acentuado crescimento de páginas terroristas na *Deep Web*. Ficou, por exemplo, claro que a o grupo terrorista Al-Qaeda fez uso da *Deep Web* para levar a cabo seu plano de execução nos Estados Unidos em 2001. O grupo *Anonymous*, a exemplo mencionado, utiliza-se da *Deep Web* para se organizar e realizar ativismo político no momento atual. Todas essas ações orquestradas por atores não-estatais têm mostrado consistência no plano real geográfico, influenciando novos resultados.

Assim discorre Grammatikopoulo (2013):

Como seu trabalho depende da participação do público, ele pode ser visto como um convite para alterar a forma que pensamos e agimos dentro de um quadro político. [...] Enquanto práticas *hackers*, o *hackativismo* e a pirataria se tornam ferramentas diárias nas mãos de grande parte da população e estão fermentando uma multidão de mudanças no tecido social por permitir a distribuição de informação além da rede convencional, deste modo, capacitando a formação de novas comunidades e grupos de ações. É um processo que traz novas ideologias à dianteira, as 'ideologias da era da informação' que desafiam o atual *status quo* político e financeiro. (GRAMMATIKOPOULOU, 2013, p.215).

Quanto ao crime organizado, Strange afirma ainda que:

[...] Para reduzir ou até limitar a riqueza econômica, e o potencial para o rompimento político e social desses grupos transnacionais criminosos, e assim trazer para níveis controláveis desferiria um golpe no coração da soberania nacional – a responsabilidade para manter a lei e a ordem e administrar a justiça criminosa. Isso requeriria uma autoridade policial global com poderes extensivos para prender e processar criminosos ao redor do mundo, bem como exigiria uma corte internacional de justiça criminal com competência para julgar e punir. Isso é algo que, até agora, nenhum governo de nenhuma nação-Estado já contemplou. (STRANGE, 1996, p.120)

A autora ainda indaga sobre os danos causados à autoridade do Estado territorial, o que nos serve como reflexão em face das atividades ocorridas e desenvolvidas na *Deep Web*. Assim segue que “o dano já cometido na legitimidade e na viabilidade da sociedade internacional baseada na autoridade do Estado como aquele que garante a ordem e provê o bem-estar pode ainda evidenciar estar longe de reparos”. (STRANGE, 1996, p.212)

Em face da *Deep Web*, o que se observa é o aumento da difusão do poder relativo. Esse aumento ocorre na medida em que grupos políticos – partindo da definição de que política ocorre quando um projeto requer o apoio da vontade dos outros e compreende consequências enquanto a associação durar e com determinados resultados – obtém uma maior habilidade para afetar os resultados de forma que suas preferências tenham precedência sobre a preferência dos outros, porque estão em posse de uma ferramenta inovadora, que é capaz de assegurar o anonimato do envio e recebimento de informações sem o constante monitoramento do Estado. As consequências são observadas no campo real geográfico, com o sucesso de operações ilícitas que desafiam a autoridade do Estado.

## CONSIDERAÇÕES FINAIS

O presente estudo teve como objetivo analisar em que medida a *Deep Web* aumenta a difusão de poder. Para isso, propôs-se trabalhar o conceito de poder segundo a definição de Susan Strange (1996). A partir disso, abordou-se o aspecto histórico da Internet, e em especial a *Deep Web*, bem como seu funcionamento e características que a distinguem da *Surface Web*, cujo conteúdo é indexado pelos mecanismos de busca e, portanto, visível ao usuário médio comum. Valendo-se do anonimato, do dinamismo dos sites, da criptografia, a *Deep Web* atraiu segmentos da sociedade que veem nessas qualidades um meio de agir em privacidade.

Abordou-se o caso da *Wikileaks*, cuja inovação jornalística apresenta desafios acerca da ética, que teve suas operações realizadas por meio de *crowdsourcing* em páginas não indexadas. Além disso, foi possível observar outros grupos políticos como o *Anonymous* que, apesar de ter sido iniciado como um grupo *troll*, posteriormente se desenvolveu como um relevante ator do *hackativismo* que desafia a autoridade estatal. Também se observou a constituição e o funcionamento de mercados negros como o *Silkroad*, que em função da configuração da estrutura da *Deep Web*, se tornou um grande mercado de substâncias ilícitas - principalmente. Também foi discutido o funcionamento de grupos terroristas nas profundezas da Internet, bem como suas operações, seu planejamento e coordenações de atividades realizadas por meio da criptografia – o que dificulta o acesso ao conteúdo da informação e aumenta o sucesso da comunicação sigilosa.

Finalmente, observou-se o aspecto da construção da moeda virtual *Bitcoin* e de que forma a mesma surgiu como uma alternativa às moedas reais no que tange ao financiamento de grupos, bens e serviços ilícitos. Seu caráter “democrático”, com a ausência de uma agência reguladora central, e anônimo, permite que a mesma seja largamente utilizada como um popular meio de pagamento em *websites* da *Deep Web*.

Utilizando-se de larga bibliografia, concluiu-se que a *Deep Web* contribui para a difusão do poder relativo na medida em que grupos políticos obtêm uma maior habilidade para afetar os resultados ao utilizarem da *Deep Web* - meio de comunicação inovador pelo acentuado grau de dificuldade de rastreamento e monitoramento das atividades por parte do Estado. Tais resultados têm impacto no plano real geográfico. Cabe lembrar ainda que Strange (1996) define o poder relativo como sendo “poder sobre algo” ao invés de “poder derivado de algo”.

Este trabalho não pretende dar uma resposta definitiva quanto ao assunto abordado, mas espera que sirva de indagação para futuros trabalhos relacionados com a área.

## REFERÊNCIAS BIBLIOGRÁFICAS

ARIZA, Luis Miguel. **The Virtual Jihad: The internet as the ideal terrorism recruiting tool.** 2005. Disponível em: <<http://www.scientificamerican.com/article/virtual-jihad/>>. Acesso em: 15 out. 2014.

BERGMAN, Michael. **White paper: the Deep Web: surfacing hidden value.** Journal of electronic publishing. Michigan: University of Michigan Library, vol.7, Ed.1, 2001.

BERGMAN, Michael. **About Mike.** 2013. Disponível em: <<http://www.mkbergman.com/about-mike/>>. Acesso em: 31 set. 2014.

CAMPOS, Iberê. **Entendendo os roteadores.** Disponível em: <[http://www.thecnica.com/artigos/PnP\\_13\\_06.pdf](http://www.thecnica.com/artigos/PnP_13_06.pdf)>. Acesso em: 29 set. 2014.

CASTELLS, Manuel; CARDOSO, Gustavo. **The Network Society: From Knowledge to Policy.** Washington, DC: John Hopkins Center for Transatlantic Relations, 2005.

CASTELLS, Manuel. **Fim de Milênio.** 2 ed. São Paulo: Paz e Terra, 1999. 3.v. (A era da informação: sociedade, economia e cultura).

CIANCAGLINI, Vincenzo et al. **A Trend Micro Research Paper: Deep Web and cybercrime: it's not all about TOR.** Cupertino: Trend Micro. 2013

CHRISTIN, Nicolas. **Traveling the silkroad: a measurement analysis of a large Anonymous online market place.** Pittsburgh: Carnegie Mellon Univeristy. 2012

CNN LIBRARY. **September 11th Fast Facts.** 2014. Disponível em: <<http://edition.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/>>. Acesso em: 19 out. 2014.

COHEN, Benjamin J.. **International Political Economy: An Intellectual History.** Princeton: Princeton University Press, 2008.

COHEN-ALMAGOR, Raphael. **In Internet's Way: radical, terrorist islamists on the Free Highway**. International Journal Of Cyber Warfare And Terrorism, Hershey, v. 2, n. 3, p.39-58, set. 2012. Disponível em: <[http://www.hull.ac.uk/rca/docs/articles/Terrorism on the Free Highway-Final.pdf](http://www.hull.ac.uk/rca/docs/articles/Terrorism%20on%20the%20Free%20Highway-Final.pdf)>. Acesso em: 12 out. 2014.

COLEMAN, Gabriella. **Hacker Politics and Publics**. Public Culture, New York, v. 23, n. 3, p.511-516, out. 2011. Disponível em: <<http://gabriellacoleman.org/wp-content/uploads/2012/08/Coleman-hacker-politics-publics.pdf>>. Acesso em: 10 out. 2014.

COMPUTER HOPE (Org.). **URL**. Disponível em: <<http://www.computerhope.com/jargon/u/url.htm>>. Acesso em: 02 out. 2014.

COMPUTER HOPE (Org.). **Codename**. Disponível em: <<http://www.computerhope.com/jargon/c/codename.htm>>. Acesso em: 12 out. 2014.

CNN LIBRARY. (Org.). **September 11<sup>th</sup> Fast Facts**. Disponível em: <<http://edition.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/>>. Acesso em: 05 out. 2014.

EASTON, David. **The Political System: an inquiry into the state of political science**. New York: Alfred A. Knopf, 1953.

FATF. **Trade-Based Money Laundering**. Disponível em: <<http://www.fatf-afi.org/topics/methodsandtrends/documents/trade-basedmoneylaundersing.html>>. Acesso em: 18 out. 2014.

FBI. **Bitcoin virtual currency: unique features present distinct challenges for deterring illicit activity**. Estados Unidos: Federal Bureau Of Investigations, 2012. Disponível em: <[http://www.wired.com/images\\_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf](http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf)>. Acesso em: 19 out. 2014.

GENERAL INTELLIGENCE SERVICE. **Jihadism on the web**. Países Baixos: AIVD, 2012. Disponível em: <[https://www.aivd.nl/publish/pages/2402/het\\_jihadistisch\\_internet\\_eng.pdf](https://www.aivd.nl/publish/pages/2402/het_jihadistisch_internet_eng.pdf)>. Acesso em: 16 out. 2014.

GRAMMATIKOPOULOU, Christina. **From the *Deep Web* to the city streets: hacking, politics and visual culture**. Quaderns-e, Barcelona, v. 1, n. 19, p.202-2019, 21 maio 2013. Disponível em: <[http://www.antropologia.cat/files/13\\_Grammatikopoulou,\\_Christina\\_dossier2.pdf](http://www.antropologia.cat/files/13_Grammatikopoulou,_Christina_dossier2.pdf)>. Acesso em: 22 out. 2014.

HERMANN, Margaret. HERMANN, Charles. **Who makes foreign policy decisions and how: an empirical inquiry**. International Studies Quarterly, vol. 33, n. 4. 1989. p.361-387

INTERNATIONAL CENTRE FOR MISSING & EXPLOITED CHILDREN. Thomson Reuters. **The digital economy: potential, perils and promises: A report of the digital economy task force**. New York: Thomson Reuters, 2014. 36 p. Disponível em: <<http://www.europeanfinancialcoalition.eu/private10/images/document/8.pdf>>. Acesso em: 12 out. 2014.

KEOHANE, Robert. **After hegemony: cooperation and discord in the world political economy**. Princeton: Princeton University Press. 1984

KINDLEBERGER, Charles. **On the rise and decline of nations**. International Studies Quarterly. 1983, p.5-p.10

MARTINS, Caio Arthur Lopes da Silva; SILVA, Maria Helena Barriviera e. **A dualidade da *Deep Web***. E-f@tec, Garça, v. 3, n. 2, p.1-7, 2013. Disponível em: <[http://www.fatecgarca.edu.br/revista/Volume3/artigos\\_vol3/Artigo\\_16.pdf](http://www.fatecgarca.edu.br/revista/Volume3/artigos_vol3/Artigo_16.pdf)>. Acesso em: 05 out. 2014.

MING-TE, Hung. LIU, Tony Tai-Ting. **Hegemonic stability and northeast asia: what hegemon? What stability?**. Journal of Asia Pacific Studies, vol.2., n.2. 2011, p.216-230

NASCIMENTO, Barbara Luiza Coutinho do. **Liberdade de expressão, honra direito e privacidade na internet: a evolução de um conflito entre direitos fundamentais**. 2009. 95 f. Monografia (Especialização) - Curso de Direito, Escola de Magistratura do Estado do Rio de Janeiro, Rio de Janeiro, 2009

NYE, Joseph. **Bound to lead: the changing nature of American power**. New York: Basic Books. 1990

OLIVEIRA, Fabio Machado; TOTTI, Maria Eugênia Ferreira; SOUZA, Carlos Henrique Medeiros. **A web invisível e seus aspectos tecnológicos e sociais**. In: CONGRESSO INTERNACIONAL INTERDISCIPLINAR EM SOCIAIS E HUMANIDADES, 2., 2013, Belo Horizonte. Anais... . Belo Horizonte: Coninter, 2013. p. 1 - 12. Disponível em: <[www.2coninter.com.br/artigos/pdf/280.pdf](http://www.2coninter.com.br/artigos/pdf/280.pdf)>. Acesso em: 23 set. 2014.

OLIVEIRA, Daniela Sofia Guerreiro de. **O poder da informação na política internacional: a Wikileaks e a revolução na Tunísia**. 2012. 82 f. Dissertação (Mestrado) - Curso de Ciência Política e Relações Internacionais, Universidade Nova de Lisboa, Lisboa, 2012. Disponível em: <[http://run.unl.pt/bitstream/10362/7366/1/Dissertação DGO2012.pdf](http://run.unl.pt/bitstream/10362/7366/1/Dissertação%20DGO2012.pdf)>. Acesso em: 19 set. 2014.

PACHECO, Liliana. **Wikileaks e Internet: o que poderá mudar no jornalismo a partir daqui**. Estudos em Comunicação, Lisboa, v. 0, n. 9, p.31-43, maio 2011. Disponível em: <<http://www.ec.ubi.pt/ec/09/pdf/EC09-2011Mai-02.pdf>>. Acesso em: 09 out. 2014.

PISA, Pedro. **O que é criptografia**. 2012. Disponível em: <<http://www.techtudo.com.br/artigos/noticia/2012/06/o-que-e-criptografia.html>>. Acesso em: 29 set. 2014.

PISAREWICZ, Piotr. **Privacidade na Rede Aberta**. 2013. 86 f. TCC (Graduação) - Curso de Computação, Universidade de Brasília, Brasília, 2013.

POMPÉO, Wagner Augusto Hundertmarck; SEEFELDT, João Pedro. **Nem tudo está no Google: Deep Web e o perigo da invisibilidade**. In: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE> MÍDIAS E DIREITOS DA SOCIEDADE EM REDE, 2., 2013, Santa Maria. Anais... . Santa Maria: Ufsm, 2013. p. 436 - 449. Disponível em: <[www.coral.ufsm.br/congressodireito/anais/2013/3-11.pdf](http://www.coral.ufsm.br/congressodireito/anais/2013/3-11.pdf)>. Acesso em: 27 set. 2014.

SILVA, Guilherme Carvalho da. **O ciberespaço como categoria geográfica**. Brasília: GEAH/IH/Unb, 2013.

SIMON, Herbert. **Models of Bounded Rationality**. Cambridge: MIT Press. 1982

STRANGE, Susan. **The Retreat of the State: the diffusion of Power in the world economy**. Cambridge: Cambridge University Press, 1996.

STRANGE, Susan. **States and Markets**. 2. ed. London: Pinter Publishers, 1994. 266 p.

THOMSON REUTERS. **Technology in the fight against money laundering in the new digital currency age**. 2013. Disponível em: <[http://accelus.thomsonreuters.com/sites/default/files/GRC00403\\_0.pdf](http://accelus.thomsonreuters.com/sites/default/files/GRC00403_0.pdf)>. Acesso em: 18 out. 2014.

ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig von Mises Brasil, 2014. 100 p.

VAN HOUT, Marie Claire; BINGHAM, Tim. **Surfing the Silk Road: A study of user's experiences**. *International Journal Of Drug Policy*, [s. L.], v. 24, n. 6, p.524-529, set. 2013. Published Online.. Disponível em: <<http://www.gwern.net/docs/sr/2013-van-hout-2.pdf>>. Acesso em: 10 out. 2014.

VAN HOUT, Marie Claire; BINGHAM, Tim. **Responsible Vendors, Intelligent Consumers: Silk Road, the online revolution in drug trading**. International Journal Of Drug Policy, [s. L.], v. 24, n. 2, p.183-189, 22 nov. 2013. Publicado online. Disponível em: <<http://bitcoinmenow.com/wp-content/uploads/2013/12/Responsible-vendors-intelligent-consumers-Silk-Road-the-online-revolution-in-drug-trading.pdf>>. Acesso em: 10 out. 2014.

VIANO, Emilio C.. **Globalization, Transnational Crime and State Power: the need for a new criminology**. Rivista di Criminologia, Vittimologia e Sicurezza, Bologna, v. 4, n. 1, p.63-85, abr. 2010.