**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ**
**DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO**
**DEPARTAMENTO ACADÊMICO DE ELETRÔNICA**
**CURSO DE ESPECIALIZAÇÃO EM REDES DE COMPUTADORES E TELEINFORMÁTICA**

**DILMAR JOSÉ KOZAKIEWICZ**

# DEEP WEB E SEGURANÇA DA INFORMAÇÃO: UMA ANÁLISE E SEUS IMPACTOS NA SOCIEDADE E NAS ORGANIZAÇÕES

**MONOGRAFIA DE ESPECIALIZAÇÃO**

**CURITIBA**
**2018**

**DILMAR JOSÉ KOZAKIEWICZ**

# DEEP WEB E SEGURANÇA DA INFORMAÇÃO: UMA ANÁLISE E SEUS IMPACTOS NA SOCIEDADE E NAS ORGANIZAÇÕES

Monografia de Especialização, apresentada ao Curso de Especialização em Redes de Computadores e Teleinformática, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Esp. Douglas Eduardo Basso

**CURITIBA**

**2018**

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização em Redes de Computadores e Teleinformática

# TERMO DE APROVAÇÃO

DEEP WEB E SEGURANÇA DA INFORMAÇÃO: UMA ANÁLISE E SEUS IMPACTOS NA SOCIEDADE E NAS ORGANIZAÇÕES

por

DILMAR JOSÉ KOZAKIEWICZ

Esta monografia foi apresentada em 10 de Julho de 2018 como requisito parcial para a obtenção do título de Especialista em Redes de Computadores e Teleinformática. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Esp. Douglas Eduardo Basso
Orientador

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Membro titular

_____
Prof. M.Sc. Danillo Leal Belmonte
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

## RESUMO

KOZAKIEWICZ, Dilmar José. **Deep Web e segurança da informação: uma análise e seus impactos na sociedade e nas organizações**. 2018. 51 f. Monografia de Especialização em Redes de Computadores e Teleinformática, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

Este trabalho busca mostrar a presença cada vez mais intensa das redes em nossas vidas. Traz uma discussão sobre a internet obscura, em como ela pode ser usada tanto para bem quanto para o mal e a segurança que ela nos proporciona quando se fala de privacidade. Através de pesquisa qualitativa, usando como fonte principal a própria rede, buscou-se mostrar como esse tema traz mudanças nas nossas vidas, nas organizações e na sociedade em geral. Busca também mostrar características da internet aberta e da Deep Web, esta como sendo uma alternativa para a privacidade, mas também como ambiente propício para ações ilícitas. O tema “Deep Web” em si é dinâmico e pouco se encaixa nas literaturas de redes já consagradas; é um assunto em constante atualização. Através das fontes levantadas buscou-se também fazer uma análise dedutiva do que se espera com evolução natural ou lógica sobre tudo o que envolve o assunto. Também trata-se sobre o tema Segurança da Informação, estabelecendo um paralelo da informatização das empresas com o advento das redes e seu crescimento. E finalmente deixar como legado uma discussão, que acredita-se ainda não ter chegado a um termo, sobre o que se aguarda no futuro, quando referir-se ao estado da arte da informática e o que ela abrange: redes, anonimato, segurança e privacidade.

**Palavras-chave**: Deep Web. Redes Anônimas. Internet.

## ABSTRACT

KOZAKIEWICZ, Dilmar José. **Deep Web and information security: an analysis and its impacts on society and organizations**. 2018. 51 f. Monografia de Especialização em Redes de Computadores e Teleinformática, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

This work seeks to show the increasingly intense presence of networks in our lives. It brings a discussion about the obscure internet, how it can be used for both good and evil, and the security it gives us when it comes to privacy. Through qualitative research, using as its main source the network itself, we sought to show how this theme brings changes in our lives, in organizations and in society in general. It also seeks to show characteristics of the open internet and the Deep Web, as an alternative to privacy, but also as an environment conducive to illegal actions. The theme "Deep Web" itself is dynamic and hardly fits the literatures of already established networks; is a subject constantly updated. Through the raised sources we also sought to make a deductive analysis of what is expected with natural or logical evolution on everything that involves the subject. We also deal with the issue of Information Security, establishing a parallel of the computerization of companies with the advent of networks and their growth. And finally leave as a legacy a discussion, which we believe has not yet come to a term, about what awaits us in the future, when we refer to the state of the art of information technology and what it covers: networks, anonymity, security and privacy.



**Keywords**: Deep Web. Anonymous Networks. Internet.

## LISTA DE FIGURAS

## LISTA DE SIGLAS

| | |
|---|---|
| CIA | *Central Intelligence Agency* |
| DNS | *Domain Names System* |
| HTML | *HyperText Markup Language* |
| HTTP | *HyperText Transfer Protocol* |
| ISP | *Internet Service Provider* |
| LAN | *Local Area Network* |
| OSI | *International Organization for Standardization* |
| RH | Recursos Humanos |
| TCP/IP | *Transmission Control Protocol / Internet Protocol* |
| TOR | *The Onion Routing* |
| www | *world wide web* (teia ou rede) |

**SUMÁRIO**

# 1 INTRODUÇÃO

Atualmente tudo o que se faz, ou pelo menos boa parte, nos ambientes de trabalho, lazer, estudo ou pesquisa, tem a informática e redes como pano de fundo. Tudo o que se registra e interage tem um computador ou algum processamento que se conecta com uma rede. E toda essa vida virtual, ou vida no espaço virtual, carrega informações e deixa rastros. Isso exige um cuidado especial com detalhes de coisas que não se dá muita atenção, mas que se não forem tratadas adequadamente, podem trazer muitos transtornos.

## 1.1 CONTEXTUALIZAÇÃO

Ao lidar com informações e dados sensíveis deve-se ter especial atenção com coisas como autenticações de usuário e senha, informações de documentos, dados relativos às rotinas e sites que costuma-se visitar. Tem-se a tendência cada vez maior de registrar as informações nos computadores e dispositivos. E ainda esses repositórios de dados estão em locais físicos distantes das próprias casas e escritórios, ou seja, servidores distantes fisicamente. E o que no meio de todos esses computadores e dispositivos eletrônicos possibilita tudo isso? As redes.

## 1.2 PROBLEMA

Hoje em dia tudo está conectado à grande rede que é a internet; desde os computadores pessoais, celulares e até as televisões. Isso deixa um rastro que pode ser registrado. Registro esse que pode ser usado para fins comerciais, políticos, censura e até repressão, dependendo do pais onde a pessoa vive. Com isso a necessidade de privacidade e mesmo anonimato é importante em alguns cenários. Este trabalho aborda esse aspecto na necessidade real de privacidade e anonimato (ABREU; NICOLAU, 2014).

Os recursos de tecnologia tanto podem ser usados para o bem quanto para o mal. Em um local de anonimato também podem se proliferar ações de pessoas de má índole, tendo como objeto coisas ilícitas e ações à margem da lei. Se a *Deep Web* é um local onde a segurança de privacidade é bem vista para pessoas que dela necessitam, também existe o outro lado da moeda, ou seja, pessoas que fazem mal uso desses ambientes anônimos para prática de seus delitos (MARCON; DIAS, 2014).

> "[...] 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 [...]" (CALDERON, 2014)

## 1.3 OBJETIVOS

Nesta seção são apresentados os objetivos geral e específicos do trabalho, relativos ao problema anteriormente apresentado.

### 1.3.1 Objetivo Geral

*Deep Web*, segurança da informação e análise dos seus impactos na sociedade e nas organizações traz uma discussão de um tema específico, que é a *Deep Web*, ou internet obscura, e o que ela influencia e impacta na sociedade, nas organizações e até governos. Esse tema para um leigo ou pessoa ainda pouco informada pode trazer ideias e conclusões incompletas e até erradas. Por isso há a necessidade de se estudar e debater o tema.

### 1.3.2 Objetivos Específicos

O motivo deste trabalho é trazer à luz do conhecimento tema tão importante quanto misterioso, pois até existe uma boa divulgação na internet, em vídeos, matérias e artigos livres, mas sempre deixam um ar de mistério. Muito se fala da *Deep Web* como um local obscuro e fora da lei somente; mas nada mais injusto e preconceituoso. Existe o lado bom que justifica a existência desta rede. Nela estão envolvidas questões polêmicas como divulgação de informações censuradas pelos governos. Isso é do nosso interesse, como sociedade, porque causa algum impacto trazendo a luz do público assuntos que dificilmente os governos revelariam ou admitiriam. Facilita a segurança e privacidade para algumas atividades profissionais importantes, como jornalistas e ativistas políticos contrários a regimes autoritários.

## 1.4 JUSTIFICATIVA

O trabalho foi desenvolvido a partir de uma ideia inicial e linha principal de explorar como funciona a arquitetura da *Deep Web*, na sua versão atual mais famosa

que hoje se chama *TOR - The Onion Router* (a rede “cebola”, ou rede em camadas). Também serão rapidamente citadas outras redes anônimas que existem, mas que não são tão famosas e abrangentes como o Projeto TOR. Junto com o TOR existe também o seu navegador mais usado que tem o mesmo nome, e foi desenvolvido pela Mozilla, mesma empresa que desenvolveu o navegador Firefox. Será mostrado também como funciona na prática o navegador TOR com alguns exemplos.

## 1.5 ESTRUTURA DO TRABALHO

Para elaboração deste trabalho foram desenvolvidos os temas conceituais com o apoio de bibliografia em forma de trabalhos acadêmicos, mas não somente, que abordam assuntos como segurança da informação, que está relacionada ao tema.

No capítulo 2 foi procurado dar uma noção do que são redes de computadores e como as informações trafegam a partir delas, desde as redes locais, as intranets, até a interligação com redes geograficamente separadas, alcançando assim qualquer lugar do mundo através da internet aberta. Foi falado inicialmente também sobre a *Deep Web* e aspectos de segurança da informação.

O capítulo 3 explica com mais detalhes os conceitos da *Deep Web* e suas características, sua arquitetura e funcionamento. Trata de como ela fornece o anonimato, suas consequências e benefícios.

O capítulo 4 traz informações do que são redes anônimas com dois exemplos de redes anônimas. Também já nos apresenta o projeto da rede TOR - *The Onion Routing*, que é a responsável por possibilitar a *Deep Web*.

O capítulo 5 trata do aspecto negativo do uso da *Deep Web* e do anonimato em que pessoas mal-intencionadas fazem uso. Foram citados crimes virtuais cometidos nesse ambiente.

O capítulo 6 traz como exemplo de uso prático o navegador mais usado na *Deep Web*, com documentação e explicações sobre o projeto TOR e seu navegador que leva o mesmo nome.

Foram usadas pesquisas todas *online* direto nos sites do Projeto Onion. Ora, em se tratando assunto de rede e internet, nada melhor do que usar o próprio ciberespaço para realizar as pesquisas. As demais referências dos assuntos apontados foram pesquisadas em locais diversos, como sites de notícias mais

famosos ou conceituados, para que o trabalho tenha mais credibilidade quanto às suas fontes.

Finalmente nas considerações finais, foi sugerido o que se espera deixar como legado com esse estudo, porque é importante estudar e dar atenção a esse tema: o porquê da importância e popularidade das redes anônimas.

## 2 SEGURANÇA DA INFORMAÇÃO, DEEP WEB E REDES

Segurança da informação é algo essencial para a vida das empresas hoje em dia. Principalmente para que sua atuação, e consequentemente sobrevivência no mercado, não seja comprometida.

Para quem não sabe muito bem o que isso significa, é a proteção das informações sensíveis que a empresa produz ou tem sob seu domínio. Pode parecer para o leigo que pouco importa ver um fluxo de vendas que uma empresa realizou em determinada época do ano. Mas para os concorrentes dessa empresa, isso pode revelar informações preciosas. Com o mundo digitalizado de hoje em dia, isso pode ser muito fácil de conseguir.

As informações dentro de uma empresa podem ter níveis de importância diferenciados, desde dados menos importantes quanto os mais sigilosos. Saber o fluxo de vendas é uma coisa, mas saber qual carteira de clientes ou mesmo os planos de atuação no mercado tem importância mais forte. O que dirá então de informações como propriedade intelectual ou pesquisas que se traduzem em patentes ou produtos novos? Mas vale a pena lembrar também que algumas informações são de acesso público, pois devem atender às exigências das legislações específicas.

Fazendo essa descrição inicial do que é informação para uma empresa, será também abordado um pouco sobre a segurança e a forma como a informação é guardada e manipulada.

Hoje em dia tudo está baseado em tecnologia de informática ou sistemas computacionais. Para os mais jovens pode parecer que a tecnologia como conhece-se sempre existiu, mas isso não é verdade. Se for utilizada a geração que entrou no mercado de trabalho até mais ou menos antes dos anos de 1990, o acesso público aos primeiros computadores e sistemas que era ainda muito restrito. A capacidade dos primeiros PCs que começaram a entrar nos lares era muito limitada. As linguagens de programação eram de baixo nível, como se diz no jargão de informática. Não existia ainda as interfaces gráficas que dominam os sistemas operacionais e aplicativos.

É necessário fazer essa ligação da “pré-história” da informática com a maturidade ou estado da arte que tem-se hoje em dia no tocante à tecnologia da informação. A coisa evoluiu mais ou menos do termo “tecnologia da informática” ou simplesmente “informática” para “TI - Tecnologia da Informação”. É um termo mais abrangente que coloca tudo num mesmo conceito que envolve *software*, *hardware*,

redes, serviços, tele atendimento, entre outros. Antes do domínio dos computadores o que tinha-se eram sistemas de trabalho desenvolvidos, mas sem o processamento e registro informatizados, ou seja, era tudo feito à mão.

## 2.1 SEGURANÇA DA INFORMAÇÃO

Toda empresa deve ter bem definida, com os seus colaboradores, uma política de segurança da informação, estabelecendo ações e cuidados no que diz respeito a dados de usuários e senhas, engenharia social, aspectos legais na manipulação e guarda da informação, propriedade da informação, uso de recursos computacionais, etc. São estratégias importantes para evitar que o seu bem mais precioso, a informação, seja roubada. Isso vale tanto para o nosso local de trabalho como a própria casa com as respectivas informações pessoais.

Não existe uma única solução técnica que consiga solucionar todos os problemas. O que funciona na prática são várias ações estratégicas combinadas para diminuir ao máximo os riscos às informações corporativas e pessoais.

A segurança da informação se promove principalmente com o desenvolvimento de uma cultura dentro das organizações com as pessoas. Estabelecer criptografias, senhas fortes, análise de tráfego, cuidado com programas suspeitos baixados em anexos de *e-mails,* são ações seguras. Mas nada disso tem valor se o usuário final é descuidado com a sua segurança digital pessoal (ARRUDA, 2011).

## 2.2 SEGURANÇA DE INFORMAÇÃO CORPORATIVA

Antes de falar mais da internet em si e *Deep Web*, é necessário falar da segurança da informação dentro de uma organização. Em uma estrutura organizacional há a divisão de tarefas através de cargos e funções. Alguns de nível mais crítico ou restrito e outros de nível mais baixo. Dentro desta lógica é necessário estabelecer uma limitação sobre o que um funcionário, de um determinado nível mais baixo na hierarquia funcional, pode ou não ter direito de acesso à informação de nível mais alto ou sigiloso. Os dados estratégicos e planos de ação, que são de responsabilidade de uma diretoria, não deveriam ser acessados ou vistos por funcionários de escalão mais baixo. E mesmo os funcionários que têm acesso a informações confidenciais da empresa, por exemplo, tem uma responsabilidade

inerente à função, como um funcionário do RH, que acessa dados pessoais de empregados dentro da empresa. O sigilo e a segurança dessas informações neste caso são imprescindíveis, caso contrário a empresa terá potenciais problemas sérios (MITNICK; SIMON, 2003).

Na época do arquivo de papel e armário de aço fechado com chave a segurança era um conceito mais plausível. De fato, fisicamente, uma pessoa não autorizada não conseguia ver a informação. Mas hoje em dia, com um usuário e senha, a pessoa pode, mesmo não vendo fisicamente o arquivo de papel, acessar qualquer informação da empresa. Tudo a um clique de distância. E o que possibilita isso? Os computadores interligados através das redes. Então é correto afirmar desde já, que mesmo no âmbito de uma rede local de computadores, a segurança da informação através de políticas de segurança já se faz muito importante (WASCHBURGER, 2015).

Com a explosão da popularidade da internet, que começou há poucos anos, a questão da segurança da informação se tornou crítica. A expansão das redes deixou de ser unicamente local; passou a ser de alcance geográfico além dos domínios físicos das organizações: não são somente as LANs. O que era antes um conceito de cliente-servidor, hoje já são bancos de dados que podem ser acessados através de navegadores em qualquer lugar do mundo. A internet possibilitou o mundo se tornar uma aldeia global. A expansão mais significativa da internet se deu na década de 1990, e mais no seu final, e na década do ano 2000, entre criação do protocolo HTTP e código HTML, junto com a criação e desenvolvimento dos navegadores (BARWINSKI, 2009).

Internet nada mais é do que múltiplas redes se interligando e trocando informações. Entre os computadores e redes interligadas existe o tráfego de rede. Nesse tráfego existe a informação indo de um ponto ao outro, passando por caminhos ou rotas. Uma pessoa mal-intencionada pode capturar esse tráfego e ler o conteúdo, caso ele não esteja cifrado. Acaba sendo o mesmo perigo de acesso indevido a um arquivo restrito dentro de uma empresa. Se o assunto de segurança de informação já era importante, agora com expansão das redes pelo mundo todo, é um tema de grande importância (TANENBAUM, 2003).

## 2.3 ASPECTOS RELACIONADOS À SEGURANÇA DA INFORMAÇÃO

Kevin Mitnick é um programador e *hacker* americano que ganhou notoriedade a partir da década de 1990. Este famoso *hacker* foi um dos mais notórios exploradores das falhas e recursos ligados a computadores e redes. E grande parte do seu talento não se resume exclusivamente em dominar tecnicamente os recursos computacionais: ele usava muito do que se chama “engenharia social” para atingir o objetivo. Infelizmente quando se fala em segurança da informação, o elo mais fraco da cadeia sempre vai ser o ser humano.

## 2.4 SEGURANÇA DE INFORMAÇÕES, REDES, SERVIÇOS, ACESSO INSTANTÂNEO A DADOS

As redes que ligam computadores entre si surgiram inicialmente em nível físico local ou próximos uns dos outros. A necessidade de se trocar informações em locais separados geograficamente era feita de maneira indireta, como caixas postais, onde “lotes de arquivos” eram guardados e depois acessado pelo computador destino, que pegava essa informação e processava junto aos seus sistemas internos.

Nos primórdios ainda, antes do advento da internet como se conhece hoje, algumas redes locais poderiam ser interligadas entre localizações geográficas distantes através de ligações cabeadas diretas. Para isso eram utilizados *modems* especiais com ligação por fio metálico direto ou alguma outra forma de modulação. Mais isso eram basicamente ligações diretas e dedicadas. E com um custo mais elevado. A interligação entre redes locais era feita de maneira indireta. Mas com o advento da internet, as redes foram se expandindo até chegar ao que se tem hoje. Surgiram novas tecnologias como protocolos de uso comum e novos equipamentos de rede. Desenvolveu-se uma inteligência em como as redes trocam informações entre si. Foram estabelecidos padrões de funcionamento, através de instituições regulamentadoras. Surgiram as camadas conceituais de rede do modelo OSI e TCP/IP. Tudo isso serve para abstrair os recursos disponíveis na internet. Pode-se digitar um endereço web no navegador e esse site ser acessado estando hospedado fisicamente em qualquer lugar no mundo. Para quem usa o recurso isso é transparente; toda a tecnologia de redes que se tem hoje se encarrega da inteligência para trazer a informação até os consumidores.

As informações das organizações hoje na internet ficam expostas para o mundo inteiro, tudo a um clique de distância ou a um comando no *prompt* de comando do sistema operacional (COMER, 2016).

## 2.5 DIVULGAÇÃO DE INFORMAÇÃO SIGILOSA

Recentemente saiu na mídia a revelação de assuntos reservados sobre questões dos Estados Unidos. A pessoa por responsável por essa divulgação se chama Edward Snowden. Este cidadão, que era agente da CIA, tinha acesso a informações sigilosas sobre assuntos relacionados com a segurança nacional. De alguma forma conseguiu copiar informações e passá-las para a *Deep Web*. Esse ambiente é o ideal para propagação de informação que não é divulgado ao público pelas autoridades. De outra forma não seria muito prático que uma informação reservada pudesse atingir todos os países. A *Deep Web* provavelmente possibilitou a disseminação dos dados sigilosos.

## 2.6 ACESSO A INFORMAÇÕES RESTRITAS

Qualquer informação que seja classificada como secreta pelos órgãos do governo tem, com certeza, algum conteúdo que esconde questões da população. Dados sigilosos, como por exemplo, informações sobre cadastro de pessoas, são reservados e não devem ser divulgados publicamente. Mas tem as informações que são escondidas propositalmente para não deixar a população ciente do que ocorre, muitas vezes sobre assuntos considerados segredos de estado.

Algumas informações dizem respeito a ações governamentais pouco populares ou éticas perante a população ou não baseadas na legalidade. Outras questões são informações sobre fatos que poderiam causar comoção social. Mas na maioria dos casos são informações sobre atos que os governos escondem. E a revelação dessas informações sigilosas ao público em geral é feita através da disseminação pela internet obscura.

A mídia oficial não reconhece qualquer assunto relacionado a isso, mas as vezes ocorre uma inquietação tão grande na sociedade, que os canais de comunicação oficiais acabam falando a respeito. Um exemplo mais notório sobre isso foi o do próprio Edward Snowden, citado anteriormente, que ficou famoso ao divulgar informações da Agência de Inteligência Americana (*Central Intelligence Agency* - CIA).

## 2.7 IMPACTO NA SOCIEDADE DA DIVULGAÇÃO DE MATERIAL SIGILOSO

A ação de hackers tem certo impacto na sociedade. É uma questão complexa e polêmica a divulgação de informação que pode causar instabilidade na opinião pública. Algumas informações são sistematicamente negadas pelas autoridades do Estado. O não reconhecimento pelos governos sempre coloca em dúvida a autenticidade das informações divulgadas na internet. Hoje existe até um termo para isso: o "*fake news*". Porém existem algumas coisas que são incontestáveis e quando divulgadas fica difícil o Estado conseguir desmentir. A divulgação de informações sensíveis sempre causa impacto nas pessoas. Mesmo os governos não admitindo a veracidade das informações, isso leva a uma polêmica. E isso pode provocar consequências políticas.

## 2.8 EVOLUÇÃO DA INFORMÁTICA E INTERNET: O LADO BOM E O LADO RUIM

Já discutiu-se sobre isso, da *Deep Web*, do lado bom e do lado ruim. E a internet aberta também tem seu lado ruim, embora ali as coisas são tratadas de maneira mais clara. Tanto internet aberta quanto *Deep Web* podem ser destinadas a trazer boas ferramentas e informações, mas pode também serem usadas para o mal. A internet aberta em si pode ser um verdadeiro instrumento de decadência moral e fonte inesgotável de coisas inúteis. Para tudo o que se aborda em matéria de tecnologia vai existir o uso para o bem ou para o mal. As coisas boas e ruins sempre estarão ao alcance, à distância de um clique. Cabe ao usuário final colocar juízo de valor nos conteúdos disponíveis de maneira tão fácil e rápida nas redes. E cabe às autoridades investigarem e a justiça punir os autores de informação prejudicial ou detentores de material ilegal.

## 2.9 DIVULGAÇÃO DE MATERIAL DE PROPRIEDADE INTELECTUAL

Redes anônimas, redes que estão na *surface web* e, principalmente, a *Deep Web*, à luz da legalidade, podem trazer prejuízos aos conteúdos que possuem propriedade intelectual e autoral. Alguém pode declarar que acessar conteúdo pago de maneira indevida se justifica, pois, a pessoa não tem dinheiro para pagar. Mas igual prejuízo terá o autor de conteúdo proprietário que investiu seus recursos de tempo e dinheiro para produzi-lo. Não se está aqui para discutir justiça social. Faz-se

uma análise em que os autores de determinado material ou obra gastam dos seus recursos, esperando uma retribuição posterior através da comercialização e lucro do seu produto; e tem um prejuízo grande quando veem seu produto ser copiado gratuitamente pelas redes. A falta do retorno planejado em um investimento na produção de software ou conteúdo artístico, por exemplo, eleva o custo final para as pessoas que adquirem o produto legalmente. Acaba ficando caro para todo mundo.

### 2.9.1 Divulgação de Informação Escondida

Direito à informação é algo desejado por todos na sociedade. As pessoas que fazem o trabalho de divulgar informações reservadas na *Deep Web* usam o princípio que todos têm direito à informação. Já entrando um pouco no tema mais político, ocultar informações pode ajudar a encobrir atos questionáveis da administração pública. De qualquer modo, sempre haverá esse debate acalorado entre o direito das pessoas à informação contra informações mantidas de forma reservada, com a justificativa de poderem ter um conteúdo que cause instabilidade na sociedade.

## 2.10 HACKERS E POSSE DE CONTEÚDO PROIBIDO

O termo *hacker* na sua essência de criação ou quando surgiu, não era necessariamente para intitular um “fora da lei da informática”. Eram pessoas que tinham uma grande curiosidade tecnológica e exploravam todos os recursos dos computadores. As primeiras versões de softwares e computadores não conseguiam prever todos os problemas possíveis; e também não tinham como prever questões como brechas e falhas de segurança. Tudo ainda era muito novo. Por isso os fabricantes de software publicam correções e atualizações dos seus softwares regularmente para corrigir problemas que vão sendo revelados.

Os *hackers* são *experts* em descobrir as brechas nos sistemas; inicialmente faziam isso só por diversão. Mas logo muitas pessoas mal-intencionadas usavam essas técnicas para proveito próprio e com intenção de enriquecimento ilícito e roubo propriedade intelectual. São “ladrões virtuais” propriamente ditos. Também tem os ataques que visam causar instabilidade em serviços públicos essenciais, como controle de tráfego aéreo, podendo gerar muitos problemas sérios contra a segurança de pessoas. A esse tipo de pessoa é mais correto, segundo os próprios *hackers*, a atribuição do termo “*cracker*”.

Computadores estão sujeitos a ataques por que estão interligados em uma rede. E uma rede gera tráfego de dados. Se esta rede estiver desprotegida ou mal configurada, é um aspecto de falha de segurança. Dados que não estiverem criptografados são facilmente interceptados em qualquer ponto da rede.

Os administradores de TI ou de redes podem contar com o recurso dos chamados *Firewalls*, que na tradução literal se chamaria “parede de fogo”. Esse tipo de recurso essencialmente barra algum tipo de pacote de informação suspeito que tente entrar de uma outra rede, normalmente fora da nossa rede local, e que poderia causar danos nos computadores da rede interna que estão abaixo desse *Firewall*.

# 3 DEEP WEB

*Deep Web* tem uma boa relação com a segurança da informação e assunto de rede. Em uma rede se não houver uma política de segurança de informação, haverá muitos problemas. Em se tratando de regulamentações, segurança da informação, segurança de redes, políticas de segurança, a *Deep Web* pode ser comparada e associada a esses itens. Na parte de regulamentação, por exemplo, a *Deep Web* não tem qualquer norma que norteie seu funcionamento. Mas comparativamente, o sigilo na troca de informação é muito grande. É um tipo de rede agregada e que funciona em cima das redes abertas.

## 3.1 REDE DENTRO DA REDE

E uma vez trazido à tona toda essa questão, deve-se também pensar: e onde essas pessoas “vivem” virtualmente com seus conteúdos, identidades e perfis? Qualquer um desses conteúdos que tenham propriedade intelectual, sigiloso ou até mesmo proibido, se forem guardados na *surface web*, são facilmente detectados pelos administradores de rede e rapidamente bloqueados. Como tudo na rede pública é indexado, localizar informações protegidas é bastante fácil. Também é fácil descobrir quem são as pessoas ligadas ao perfil ou conta onde essas informações eram guardadas. É óbvio que criminosos virtuais não vão colocar seus conteúdos ilícitos na internet aberta.

O lugar onde esse tipo de usuário “vive” é na *Deep Web*. É sempre bom lembrar que *Deep Web* é um conceito. De fato, a informação estará fisicamente gravada em algum disco de computador escondido em algum lugar, mas a forma como essa informação circula compartilhada pela *Deep Web* é o que caracteriza ela como obscura. Os próprios nós dessa rede são desconhecidos. E o tráfego inter-rede ou entre esses servidores mais o tráfego cliente servidor é tudo feito por criptografia. Para isso é usado um navegador especial. Sabe-se que qualquer dado criptográfico é muito difícil de ser detectado e interpretado a tempo para que se tome alguma medida legal cabível.

O acesso à *Deep Web* e seu conteúdo é feito em cima da internet aberta. A forma como as informações trafegam nessa rede escondida é diferente. Dentro de

qualquer organização pode-se ter conteúdo da *Deep Web* trafegando sem que os administradores da rede consigam detectar, pois toda a informação é criptografada.

## 3.2 REDE OBSCURA DENTRO DA INTERNET

A internet é uma grande rede mundial. Se analisar há uma visibilidade para identificar quem é quem. Internet é um “local público”. E fazendo uma comparação como se fosse uma cidade, você pode ir a qualquer lugar desse espaço público. Existem lugares que são protegidos e só se acessa com uma “chave de acesso” que pode-se dizer que são usuários e senhas. E continuando a fazer um paralelo de comparação com uma cidade, existe também uma região obscura, que poucas pessoas se aventurariam a entrar sem saber dos riscos que correm. Podem ser regiões até perigosas. Nesses lugares obscuros de uma cidade, tudo que tem lá é escondido, e mesmo as informações trocadas entre as pessoas desse local, são em forma de código. Tudo isso para dificultar uma possível ação de uma força policial que possa identificar essas pessoas e ligar elas a uma prova de um ilícito. Tudo é feito em código. Na rede pública de computadores existe essa região que é chamada de *Deep Web*.

É complexo querer fazer classificações e determinar camadas ou regiões da *Deep Web*. O que existe hoje é uma convenção de alguns termos para descrever algumas camadas mais profundas desta rede. Não deseja-se aqui descrever com detalhes os níveis ou camadas dessa parte obscura da internet, pois pelo próprio princípio dessa rede, seria infrutífero. E também pouco prático determinar quem estabelece essas regras. O que pode-se tentar descrever é o que se observa através de deduções e análise comportamental pelo que se conhece e o uso que fazem dessa rede. Tampouco vai-se achar um site para usar como referência bibliográfica que fale com autoridade da *Deep Web*. Isso pelo simples motivo da obscuridade, criptografia e natureza dessa rede. O que pode-se falar é de uma maneira conceitual mais ampla.

## 3.3 PROTEÇÃO POR CRIPTOGRAFIA

Tudo feito na *Deep Web* é por criptografia. Portanto é difícil saber a localização do destino ou endereço onde determinada página está hospedada. Pode-se saber o endereço em forma de código para acessar determinado conteúdo, porém esse endereço só aponta para o próximo servidor da rede.

“Em linhas gerais, criptografia é o nome que se dá a técnicas que transformam informação inteligível em algo que um agente externo seja incapaz de compreender.” (GARRET, 2012).

A página que estou querendo acessar pode estar no próximo servidor do nó dessa rede ou em qualquer outro; não tem-se como saber, pois, a comunicação com o outro servidor ou próximo nó na rede é feita com criptografia. Assim é praticamente impossível saber a rota da informação final que se está acessando. Os endereçamentos e chaves criptográficas são dinâmicos, renovados de tempos em tempos.

## 3.4 TRÁFEGO POR CRIPTOGRAFIA SEM REGULAMENTAÇÃO

Pode-se capturar e armazenar um conteúdo criptografado trafegando em uma rede. Posteriormente usa-se ferramentas para tentar quebrar o código de criptografia e ler o conteúdo que foi capturado. Porém isso demanda tempo e só teria alguma utilidade no caso de computação forense, onde se deseja identificar evidências de algum fato ocorrido que esteja sob investigação. Porém fazer isso dinamicamente com as informações trafegando nas redes é pouco prático. É isso que torna a D*eep Web* invisível e com poucas chances de regulamentação. Se não se tem como identificar as pessoas ou organizações envolvidas nessa troca de informações, não há como estabelecer uma normatização, ou mesmo tentar aplicar a lei vigente.

## 3.5 NÃO TEM INDEXAÇÃO

Como já foi discutido sobre a demora para se quebrar códigos criptografados, tentar fazer indexação do conteúdo das páginas *Deep Web* é praticamente impossível. Determinado *link* de acesso a uma página da rede pode estar ativo hoje, mas no dia seguinte já pode ter sido alterado. Os indexadores de conteúdo que vasculham a internet aberta, como a Google, fazem o que se chama de indexação dos conteúdos dos servidores; ou seja, eles leem todo o conteúdo dos servidores web que não estão protegidos por senha de acesso e verificam todo o código HTML desse conteúdo, estabelecendo ligações entre os *links* encontrados de uma página para outra. Para isso funcionar, a maior parte desse conteúdo precisa estar acessível para leitura publica sem restrição de acesso. A maioria das páginas de qualquer site é assim: está estaticamente disponível. Somente são bloqueados os conteúdos privados que

necessitam de alguma autenticação, como usuário e senha. No restante os motores de busca desses indexadores conseguem ler todo o conteúdo público, fazer cópia e estabelecer ligações de uma página a outra. Como a *Deep Web* não tem acesso aberto, uma eventual indexação é pouco prática.

## 3.6 SEM CONTROLE PELOS ÓRGÃOS OFICIAIS

Se a informação é tratada como bem valioso nas organizações e é protegida, tornando difícil seu acesso, de maneira semelhante os conteúdos da *Deep Web* são mais difíceis de serem acessados. Para conseguir acessar qualquer página *Deep Web* é preciso saber precisamente o *link* de acesso que é construído de maneira codificada. Os serviços de DNS não estão associados a esses endereços e, portanto, esses endereços não aparecem em forma de siglas mais inteligíveis, como o formato “www.site.com.br”. É praticamente impossível saber em qual IP determinado conteúdo HTML está hospedado na *Deep Web*, porque além de escondido esses servidores podem ter IPs dinâmicos que mudam periodicamente, além do próprio endereço *Deep Web* também mudar constantemente. Então mesmo que um conteúdo ilegal possa ser visto e constatado por uma autoridade policial, saber quem é o dono dessa informação e onde ela está localizada (que seria a evidência do crime) é mais complicado. Como a *Deep Web* é dinâmica, a dificuldade de decifrar conteúdos pode tornar inviável investigações.

## 3.7 ACESSO LENTO POR CAUSA DA CRIPTOGRAFIA

Na internet normal as informações vão de um lado para o outro através de camadas de rede e com a identificação de origem e destino. A identificação da rede destino e até do servidor específico são facilmente identificados, porém não o conteúdo do pacote, pois este pode estar criptografado. Para a internet aberta isso já é o suficiente. Dados como endereço origem e endereço destino são abertos. A informação que eles carregam é que pode ou não ser aberta. Isso não interfere na velocidade normal de troca de informações da rede. Porém já na *Deep Web*, o tráfego em si é criptografado. O que chama-se de cabeçalhos, redes origem e destino, não aparecem de maneira aberta. É aí que está a obscuridade desta rede. Mas isso afeta a velocidade com relação a um conteúdo aberto, pois todos os pacotes que vem da origem para o destino precisam estar protegidos. E existe um custo de processamento

para essa criptografia e descriptografia de tudo que é mandado de um ponto origem para um ponto destino. Torna-se mais demorado o tráfego das informações em comparação com a internet comum.

## 3.8 NÓS DE SERVIDORES

A interligação da *Deep Web* é feita através de servidores e não de roteadores, conceitualmente falando. Cada servidor age como um nó, que se comunica com o outro nó. Algo parecido com os roteadores onde um é interligado a outro e existe uma tabela dinâmica entre eles que registra quem são os seus vizinhos e como chegar a um endereçamento desejado. A pessoa pode configurar seu computador para se tornar um nó ativo na *Deep Web*. Os endereços não são iguais aos de uma página web comum: é uma sequência de códigos que não fazem sentido tanto no formato “www” quando no formato IP. Esse endereço codificado é executado em um navegador próprio e ele vai se encarregar de procurar o nó da rede e onde o conteúdo procurado está hospedado.

## 3.9 CRIPTOGRAFIA E REGULAMENTAÇÃO

Criptografia é algo difícil de quebrar. Nos Estados Unidos existe uma determinação que proíbe qualquer pessoa ou organização de usar criptografia forte nas suas comunicações. Isso em tese permite ao governo bisbilhotar e decodificar qualquer informação que circule na internet. Justificam isso como assunto de segurança nacional.

Uma criptografia forte é basicamente impossível de ser decodificada, por mais que um governo ou instituição tenha os mais poderosos computadores disponíveis. E criptografia é o que viabiliza a existência da *Deep Web*. Essa rede, em certo ponto de vista, existe como movimento de contracultura do que é hoje estabelecido e regulamentado. Tentar fazer qualquer regulamentação a respeito, inviabiliza a proposta inicial de um ambiente virtual onde tudo fica escondido. Se isso é certo ou não, é um outro assunto a ser discutido.

# 4 REDES ANÔNIMAS

Um dos aspectos que mais coloca a *Deep Web* em discussão é o anonimato. Quem quer anonimato tem nela o lugar ideal. Há um boato que se não fosse com o apoio dessa rede, as informações como as divulgadas pela *Wikileaks* não teriam o alcance e impacto mundiais que tiveram. Alguns exemplos de redes anônimas: TOR, I2P e Freenet.

## 4.1 FREENET

A rede Freenet existe desde os anos 2000. Lida com o conceito de nódulos em um circuito. Cada nódulo no circuito engloba um subconjunto de recursos disponíveis na rede e é mantido colaborativamente. Cada nódulo mantém uma lista de nódulos vizinhos. Esta rede é mais utilizada para servir conteúdos estáticos, e não dinâmicos. Tem menos flexibilidade.

## 4.2 I2P

Evolução da *Freenet*, usa túneis de comunicação. Foi desenvolvida em 2003. Tem como característica a criptografia em múltiplas camadas: criptografia entre remetente e destinatário; entre roteadores de rede; e entre túneis de comunicação.

É mais destinada para serviços como *torrent* e e-mail. Tem proteção em mais de uma camada.

## 4.3 THE ONION ROUTING (TOR)

Existem projetos que pesquisam, constroem e desenvolvem sistemas de comunicação anônimos. Esses estudos compõem o que é chamado de programa *Onion Routing*. O foco deste estudo está baseado em internet de baixa latência que tem como característica resistência à análise de tráfego, ataques de espionagem tanto interno quanto externo em uma organização.

O roteamento *Onion* tem como característica impedir que no transporte de dados se saiba quem está se comunicando com quem; a rede só sabe que a comunicação está ocorrendo. A comunicação está livre de interceptadores até o ponto em que o tráfego da rede *Onion* chega ao servidor destino.

O *Onion Routing* teve sua implantação em meados de 1996. Aqui já era tratada como rede de segunda geração. Em 1998 já haviam várias redes independentes implantadas com cerca de uma dúzia de nós cada uma em várias plataformas, mas ainda não eram acessíveis publicamente. Em meados de 2002 a nova versão da rede se tornou o TOR, sendo a terceira geração do *Onion* e como é conhecida hoje (SYVERSON, 2005).

# 5 DEEP WEB E CRIMES VIRTUAIS

A internet pública é nos dias de hoje fundamental na nossa vida em vários sentidos. E em contraposição pode-se dizer que a *Deep Web* é algo obscuro, contrária à internet pública e onde só se esconderia quem faz algo à margem da lei ou que tem intenções ocultas.

Mas essa afirmação não é totalmente verdadeira. Um lugar obscuro pode ser onde pessoas criminosas se escondem e onde pode se achar coisas ilegais. Porém existe também um lado da *Deep Web* onde se compartilham informações úteis. Já apresentado anteriormente o valor que a informação tem para uma empresa e como ela deve ser protegida. A propriedade intelectual é algo inegável. Porém existe muito conhecimento no mundo que é negado às pessoas e isso é feito de maneira a se estabelecer um domínio. Se qualquer pessoa quer ter algum conhecimento, tem que pagar, e muitas vezes, pagar caro. Isso é uma forma de manipular e manter na ignorância a maior parte das pessoas que não tem recursos para estudar. Existe um ditado que fala que conhecimento é poder e outro ditado que fala que o conhecimento liberta (CALDERON, 2014).

Muitas informações que não são distribuídas ou oferecidas de maneira pública na sociedade, na *Deep Web* estão disponíveis. Nessa rede pode-se ter acesso a informações úteis, como livros, que de outra forma seriam muito caros para serem comprados. Essa é a “parte boa” da rede escondida, onde a informação útil é compartilhada de maneira livre.

Mas é óbvio que num ambiente que não tem regulamentação legal, se prolifera também a ação de ladrões e pessoas sem escrúpulos.

## 5.1 PEDOFILIA

Uma operação policial realizada e que foi noticiada em 21 de outubro de 2017, foi batizada de Luz na Infância. Depois de seis meses de investigação pela Polícia Civil foram cumpridos 7 mandados de busca e apreensão e realizados 4 prisões. O crime de pedofilia se caracterizou pela cópia (*download*) de arquivos para o computador, de material pornográfico envolvendo crianças. A operação envolveu 24 Estados e o Distrito Federal. Das pessoas presas, três eram de Palmas/TO e uma de Ponte Alta do Tocantins.

A operação policial e o porquê do seu nome: “Luz na Infância significa propiciar a crianças e adolescentes vítimas de abuso e violência sexual o resgate da dignidade, bem como, tirar esses criminosos da escuridão, para que sejam julgados à luz da Justiça." (G1 TOCANTINS, 2017).

A notícia desta operação policial batizada como “Luz na Infância” faz referência a *Deep Web* como “internet obscura”, outro termo pouco usado no jargão técnico: "...os criminosos agem nas sombras e guetos da rede mundial de computadores. Luz significa propiciar a essas crianças e adolescentes – vítimas - o resgate da sua dignidade bem como retirar da obscuridade esses criminosos." (G1 TOCANTINS, 2017).

Essa definição declarada em entrevista ao site que noticiou a operação não entra em detalhes das técnicas ou ferramentas utilizadas para levantar evidências que levaram às prisões e aos mandados de busca. Esta operação policial foi deflagrada em vários estados brasileiros. As duas referências apresentadas, G1 Tocantins (2017) e G1 São Paulo (2017), dizem respeito à mesma operação, com detalhes diferentes, mas complementares a cada Estado, sobre a mesma notícia. Desta forma pode-se referenciar os termos apresentados sobre a *Deep Web*.

## 5.2 DARKNET: DE ARMAS A DROGAS

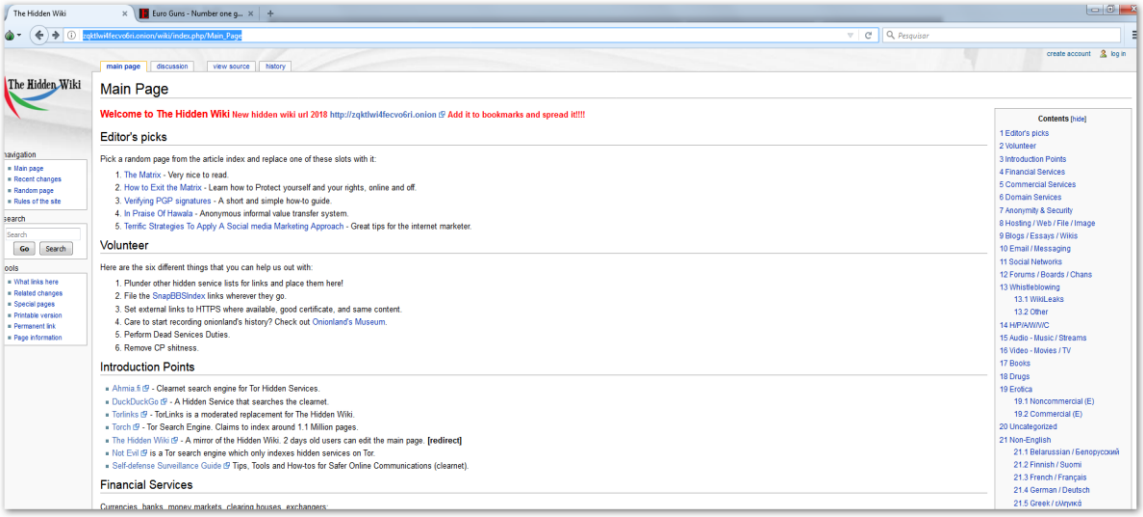
*Darknet* é outro nome que se dá à *Deep Web* quando ela é vista como local de cometimento de crimes.

O site de assuntos relacionados à Alemanha - Deutsche Welle (http://www.dw.com) - com notícias publicadas em português, diz que aproximadamente 10% das drogas ilícitas consumidas na Inglaterra foram vendidas pela plataforma da *Darknet*. Mas são pesquisas difíceis de estimar, obviamente. (RESNECK; HEIN. 2016).

Mais alguns exemplos de sites com oferta de produtos ilícitos:

- “The Hidden Wiki - Main Page”: na Figura 1, pode ser observada uma página de *links* diversos a assuntos e negócios obscuros e ilegais que dificilmente serão encontrados na internet aberta.

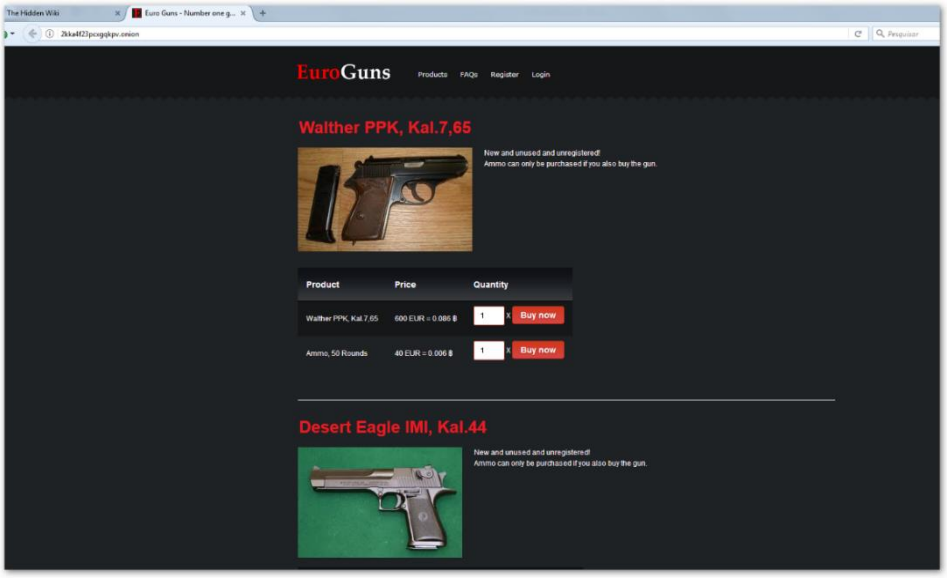
**Figura 1. Site “The Hidden Wiki” encontrado na Deep Web**




**Fonte: Autoria própria. Criada pelo navegador TOR em: 16 mai. 2018.**

- Site denominado “EuroGuns” acessado no navegador TOR através de endereço que só funciona dentro desse programa. Um exemplo de site que vende armas livremente sem qualquer exigência de regulamentação, como mostra a Figura 2.

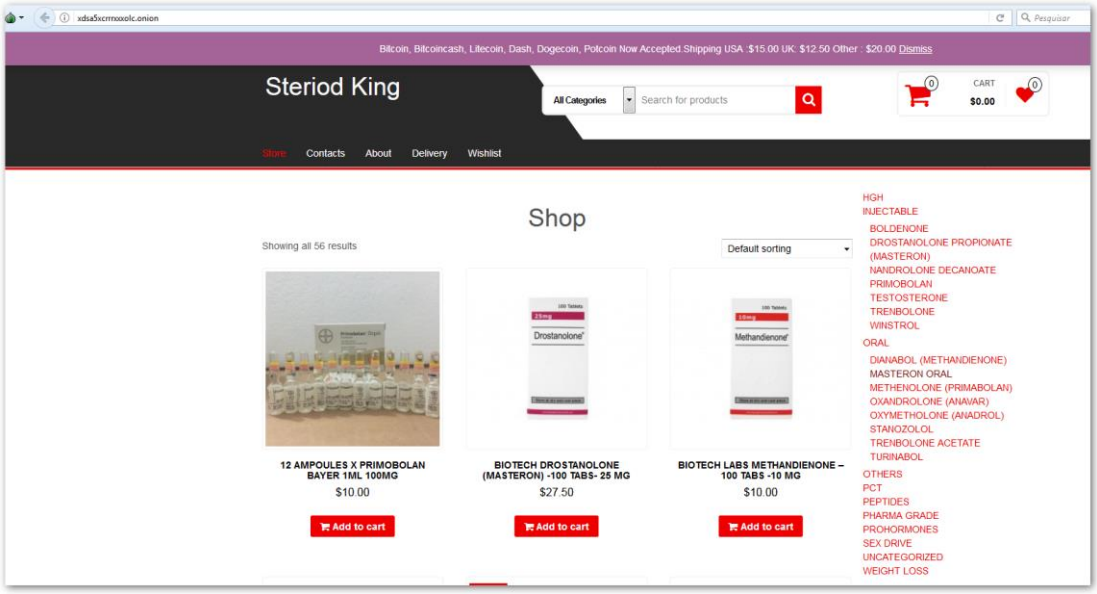
**Figura 2. Site denominado “Euro Guns” de comércio de armas**




**Fonte: Autoria própria. Criada pelo navegador TOR em: 16 mai. 2018.**

- A Figura 3, mostra a venda de esteroides em um site denominado “Steroids King” (Rei dos Esteroides), que inclusive foi escrito de forma incorreta no site.

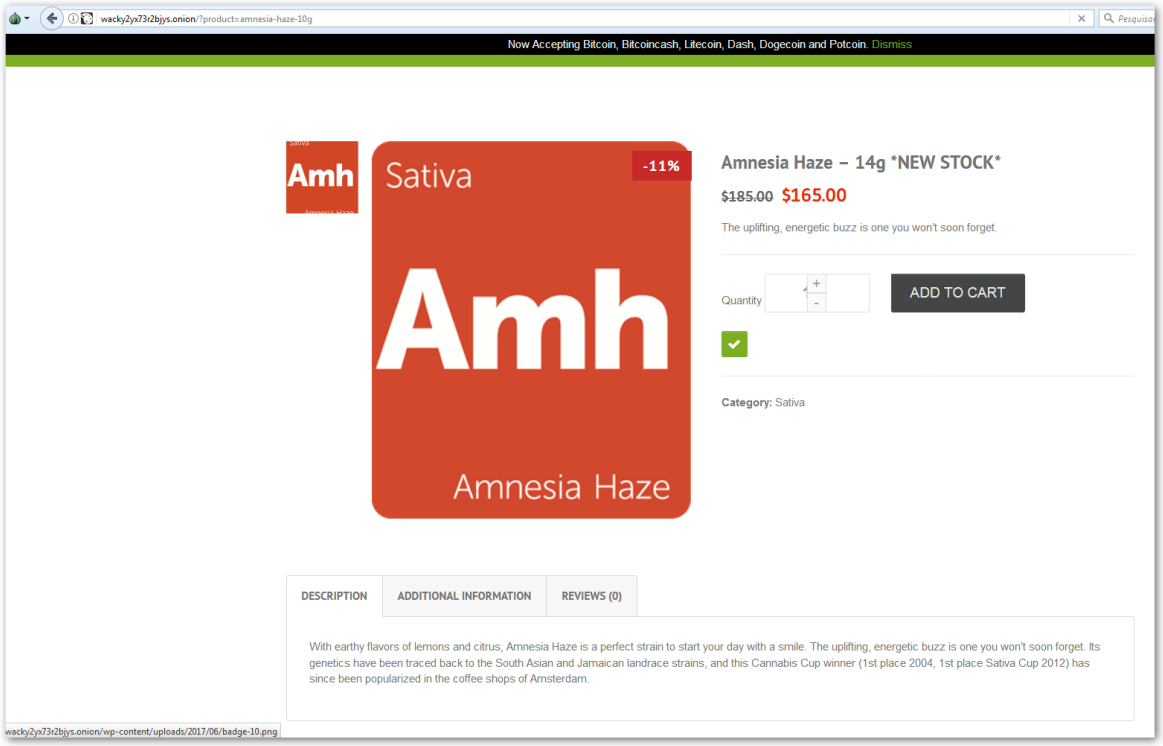
**Figura 3. Venda de anabolizantes no site chamado “Steroids King”**




**Fonte: Autoria própria. Criada pelo navegador TOR em: 16 mai. 2018.**

- Este outro site “*Wacky Weed*” mostra o comércio do que parece serem drogas variadas; e no exemplo é mostrado um tipo de energético (Figura 4).

**Figura 4. Site “Wacky Weed” de vendas online de medicamentos**




**Fonte: Autoria própria. Criada pelo navegador TOR em: 16 mai. 2018.**

Poderiam ser mostrados vários outros sites que também trazem comércio aberto de drogas, explosivos, produtos químicos, entre outros. Preferiu-se não pesquisar sobre assuntos mais preocupantes e de grau de complexidade como

pedofilia, mutilações, sexo, entre outros, pois não é objetivo deste trabalho fazer um manual de acesso à internet obscura e sim retratar muito superficialmente o que pode ser encontrado. Nos exemplos acima, os assuntos de drogas, anabolizantes e armas foram facilmente encontrados, sem muito esforço. Com alguma dedicação e esforço, o internauta com certeza pode acessar informação cada vez mais sensível e moralmente ofensiva, sem falar de coisas ilícitas.

# 6 NAVEGADOR TOR

## 6.1 REDE TOR

A rede TOR é composta por servidores interligados entre si sobre a internet pública. Esses servidores são conhecidos como nós. Funciona com voluntários colaboradores que disponibilizam seus computadores para servirem de relays na intercomunicação entre os circuitos da rede. Porém é necessário saber que tipo de relay dentro dessa rede seu servidor será.

## 6.2 TIPOS DE RELAYS

Dentro da arquitetura da Rede TOR, qualquer pessoa pode tornar disponível um computador para servir de servidor ou nó colaborativo. Porém nem todas as configurações de servidores são iguais. Dependendo do tipo de servidor colaborativo que a pessoa esteja disposta a fornecer, há uma configuração específica a ser considerada. Esses nós ou servidores, em tempo de execução, são chamados de *relays* e tem três formas, descritas a seguir:

- Relay Médio: todo circuito usa pelo menos 3 *relays* antes de chegar ao destino. Os dois primeiros são chamados de médios, pois recebem o tráfego e repassam para os demais;
- Relay Ponte: *relays* que não são públicos. São fundamentais nos países onde os *relays* públicos são bloqueados regularmente;
- Relay Saída: é um *relay* público que conecta sem criptografia com o servidor destino. Dentro da arquitetura da rede, o *relay* de saída sempre é conhecido.

## 6.3 REQUISITOS DOS SERVIDORES

O requisito para um servidor vai depender do tipo de *relay* este servidor será. Os requisitos para um servidor são:

- Largura de banda e conexões;
- Tráfego de saída mensal;
- Endereço IPv4 público;
- Memória;
- Armazenamento em disco;

- CPU;
- Tempo de atividade.

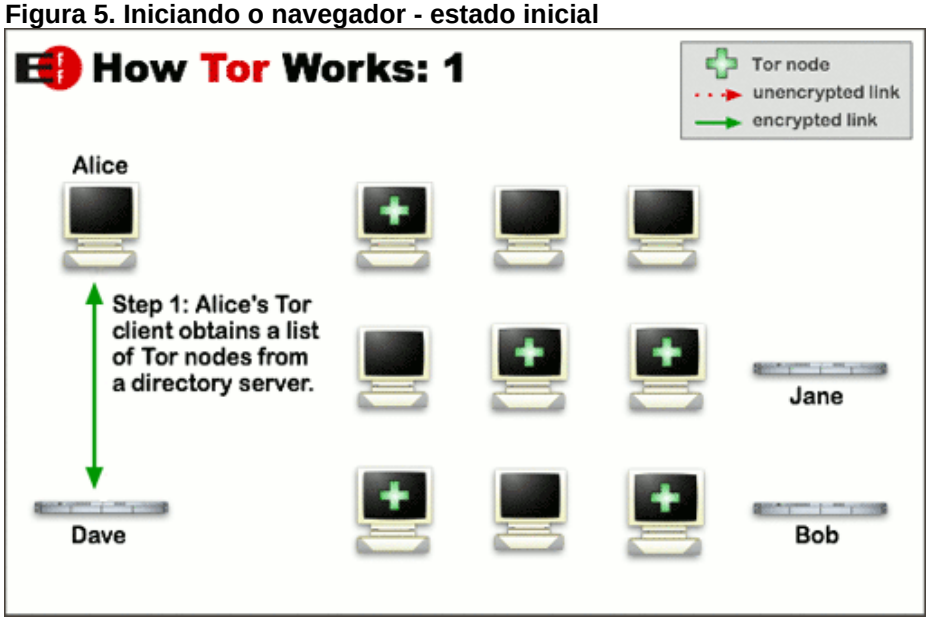
O último *relay* de saída é o mais vulnerável a receber reclamações e sofrer bloqueios, pois é o endereço de origem público que aparece na conexão com o servidor destino. Maiores detalhes das informações necessárias para ser um nó dentro da rede TOR são encontradas no endereço, disponível em: <https://trac.torproject.org/projects/tor/wiki/TorRelayGuide#Partone:decidingtorunarelay>, acesso em: 28 jun. 2018.

## 6.4 COMO FUNCIONA UM ACESSO PELO TOR

Um acesso a determinado site dentro da *Deep Web* dentro da rede TOR obedece a uma sequência de três passos, onde todo o circuito é estabelecido desde o computador origem até o servidor final:

- Passo 1: lista de nós do TOR. Como o TOR funciona na prática? Ao iniciar o navegador, uma lista de nós de rede é carregada de um servidor de diretórios, como mostra a Figura 5.

**Figura 5. Iniciando o navegador - estado inicial**

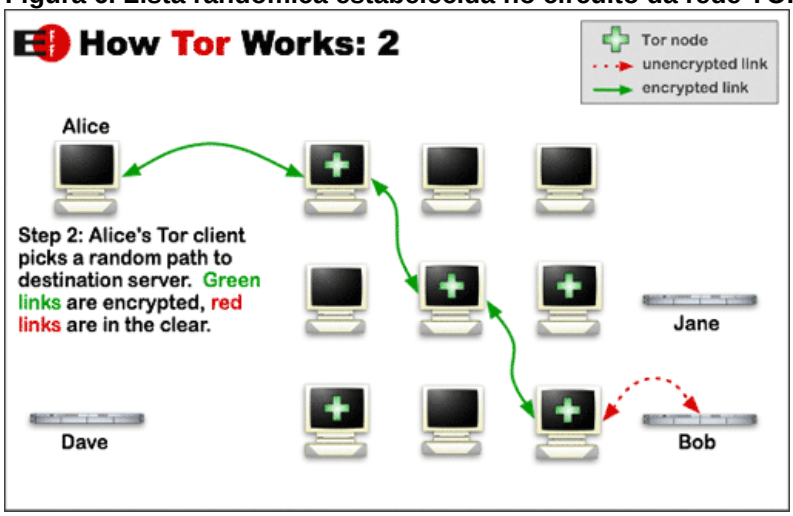



**Fonte: Autoria própria. Disponível em: <https://www.torproject.org/about/overview.html>. Acesso em: 02 jul. 2018.**

- Passo 2: ao informar o endereço desejado, uma lista randômica e aleatória é estabelecida para o servidor destino. Todos os *links* desde o cliente TOR até o

último nó estabelecido são criptografados. Somente o *link* entre o último nó da rede TOR e o servidor destino é que não são criptografados, como mostra a Figura 6.

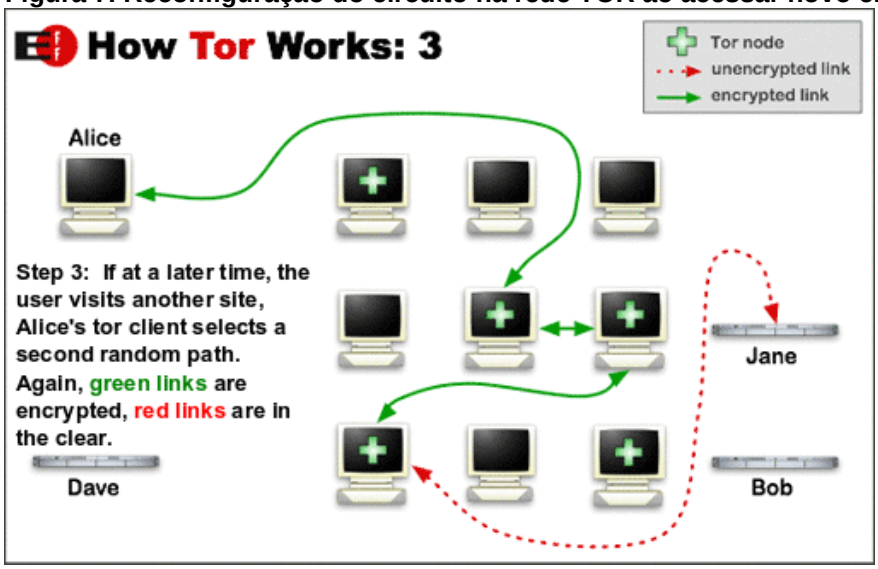
**Figura 6. Lista randômica estabelecida no circuito da rede TOR**




**Fonte: Autoria própria. Disponível em: <https://www.torproject.org/about/overview.html>. Acesso em: 02 jul. 2018.**

- Passo 3: Se mais tarde o cliente TOR acessar outro site, um segundo caminho randômico e aleatório é estabelecido, seguindo a mesma regra. Caso o cliente permaneça mais tempo no mesmo site, novo caminho randômico é estabelecido, como mostra a Figura 7.

**Figura 7. Reconfiguração do circuito na rede TOR ao acessar novo endereço**




**Fonte: Autoria própria. Disponível em: <https://www.torproject.org/about/overview.html>. Acesso em: 02 jul. 2018.**

As transações são divididas e distribuídas em vário locais da internet. Ou seja, uma transação pode ser dividida em partes e serem distribuídas nos diversos nós da rede, sendo reagrupados novamente no ultimo nó e entregues ao servidor final. Como

cada nó da rede é criptografado com uma chave diferente, uma tentativa de rastreamento se torna bem mais difícil.

Quando o TOR é executado, ele acessa um servidor que contém uma lista dos servidores da rede. Conforme o que vai sendo acessado, é estabelecido um caminho novo aleatório entre os nós. E cada nó na rede se encarrega de encobrir suas trilhas. Cada salto dentro dessa rede é criptografado incrementalmente. Ou seja, a cada salto entre os nós é negociada e trocada uma nova chave de criptografia. Uma mesma chave nunca é usada novamente entre outros nós. Os circuitos são estabelecidos em um salto de cada vez. Os nós de rede conhecem sempre o nó anterior e o próximo nó, mas nunca sabem o caminho completo.

Saltos, *relays* e *nós* tem um significado específico na rede TOR. “Nós” são a quantidade de computadores que integram e compõe a rede como um todo. Também podem ser chamados de *relays* conforme seu comportamento no momento em que o circuito é estabelecido. Os saltos, assim como na internet aberta, também existem, porém não podem ser rastreados de maneira completa. Os saltos são determinados a cada conexão, por tempo determinado e aleatoriamente, diferente da internet normal onde toda uma rota pode permanecer estática por muito tempo. Por padrão, um circuito dentro da rede TOR tem validade de 10 minutos. Depois disso ele é autoconfigurado novamente, para evitar uma possível rastreabilidade dos dados trafegados.

## 6.5 BLOQUEIO E PRIVACIDADE

TOR é usado para contornar a censura, uma vez que muitos conteúdos existentes na internet são bloqueados de alguma forma. Países como a China tem bloqueios nacionais a sites que possam trazer informações que a política do Estado considere inadequada para o regime vigente.

O tráfego da internet é passível de análise. Através de rastreamento, pode se identificar a origem e o destino do acesso de determinado computador, podendo inclusive ser identificado o responsável pelo acesso. As informações de início e destino dos pacotes de informações, e toda a sua rota, são gravadas nos cabeçalhos. O cabeçalho, ao contrário dos dados, pode ser lido por qualquer pessoa. Essa informação pode fornecer pistas do comportamento do usuário revelando, por inferência, seu comportamento. Ou seja, conforme os sites que o internauta visita,

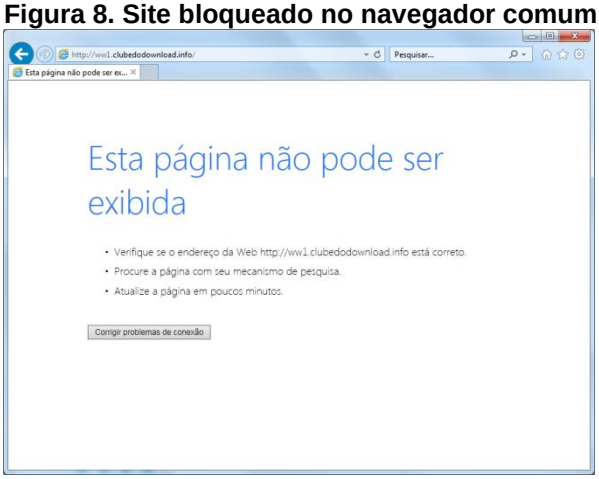
pode-se deduzir seus interesses. Esses dados podem revelar informação valiosa para as empresas comerciais. O TOR torna essa análise e comportamento circunstancial inútil, pois conta com recursos dentro da sua rede para ofuscar qualquer tentativa de rastreamento do tráfego interceptado.

Os bloqueios a sites e serviços podem ocorrer em diversos pontos na internet: pode ser uma censura a nível nacional, pode ser um bloqueio de um provedor de acesso ou até dentro de uma intranet de uma empresa ou organização. Assim, o TOR conecta sites, serviços e mensagens instantâneas quando os mesmos são bloqueados nas formas citadas.

Exemplos de sites bloqueados:

- Quando acessa-se a internet, primeiramente, liga-se a uma rede local ou a um provedor de serviços de internet. Dependendo da configuração rede local ou da política do provedor de internet, pode-se encontrar bloqueios a determinados sites. A Figura 8, mostra um site de *downloads* bloqueado em alguns provedores do Brasil.

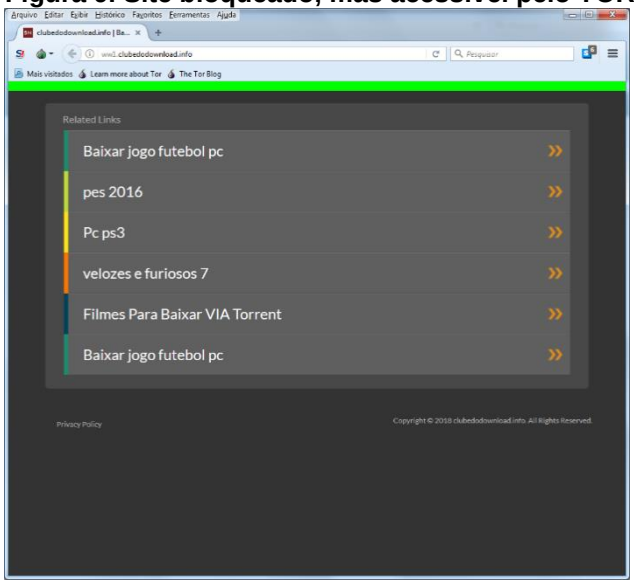
**Figura 8. Site bloqueado no navegador comum**




**Fonte: Autoria própria. Disponível em: <http://ww1.clubedodownload.info>. Acesso em: 16 mai. 2018.**

- Mas usando o navegador TOR aparece uma página inicial do site que foi bloqueado em um navegador comum, como mostra a Figura 9.

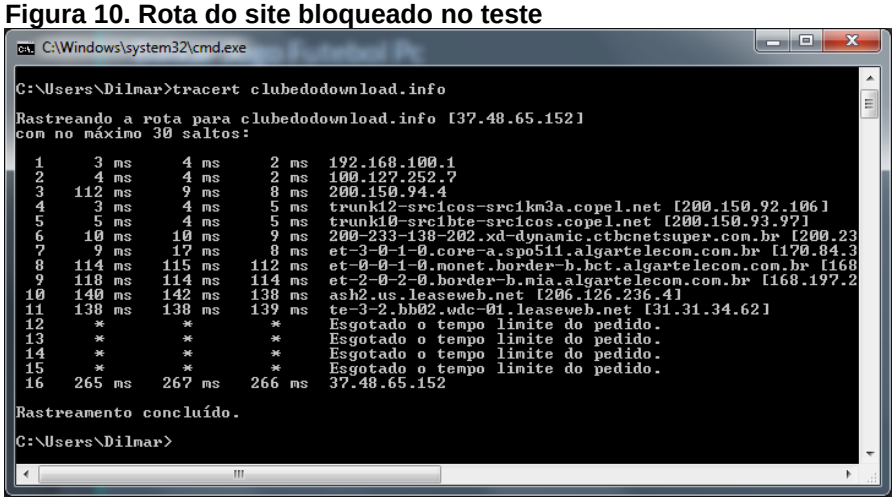
**Figura 9. Site bloqueado, mas acessível pelo TOR**




**Fonte: Autoria própria. Disponível em: <http://ww1.clubedodownload.info>. Acesso em: 16 mai. 2018.**

- Na Figura 10, com o comando de "*trace route*" do Windows, pode-se verificar todos os saltos de onde este site está hospedado. Significa que ele existe, mas está bloqueado em algum ponto da sua saída para internet.

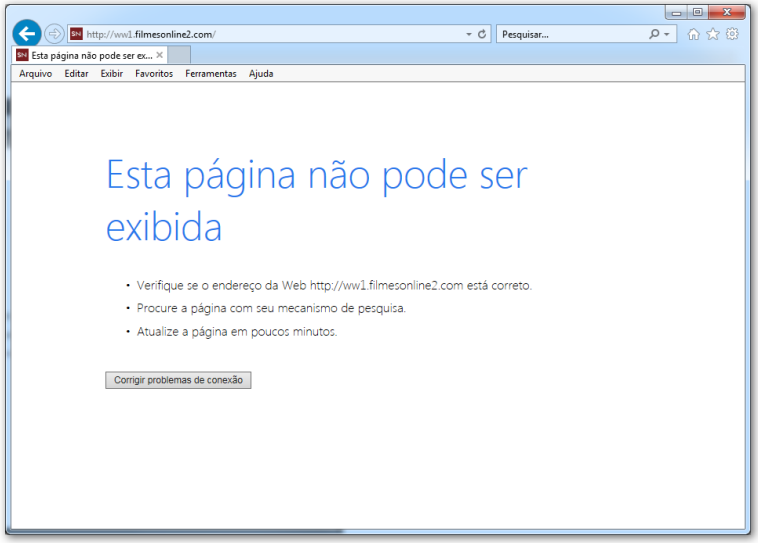
**Figura 10. Rota do site bloqueado no teste**




**Fonte: Autoria própria.**

- Os bloqueios podem obedecer aos mais diversos motivos dentro de provedores de internet ou organizações. Pode-se observado outro exemplo na Figura 11.

**Figura 11. Outro exemplo de site bloqueado**




**Fonte: Autoria própria. Disponível em: <http://www.filmesonline2.com> Acesso em: 16 mai. 2018.**

- E mais uma vez usando o TOR, como mostra a Figura 12, aparece a página inicial do site onde o acesso foi bloqueado em um navegador comum.

**Figura 12. Outro exemplo de site bloqueado, mas acessível pelo TOR**


**Fonte: Autoria própria. Disponível em: <http://www.filmesonline2.com>. Acesso em: 16 mai. 2018.**

O bloqueio de sites pode ser específico da rede local. Os dois exemplos foram retirados de uma lista de servidores que, segundo divulgação, foram bloqueados em Portugal. No exemplo, o teste de acesso foi realizado com o serviço de internet fornecido pelo provedor Copel Fibra. Através deste ISP as páginas testadas foram bloqueadas. Porém no teste de acesso através de uma rede diferente, dentro do ambiente de rede da UTFPR, os sites eram acessíveis em qualquer navegador. Portanto, o bloqueio de sites vai depender de como são configurados os acessos da rede local, como *proxy*, *gateway*, *firewall* e até roteadores.

## 6.6 CLIENTES DO TOR

Alguns profissionais específicos como os da imprensa, grupos ativistas e ONGs podem usar a rede TOR para permanecer no anonimato. Dependendo da atividade que a pessoa exerça, o anonimato é fundamental para sua segurança e para evitar perseguições e retaliações. As corporações também têm usado a rede TOR para substituir as VPNs tradicionais.

Agências de segurança dos Estados Unidos usam o TOR para coletar informações de fonte aberta. Fazem a vigilância de sites da web sem deixar seus registros que revelariam sua identidade.

TOR é uma rede anônima distribuída pelo mundo todo. Os chamados nós da rede ou relays, trocam informações criptografadas entre si. Quanto maior a variedade de pessoas usando o TOR, mais seguro ele se torna.

## 6.7 SEGURANÇA E ANONIMATO

O TOR não resolve todos os problemas e não é 100% anônimo. O último nó que acessa o servidor destino não é criptografado. Toda a rota aleatória que é criada dentro da rede é como um caminho sinuoso para tentar despistar um eventual rastreamento. Porém o servidor que você acessa sabe quem você é, mas não sabe de onde você veio. Portanto, para garantir seu total anonimato nos sites e serviços acessado via TOR, evite informar dados pessoais ou qualquer outra informação que o identifique. Nesse sentido, vale a mesma regra da internet aberta, com a diferença que na internet aberta você pode ser identificado de outras maneiras.

Do mesmo modo que a rede TOR pode deixar ocultas pessoas mal-intencionadas, o enfraquecimento das redes anônimas também significa um perigo na ausência de segurança para troca de informações confidenciais importantes.

## 6.8 STATUS DA REDE TOR

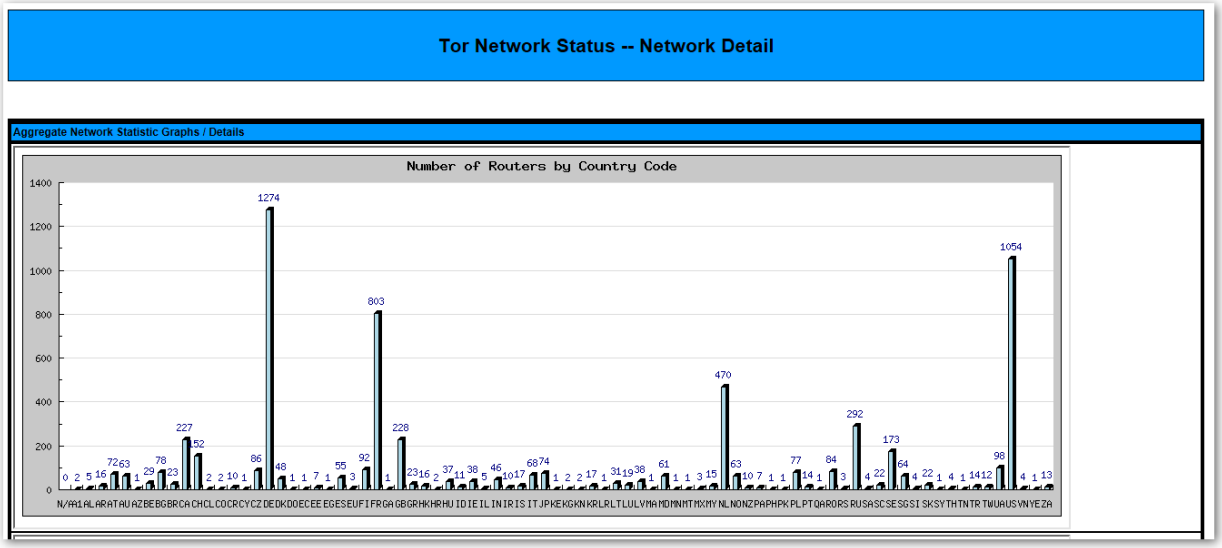
Esta página (Figura 13) mostra o estado atual de toda a rede TOR no mundo. Ela pode ser acessada em qualquer navegador, mas já no início existe um alerta que que indica de forma negativa que se está dentro do navegador TOR, que seria o necessário para a navegação anônima.

**Figura 13. TOR - status da rede**


**Fonte: Autoria própria. Disponível em: <http://torstatus.blutmagie.de>. Acesso em: 02 jul. 2018.**

A página oferece um menu de opções com dados estatísticos variados para serem consultados. Oferece gráficos com detalhes da rede TOR trazendo informações como quantidade de roteadores por pais, quantidade de *relays* de saída (os computadores que aparecem publicamente), velocidade de banda, plataforma, etc. O exemplo mostrado na Figura 14 os números roteadores por país.

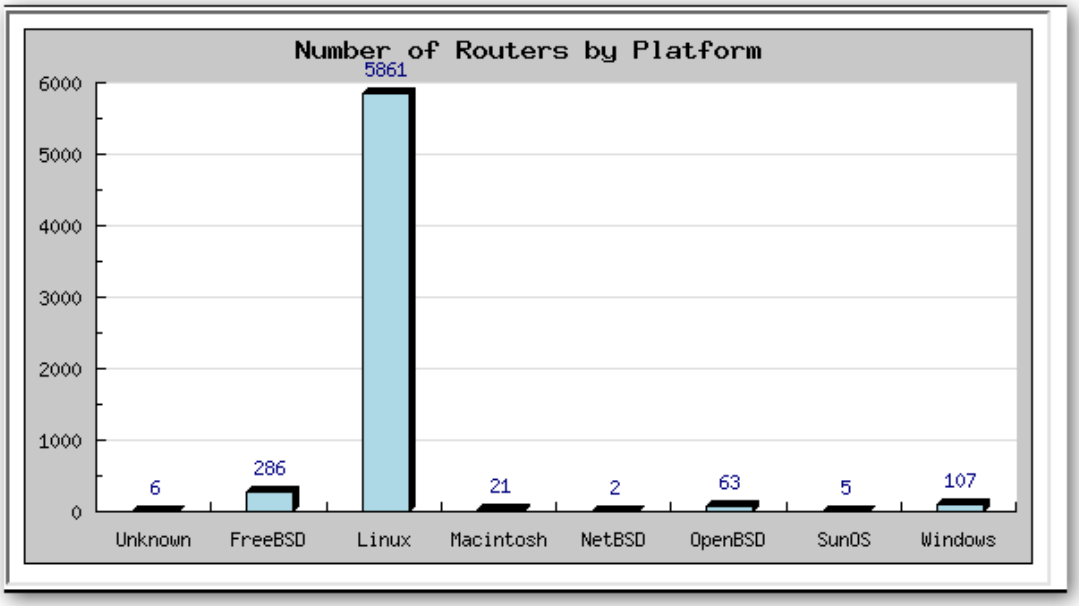
**Figura 14. Roteadores da rede TOR por país**




**Fonte: Autoria própria. Disponível em: <http://torstatus.blutmagie.de>. Acesso em: 02 jul. 2018.**

A Figura 15, traz informações estatísticas da quantidade de roteadores por plataforma operacional. Neste exemplo, nota-se a predominância da plataforma Linux.

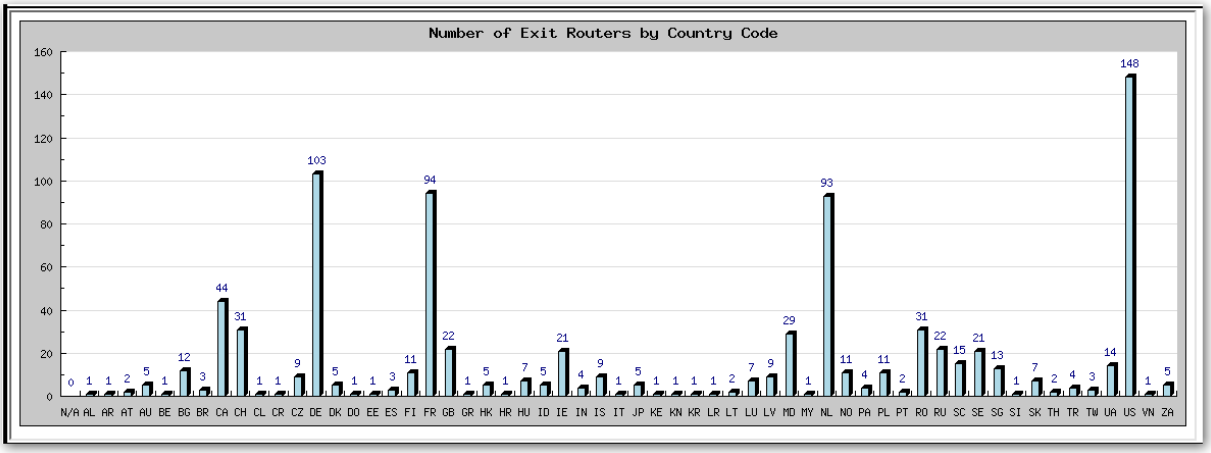
**Figura 15. Roteadores da rede TOR por plataforma operacional**




**Fonte: Autoria própria. Disponível em: <http://torstatus.blutmagie.de>. Acesso em: 02 jul. 2018).**

A Figura 16, mostra a quantidade de roteadores de saída por país, que são os computadores que aparecem publicamente na internet.

**Figura 16. Roteadores de saída da rede TOR por país**

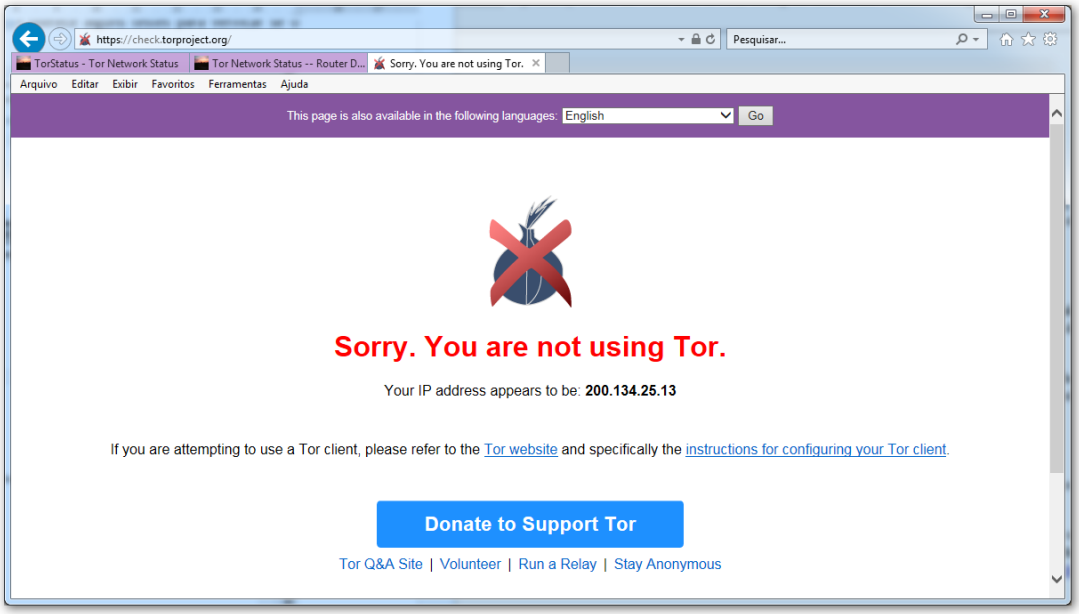



**Fonte: Autoria própria. Disponível em: <http://torstatus.blutmagie.de>. Acesso em: 02 jul. 2018.**

## 6.9 TESTE COM A REDE TOR

O site mostrado na Figura 17 oferece alguns testes para verificar se o navegador usado está compatível com a rede. Aqui um exemplo de um navegador comum usado para testar a rede TOR, mostrando inclusive qual o IP público do computador.

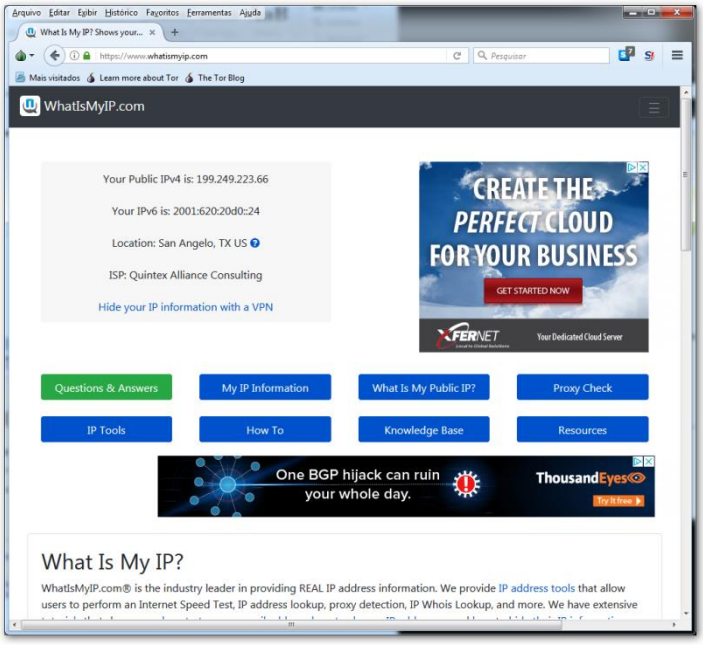
**Figura 17. Teste com navegador comum na rede TOR**




**Fonte: Autoria própria. Disponível em: <https://check.torproject.org>. Acesso em: 16 mai. 2018.**

Na Figura 18, o mesmo teste de verificação feito com o navegador TOR, informando que o browser é apropriado para a rede TOR. Informa inclusive qual o seu IP mascarado, que é o *relay* de saída.

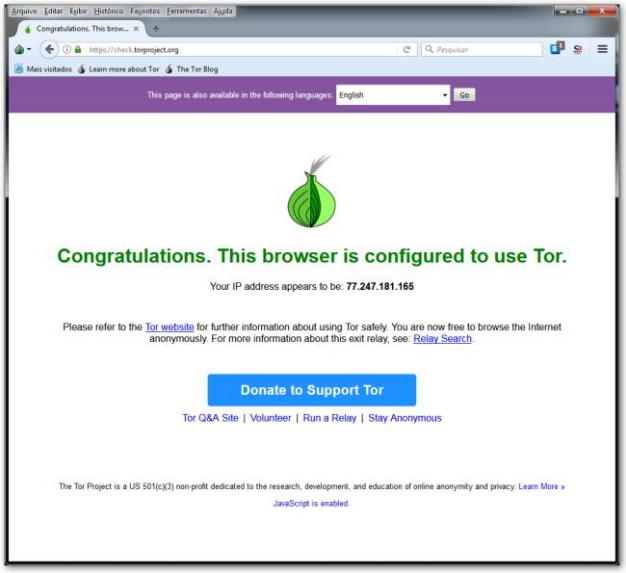
**Figura 18. Teste da rede com navegador TOR**




**Fonte: Autoria própria. Disponível em: <https://www.whatismyip.com>. Acesso em: 16 mai. 2018.**

A Figura 19, mostra também o teste de IP no serviço “WhatIsMyIP” informando o IP visível para o mundo que o TOR associou para a sessão ativa neste navegador.

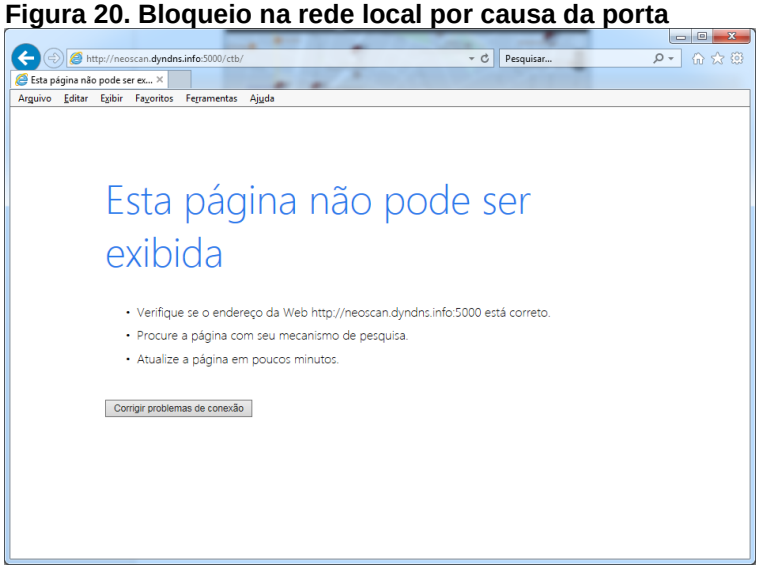
**Figura 19. IP mascarado que o TOR apresenta na sessão**




**Fonte: Autoria própria. Disponível em: <https://check.torproject.org>. Acesso em: 16 mai. 2018.**

Mais um teste (Figura 20) de acesso a uma página que realmente está bloqueada em muitas redes corporativas, provavelmente por causa do uso incomum da porta 5000.

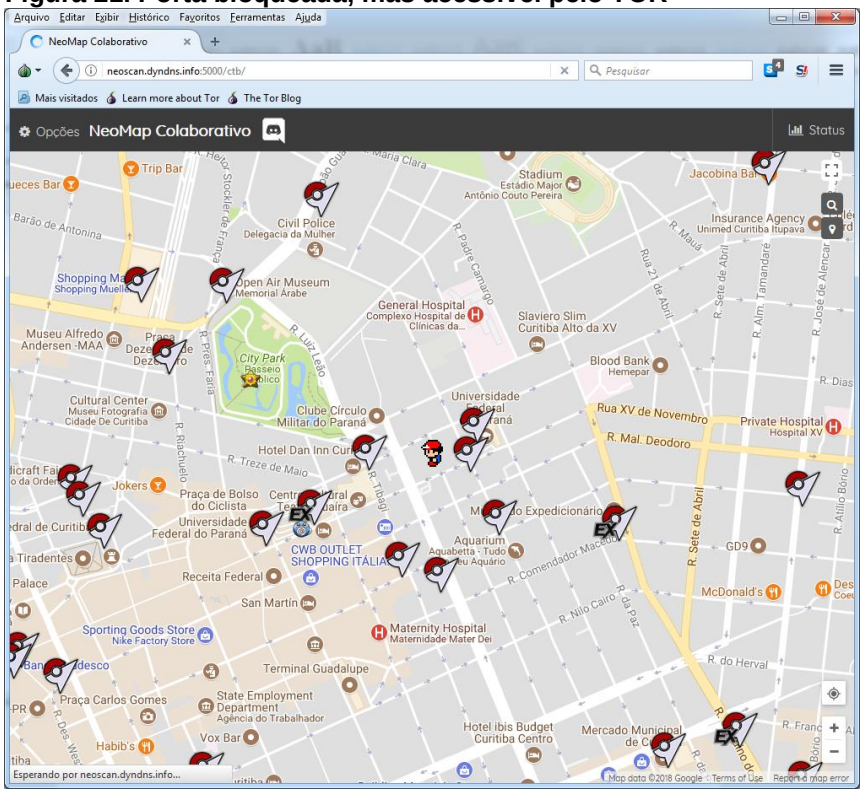
**Figura 20. Bloqueio na rede local por causa da porta**




**Fonte: Autoria própria. Disponível em: <http://neoscan.dyndns.info:5000/ctb>. Acesso em: 16 mai. 2018.**

Site acessado pelo TOR na mesma rede corporativa, como mostra a Figura 21. O navegador consegue contornar o bloqueio e fazer o acesso normalmente.

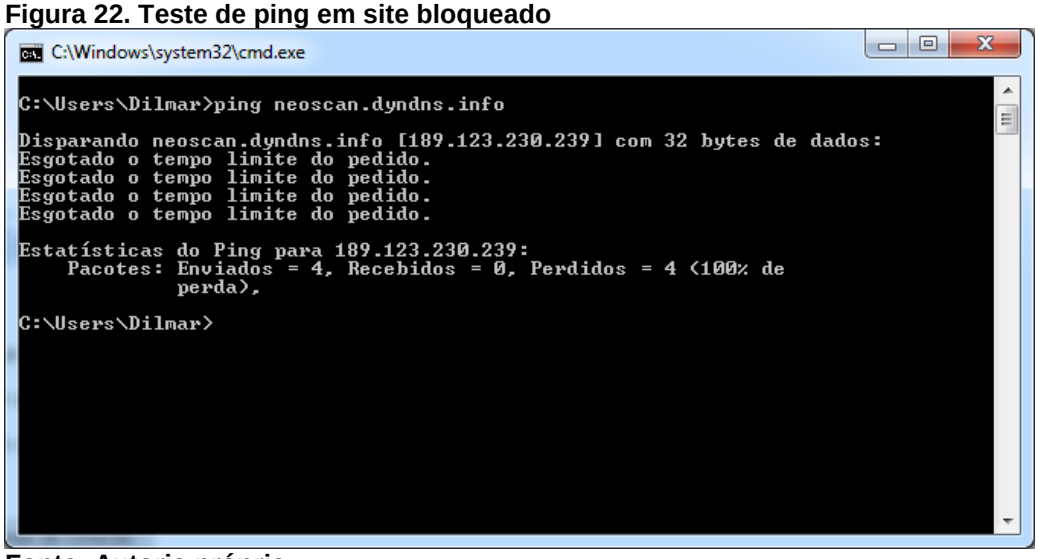
**Figura 21. Porta bloqueada, mas acessível pelo TOR**




**Fonte: Autoria própria. Disponível em: <http://neoscan.dyndns.info:5000/ctb>. Acesso em: 16 mai. 2018.**

O comando *ping*, mostrado na Figura 22, para este endereço de domínio, mostra que ele existe com declaração de DNS, porém a resposta não volta por causa de possível bloqueio tanto de domínio quanto do servidor de origem, que também pode ser configurado para não responder.

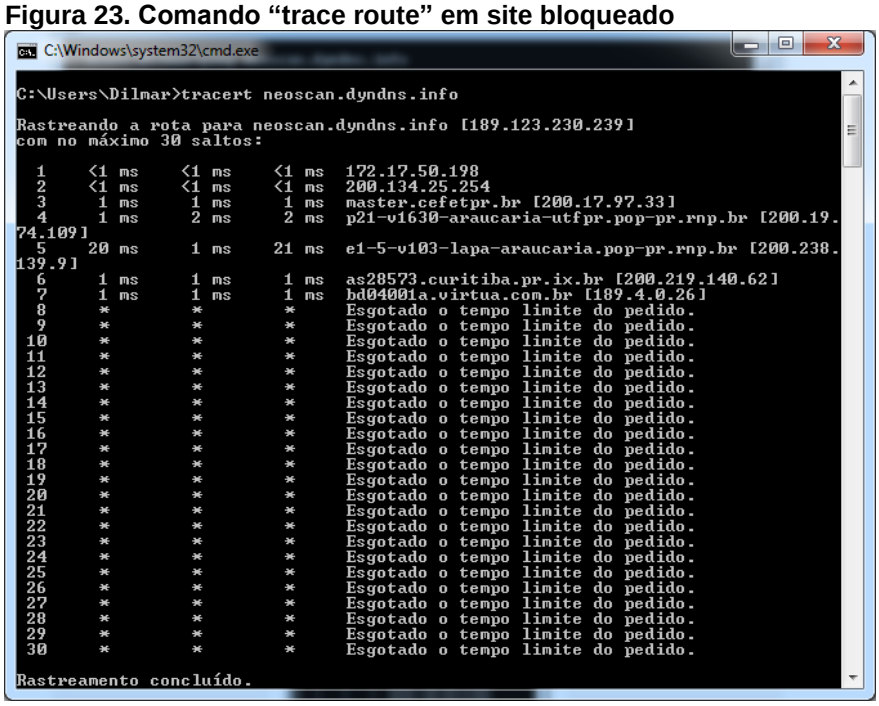
**Figura 22. Teste de ping em site bloqueado**




**Fonte: Autoria própria.**

O comando *trace route* mostra os saltos da rede até onde acesso é permitido, e para no último nó acessível, como mostra a Figura 23.

**Figura 23. Comando “trace route” em site bloqueado**




**Fonte: Autoria própria.**

## 7 CONSIDERAÇÕES FINAIS

Este trabalho procurou fazer um breve histórico da evolução da rede pública de computadores - a internet, e também a falta de privacidade que ela traz junto. É comum hoje em dia ouvir alguém falar “está tudo na rede” ou “jogue seus arquivos na nuvem”. Tudo está na rede, tudo está *online*. A presença da internet é cada vez mais intensa na nossa vida, com tudo a um clique de distância. Porém novas tendências ou novas tecnologias também demandam uma mudança de comportamento e cuidados que antes não se faziam necessários. Como a internet é uma rede pública, é fácil alguém interceptar o tráfego de dados e inferir o que determinada pessoa conectada na rede está fazendo.

As artérias ou vias de acesso que compõe toda a internet pública são as redes interligadas. E toda informação que circula deixa rastros, como foi explicado. Na mão de mentes habilidosas, esses rastros podem revelar informações preciosas a respeito das pessoas, que podem ser usadas para satisfazer o interesse de outros, nem sempre com boas intenções. Para evitar esse rastreamento foram surgindo as redes anônimas, o que acabou criando o conceito de rede obscura; ou simplesmente *Deep Web*. Em essência a *Deep Web* fornece o anonimato, bem-vindo a pessoas que necessitam dela para ocultar e proteger sua vida virtual, como ativistas de direitos humanos e jornalistas, mas que favorecem também pessoas que agem à margem da lei, cometendo crimes. No contexto da *Deep Web* onde são praticados crimes, ela também é conhecida como *Dark Web*.

Todo conhecimento e recurso disponível é uma faca de dois gumes. Pode ser usado tanto para o bem como para o mal. Através do Projeto TOR e seu navegador que leva o mesmo nome, a *Deep Web* pode ser usada por pessoas com motivações ilícitas e imorais, mas também pode ser usada para garantia de segurança, sigilo e confidencialidade válidos. Prefere-se e deve-se sempre defender o uso da tecnologia para o bem das pessoas. Uma expansão da rede TOR só fortalece ainda mais a sua segurança e anonimato. Segurança essa que sempre é benvinda para profissionais que trocam e acessam informações referentes a assuntos corporativos, diplomatas, serviços governamentais e todo o tipo de assunto que possa envolver segurança de pessoas e serviços essenciais.

Também pode-se perguntar: qual será a tendência tecnológica no que tange redes e nossa vida *online* em questão da privacidade e segurança? Tudo hoje em dia

é processado em cima das redes, seja particular ou trabalho; e tudo isso deixa um rastro que revela nosso comportamento. A busca por redes privadas seria uma nova tendência na maturidade da tecnologia da informação? A rede TOR está aí para provar isso e mostra claramente os impactos de algo que ganha espaço, além da privacidade, que é o anonimato.

## REFERÊNCIAS

ABREU, Giovanna; NICOLAU, Marcos. **A estética do anonimato na Deep Web: a metáfora das máscaras e do homem invisível aplicada ao "submundo" da internet**. Revista do Programa de Pós-Graduação em Comunicação da Universidade Federal da Paraíba. Edição 12. Jan-jun/2014. Disponível em: <http://periodicos.ufpb.br/ojs2/index.php/cm/article/download/19746/10908>. Acesso em: 03 jul. 2018.

ARRUDA, Felipe. **Engenharia Social: o malware mais antigo do mundo**. TECMUNDO, publicado em: 11 fev. 2011. Disponível em: <https://www.tecmundo.com.br/seguranca/8445-engenharia-social-o-malware-mais-antigo-do-mundo.htm>. Acesso em: 23 abr. 2018.

BARWINSKI, Luísa. **A World Wide Web completa 20 anos, conheça como ela surgiu**. TECMUNDO, publicado em: 20 mar. 2009. Disponível em: <https://www.tecmundo.com.br/historia/1778-a-world-wide-web-completa-20-anos-conheca-como-ela-surgiu.htm>. Acesso em: 23 abr. 2018.

CALDERON, Barbara Idaerla Santos. **Em que medida a Deep Web aumenta a difusão de poder.** 2014. 59 f. TCC (Graduação) – Curso de Relações Internacionais, Departamento de Economia e Relações Internacionais, Universidade Federal de Santa Catarina, Florianópolis, 2014.

COMER, Douglas E. **Redes de computadores e internet**. 6. ed. Porto Alegre: Bookman, 2016.

G1 SÃO PAULO. **Presos por suspeita de pedofilia usavam rede específica para compartilhar arquivos**. GloboNews, publicado em: 20 out. 2017. Disponível em: <https://g1.globo.com/sao-paulo/noticia/presos-em-operacao-contra-pedofilia-tinham-videos-de-bebes-molestados-e-cartilha-para-abusos-diz-policia.ghtml>. Acesso em: 04 jul. 2018.

G1 TOCANTINS. **Presos por suspeita de pedofilia usavam rede específica para compartilhar arquivos**. TV Anhanguera, publicado em: 21 out. 2017. Disponível em: <https://g1.globo.com/to/tocantins/noticia/presos-por-suspeita-de-pedofilia-usavam-rede-especifica-para-compartilhar-arquivos.ghtml>. Acesso em: 26 abr. 2018.

GARRET, Filipe. **O que é criptografia?** TechTudo, publicado em: 21 jun. 2012. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/06/o-que-e-criptografia.html>. Acesso em: 03 jul. 2018.

MARCON, João Paulo Falavinha; DIAS, Thais Pereira. **Deep Web: o lado sombrio da internet**. Conjuntura Global, v.3, n.4, out/dez 2014, p. 233-243. Disponível em: <https://revistas.ufpr.br/conjgloblal/article/view/40071/24471>. Acesso em: 26 abr. 2018.

MITNICK, Kevin D.; SIMON, William L. **Mitnick: a arte de enganar**. São Paulo: Pearson Makron Livros, 2003.

RESNECK, Jacob; HEIN, Matthias Von. **Na Darknet se compra tudo anonimamente, de armas a drogas**. DW, publicado em: 25 jul. 2016. Disponível em: <http://www.dw.com/pt-br/na-darknet-se-compra-tudo-anonimamente-de-armas-a-drogas/a-19426408>. Acesso em: 26 abr. 2018.

SYVERSON, Paul. **Onion routing.** 2005. Disponível em: <https://www.onion-router.net/>. Acesso em: 18 jun. 2018.

TANENBAUM, Andrew S. **Redes de computadores.** 4. Ed. São Paulo: Ed. Campus, 2003.

WASCHBURGER, Lucas Rafael. **Segurança da informação: conhecimentos necessários para as empresas atuais**. 2015. 39 f. Monografia de Trabalho de Conclusão de Curso (II Curso de Especialização em Redes de Computadores), Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2015.

## GLOSSÁRIO

| | |
|---|---|
| *Cracker* | pessoa que investiga falhas de segurança em sistemas computacionais com finalidade ilícita. |
| *Darknet* | rede escura. |
| *Download* | ação de copiar arquivos da rede para um disco de computador local. |
| *Fake news* | notícias falsas. |
| *Firewall* | parede de fogo. |
| *Hackers* | pessoa com grande interesse de investigar tecnologias da computação. |
| *Hardware* | máquinas ou computadores. |
| *Link* | ligação. |
| *Onion Routing* | roteamento cebola. |
| *Prompt* | linha de comando no jargão de informática. |
| *Software* | programa ou sistema. |
| *String* | corda. |
| *Surface web* | rede de superfície. |
| *Torrent* | serviço de troca de arquivos pela internet com conexão dois a dois - P2P. |
| *Wikileaks* | site de divulgação pública de notícias reservadas. |