Tor *Browser*: Navegando com Segurança no Ciberespaço[1]

Felipe BERNARDO[2]
Andrélia SANTOS[3]
Nadja CARVALHO[4]
Universidade Federal da Paraíba, João Pessoa, PB

RESUMO
Este artigo tem como finalidade mostrar que o Tor não é apenas mais um navegador, mas também é uma ferramenta inserida em uma nova configuração midiática e política, dentro e fora do ambiente virtual. Pensando nessa discussão, o artigo pretende através de referências e questionário demonstrar a importância desse navegador, bem como sua utilização por diversos setores da sociedade, evidenciando a existência de uma *militarização do ciberespaço*, da qual governos e empresas se utilizam da tecnologia para atacar a privacidade e ameaçar a liberdade em rede, porém é possível também usar a tecnologia para se proteger das ameaças. E a utilização de ferramentas criptográficas como o Tor, apresenta-se como uma alternativa.

PALAVRAS-CHAVE: Tor *browser*; criptografia; privacidade; vigilância; web.

CRIAÇÃO DO TOR BROWSER

A preocupação com ambientes seguros e os cuidados com a preservação das comunicações do governo, quanto a possíveis interceptações em rede, levou o grupo de pesquisadores do matemático Paul Syverson e dos cientistas da computação Michael Reed e David Goldschlag, do Laboratório de Pesquisa Naval dos Estados Unidos, a desenvolver o princípio de roteamento por camada, em meados de 1990, identificado pela sigla Tor (The Onion Router), conhecido como "navegador cebola".

O projeto passou a ser desenvolvido, por volta de 1997, sob os cuidados da Agência de Pesquisa Avançada de Projetos de Defesa (DARPA). Até que uma versão do projeto Tor, desenvolvida por Roger Dingledine, Nick Mathewson, e Paul Syverson, é apresentada em setembro de 2002. Dois anos depois é lançada "a segunda geração *onion router*", em agosto de 2004, no 13º Simpósio de Segurança Usenix, na Califórnia[5].

O Tor garante o acesso à internet sem a necessidade do usuário se identificar. Por

[1]Trabalho apresentado no DT 5 – Rádio, TV, Internet do XVII Congresso de Ciências da Comunicação na Região Nordeste, realizado de 2 a 4 de julho de 2015.
[2]Graduando do curso de Comunicação em Mídias Digitais da UFPB. E-mail: bernardofeli@gmail.com
[3]Graduanda do curso de Comunicação em Mídias Digitais da UFPB. E-mail: andrelia.santos@gmail.com
[4]Professora no curso de Comunicação em Mídias Digitais da UFPB. E-mail: naddj@ig.com.br
[5]SIMONS, Jake Wallis (2014). Disponível em: http://www.publico.pt/tecnologia/noticia/a-rede-secreta-1673221. Acesso em: 19 maio 2015.

outro lado, ironicamente, a principal fonte de financiamento deste projeto tem sido de governos, entre eles o Norte-Americano. Desenvolvido por Tor Project (2006), organização sem fins lucrativos, o projeto tem o apoio financeiro de três colaboradores: Departamento de Estado Norte-Americano, Conselho de Radiodifusão de Governadores e National Science Foundation. Calcula-se que, 60% do orçamento vêm do governo Norte-Americano, os demais 40% vem de outros governos, usuários e empresas como Google, Human Rights Watch e a Fundação de Divisão Eletrônica (EFF).

A rede Tor em 2013 contava com 500 mil usuários diários e hoje alcança mais de 4 milhões de usuários em todo o mundo, em razão das revelações de Edward Snowden, ex-funcionário da National Security Agency (NSA). O que provocou debates sobre a utilização do navegador e da criptografia feita pela sociedade. Nos últimos anos, o "navegador cebola" tem ampliado sua rede devido a campanhas e divulgações da EFF, capitaneadas por ciberativistas e organizações que defendem a privacidade e a liberdade de comunicação em rede.

O navegador vem sendo utilizado ao redor do mundo. Um dos usos mais conhecidos e emblemáticos ocorreu em 2013, quando Snowden utilizou o navegador e outra ferramenta de "criptografia de chave pública" (PGP)[6], para dizer ao mundo o quanto estamos sendo vigiados. Revelou como o governo Norte-Americano monitora a vida privada de bilhões de pessoas, incluindo líderes políticos como as vítimas de espionagem a presidente Dilma Roussef (BR) e a chanceler Angela Merkel (AL)[7].

A principal função do navegador é mascarar o endereço IP do usuário, levando as solicitações de acesso a páginas por uma via criptografada de computadores de colaboradores espalhados pelo mundo, garantindo o anonimato do que o usuário faz na rede. Mas é importante afirmar que existem brechas que permitem a invasão de terceiros e por isso devem ser tomados alguns cuidados.

UMA FERRAMENTA POLÍTICA

Conforme Snowden alertou, todos os nossos passos em rede são passíveis de rastreamento. Como podemos navegar pela internet sem sermos espionados ou termos

[6]A sigla PGP do inglês Pretty Good Privacy (privacidade bastante boa) refere-se a um programa de encriptação de chave pública, criado num padrão confiável de trocas de informações, usado por Edward Snowden em comunicação com Gleen Greenwald, por ocasião das denúncias de Snowden, publicadas no The Guardian por Greewald, com revelações sobre os programas de vigilância global dos Estados Unidos (NSA), em junho de 2013.
[7]Brasil e Alemanha apresentam proposta contra espionagem na ONU. Disponível em: http://oglobo.globo.com/mundo/brasil-alemanha-apresentam-proposta-contra-espionagem-na-onu-10645353. Acesso em 21 de maio de 2015.

nossos dados roubados? Especialistas apostam na criptografia como saída, por ser um sistema que permite a proteção de dados, em razão do método de "misturar ou codificar a informação, de modo que usuários não autorizados dificilmente consigam entender o significado, e que os destinatários possam reorganizar ou decodificar o material de modo simples" (DERTOUZOS, 1997, p.138).

Até 2013 mal se falava no navegador ou em outros métodos de encriptação, mesmo quando se tratava de comunidades acadêmicas ou mesmo no meio tecnológico. Porém, as revelações sobre o sistema global de vigilância do governo americano, empresas e outros governos, incentivaram a procura por programas baseados em criptografia. Mesmo assim o Tor se tornou alvo de críticas, em razão de apontado como um ambiente facilitador para esconder pedófilos, traficantes, terroristas e comerciantes de armas e drogas. Essa tendência migratória, atraente às organizações criminosas, decorre do novo território ser considerado mais seguro e oferecer menos riscos de serem descobertos.

É preciso ficar atento, por outro lado, quando governos e agências argumentam a contenção de crimes no meio digital. Concordamos que, "a falta de sigilo nas comunicações pode acabar custando à vida ou a liberdade de ativistas pacíficos - por isso, ferramentas como o Tor são tão importantes" (CRUZ *apud* SOUZA, 2014, p.8)[8].

Em defesa da liberdade de comunicação que tem sido ameaçada pela *militarização do ciberespaço*[9], o "navegador cebola" vem garantir que qualquer pessoa, em qualquer lugar do mundo com acesso à internet, possa se comunicar sem limitações e de forma segura, contudo, sabe-se que o Tor: "não é uma tecnologia perfeita, mas é a melhor opção nos dias de hoje" (CRUZ *apud* HOEPERS, 2014, p.8)[10].

A Fundação de Software Livre (FSF), em seu Projeto de utilidade pública de 2011, define o navegador como "um projeto de interesse social", no qual a utilização do *software* Tor permitiu que cerca de 36 milhões de pessoas em todo o mundo

[8]Francisco Brito CRUZ é pesquisador do Núcleo de Direito, Internet e Sociedade da Faculdade de Direito (USP). In: Antônio SOUZA, Abaixo da superfície... (2014), Revista.br. Disponível em: http://issuu.com/nic.br/docs/revista_br_6_site. Acesso em: 19 maio 2015.
[9]Termo é usado por ASSANGE, Julian et. al. Cypherpunks**...** São Paulo: Boitempo Editorial, 2013.
[10]Cristina HOEPERS é analista de segurança sênior e gerente geral do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). In: Antônio SOUZA, Abaixo da superfície... (2014), Revista.br. Disponível em: http://issuu.com/nic.br/ docs/revista_br_6_site. Acesso em: 19 maio 2015.

experimentassem a liberdade de acesso na internet, assegurando-lhes o controle pessoal da privacidade e do anonimato[11].

Apesar de sabermos que um ambiente que assegura o anonimato das pessoas não consegue ficar livre de crimes, e nem por isso deixa de ser importante em conquistas como as dos dissidentes que protagonizaram a "Primavera Árabe". Um dos maiores especialistas em web profunda e investigação de crimes digitais defende o Tor e recomenda "todos nós precisamos aumentar o entendimento disso entre os reguladores, autoridades e governos, além da mídia e da população geral da Internet" (SANTORELLI, 2014, p.10)[12].

Acreditamos em via de mão dupla quando se trata dos percalços da tecnologia: "É possível usar a tecnologia da informação para atacar nossa privacidade, mas também para protegê-la" (DERTOUZOS, 2002, p.135). Ao final nos resta o consolo de que: "informantes de conteúdos, jornalistas, dissidentes ou qualquer um que deseje se esconder em seu anonimato podem livremente navegar pela web profunda para evitar ser rastreado ou ainda esquivar-se de países autoritários" (PAGANINI *apud* SOUZA, 2014, p.8)[13]·. De todo modo, a internet profunda é um ambiente explorado por usuários específicos e com necessidades bem definidas.

DAS CRIPTOGUERRAS AO CASO SNOWDEN

Com o crescimento da comunicação mediada por computadores e a capacidade de governos e empresas armazenarem as informações de países inteiros em grandes servidores, naturalmente, aumentou a necessidade de se comunicar com segurança. Isso tem concorrido para que cientistas, *hackers* e pesquisadores criem novos métodos de comunicação mais livre e segura, com o uso de criptografia. No início dos anos 90, por exemplo, os governos tentaram restringir esse uso às forças armadas e aos governos, o que gerou conflitos acerca do direito à criptografia, conhecidos como criptoguerras.

As investidas dos EUA e de países europeus para controlar o uso da criptografia foram significativas e as tentativas acabaram organizando e unindo usuários da rede em defesa da escrita cifrada como forma de proteger suas comunicações. Desta organização, iniciada em 1992, foi criada uma *mailing lists* (de correspondentes) com a finalidade de

[11]Fundação de Software Livre (FSF). Projeto de utilidade pública 2011. Disponível em: http://www.fsf.org/news/ 2010-free-software-awards-announced. Acesso em: 31 julho 2014.
[12]Steve SANTORELLI é diretor da Team Cymru. In: Entrevista concedida à Revista.br. Disponível em: http://issuu.com/nic.br/ docs/revista_br_6_site. Acesso em: 19 maio 2015.
[13]Pierluigi PAGANINI é especialista em cibersegurança. In: Antônio SOUZA, Abaixo da superfície... (2014), publicada na Revista.br. Disponível em: http://issuu.com/nic.br/ docs/revista_br_6_site. Acesso em: 19 maio 2015.

debater questões como privacidade, monitoramento e controle corporativo de informações.Foram realizadas discussões que envolveram criptografia, matemática, ciências da computação, política, comunicação e filosofia, e outras[14].

O matemático Eric Hughes criou o *Manifesto de um Cypherpunk* (1993), onde combinou várias ideias e discussões acerca do espírito individualista no ciberespaço; contemplou inclusive o uso de criptografias e tratou da necessidade de assegurar a privacidade em uma sociedade, dentre outros assuntos correlatos. As ideias básicas do manifesto são as seguintes:

> A privacidade é necessária para uma sociedade aberta, na era eletrônica. Privacidade não é segredo. Um assunto privado é uma coisa que alguém não quer que o mundo inteiro saiba. Um segredo é uma coisa que alguém não quer que ninguém saiba. A privacidade é o poder de revelar-se seletivamente para o mundo [...]. Não podemos esperar que os governos, corporações e outras grandes organizações nos garantam privacidade como uma espécie de caridade [...]. Devemos defender nossa própria privacidade, se planejamos ter alguma [...]. Cypherpunks escrevem códigos. Nós sabemos que alguém tem que fazer software a fim de defender a privacidade, e como não se pode realmente ter privacidade a não ser que todos a tenham, nós mesmos vamos fazer o software (HUGHES *apud* BERNARDO, 2014, p.3)[15].

De um lado, as agências de governos e, do outro, ativistas e *hackers*. A luta pela comunicação livre estava anunciada e foi assim que os *Cypherpunks* ficaram conhecidos como o grupo que utilizava a criptografia para se comunicar. O conhecimento gerado a partir daí foi compartilhado em fóruns e *mailing lists*. Mais de vinte anos depois das primeiras criptoguerras, documentos secretos da Agência Nacional de Segurança dos EUA, revelados por seu ex-agente, foram divulgados em jornais como *The Guardian*, *Washington Post* e G1.

A segurança da rede Tor e sua oposição aos órgãos de vigilância global e ainda a essa *militarização do ciberespaço* é incontestável. Entendemos ser de extrema importância quando se tem referências como estas a seguir:

> É como ter um tanque de guerra dentro do quarto. É como ter um soldado entre você e a sua mulher enquanto vocês estão trocando mensagens de texto. Todos nós vivemos sob uma lei marcial no que diz respeito às nossas comunicações, só não conseguimos enxergar os tanques – mas eles estão lá (ASSANGE, 2013, p.53).

[14]CRIPTOGRAFIA. In: Wikipédia, a enciclopédia livre. Flórida: Wikimedia Found., 2013. Disponível em: http://pt.wikipedia.org/wiki/Criptografia Acesso em: 19 maio 2015.
[15]Eric HUGHES, Matemático da Universidade da Califórnia, Berkeley. É Considerado um dos fundadores do movimento cypherpunk. In: Felipe BERNARDO, Bruno NASCIMENTO. Cypherpunks: Caminhando por uma estrada orwelliana. Trabalho apresentado no Intercom Regional, XVI Congresso de Ciências da Comunicação na Região Nordeste, realizado na Universidade Federal da Paraíba, João Pessoa-PB, de 15 a 17 de maio de 2014.

Os documentos revelados por Snowden demonstram que a NSA tem o objetivo de quebrar a proteção oferecida pela rede Tor aos seus usuários. Em seus slides, a agência afirma que não obtiveram "nenhum sucesso em revelar a identidade de algum usuário"; a agência NSA considera o Tor como "muito seguro" e ainda, em uma das suas apresentações, chamada de *Top secret*, a agência atribuiu ao navegador o título de *Tor fede*. Nessa podemos ler: "Nunca seremos capazes de revelar a identidade de todos os usuários do Tor..." (RONCOLATO, 2013)[16].

A organização Tor Project se pronunciou sobre as investidas de quebra de protocolo do seu navegador Firefox, no qual o Tor está baseado, dizendo que: "As boas notícias são que eles tentaram explorar falhas no navegador [...], o que significa que eles não podem quebrar o protocolo do Tor ou analisar o tráfego da rede". E acrescenta:

> Infectar o computador ainda é o jeito mais fácil de saber quem está por trás do teclado, mas o Tor ajuda nisso; eles podem explorar falhas de navegação em usuários individuais, mas, se atacarem muitos usuários logo alguém irá notar. Então, nem a NSA pode vigiar todos, em todos os lugares (SOUZA, 2014, p.6-7)[17].

Em resumo, a utilização de *software* antiespionagem se mostra fundamental na privacidade, utilizado por uma grande quantidade de pessoas de diferentes partes do mundo, com intenções das mais nobres e despretensiosas às mais terríveis e ofensivas.

LIBERDADE E VIGILÂNCIA EM REDE

As tecnologias da informação e comunicação, bem como o uso das redes e mídias de compartilhamento como vídeo, *podcast* e *blog*, têm contribuído para ampliar questionamentos político-sociais, ou seja, as junções dessas ferramentas emancipadoras alavancam protestos por todo mundo contra ditaduras, promove, organiza e divulga ideias de comunicação livre. A adoção de novos recursos tecnológicos demonstra as mudanças que alteraram a forma como nos comunicamos. Buscadores como Google, por exemplo, definem o modo como navegamos na web; ou ainda, atualmente, navegar na web profunda tem se mostrado cada vez mais necessário.

Uma questão pode ser levantada: A internet é um lugar de liberdade? Ela "nasceu com o propósito de permitir a livre circulação de informação pela rede. Não havia o

[16]Murilo RONCOLATO. Documentos revelam: NSA não consegue espionar quem usa TOR (2013), matéria publicada na Revista Galileu. Disponível em: http://revistagalileu.globo.com. Acesso em: 19 maio 2015.
[17]Antônio SOUZA, Abaixo da superfície...(2014), matéria publicada na Revista.br. Disponível em: http://issuu.com/nic.br/ docs/revista_br_6_site. Acesso em: 19 maio 2015.

conceito de cibervigilancia e de monitoramento da rede" (PAGANINI *apud* SOUZA, 2014, p 6)[18].

Mas o ciberespaço vem sendo vigiado e controlado por empresas e governos, ou seja, os "novos tipos de comunicação antes privados, agora são interceptados em massa pelo governo ou pelo setor privado onde quer que ele esteja" (ASSANGE, 2013, p.43). A internet livre como conhecemos não existe, ela passou a ser censurada, controlada e manipulada por governos totalitários e também democráticos, o que torna o ciberespaço inseguro para a democracia e a liberdade de expressão.

Se pegarmos alguns países listados pela organização *Repórteres sem fronteiras*[19], veremos o quanto se mostra diversa e global a tentativa de frear a utilização da rede como ferramenta de mobilização na era das *sociedades do conhecimento*[20]·. Conceito que "inclui uma dimensão de transformação social, cultural, econômica, política e institucional [...], preferível ao da "sociedade da informação" já que expressa melhor a complexidade e o dinamismo das mudanças que estão ocorrendo (KHAN *apud* BURCH)[21].

Ou seja, não adianta trocar a privacidade por muita informação sem que seja possível o compartilhamento livre das ideias. Navegar na rede é mais que buscar por informações, as pessoas buscam prazer, diversão, relacionamentos, responsabilidade social ou apenas *besteirol* no Youtube. Porém, essas pessoas devem ter garantido seu direito à privacidade. Tendo preservadas suas preferências sexuais, opiniões, sejam elas quais forem. Segundo a Declaração Universal dos Direitos Humanos, entende a vida privada como um direito humano: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de ataques a sua honra ou reputação. Contra tais intromissões ou ataques toda pessoa tem direito à proteção da lei" (OHCHR.ORG, 2014)[22].

[18]Pierluigi PAGANINI,já referenciado anteriormente. In: Antônio SOUZA, Abaixo da superfície...(2014), publicada na Revista.br. Disponível em: http://issuu.com/nic.br/docs/revista_br_6_site. Acesso em: 19 maio 2015.
[19]ONG, cujo objetivo é defender a liberdade de expressão e informação no mundo. Disponível em: http://en.rsf.org/who-we-are-12-09-2012,32617.html, Acesso em: 21 de maio de 2015.
[20]A noção de "sociedade do conhecimento" (knowledge society) surgiu no final da década de 90. É empregada, particularmente, nos meios acadêmicos como alternativa que alguns preferem à "sociedade da informação". Sally BURCH, Sociedade da informação/ Sociedade do conhecimento. Disponível em: http://vecam.org/archives/article 519.html. Acesso em: 23 de maio de 2015.
[21]Abdul Waheed KHAN é subdiretor-geral de Comunicação e Informação (UNESCO). In: Sally BURCH, Sociedade da informação/ Sociedade do conhecimento. Disponível em: http://vecam.org/archives/article519.html Acesso em: 23 de maio de 2015.
[22]Artigo 12º da Declaração Universal dos Direitos Humanos adotado pela Assembléia Geral das Nações Unidas. Disponível em: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf. Acesso em: 9 julho de 2014.

Ao contrário disso, o que ocorre é uma interceptação em massa de qualquer forma de comunicação em rede. E quem deveria garantir e zelar pela privacidade está infiltrado, sobretudo nas redes sociais, estas que se tornaram espaços de vigilância mais fáceis e até aceitos - de certo modo inconsciente - por quem utiliza para se relacionar com a família, amigos e colegas de trabalho.

Tendo em vista a sociedade da informação sujeita a esse espaço de vigilância, podemos dizer que o direito à privacidade não está disponível na rede, é preciso perceber que até estamos preocupados com a segurança dos nossos dados, mas pouco sabemos o que fazer para nos proteger.

As revelações de Snowden apontam para o interesse por parte dos governos e das empresas em monitorar o ciberespaço, não se limitando a seguir rastros de terroristas, empresas ou políticos, na verdade, todos estão sob a mira da vigilância ao utilizar internet, celular, serviços bancários, games, etc. Na divisão dos papéis para Assange (2013), a *privacidade* é para os fracos e a *transparência* para os poderosos. Perdemos todos cada vez mais a privacidade e agora sabem mais sobre nós do que nós mesmos.

Com justificativa ou não, direito ou não, o combate ao crime virtual não pode transformar todos em terroristas, desse modo, conforme diz Agamben (2015)[23], todo cidadão será visto como um terrorista potencial. O ciberespaço está se tornando um ambiente armado, assim como as forças armadas entram em combate em qualquer lugar do mundo, elas estão agora em confronto com a privacidade e na disputa por nossas informações.

A criptografia é hoje uma ferramenta utilizada por pequenas comunidades, mas isso não vai perdurar por muito tempo e, de certo, irá se tornar ampla conforme as futuras necessidades de se manter a privacidade e combater a vigilância. Assim que a maioria de nós perceber que não existe comunicação, privacidade e segurança sem risco, novas medidas de segurança criptográficas irão surgir, bem como o surgimento progressivo de novos dispositivos e objetos conectados à internet, exigirão o conhecimento das sociedades sobre os riscos da vigilância global.

[23]Como a obsessão por segurança muda a democracia. Disponível em: http://www.diplomatique.org.br/artigo.php?id=1568. Acesso em: 17 maio 2015.

ACESSO À REDE TOR

Será preciso distinguir *software* Tor, rede Tor, Tor Project e usuário Tor? Acreditamos que não. Contudo é interessante atentar para a semelhança ortográfica entre os nomes "Tor"[24] e deus "Thor", este último decorre da anglicização do antigo nome nórdico "pórr" da era viking no século XVII. Pode-se dizer que, a proximidade entre os termos agrega sentidos mitológicos ao Tor *browser*, em razão dos atributos do deus Thor, a seguir: grande em sua honestidade e repugnância contra o mal, ele usa um martelo de guerra mágico, segurado por luvas de ferro também mágicas, e usa ainda um cinturão que aumenta sua força em até dez vezes, resultaque munido desse instrumental derrotou gigantes, *trolls*, monstros, *berserker* e feras.

O navegador Tor atrai expectativas com a promessa de garantir a segurança das comunicações, em razão de seus poderes em saltar em torno de uma rede distribuída por relés de proteção, que pode ser executada ao redor do mundo. Assim como o deus Thor, ele também tem grandes poderes e procura salvaguardar a informação livre da censura e vigilância. O *software* Tor encontra-se disponível para os principais sistemas operacionais, pode ser usado no Windows, Mac OS X ou Linux, não sendo necessária a sua instalação.

Para utilizar este navegador, primeiramente, é preciso acessar o site Tor Project[25] e fazer o *download* (Fig.1), do programa e executá-lo. O navegador Tor funciona através de protocolo da internet que encaminha pacotes entre cliente-servidor por meio de servidores como *proxy socks 5*, fornecendo um servidor *bind* que, em geral, na porta (9050) local da máquina.

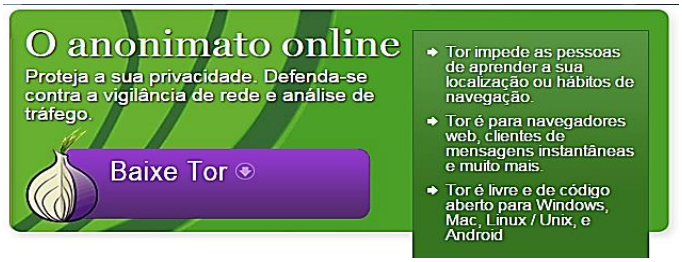

Figura 1 - *Download* da ferramenta Tor
Fonte: *Print screen* do site do Tor Project.

[24]O termo "Tor" remete ao acrônimo "The Onion Router" (roteador cebola), a alusão refere-se ao lado oculto das cascas da cebola. Disponível em: http://en.wikipedia.org/wiki/Tor_(anonymity_network). Acesso em: 31 março 2014.
[25]O site do Tor Project é de fácil utilização e bem orientado. Disponível em: https://www.torproject.org. Acesso em: 4 março 2015.

Em seguida, os programas *web browser*, *emule* etc., devem ser configurados para usar o servidor *proxy*, apontado para o endereço localhost (127.0.0.1). Depois de configurado, o navegador roteará o tráfego do computador através dos túneis *HTTP* da rede Tor até seu destino, cada vez que alguém se conectar irá receber um novo endereço IP (*Internet Protocol*)[26].

Desse modo, o navegador Tor previne a vigilância nas conexões e impede formas de monitoramento na sua localização e ainda que sejam identificados quais sites você visita. O endereço informado será o de algum cliente-servidor (voluntário) da rede, na ocasião de sua saída da rede Tor para a rede da web da superfície. O tráfego é roteado por vários nós da rede, o que deixa o acesso lento e desse modo com endereços de IP aleatórios, graças à topologia caótica da rede Tor.

O próximo passo é a execução do mesmo, o programa mostra o navegador que o usuário utiliza para acessar a rede, um *browser* de internet pré-configurado (Firefox ESR). Quando ele é iniciado, o *software* abre o navegador modificado e um painel de configuração e ao iniciar a conexão, uma tela de boas-vindas é mostrada e um link onde pode encontrar seu endereço de IP (Fig.2). Após isso, o usuário pode navegar na rede Tor.

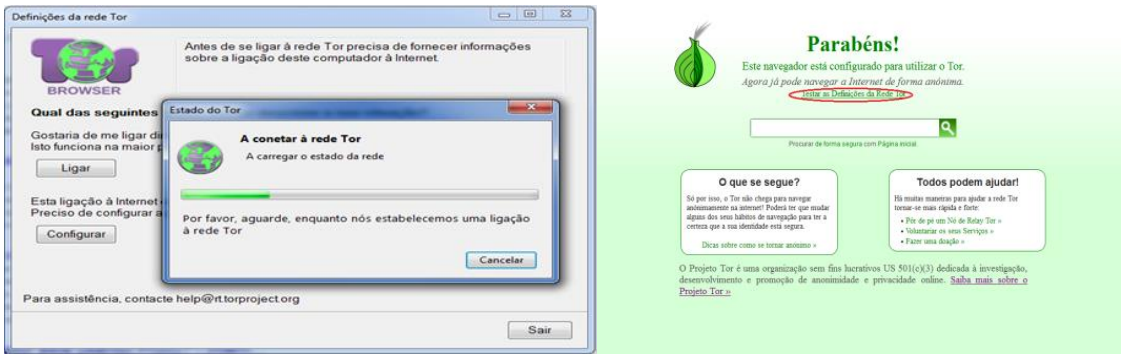

Figura 2- Configuração e página inicial do Tor *browser*.
Fonte: *Print screen* durante os testes.

Geralmente quando fazemos o acesso a um site na web de superfície, o servidor desse site identifica o IP de quem o acessou, mas no Tor isso não acontece, pois, antes que a requisição chegue ao servidor, ele inicia uma ponte criptografada (PEREIRA, 2012) e isso garante o anonimato da rede. A ferramenta Tor utiliza essa ponte criptográfica, que consiste em saltar por vários nós da rede antes de chegar a seu destino, o que faz com que a identificação do usuário seja maquiada.

[26]Internet Protocol (IP) é o número de identificação de qualquer dispositivo em rede (computador, celular, impressora, roteador, etc.). O usuário não pode escolher o endereço final de IP na rede Tor e consequentemente a sua localização geográfica.

O navegador em si não garante o anonimato ao se ligar a rede, utilizando o Tor é importante salientar que não estamos livres da vigilância, acessar alguns serviços como Facebook e emails fragiliza a blindagem do navegador. Qualquer usuário pode de alguma maneira estar sendo rastreado pela Polícia Federal, FBI ou NSA. Um exemplo ocorreu no caso da prisão do operador da Freedom Hosting[27], *Eric Eoin Marques* - considerado pelo FBI um facilitador de conteúdo sobre pedofilia-, preso em 2013, quando o FBI explorou uma vulnerabilidade do Firefox 17.0 e conseguiu capturar informações acerca do criminoso (ROHR, 2013).

É preciso ter cautela ao usar o Tor, principalmente ao acessar a *deep web* já que o anonimato atrai diferentes tipos de usuários, os quais utilizam a rede por motivações diversas até as repulsivas como a pedofilia. Mas não é apenas o Tor que dá acesso a *deep web*, outros navegadores[28] como o I2P e o Freenet também são populares, além de navegadores o sistema Linux em razão da sua forte segurança. De qualquer modo, o Tor *browser* permanece sendo o mais popular por deixar "invisível" o usuário[29].

ACERCA DA MÁ FAMA DO TOR

As acusações de que a rede Tor é um ambiente propício para pedófilos, ladrões, terroristas, traficantes e comerciantes de armas, e ainda empresários mal intencionados, constituem algumas das críticas atribuídas ao Tor *browser*, em parte elas podem tentar alardear uma má fama para tentar coibir o uso deste navegador e de outras ferramentas criptográficas. Mas há sempre quem aponte um grupo mais amplo de usuários da rede Tor, entre os quais estão jornalistas e veículos de comunicação, ativistas, profissionais da lei, empresas, executivos, *blogueiros*, profissionais de tecnologia da informação, políticos, governos, forças armadas, e outros.

O ambiente da rede Tor[30] dribla sociedades com regimes de governos totalitários e repressores, ancorados em leis que proíbem o acesso a informações sobre AIDS, controle de natalidade, religião, mídias e redes sociais, desse modo, seu usuário é

[27]Altieres ROHR. FBI prende operador...(2013).*Freedom Hosting* era um serviço de hospedagem especializada em oferecer serviços para criar sites secretos dentro da rede Tor. Disponível em: http://g1.globo.com/tecnologia/noticia/2013/08/fbi-prende-operador-de-servicos-ocultos-na-rede-anonima-tor.html. Acesso em: 19 março 2015.
[28]A I2P é uma rede de sobreposição anônima e a *Freenet* é um software livre que permite compartilhar arquivos anonimamente, navegar, publicar e conversar em fóruns sem censura. *Freenet* se utilizado no modo "*darknet*", onde os usuários se conectam apenas com seus amigos, é muito difícil de detectar. Disponíveis em: https://geti2p.net/pt-br/ e https://freenetproject.org/whatis.html. Acessos em: 27 de fevereiro de 2015.
[29]A primeira e a mais conhecida camada da *deep web* é a "*Onion*", ela possibilita aos usuários navegar de forma segura, onde todas as informações são criptografadas e o acesso é permitido na utilizando o programa Tor.
[30]*The Tor Project* foi lançado em 20 de setembro de 2002 e até hoje a autoria de criação do Tor (*The Onion Router*) não é consensual, alguns dizem que foi criado pelo governo dos EUA.

favorecido pela proteção através topologia da rede[31]. Alguns ativistas, por exemplo, fazem uso deste navegador e de PGP para denunciar crimes, abusos, manter contato com jornalistas, alimentar a rede com fotos, *podcasts*, vídeos, *blogs*, manuais e relatos sobre atentados e confrontos.

Empresas usam este navegador para pesquisas de concorrência, com o propósito de preservar estratégias de negócio; bem como pessoas sem vínculo empresarial ou organizacional, mas com motivações e vínculos estritamente pessoais, também fazem uso da rede Tor para manter suas conversas entre parentes e relacionamentos em sigilo. Em se tratando de um navegador ainda envolto a especulações de toda ordem, muito mais por falta de conhecimento e de experiência de navegação, ao que tudo indica, do que por razões concretas de se constituir em uma ameaça social.

Existe uma discussão frágil, pode-se dizer sobre alguns aspectos considerados essenciais à comunicação, quase sempre imersos a críticas quando, por exemplo, está em jogo o direito à mídia livre, ao contra poder midiático. São recorrentes expressões como: Isso não é errado? Não é do mal? É uma ameaça aos meios de comunicação? Os autores desta comunicação, por sua vez integram o curso de Comunicação em Mídias Digitais (DEMID/UFPB) e, por isso mesmo, optaram por se afastar dos "palpites" e encaminhar questões para verificar suas impressões, recorremos então a uma consulta feita a alunos e professores do nosso curso[32].

Três perguntas nortearam a nossa consulta: 1. Conhece o navegador Tor? 2. Já utilizou o navegador Tor? 3. Você se preocupa com sua privacidade na internet? A sondagem serviu para constatar que existe desinformação sobre o Tor *browser*, mesmo em um curso voltado para as mídias digitais[33]. Por outro lado, além de estarmos falando de uma ferramenta nova, a questão a ser apreciada não se pauta na mera constatação da "desinformação", ela é mais ampla e atrai a complexidade de "necessidades" corporativas, governamentais, ativistas, e até mesmo de interesse estritamente pessoal, as

[31]*Firewall* é um software (ou hardware) que de acordo com sua configuração pode identificar informações vindas de uma rede ou da internet, e assim bloquear ou permitir que a mensagem chegue ao computador.
[32]A consulta foi feita por Felipe Bernardo, aluno do 6º período de Comunicação em Mídias Digitais, realizada em ambiente acadêmico, com alunos e professores do Departamento de Mídias Digitais (DEMID/UFPB), no período de 18 a 26 de março de 2015. Essa sondagem prévia teve por objetivo fornecer subsídios para o trabalho de conclusão de curso (TCC–Prático), a ser desenvolvido por Felipe Bernardo e Andrélia Santos, sob a orientação da professora Nadja Carvalho.
[33]Ressaltamos que este resultado não se deve a um grupo de pessoas com perfil de iniciantes, inclusive o curso Comunicação em Mídias Digitais recebeu nota máxima, atribuída recentemente pelo MEC (18 de maio de 2015), em avaliação de reconhecimento, não há dúvidas de que sua equipe esteja bem aparelhada acerca de informações atuais da área.

quais necessariamente não se coadunam com a política de transparência de alguns setores públicos, envolvidos com a educação e pesquisa.

Em nossa sondagem exploratória não recolhemos dados acerca do perfil do usuário da rede Tor, a nossa motivação foi saber se de fato ele existia, e se usava a rede em favor da sua privacidade, ao final, 59 pessoas responderam ao questionário, dentre elas 55 alunos e 04 professores, conforme pode ser observado em quadro comparativo das três perguntas (Fig. 3).

QUESTÕES	SIM	NÃO
1. Conhece o Tor?	47%	53%
2. Já utilizou o Tor?	16%	84%
3. Preocupa-se com sua privacidade?	88%	12%

Figura 3– Quadro comparativo de resultados
Fonte: Confecção com base em consulta feita por Felipe Bernardo (2015).

Embora a maioria desconheça a existência do Tor *browser*, ainda assim, há um pequeno percentual (apenas 3%) entre os que conhecem e aqueles que desconhecem. Não há uma total falta de informação sobre este *browser*, por outro lado, dos 47% que conhecem não se pode esperar que, em sua maioria, utilizem o navegador ou que tenham interesse em se proteger, seja por considerar não ter nada a esconder ou mesmo por não ser necessário em suas atividades de estudo e pesquisa.

Há um elevado percentual de não utilização do Tor *browser*, um total de 84% que nunca utilizou, contra 16% que já navegou na rede Tor. Observa-se que, independente do grau de conhecimento que eles possam ter, poucos são os que navegam com o Tor *browser*. Já acerca da preocupação com a privacidade, um total de 88% afirmou se preocupar e apenas um total de 12% disse não se preocupar, ou seja, embora a maioria esteja preocupada, na prática um reduzido número de pessoas utiliza o Tor *browser*. Há de se observar em sondagem subsequente[34], quais são as motivações daqueles que usam o navegador e, por outro lado, também interessa saber o que tem impedido uso do Tor *browser* entre os que consideraram importante a privacidade de suas comunicações.

[34]Com a aplicação de um questionário mais amplo, constituído por perguntas abertas e fechadas, retomaremos a mesma amostra de alunos e professores já pesquisados para reverter dados importantes, com o propósito de ajudar na confecção de material informativo (Manual do Tor browser) para atender a exigências de Trabalho de Conclusão de Curso (TCC), no curso de Comunicação em Mídias Digitais da UFPB, a ser realizado em 2016.

CONSIDERAÇÕES

A vigilância política de grandes potências faz uso de tecnologias para ameaçar a privacidade de práticas democráticas e desestabilizar a diplomacia de governos com interesses comerciais em competição. É natural que, o combate a esse tipo de investida de natureza política e comercial lance mão de tecnologia para coibir o monitoramento e ocultar os passos em rede, proteger as comunicações; também é necessário promover debates e realizar protestos que permitam a organização de movimentos sociais, que sejam respeitados os interesses da população contra atos de governos totalitários, os quais impõem restrições ao acesso de conteúdos, sites, redes sociais, etc.

Dessa forma, entendemos que a utilização de ferramentas encriptadas pode possibilitar experiências livres de comunicação e avançar em práticas de liberdade de expressão, tão importantes para o exercício de cidadania. Assim, o uso do navegador Tor não deveria ser uma exceção, mas uma regra. O que ainda não acontece por ser muito recente e pouco divulgado, mas se a criptografia tem resistido e cada vez mais tem difundido sua bandeira de informação livre, e, hoje mais que nunca, ela está viva mesmo com o mundo correndo o risco de se tornar uma grande estrada *Orweliana* por se conectar de qualquer forma.

REFERÊNCIAS

AGAMBEN, Giorgio. **Como a obsessão por segurança muda a democracia**. Disponível em: http://www.diplomatique.org.br/artigo.php?id=1568. Acesso em: 06 de abril de 2015.

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

BERNARDO, Felipe; NASCIMENTO, Bruno. **Cypherpunks:** Caminhando por uma estrada orwelliana. Trabalho apresentado no Intercom Regional, XVI Congresso de Ciências da Comunicação na Região Nordeste, realizado na Universidade Federal da Paraíba, João Pessoa-PB, de 15 a 17 de maio de 2014. Disponível em: http://www.portalintercom.org.br/anais/nordeste2014/resumos/R42-0055-1.pdf. Acesso em: 23 de maio de 2015.

BURCH, S. **Sociedade da informação/ sociedade do conhecimento.** In: AMBROSI, A.; PEUGEOT, V. & PIMIENTA, D. (coord.) Desafios de Palavras: Enfoques Multiculturais sobre as Sociedades da Informação. França: C&F editions, 2005.

CRIPTOGRAFIA. In: **Wikipédia**, a enciclopédia livre. Flórida: Wikimedia Found., 2013. Disponível em: http://pt.wikipedia.org/wiki/Criptografia. Acesso em: 19 de maio de 2015.

CYPHERPUNK. In: **Wikipédia**, a enciclopédia livre. Flórida: Wikimedia Found, 2013. Disponível em: http://en.wikipedia.org/wiki/Cypherpunk. Acesso em: 31de março de 2014.

DERTOUZOS, Michael Leonidas. **A revolução inacabada**. São Paulo: Futura. 2002. Disponível em: http://revistagalileu.globo.com/Revista/Common/0,, EMI343793-17770,00-DOCUMENTOS+REVELAM+NSA+NAO+CONSEGUE+ESPIONAR+QUEM+USA+TOR. html. Acesso em: 19 maio 2015.

_____, Michael Leonidas. **O que será**: como o novo mundo da informação transformará nossas vidas. São Paulo: Companhia das Letras, 1997.

FSF. **Projeto de Utilidade Pública 2011**. Disponível em: http://www.fsf.org/news/ 2010-free-software-awards-announced. Acesso em: 31de julho de 2014.

HUGHES, Eric. **A cypherpunk's manifesto**. Berkeley, 1993. Disponível em: http://www.activism.net/cypherpunk/manifesto.html. Acesso em: 31 de março de2014.

OHCHR, **Declaração universal dos direitos humanos 2014**. Disponível em: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf. Acesso em: 22 de julho de 2014.

PEREIRA, L. 2012, "**Deep web**: saiba o que acontece na parte obscura da internet", Disponível em: http://olhardigital.uol.com.br/noticia/deep-web-saiba-o-que-acontece-na-parte-obscura-da-internet/31120, Acesso em: fevereiro 2014.

ROHR, A. **FBI prende operador de serviços ocultos na rede anônima Tor.** Disponível em: http://g1.globo.com/tecnologia/noticia/2013/08/fbi-prende-operador-de-servicos-ocultos-na-rede-anonima-tor.html. Acesso em: 19 de março de 2015.

RONCOLATO, Murilo. **Documentos revelam: NSA não consegue espionar quem usa TOR**. A agência norte-americana tenteou, mas não conseguiu revelar identidades de quem navega anonimamente usando o protocolo. In: Revista Galileu, postagem em: 10 de outubro de 2013.

RSF, **Quem nós somos**. Disponível em: http://en.rsf.org/who-we-are-12-09-2012,32617.html. Acesso em: 21 de maio de 2015.

SIMONS, Jake Wallis. **A rede tem estado implicada em centenas de casos de fraude, roubos de identidade e pedofilia.** A Marinha dos Estados Unidos continua a garantir a maior parte do seu financiamento (Postado em 19 de outubro de 2014). Disponível em: http://www.publico.pt/ tecnologia/noticia/a-rede-secreta-1673221. Acesso em: 19 maio 2015.

SOUZA, Antônio. **Abaixo da superfície:** Escândalo de espionagem dos EUA aumenta interesse por web profunda, fora do alcance dos abutres buscadores. In: Revista.br- Publicação do Comitê Gestor da Internet no Brasil. Ano 05, Edição 06, 2014. Disponível em: http://issuu.com/nic.br/docs/revista_br_6_site. Acesso em: 19 de maio de 2015.

TOR (Anonymity Network) In: **Wikipédia**, a enciclopédia livre. Flórida: Wikimedia Found. 2013. Disponível em: http://en.wikipedia.org/wiki/Tor_(anonymity_network). Acesso em: 31 de março de 2014.