**UNIJUÍ - UNIVERSIDADE REGIONAL DO NOROESTE
DO ESTADO DO RIO GRANDE DO SUL
CURSO DE DIREITO**

**LUCAS BROMBERGER MARTINS**

# A INCAPACIDADE DO ESTADO EM REGULAR A LIBERDADE DE EXPRESSÃO NA INTERNET NÃO INDEXADA (DEEP WEB)

**IJUÍ - RS
2022**

**LUCAS BROMBERGER MARTINS**

# A INCAPACIDADE DO ESTADO EM REGULAR A LIBERDADE DE EXPRESSÃO NA INTERNET NÃO INDEXADA (DEEP WEB)

Trabalho de Conclusão do Curso de Graduação em Direito objetivando a aprovação no componente curricular Trabalho de Conclusão de Curso - TCC.
UNIJUÍ - Universidade Regional do Noroeste do Estado do Rio Grande do Sul.

**Orientador(a): Dr. Mateus de Oliveira Fornasier**

**IJUÍ - RS**
**2022**

*Dedico este trabalho à minha família, pelo incentivo, apoio e confiança em mim depositados durante toda a minha jornada.*

## AGRADECIMENTOS

Primeiramente agradeço ao meu orientador Dr. Mateus de Oliveira Fornasier por aceitar conduzir meu trabalho de pesquisa e por todo auxílio prestado.

Aos demais professores do curso de Direito da Universidade Regional do Noroeste do Estado - UNIJUÍ, que demonstram todo comprometimento e qualidade de ensino.

Aos meus pais Pedro e Nairana, que sempre me apoiaram e incentivaram a trilhar o caminho do estudo, além da compreensão e auxílio durante todo o período acadêmico.

*“Só engrandecemos o nosso direito à vida cumprindo o nosso dever de cidadãos do mundo.” Mahatma Gandhi*

## RESUMO

O presente trabalho de conclusão de curso, com o objetivo elucidativo, faz uma análise dos Direitos Fundamentais, sua positivação constitucional, no âmbito digital, visto que, as ferramentas tecnológicas se mantêm em constante evolução e a capacidade do estado em regular a liberdade de expressão é vista como falha. Analisa o anonimato como forma possibilitadora, caracterizando ato de resistência, para em locais da web, os usuários possam se conectar e expressar suas ideias. Aborda a jurisdição substituída e a atual, onde prevê forma de solução para o regulamento dos Direitos Fundamentais mas consequentemente a falta de regulação devido a evolução vertiginosa das ferramentas na web e, com isso, uma morosidade processual que vem provocando muitos questionamentos. Estuda as formas e dispositivos dispostos na web, que proporcionam o anonimato além do esperado pelo Estado. Faz uma breve análise das propostas legislativas e tece considerações sobre as mesmas. Finaliza concluindo que se deve priorizar a pacificação social e, diante dessa prioridade, a necessidade de criação de demais dispositivos legais, além de conceituar e trazer entendimento a respeito da atribuição demasiada dos Direitos Fundamentais aos usuários da rede e, com isso, o que pode causar.



**Palavras-Chave:** Direitos Fundamentais; deep web; liberdade de expressão.

**ABSTRACT**

The present work of constant course conclusion, with the elucidative objective, an analysis of the prohibited foundations, its constitutional prohibition, in the digital scope, makes that, as technological tools keep in the evolution and in the capacity of the state to regulate the freedom of expression is seen as failure. It analyzes anonymity as an enabler, characterizing an act of resistance, for web sites, so that it can connect and create its users. An approach to regulating the form of human resources and the current regulation, which provides for the form of fundamental resources for the solution, consequently, a lack of regulation due to the dizzying evolution of the web and, with that, has been demanding many questions. As esteemed forms and devices on the web beyond, which offer what they expect from the state. It makes a brief analysis of the legislative proposals and makes considerations about them. It ends by completing the prioritization of, in this way of creating allowed devices, in addition to allowing the network to allow and allow the creation of allowed devices, which may be necessary and allow the creation of allowed devices, with this, which can be allowed, with this, allow the network to be necessary to cause.

**Keywords:** Fundamental rights; deep web; freedom of expression.

**SUMÁRIO**

# 1 INTRODUÇÃO

O presente trabalho apresenta um estudo acerca das ferramentas que não se encontram registradas na internet e das noções sobre a incapacidade do Estado em regular os Direitos Fundamentais, focando na liberdade de expressão, a fim de efetuar uma investigação em busca da construção de alternativas à jurisdição. Essa busca é necessária face à crescente insatisfação coletiva em relação à prestação jurisdicional atual do Estado, que além de morosa em razão da complexidade processual e da grande demanda existente. Buscou-se pesquisas bibliográficas e por meio eletrônico, analisando também as propostas legislativas em andamento, a fim de enriquecer a coleta de informações e permitir um aprofundamento no estudo da Deep e Dark Web, revelando a importância nessa parte da Internet a respeito da regulamentação dos Direitos Fundamentais.

Inicialmente, foi feita uma abordagem do que é a Deep, Dark Web e a diferença de há nelas. A Deep Web é considerada uma parte da Internet que não é possível aceder a motores de busca comuns. Necessitando utilização de software a fim de mascarar IP, concedendo anonimato ao usuário. Por conceder estado ou característica do que é anônimo, seus utilizadores acabam por praticar atos ilícitos, o que gera dúvida a respeito da demasiada liberdade dada ao usuário.

Diante da falta de respeito em qualquer assunto, é válida a reflexão sobre quais seriam os limites impostos pela liberdade de expressão no mundo contemporâneo. A internet, na sua proporção da Surface Web, englobando as redes sociais, alimentam os debates públicos e anônimos, portanto, consequentemente, a manifestação de ideias que não enxerga o respeito ao próximo, chega aos debates.

Tendo em vista o crescimento absurdo da World Wide Web (Rede Mundial de Computadores), espelhar-se nela, o mesmo do mundo real, ou o que preside na Surface Web, portanto, após esse avanço tecnológico, algumas pessoas acolheram-se e perceberam que o anonimato em ferramentas de criptografia, lhes protege. A segurança e anonimato viabilizados por meio da Deep Web.

A partir disso, o que é a Deep Web? Como se dá o anonimato para que possibilite a liberdade que seus usuários sentem ter? Qual a capacidade do Estado em controlar a liberdade de expressão em seu âmbito?

Com o avanço absurdamente abrupto da tecnologia, especificamente da Internet, suas ramificações tiveram grande avanço, fala-se precisamente do ramo classificado como parte obscura, devido ao acesso restrito, sendo necessário criptografia para assim acessar. Desenvolvida no Laboratório de Pesquisas da Marinha dos Estados Unidos, a Deep Web, objetiva ser um sistema de comunicações secreto, responsável por enviar dados e análises de sistemas anonimamente e é denominada como hall de entrada para a parte oculta da Internet. A Deep Web nada mais é do que uma parte oculta onde visa o anonimato, portanto seus sites não são indexados, seus usuários prezam pela obscuridade, propositalmente que seu conteúdo não seja rastreado ou controlado por demais internautas. Estudos apontam que a Deep Web seja quinhentas vezes maior que a Surface Web, que a Internet comum que navegamos, representa cerca de 4%, enquanto o restante que permanece oculto, representaria o restante de 96%.

Por causa de sua privacidade, muitas instituições e até mesmo cidadãos comuns recorrem a essa internet invisível para compartilhar e hospedar arquivos, porém o anonimato permitiu o surgimento de atos ilícitos, como fóruns em que os usuários extrapolam a liberdade de expressão, tornando-se indesejável. Os internautas utilizam softwares capazes de mascarar o IP (Internet Protocol), o mais famoso deles, tem o nome de TOR (The Onion Routing), o browser labuta inibindo a consulta das informações reais, fornece dados de forma padrão, para assim fazer com que todos os usuários pareçam iguais, sendo assim, impede que um perfil seja traçado. Sua criptografia funciona graças ao seu mecanismo em que utiliza uma rede de transmissão de dados que passa por diversas máquinas, impedindo saber sua localização exata, além de ter uma função que possibilita esconder a mesma.

Após é analisado os Direitos Fundamentais e o acesso à web profunda, trazendo posicionamento legal e constitucional. Buscando verificar se considerando os dispositivos legais, seria possível vedar o acesso a esta parte da rede. Se mesmo em locais que impera o anonimato e a lei vedando constitucionalmente a prática do mesmo, se entraria de alguma forma em equilíbrio, a ponto de diminuir ou até mesmo uma eventual proibição.

A partir desse estudo se verifica, de acordo com a legislação prevista, e faz uma reflexão a respeito dos direitos fundamentais se eles se sobrepõem, se podem

ou não ser encarados como absolutos em determinadas situações. Conceituando o direito à privacidade e demais elencados no dispositivo legal, analisando a possibilidade de relacionar os direitos fundamentais, para buscar uma correlação, chegando ao consenso para sopesar a vedação ao anonimato em determinados casos.

Um fato que não se pode negar é que o anonimato em grande proporção, ocasiona uma maior liberdade aos usuários de certa rede, sendo assim, os internautas sentem maior autonomia, por sentirem que não estão sendo monitorados a todo instante. Entretanto a Deep Web oferece tanto conteúdos benéficos como maléficos, basta a intenção positiva e não ser negligente quando, para assim, navegar de forma pacífica. A mesma positivamente desempenha papel libertador em circunstância de censura, possibilitando que os sujeitos incluídos nesse meio possam exercer plenamente sua cidadania, assim garantindo aos seus usuários pleno exercício da liberdade de expressão, mesmo em países onde a vigilância e a repressão são incessantes. Portanto a utilidade da parte oculta da internet, pode ser positiva, propiciando a disseminação do conhecimento que nela pode ser encontrado.

A construção deste trabalho foi realizada através do método de pesquisa exploratória, sendo utilizado fontes bibliográficas disponíveis em meios físicos e eletrônicos. Entretanto, também foi utilizado a legislação brasileira vigente, verificando os direitos fundamentais e a capacidade de regular as ferramentas digitais que se encontram em constante evolução.

## 2 O QUE É INTERNET NÃO INDEXADA E SUAS FERRAMENTAS TECNOLÓGICAS OCULTAS

Com o avanço abrupto da tecnologia, especificamente da Internet, suas ramificações tiveram grande avanço, fala-se precisamente do ramo classificado como parte obscura, devido ao acesso restrito, sendo necessário criptografia para se acessar. Desenvolvida no Laboratório de Pesquisas da Marinha dos Estados Unidos, a Deep Web, objetiva ser um sistema de comunicações secreto, responsável por enviar dados e análises de sistemas e é denominada como hall de entrada para a parte oculta da Internet. A Deep Web nada mais é do que uma parte oculta onde visa o anonimato, portanto seus sites não são indexados, seus usuários prezam pela obscuridade e propositalmente para que seu conteúdo não seja rastreado ou controlado por demais internautas. Estudos apontam que a Deep Web é quinhentas vezes maior que a Surface Web, e a Internet comum que navegamos, representa cerca de 4%, enquanto o restante que permanece oculto, representaria o restante de 96%.

Por causa de sua privacidade, muitas instituições e até mesmo cidadãos comuns recorrem a essa internet invisível para compartilhar e hospedar arquivos, porém o anonimato permitiu o surgimento de atos ilícitos, como fóruns em que os usuários extrapolam a liberdade de expressão, tornando-se indesejável. Os internautas utilizam softwares capazes de mascarar o IP (Internet Protocol), o mais famoso deles, tem o nome de TOR (The Onion Routing), o browser labuta inibindo a consulta das informações reais, fornece dados de forma padrão, para assim fazer com que todos os usuários pareçam iguais, sendo assim, impede que um perfil seja traçado.

Um fato que não se pode negar é que o anonimato, em grande proporção, ocasiona uma maior liberdade aos usuários de certa rede, sendo assim os internautas experienciam maior autonomia, por sentirem que não estão sendo monitorados a todo instante. Entretanto a Deep Web oferece tanto conteúdos benéficos como maléficos, basta a intenção positiva e não ser negligente para assim, navegar de forma pacífica. A Deep Web positivamente desempenha um papel libertador em circunstância de censura, possibilitando que os sujeitos incluídos nesse meio possam exercer plenamente sua cidadania, assim garantindo aos seus usuários, pleno exercício da liberdade de expressão, mesmo em países onde a

vigilância e a repressão são incessantes. Portanto a utilidade da parte oculta da internet, pode ser positiva, propiciando a disseminação do conhecimento que nela pode ser encontrado.

## 2.1 CONCEITO E DIFERENCIAÇÃO DA DEEP, DARK E SURFACE WEB.

Cibercultura é classificado como uma cultura de grupos que atuam com a expansão das redes informacionais, já a internet, seria denominada como subcultura que ocorre no ciberespaço, tanto podendo ser um espaço de comando e controle como um espaço de fluxo, organizado em torno de uma lógica e práticas reconfigurantes, onde seria modificada por certos grupos e pela cultura dos mesmos. Assim o criador da palavra *ciberespaço*, William Gibson (1984 p. 69), descreve como sendo:

> Ciberespaço. Uma alucinação consensual vivenciada diariamente por bilhões de operadores autorizados, em todas as nações, por crianças que estão aprendendo conceitos matemáticos... uma representação gráfica de dados de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz alinhadas no ar nãoespaço da mente, aglomerados e constelações de dados. Como luzes da cidade se afastando...

Alex Antunes, tradutor da obra Neuromancer de Gibson, no prefácio à edição brasileira (2003), exemplifica dizendo que “o conceito criado por Gibson neste livro, o ciberespaço, é uma representação física e multidimensional do universo abstrato da ‘informação’. Um lugar para onde se vai com a mente, catapultada pela tecnologia, enquanto o corpo fica para trás” (GIBSON, 2003, p. 5-6).

Esclarecendo e trazendo mais ao atual, o teórico francês Pierre Levy explicitou sobre o ciberespaço: “Eu defino o ciberespaço como o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores (LEVY, 1999, p. 92, grifos do autor).

Portanto definido como um mundo virtual, sendo um espaço desterritorializado, em um mundo não palpável, existente em outra realidade, que a descrição de Gibson se faz como um espaço de construção de sentidos, onde abrem-se janelas para outros campos com uma incursão finita, mas que nos leva a infinitos lugares.

Conceituado o ciberespaço, podemos dizer com certeza que entre os usuários da Deep Web, há a mesma interação social virtual que ocorre no âmbito comunicacional, ao entender de Levy (1999 p. 15-16) consiste em entender um pouco mais simplificado que:

> Como uso diversas vezes os termos "ciberespaço" e "cibercultura", parece-me adequado defini-los brevemente aqui. O ciberespaço (que também chamarei de "rede") é o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo. Quanto ao neologismo "cibercultura", especifica aqui o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço.

Sendo assim, é possível afirmar a existência de um espaço virtual, onde o amplo conteúdo armazenado se organiza e seus usuários se comunicam anonimamente.

Monteiro e Fidêncio (2013, p. 35-46) definem a internet invisível como um conteúdo do ciberespaço, que não é indexado pelos mecanismos de busca. Em uma pesquisa sobre a web invisível e os motores de busca dessa web no ciberespaço, tinham por objetivo destruir com a polissemia do tema, buscando um nome correto ao (des) território. Durante o estudo, descobriu-se um cogênero, sendo uma web verdadeiramente escura, denominada então de Dark Web, definida como paralela e underground, e como previsível da espécie humana, utilizada para o bem e para o mal.

A Deep Web representa uma web repleta de desconhecimento e prejulgamentos sobre seu conteúdo. O termo traduzido “Rede Profunda”, surgiu em 1994 por Jull Ellsworth (BERGMAN 2001, p. 03) e é também denominado como invisible web (SHERMAN; PRICE 2001, p. 283). Alguns autores ainda propagam que a Deep e a Dark Web signifiquem a mesma coisa, apenas sendo duas denominações para o mesmo objeto, porém para Fulton e McGuinness (2016, p. 95-118), há uma diferença e não se pode confundir pela dificuldade em localizar certos conteúdos e páginas na Deep Web com a obscuridade da Dark Web.

A Deep Web representa uma certa camada exponencial do ciberespaço, possuindo conteúdos não indexados e não recuperáveis pelos seus mecanismos de

busca. Isto quer dizer que ocasiona uma quantidade abundante de conteúdos não transitáveis, ou seja, não acessados em todo o ciberespaço.

Para Chris Sherman e Gary Price (2001, p. 283), os motores de busca gerais são impossibilitados de adicionar conteúdo e páginas em seus índices, não podem ou não conseguem, seja por limitações técnicas, questões definidas ou até mesmo tarifamento para acesso. Michael K. Bergman (2001, p. 01) exemplifica afirmando que os mecanismos de busca tradicionais criam seus índices nas páginas da superfície, comprovando assim a disposição dos motores em não indexas e demonstra que a indexação é deliberadamente superficial.

Bergman, traz dados fundamentais a respeito da dimensão da Web, buscando compreender a territorialidade entre as camadas invisíveis, Bergman (2001 p.01) afirma que:

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

Sendo os cem por cento divididos da seguinte fração, a totalidade de conteúdo do ciberespaço em camadas, sendo Deep Web = 90% de todo conteúdo do ciberespaço; Dark Web = 6% e a visible web = apenas 4%.

A denominada Dark Web surgiu na tese de doutorado intitulada Distributed Decentralised Information Storage and Retrieval System de Ian Clarke, na Edinburgh University em 1995 (BECKETT 2009, p. 01), a partir da tese de Clarke, foi possível a construção de uma rede paralela para acessar a internet, a web, o ciberespaço, e a Dark Web.

Esta parte da Deep Web, se destina ser anônima, específica Monteiro e Vignoli (2015, p. 692) que “[...] é bastante seguro considerar a *Dark Web* como uma nova ramificação da *Web* Invisível: suas características são próprias; sua filosofia é própria e, além de tudo, seu conteúdo é o mais enigmático e desordenado de todas as ramificações”.

A Dark Web representa um grupo coletivo de páginas da web que só podem ser acessadas usando navegadores específicos, a Deep e a Dark Web estão abaixo da superfície, no entanto, pela explicação de camadas, a Dark Web é muito mais profunda e obscura, possuindo sua gênese no anonimato, muitas vezes associado à ilegalidade.

A prerrogativa é que a Dark Web seria uma Web ímpar, com peculiaridades e formas de acesso que não são bem esclarecidas, seu acesso seria somente possibilitado por meio de proxy, caso contrário não se trata da mesma Web. Seus conteúdos seriam somente acessados por intermédio de softwares capazes de camuflar o Internet Protocol (IP).

Para melhor entendimento, de acordo com George Hurlburt (2017, p. 100-105) a Dark Web está embutida na Deep Web, porém em uma classificação de hierarquia entre as camadas desse ciberespaço, portanto a Dark Web faz parte do escopo da Deep Web, enquanto web profunda. Contudo, devido sua relevante profundeza e dificuldade de acesso somente realizado por meio de proxy e suas características distintas, trata-se de uma outra web, denominada Dark Web.

A Dark Web é apresentada como um sítio obscuro e invisível do ciberespaço. Denominada desta maneira, pelo fato de estar relacionada em comparação com a Web visível da superfície, local onde os internautas navegam. Portanto, para acessar a Dark Web seria necessário softwares intermediários, pois os motores de busca não conseguem recuperar os locais. Sua amplitude temática também é considerada constante, de acordo com Andy Beckett (2009, p.02) esta web conta com números não exatos, de 5 a 100 vezes mais informações que a surface web.

Segundo Bárbara Calderon (2017, p.06) a Deep e a Dark Web primeiramente diferenciam-se em uma sendo toda região da Rede Mundial de Computadores, sendo assim, não se encontrando nos atuais mecanismos de busca como Opera, Bing, Google ou Yahoo. Já a Dark Web, concentra-se como uma porção da classificação “Deep Web”, que tem por objetividade ser oculta, sendo

propositalmente não ser encontrada, nem que dados ou o próprio conteúdo seja vigiado ou controlado por internautas que navegam pela World Wide Web.

A Surface Web, conhecida como a parte indexada que as pessoas navegam em seus computadores, onde todos os sites de busca conseguem encontrar endereços e listar cada um deles, porém na Deep Web, encontra-se todos os sites que não são indexados e que só é possível o acesso, utilizando método específico de navegação. Nesta primeira parte denominada ainda a região da World Wide Web, pode-se encontrar centrais de e-mails, internet banking, centrais de comando entre outros demais sites comuns, não indexados. Porém dentro da imensa Deep Web, se concentra a Dark Web.

A Dark Web seria considerada como uma subdivisão da Deep Web e também uma espécie de lado negro da Internet, onde as barreiras são ainda mais dificultosas para acessar, isto pois, sua atividade seria mais associada a práticas ilícitas, como o comércio de drogas. Portanto, por se tratar disso, os métodos de acesso envolvem certa tecnologia avançada, como o uso de redes privadas e criptografia de ponta.

Os espaços não explorados ou desconhecidos, até mesmo irrastreáveis, são definidos por Marc Augé (2012, p. 71-105), que a noção de “não lugar” nos permite é algo menos rígido e talvez menos rigoroso sob o ponto de vista científico, exatamente pela ambiguidade da sua definição, como veremos neste texto. Porém, mais interessante sob o ponto de vista da análise social é encontrar uma imagem do todo que não é a recomposição minuciosa das partes, correspondendo empiricamente a um conjunto de construções com características muito diferentes.

Para esclarecimento da sociedade pós-moderna, Augé (2012, p. 74) contextualiza a predominância dos não lugares:

> Um mundo onde se nasce numa clínica e se morre num hospital, onde se multiplicam, em modalidades luxuosas ou desumanas, os pontos de trânsito e as ocupações provisórias (as cadeias de hotéis e os terrenos invadidos, os clubes de férias, os acampamentos de refugiados, as favelas destinadas aos desempregados ou à perenidade que apodrece), onde se desenvolve uma rede cerrada de meios de transporte que são também espaços habitados [...].

Sendo assim, podemos dizer que os não lugares podem ser qualquer lugar em que há uma impossibilidade de rastreamento do ambiente virtual. Ainda segunda Augé (2012, p. 98) os não lugares nunca estão prontos e sempre estão no presente.

Enfim, as características que correspondem ao ambientes pós-moderno, desterritorializados e desconstruídos, como os não lugares da Dark Web.

Richele Grenge Vignoli (2014, p. 84) em sua dissertação buscou apresentar o ambiente denominado Dark Web e estabelecer o conceito e espaço que ocupa no ciberespaço, demonstrando as características essencialmente de um não lugar, complementando o estudo avançado de Bergman (2001) e Augé (2012) a respeito dos conteúdos benéficos e maléficos que podem ser encontrados nessa web profunda.

Os usuários e computadores que navegam na rede, não podem ser rastreados na Dark Web, isto pois, há elementos adversos que podem trabalhar para a obscuridade da invisibilidade na web, bem como a incapacidade do indexador ou motores de busca, realizarem a varrição de informações, falta de publicidades como anúncios do Google, até mesmo páginas privadas de difícil acesso restrito, com acesso somente a partir de senhas, assinaturas ou logins, restrições tecnológicas, entre outros demais (MONTEIRO, FIDÊNCIO, 2013, p. 36-37). Portanto, são apresentados motivos de a Dark Web não ser encontrada ou acessada por motivos diferentes à ilegalidade.

Ainda assim, Christopher S. East (2017, p. 16. grifos do autor): “Você deve estar ciente de que sua vida diária frequentemente envolve a Deep Web de alguma forma”, isto pois sob este prisma, todo internauta em que algum momento na web, possua um login, senhas ou cadastros em certa plataforma, se envolve com a Deep Web, ainda que por desconhecimento ou com preconceitos a seu respeito (VIGNOLI; MONTEIRO, 2015, p. 695).

Dessa forma, pode-se afirmar que os preceitos da Deep Web, não são somente impedimentos e impossibilidades, mas sim, informações que não são acessíveis por questões de sigilo ou segurança. Há dados que como e-mails e mensagens instantâneas que não podem trafegar nessa web, são chamados de Dados Sensíveis.

Dados sensíveis nada mais são do que dados que não podem ser disseminados, isso por questões de ética, segurança e privacidade, também cabe destacar a confiança depositada nos administradores e nos sujeitos que aceitam os termos de uso das páginas utilizadas. Considerando isso, em 2018, no Brasil, foi publicada a Lei Geral de Proteção de Dados Pessoais, onde prevê uma relação legal da proteção de Dados Pessoais e Sensíveis:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

A falta de rastreamento fornece uma certa sensação de privacidade, oferecendo assim, uma navegação tranquila, sem observadores em busca. Dificultando a espionagem e invasão de privacidade recorrentes na superfície, além do conhecimento por parte das empresas sobre quem visita suas páginas na web. A camuflagem de IP em redes como o The Onion Router (TOR), não é considerada perfeita, mas satisfatória, cumprindo o propósito prometido, tornar-se invisível na rede.

O TOR (The Onion Router) é considerado como meio mais seguro e confiável para buscar a utilização da Web invisível, isso pois oferece uma criptografia de três camadas de proteção ao usuário, impedindo a descoberta do seu endereço de IP. Portanto, nada mais é do que um navegador que promete oferecer ao usuário a ocultação do seu endereço de IP, possibilitando assim, uma navegação anônima, evitando o rastreamento. O browser labuta com um sistema denominado de roteamento cebola, que consiste em rotear o tráfego por múltiplos servidores e criptografá-lo a cada passo do caminho. Sendo então, considerado como o navegador mais utilizado para navegação na Deep e Dark Web.

O acesso a Dark Web, é realizado com auxílio do Tor, que se constitui como uma rede e site que tem por objetividade o anonimato de acesso à internet, portanto a proteção da privacidade do usuário. O software labuta criptografando o IP (Internet Protocol) de uma máquina, portanto o acesso torna-se real com apenas o download do Tor e um endereço específico de URL.

## 2.2 EVOLUÇÃO HISTÓRICA DA FERRAMENTA TECNOLÓGICA OCULTA.

Os primeiros computadores surgiram a partir de experiências de equipes com líderes de nomes renomados nessa questão, como Alan Turing e Konrad Zuse, durante a Segunda Guerra Mundial e Howard Aiken na pós-guerra. O século XX era

marcado pelo telefone, rádio e a televisão que saía dos laboratórios e se tornava a principal mídia.

Os primeiros computadores comerciais já obtinham processadores específicos para a comunicação de dados, isto na troca de mensagens entre as máquinas, ainda bastante simples. Objetivando uma comunicação entre equipamentos, diretamente conectados, possibilitando a troca de dados de um computador com o outro. A troca de mensagens era controlada por um equipamento central, que enviava os dados aos demais, porém, o conceito de rede era apenas uma construção teórica, diferente do projeto norte-americano que revolucionou esse âmbito, denominado rede ARPANET.

Conforme apontado por Manuel Castells (2000, p. 82), uma iniciativa tomada pelo Departamento de Defesa do governo americano, deu início a criação de uma rede experimental de supercomputadores, a ARPANET. Visando garantir a comunicação entre as máquinas em caso de ataque nucleares, foi dada a solução de desenvolver uma rede descentralizada que conectasse os computadores e permitisse, em caso de ataque, rotas alternativas de comunicação, além de manter seguro os dados. Castells (2000, p. 83), ainda afirma que essa primeira rede de computadores teve início em 1° de setembro de 1969, somente acessível para os centros de pesquisa que colaboraram com o Departamento de Defesa dos Estados Unidos, sendo assim, apenas para fins acadêmico-militares. Um tempo após, ocorreu a divisão desta rede, uma parte dedicada somente a fins acadêmicos e outra somente a fins militares. Entretanto, tornando-se operacional em 1975 e subdividida em outras redes, foi desativada em 1990 e substituída pela NSFNET, que também, encerrada nos anos 90, assim os passos para a internet como elemento privado. Castells (2000, p. 83) afirma:

> Uma vez privatizada, a Internet não contava com nenhuma autoridade supervisora. Diversas instituições e mecanismos improvisados, criados durante todo o desenvolvimento da Internet, assumiram alguma responsabilidade informal pela coordenação das configurações técnicas e pela corretagem de contratos de atribuição de endereços da Internet.

Dessa forma, a Internet teve diversos entes regendo, segundos seus pressupostos e finalidades. Embora sujeita ao controle e monitoramento de um Estado, ainda é sujeita do mesmo por países a que está conectada, possibilitando

países de aplicar restrições, como ao que vai contra a concepção originária da Internet, visando garantir que uma informação alcance outra da rede, o que prejudica a utilização plena por parte dos usuários.

A ligação entre computadores para transmissão de dados militares, visava primariamente proteger as informações, com isso, mesmo em caso de um ataque inimigo, se preservaria documentos físicos e demais conhecimentos. Projetado originalmente pelo Laboratório Central da Marinha, com auxílio da DARPA (Defense Advanced Research Projects Agency), visavam criar uma rede descentralizada de computadores, nascendo a Arpanet (Advanced Research Projects Agency Network), atual internet. Em suas conexões já haviam redes secretas, com endereços que eram de certa forma invisíveis, estas redes recebiam dados da Arpanet, mas não havia possibilidade de enviar informações para fora dali. Surge então o nome usado até hoje de Dark Net, termo hoje popularizado que somente ficou conhecido nos anos 2000.

O ciberespaço é um espaço em que abriga diversos outros, nele presente as inúmeras webs existentes, bem como a Deep e Dark Web. Para Monteiro e Fidêncio (2013 p. 43) a Dark Web é o continente mais verdadeiramente escuro do ciberespaço, segundo os autores, essa web representa “[...] a rede global de usuários e computadores que operam à margem da visibilidade e das agências fiscalizadoras [...]”.

Primeiramente para adentrar no assunto, segundo o Site Leonardo Pereira, acerca do surgimento e uso da rede:

> Em grande parte, a deep web existe, assim como a própria internet, graças à força militar dos Estados Unidos. Neste caso, graças ao Laboratório de Pesquisas da Marinha do país, que desenvolveu o The Onion Routing para tratar de propostas de pesquisa, design e análise de sistemas anônimos de comunicação. A segunda geração desse projeto foi liberada para uso não governamental, apelidada de TOR e, desde então, vem evoluindo... Em 2006, TOR deixou de ser um acrônimo de The Onion Router para se transformar em ONG, a Tor Project, uma rede de túneis escondidos na internet em que todos ficam quase invisíveis. Onion, em inglês, significa cebola, e é bem isso que a rede parece, porque às vezes é necessário atravessar várias camadas para se chegar ao conteúdo desejado.

A Web classificada como a parte plenamente visível, disponíveis pelos buscadores, ou seja, a Internet que nos é disponível quando abrimos certo

navegador. A Internet que todos acessam diariamente, é mapeada pelos motores de busca, também utilizada a nomenclatura de Surface Web, seria como a Internet superficial, ou ainda podendo ser chamada de porção plenamente visível.

Com a criação da World Wide Web, conhecida como WWW, seus dados e informações armazenados em um servidor, são exibidos por hipertextos, imagens, sons e vídeos, encontrados através de provedores de busca. A busca divide-se em duas categorias, a primeira delas é denominada como Surface Web, que é a internet comum que navegamos, suas páginas são facilmente encontradas pelos mecanismos de busca, o que diferencia da segunda categoria de busca, a Deep Web, que resume as páginas que ficam alheias aos provedores, não sendo listadas como resultados de busca, essa é a forma que ocorre a indexação. A respeito dos provedores de busca, Bárbara Calderon (2017 p. 213-214) exemplifica:

> Literalmente, *crawlers* e *spiders* significam “rastejadores” e “aranhas” e, esses termos se referem aos programas automatizados que têm função de percorrer a web a fim de indexar as páginas que atendem aos seus critérios. O motor de busca lança na web múltiplos crawlers que rastejam na web a procura de páginas. Eles realizam esse “caminhar” através de elos entre as páginas, conhecidos por nós como links. Ou seja, crawlers e spiders são programas de computador que navegam pela web de forma metódica e automatizada para indexação de páginas.

Já essa parte, é classificada como não visível da Internet. Onde é presente certas barreiras para o acesso, podendo ser registros, convites, softwares específicos, entre demais possíveis. Encontra-se websites que não estão totalmente mapeados pelos buscadores e o acesso se dá necessitando um registro. Isso se deve ao fato de sites privados, seu dono não deseja qualquer pessoa navegando e olhando o conteúdo, além da possibilidade de chamar atenção de autoridades governamentais. Portanto para o acesso pleno ocorrer, somente com alguma forma de autenticação, deve haver a aprovação de um administrador do site, para o acesso pleno, já que o conteúdo seria oculto e não o domínio em si. Podemos esclarecer que o acesso poderia ser para fins lícitos e ilícitos, de comunidades virtuais, fóruns de discussão à um livre comércio de drogas.

Pode-se dizer que a surface web é tudo que conseguimos pesquisar e acessar por meio dos buscadores, ou seja, o que é indexado, portanto as páginas indexadas por motores de buscas da web, alimentados pelos programas que varrem

a internet, indexando links e informações. E todo o restante que está fora do alcance destes programas varredores, das buscas e ranqueamentos de sites, é chamado de Deep Web. Pode ser caracterizada a níveis de redes descentralizadas com fortes níveis de criptografia e permissões de acesso, até sistemas de Intranet de empresas privadas e dados específicos como os da Receita Federal. Os estudiosos da área, Monteiro e Fidêncio (2013 p. 37) exemplificam dizendo que:

> A informação na Web pode ser categorizada, para fins de indexação, em suas diretrizes: a parte visível, ou seja, páginas que podem ser somadas ao banco de dados dos buscadores, e a parte invisível, cujo conteúdo, por razões expostas, não pode ser indexado pelos buscadores tradicionais.

Nos anos 2000 quando a ferramenta se tornou mais popular, discussões sobre a forma como a rede se apresentava na época, a web invisível trazia o seguinte paradoxo: “Ao mesmo tempo em que é fácil entender por que ela existe, não é nada simples definir ou descrevê-la concretamente, em termos específicos”. (SHERMAN; PRICE, 2001, p. 02).

Muitas pessoas entendem que Dark web e Deep web são como sinônimos, porém mesmo uma estando inserida na outra, ambas se diferenciam, isto pois, a deep web apenas sinaliza a parte da web que não é indexada por buscadores de rede, já a dark web, trata de uma parte mais obscura da web. Além de não ser indexada, nela há diversas camadas de criptografia para assim dificultar seu acesso. Seu nome se origina do conceito de Darknets, ou seja, redes que só são acessadas usando protocolos diferentes do padrão da surface web, portanto com criptografia avançada. Visto seu anonimato, a Dark Web, tornou-se um âmbito repleto de atividades ilícitas, um exemplo dela seria o site Silk Road, o mesmo que foi fechado pelo FBI em 2013, site esse que era voltado ao comércio de drogas ilícitas. Porém o real motivo por optar por essa privacidade máxima, não remete somente a ilicitudes, visa evitar os cookies, proteger o conteúdo de pesquisas e compras online após uma simples busca.

Bergman consolidou a palavra Deep Web, ensejando estudos mais avançados na área pelos anos 2000. O colunista do The Guardian, Beckett (2009), relata sobre o estudo do autor:

> Michael K Bergman, um acadêmico e empresário americano, é uma das maiores autoridades nessa outra internet. No final dos anos 90, ele empreendeu pesquisas para tentar avaliar sua escala. “Lembro-me de dizer à minha equipe: 'É provavelmente duas ou três vezes maior do que a web normal' ', lembra ele. "Mas a vastidão da teia profunda ... me tirou completamente o fôlego. Continuamos revirando pedras e descobrindo coisas”.

Segundo Michael K. Bergman (2001 p. 01), criador da expressão Deep Web, a palavra tem significado de profundeza, termo em oposição a Surface Web, onde o vocábulo transmite a ideia de superficialidade. De acordo com especialistas, navegamos em apenas 20% de toda Surface Web, há analogias que se dedicam a explicar o funcionamento disso, uma delas seria a do Iceberg, portanto a Surface é representada pelo topo, o que seria de fácil visão aos olhos, enquanto a Deep Web é representada por sua base, sabe que existe o restante, mas não se pode dar a medida exata de seu tamanho, por não conseguir enxergar.

Como dito anteriormente, a Dark Web é um ramo da Deep Web, encontra-se dentro dela, sendo seu conteúdo não indexado propositalmente, permanecendo oculta. Utilizam os usuários um provedor de busca, dentre eles o mais comum seria o TOR (The Onion Router), que oferece certa privacidade, dificultando a fiscalização e o rastreio. Portanto, com esse impedimento e privacidade em demasia, cria-se um espaço iniludível às práticas ilícitas. Neste sentido o estudioso sobre o tema, André Miceli (2019), diz:

> O coordenador do MBA de Marketing e Negócios Digitais da Fundação Getúlio Vargas (FGV), André Miceli, alerta para os perigos da deep web. Segundo ele, não é um lugar interessante para adolescentes e crianças ou mesmo adultos navegarem, por ser um espaço de conteúdos ilegais –que vão desde malwares desenvolvidos por hackers, em busca de dados pessoais –, a atividades ilegais. Miceli, no entanto, esclarece que o problema está na "dark web", uma subdivisão da deep web. O especialista explica que a deep web possui 96% do conteúdo da internet, que vão desde arquivos científicos, livros raros, informações financeiras, até vírus e informações sobre crimes [...].

Ademais, as áreas apresentadas do ciberespaço, que desconhecidas por grande parte do público que navega pelo World Wide Web, mesmo após sua rápida expansão, poucos percebem que a própria Surface Web em que navegam pode se tornar um perigo, quem dirá à profundeza da Deep Web e todo anonimato nela presente. Além de ser viga mestra que se torna garantidora do direito de liberdade

de expressão, basta compreender seu funcionamento, extensão e limites, bem como analisar o posicionamento do Estado e a dificuldade em cercear a liberdade que o anonimato na plataforma oculta traz.

Visto que o maior atrativo da parte profunda da web é o anonimato, pois proporciona uma maior liberdade aos internautas que acessam a rede, sendo assim, uma maior autonomia na busca por informações, sem estar sendo vigiado constantemente, monitorados a todo momento. A navegação anônima, ocorre por intermédio do navegador TOR:

> Ao acessar um site normalmente, seu computador se conecta a um servidor que consegue identificar o IP; com o TOR isso não acontece, pois, antes que sua requisição chegue ao servidor, entra em cena uma rede anônima de computadores que fazem pontes criptografadas até o site desejado. Por isso, é possível identificar o IP que chegou ao destinatário, mas não a máquina anterior, nem a anterior, nem a anterior etc. Chegar no usuário, então, é praticamente impossível.

Esse software labora disfarçando o Internet Protocol – IP do usuário que deseja não ser detectado, assegurando o anonimato na rede durante a navegação.

O software denominado Tor (The Onion Router) foi criado na década de 1990, no Laboratório de Pesquisa Naval dos Estados Unidos, e recebeu o apoio da Eletronic Frontier Foundation, uma das organizações que se dedicam à defesa dos usuários da internet. O navegador foi criado e financiado pelos órgãos militares do país. Os cientistas responsáveis pela criação Paul Syverson, Michael G. Reed e David Goldschlag explicam que a finalidade era mascarar a identidade dos agentes que estivessem em missão. Mas somente no ano de 2003 a primeira versão estável do software foi liberada para o uso civil.

Conforme linha do tempo, revelaram-se e na década de 1990, David Goldschlag, Mike Reed e Paul Syverson, pesquisadores do Laboratório de Pesquisa Naval dos EUA, após muitas discussões e estudos avançados, tiveram a ideia de criar e implantar os primeiros projetos de pesquisa e protótipos de roteamento cebola. Assim, Tor Project, visando:

> O objetivo do roteamento cebola era ter uma maneira de usar a Internet com o máximo de privacidade possível, e a ideia era rotear o tráfego por vários servidores e criptografá-lo a cada etapa do caminho. Esta ainda é uma explicação simples de como o Tor funciona hoje.

Já nos anos 2000, Roger Dingledine, juntamente com Paul Syverson iniciaram um trabalho juntos a respeito do roteamento cebola. Porém, com a denominação de Tor (The Onion Routing), diferenciando do projeto trabalhado anteriormente. Em 2002 a rede foi finalmente implantada, sob uma licença de software livre e aberta, contava com uma rede descentralizada. Porém, ainda privada e em teste, em 2003 a rede contava com uma dúzia de voluntários. Ganhou cada vez mais espaço e visibilidade, portanto em 2004, a Electronic Frontier Foundation (EFF), após reconhecer o Tor como benefício para os direitos digitais, concordou em financiar o trabalho dos estudiosos da área, e em 2006 tornou-se uma organização sem fins lucrativos.

O navegador Tor surgiu em 2008, ficando muito popular entre usuários experientes e ativistas interessados na privacidade, protegendo a identidade dos usuários e também permitindo acessar certos conteúdos que em meio a censura era impossibilitado, bem como a mídia social, sites bloqueados e recursos críticos. Possui atualmente milhares de retransmissores e milhões de usuários por todo o mundo. Segundo a equipe, Tor Project (2006):

> Nós, do Projeto Tor, lutamos todos os dias para que todos tenham acesso privado a uma internet sem censura, e o Tor se tornou a ferramenta mais forte do mundo para privacidade e liberdade online.

Apresentando-se mais do que apenas um software, além de um trabalho com muita qualidade e paixão pela comunidade dedicada aos direitos humanos, estando profundamente comprometida com a transparência e segurança de seus usuários.

Ainda assim, cabe destacar um dos benefícios que a Dark Web possibilita exercer, como a liberdade de expressão àquelas pessoas que vivem em meio a regime totalitários, segundo David Duarte e Tiago Mealha (2016, p. 02), para países democráticos, a utilização desta ferramenta acaba se tornando um meio para a prática de diversas ilicitudes, dessa forma, tem se tornado alarmante, necessitando medidas rápidas para coibição:

> É aqui que chegamos ao centro do debate: por um lado o Tor permite, entre outras coisas, assegurar a privacidade das comunicações entre os utilizadores e visualizar artigos e blogs que não se encontram na Surface Web; por outro lado o anonimato serve de ferramenta para que ocorra a prática de atividades ilícitas. Existe uma linha muito tênue que separa a esfera pública da esfera privada.

> O Tor permite reforçar a segurança ao utilizar a Internet. Cabe ao bom senso de cada um a forma como utiliza as ferramentas ao seu dispor.

A criação da Internet foi um fenômeno extraordinário, onde abriu portas para o conhecimento, que andando juntamente com a informação, agora se encontra ao alcance de qualquer pessoa capaz de se conectar neste meio digital, tornando-se uma ferramenta universal. Ainda assim, o ciberespaço, visto como um espaço que abriga os demais, bem como as diversas partes da web, acredita-se que o conceito de não lugar esteja presente nas características da Dark Web, pois essa web é trajeto de passagens sem relações e identificações.

Ainda no contexto contemporâneo, se mantém a ideia de que tudo está presente no Google, porém poucos sabem que a internet é formada pela junção da Surface Web e Deep Web, sendo muito mais ampla do que a população mundial imagina. Havendo diversos perigos recorrentes do mal uso da ferramenta, devendo haver uma atenção maior a práticas ilícitas neste ambiente, buscando a reconstrução para assim haver o reparo.

Verificou-se que a Surface Web é muito utilizada pela massa, envolvendo o uso com ferramentas de busca, compartilhamento de informações e entretenimento. Porém há o lado de que a Deep Web é revelada como um espaço restrito, acessível somente a algumas pessoas. Equivalente a 96% de toda a internet (Bergman 2001, p. 01), e, portanto, desconhecida por grande parte do público.

Com a expansão severa da internet, poucos ainda percebem que a própria Surface Web é um perigo, quem dirá a Deep Web, que além do anonimato oferecido, é pouco conhecida e é vista com tamanha desconfiança. Cabe a compreensão de entendimento por essa web profunda, analisando como funciona seu acesso, e a necessidade da criação de medidas para coibir ações delituosas que consequentemente surgem neste espaço.

Entretanto, com a contemporaneidade em relação a internet, deveria ser uma ferramenta de auxílio e evolução para o homem, e não de sua própria destruição. Volto a discutir sobre a necessidade de regulamentação para o uso desta rede, como ações governamentais para vistorias das possibilidades do uso da web.

# 3 A LIBERDADE DE EXPRESSÃO E AS POSSÍVEIS FALHAS DE REGULAMENTAÇÃO NO ÂMBITO DIGITAL OCULTO

Segundo julga a sociedade contemporânea, seria de competência do Direito Penal o enquadramento para configurar ou não uma infração penal, e portanto, atribuir uma sanção de acordo com o grau de lesividade. Sendo assim, se faz uma análise, sob a luz da Constituição da República Federativa do Brasil de 1988.

Devido ao grande avanço tecnológico, consequentemente surgem novos mecanismos de interação digital, que visam atender às demandas dos usuários. Nesta situação, exigem certa condição, que é o zelo da privacidade ao acessar a rede, atendendo essa demanda, criou-se a Deep Web. Espaço onde reina o anonimato e os internautas interagem e navegam entre si sem haver a identificação dos mesmos.

## 3.1 A LIBERDADE DA EXPRESSÃO COMO DIREITO FUNDAMENTAL: EXTENSÃO E LIMITES

A rede é considerada um dispositivo de comunicação livre da censura e demais barreiras, também considerada como uma abundância de materiais favoráveis à cultura. Porém sua web profunda é alvo de debates jurídicos, devido sua natureza complexa, pois em sua profundidade são encontradas situações desfavoráveis às situações sociais, bem como venda de drogas, armas, incentivo ao canibalismo, etc. Sendo assim, essa parte da internet transforma-se em um meio de comunicação livre de barreiras e da censura.

Diante disso, o presente trabalho busca elucidar e realizar uma análise sobre os limites e a possibilidade da vedação ao acesso à web profunda, contando com o posicionamento constitucional, legal e doutrinário sobre os direitos e garantias. É necessário dissertar a respeito da liberdade de expressão como direito fundamental e previsto em nossa Constituição da República Federativa do Brasil de 1988, artigo 5°, IV, onde trata sobre a livre manifestação do pensamento, juntamente com a vedação ao anonimato e ainda sim acrescentar à discussão o artigo 220, do mesmo dispositivo legal, que trata da comunicação social, estabelecendo que as formas de comunicação descritas não seriam passíveis de qualquer restrição.

Daniel Sarmento (2006, p. 93), aprofunda o tema, concluindo que:

> A liberdade de expressão ocupa uma posição extremamente destacada no sistema constitucional brasileiro. O texto constitucional chegou a ser redundante ao consagrá-la: art. 5°, inciso IV – liberdade de manifestação do pensamento -; art. 5°, inciso X – liberdade de expressão de atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença -; art. 5°, inciso XIV – direito à informação e garantia do sigilo da fonte jornalística -; art. 220, caput – garantia da manifestação do pensamento, da criação, da expressão e informação, sob qualquer forma e veículo -; art. 220, §1°- liberdade de informação jornalística em qualquer veículo de comunicação social -; art. 220, §2° - proibição de qualquer censura de natureza política, artística ou ideológica. Do ponto de vista histórico, não é difícil compreender as razoes que levaram o constituinte a tamanha insistência: tratava-se de exorcizar os fantasmas do regime militar, que praticara aberta censura política e artística, e de assegurar as bases para a construção de uma sociedade mais livre e democrática.

É visto que o autor relata alguns dispositivos que levam consigo os ideais de liberdade de expressão, de forma a demonstrar um dos principais motivos, a censura praticada durante o regime militar.

O legislador conferiu status de direito fundamental à liberdade de expressão, visando garantir o pleno exercício desse direito, reprimindo qualquer questão que inviabilize sua efetivação. Além disso, adotou a liberdade de expressão como fundamento do Marco Civil da Internet – Lei número 12.965/2014, em que objetiva a disciplina do uso da Internet no Brasil, fundamentado na liberdade de expressão. Como consta em seu artigo 2°, o pleno exercício do uso da internet no Brasil fundamenta-se ao respeito à liberdade de expressão, sendo garantidos o reconhecimento da escala mundial da rede, os direitos humanos, desenvolvimento da personalidade e o pleno exercício da cidadania no âmbito digital, além da pluralidade e diversidade em rede, abertura e colaboração, a livre iniciativa, concorrência e defesa do consumidor, findando a finalidade social da rede (BRASIL 2014).

No mais, a disposta Lei, ainda se refere sobre a liberdade nas condições dos princípios, configurando essa condição para o pleno exercício do direito de acesso à internet, e ainda assegurando a liberdade de expressão, impedindo qualquer tipo de censura no ambiente virtual.

O estudioso sobre o tema, Carlos Affonso Pereira de Souza (2015, p.3), afirma que a respeito do artigo 6° da referida Lei, é dado um emprego profuso da locução liberdade de expressão em sua redação do texto, portanto revela que o intuito normativo não seria somente sancionar condutas, mas sim garantir a liberdade conquistada pelos usuários da rede:

> O Marco Civil da Internet, profícuo em menções à liberdade de expressão, explicita em seu artigo 6° que a sua vigência não visa apenas a sancionar condutas, como, mas tipicamente se esperaria de uma legislação penal, mas principalmente visa assegurar as liberdades conquistadas através do uso da rede.

Portanto, com demasiadas aparições da liberdade de expressão na redação da referida Lei, infere-se a importância dada pelo legislador, isto pois, a referida garantia visa possibilitar plena utilização da web, tornando o usuário livre para expressar-se na rede, livre de qualquer forma de censura ou repressão, tornando uma esfera vantajosa para o debate e discussão de ideias.

Entretanto, visa salientar que a liberdade de expressão não é um direito absoluto, pois existem demais direitos da personalidade, os mesmos que são classificados como características fundamentais a toda pessoa humana, além de obter o reconhecimento jurídico resultante de uma constante progressão de façanhas históricas.

Não obstante, a liberdade não pode ser classificada como absoluta, quando assim, encontrar-se em questão com demais direitos da personalidade, bem como o direito à privacidade, o mesmo que no âmbito digital deve ser muito bem verificado.

Anderson Schreiber (2013 p.135), afirma que o direito à privacidade deve abranger também o direito da pessoa humana, ou seja, proteger além da vida íntima de cada pessoa. Em sua obra Direitos da Personalidade, conclui que:

> Deve abranger também o direito da pessoa humana de manter o controle sobre os seus dados pessoais. Mais sutil, mas não menos perigosa que a intromissão na intimidade doméstica de uma pessoa, é a sua exposição ao olhar alheio por meio de dados fornecidos ou coletados de forma aparentemente inofensiva, no preenchimento de um cadastro de hotel ou no acesso a um site qualquer na internet. O uso inadequado desses dados pessoais pode gerar diversos prejuízos ao seu titular.

Sendo assim, percebe-se que o direito à privacidade possui certa importância, adequadamente à caracterização contemporânea, abrangendo, além da intimidade dos indivíduos, como também os demais dados que são munidos no amplo espaço da rede. Progressão de suma importância, visto que as relações interpessoais crescem abundantemente a cada dia no meio digital, devido a constância no avanço tecnológico.

Cumpre importantemente exemplificar a distinção entre a privacidade e a intimidade, pois no direito brasileiro já há essa discussão entre o âmbito dos direitos da personalidade. Elencados no artigo 5°, inciso X, da Constituição Federal (1988) são dados os termos: “São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Entretanto, no Código Civil (2002), especificamente o seu artigo 21, apresenta certa definição a respeito do direito à vida privada: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma”.

Desse modo, devido a apresentação em dois artigos, há autores que defendem a diferenciação entre os termos, entretanto, ainda não se concretizou uma uniformização doutrinária ou legislativa.

Junior Ferraz (1993, p.442), grande estudioso da matéria, explica a respeito da privacidade e a intimidade:

> No recôndito da privacidade se esconde, pois, em primeiro lugar, a intimidade. A intimidade não exige publicidade, porque não envolve direitos de terceiros. No âmbito da privacidade, a intimidade é o mais exclusivo dos seus direitos. Há, porém, uma certa gradação nos direitos da privacidade. Também o direito ao nome, à imagem, à reputação compõe o campo da privacidade. A imagem, a reputação, o nome, à diferença da intimidade, são exclusivos (próprios), mas perante os outros. Como direito à privacidade, demarcam a individualidade em face dos outros. Ninguém tem um nome, uma imagem, uma reputação só para si mesmo, mas como condição de comunicação.

Portanto, pode-se entender que a intimidade seria considerada na esfera de parte exclusiva, sendo assim, ao que o indivíduo reserva para só, sem visar

repercussão social, do contrário, sem que sua vida privada seja alcançada. Já a vida privada, seria cabível na classificação de que mesmo estando em isolamento, seria sempre alcançável por terceiros que em certos momentos possam estar em contato com a pessoa, como por exemplo no lar familiar, no trabalho.

Como já dito anteriormente, entende-se que a liberdade de expressão seria como uma estimativa básica para o pleno exercício do acesso à internet. Porém, esse direito não pode ser absoluto, visto que se encontra em limitações juntamente com outros direitos, como o direito à privacidade, o direito à personalidade, entre outros que também devem ser respeitados.

Sendo assim, em âmbito constitucional, o direito à privacidade é elencado como um direito fundamental, previsto no inciso X, do artigo 5° da CRFB/88, norma esta que garante a inviolabilidade da intimidade, vida privada, da honra e da imagem de todas as pessoas, além de conferir aos que sofreram algum tipo de dano, o direito a indenização.

Podemos considerar que o dispositivo abordado é de extrema relevância no ordenamento jurídico, pois o legislador fez questão de conferir a todos de maneira abrangente a revelada garantia, além de litigar judicialmente, almejando a devida reparação resultante de possível dano sofrido.

Marcel Leonardi (2011, p. 52), em sua obra Tutela e privacidade na internet, traz uma análise de o que é “o direito a ser deixado só” – *the right to be let alone* – expressão prestigiosa, elucidada por Samuel D. Warren e Louis D. Brandeis, onde difundiram o conceito do juiz norte-americano Thomas M. Cooley, e realizaram um artigo denominado *The right to privacy.* Doutor Marcel, explica que o “direito a ser deixado só” não indicaria o que realmente a privacidade representa, não servindo para denominar o que está protegido no âmbito digital:

> O direito a ser deixado só, porém, não indica o que exatamente a privacidade representa; não aponta em que circunstâncias nem sobre quais questões devemos ser deixados a sós. A ideia de “estar só” é de “ser deixado em paz”, mencionada por Warren e Brandeis e posteriormente por outros autores, é vaga e não serve como guia para definir o que está ou não incluído no seu âmbito de proteção.

Portanto, o mencionado direito seria como um instrumento de abrangência ilimitada, buscando dar aos indivíduos um isolamento intensificado. Entretanto, por promover um exacerbado isolamento social do indivíduo, seria ilógico de acordo com a situação contemporânea vivida em sociedade, visto que marcado pela intensificação das relações interpessoais.

Seria melhor relacionar o direito à privacidade com a proteção dos dados pessoais dos usuários em rede, pois os mesmos, intencionalmente ou não, deixam rastros de navegação, sendo por cadastros em sites, interações em redes sociais e até mesmo buscas em grandes sites de navegação que por coerência, são indexados.

A questão seria que, a todo instante, mesmo que inconscientemente, os indivíduos da rede deixam rastros em quantidade de dados, devendo ter adequada atenção e proteção, visto que estes dados implicam no direito à privacidade.

O legislador percebeu as mudanças que estavam ocorrendo neste âmbito contemporâneo e também no cenário internacional e optou, portanto, em seguir o mesmo rumo frente à proteção de dados pessoais. Em 15 de agosto de 2018, foi publicada a Lei de número 13.709/2018, entrando em vigor no dia 15 de janeiro de 2020.

A referida lei diz respeito ao tratamento de dados pessoais, instituindo parâmetros para regularização de modo que os dados devessem ser armazenados por instituições públicas, privadas ou até mesmo pessoas naturais, isso tudo, conforme dispõe seu artigo 1°, objetivando assegurar o direito fundamental à liberdade, privacidade e o livre desenvolvimento da personalidade de todos usuários da rede.

Também conhecida como LGPDP (Lei Geral de Proteção de Dados Pessoais), determina e diferencia os dados pessoais sensíveis, em seu artigo 5°, incisos I e II. Portanto, dados pessoais são informações relacionada a pessoa natural identificada ou identificável, e especificamente os dados pessoais sensíveis seriam mais aprofundados, sendo:

Art. 5º Para os fins desta Lei, considera-se:

> II – Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

O dispositivo normativo caracteriza em sua área de aplicação o que é considerado dados pessoais, os mesmos que ainda são classificados como sensíveis.

Portanto, é notável que a citada lei visa assegurar os direitos fundamentais dos internautas, principalmente nas questões relativas à liberdade, à privacidade e ao livre desenvolvimento da personalidade da pessoa natural, fato que constitui grande avanço à proteção de dados dos usuários da rede. Contribuindo para o usuário, visto que agora amparado pela norma, consolida-se a segurança jurídica esperada.

A Lei Geral de Proteção de Dados Pessoais (2018) tem forte impacto diretamente no tratamento dos dados pessoais, previstos no artigo 7° da referida Lei[1], versando sobre as hipóteses, ou seja, requisitos para o tratamento dos dados. Onde impacta diretamente nas instituições que ficam responsáveis por esse tratamento, pois é possível apenas mediante expressa autorização do titular.

---

[1] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Outra mudança notória seria em relação aos titulares dos dados. Portanto, tornou-se de forma facilitadora o acesso e controle de dados, presente no Capítulo III da referida legislação, tratando dos direitos do titular.

Portanto, conforme dispõe seus artigos, pode-se afirmar que nessa inovação legislativa, é cedida maior liberdade ao usuário da rede, maior autonomia ao titular dos dados, além de exemplificar sobre a utilização dos mesmos, possa realizar um manuseamento da destinação conferida. Sendo assim, o titular pode ainda requerer confirmação, correção, bloqueio e até mesmo a eliminação de dados que julgar dispensável ou desmoderado, como dispõe o artigo 18 da LGPDP (2018).

Cumpre-se salientar que esta inovação legislativa traz estabelecido sanções administrativas aos agentes de tratamento de dados que transgredirem, ficando sujeitos à uma multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, limitada no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

Sendo assim, se faz necessário a verificação sobre a referida lei, onde segue a tendência global modificando-se constantemente nos aspectos relacionados ao tratamento de dados pessoais. Como também o direito à privacidade e uma breve análise sobre seus impactos como garantia fundamental para o âmbito digital, além do “direito a ser deixado só” e o posicionamento americano, repentinamente o referido direito fundamental na Constituição da República Federativa do Brasil de 1988.

## 3.2 A (IN)CAPACIDADE DO ESTADO EM REGULAR A LIBERDADE DE EXPRESSÃO NA DEEP WEB

A internet é uma tecnologia que se encontra em constante inovação, a mesma que possibilita a transmissão de dados de um ponto, à ponto oposto do mundo. Portanto superando os demais meios de transmissão de informações tradicionais, tornando-se líder neste assunto. Podendo acarretar essa propagação frenética de informações de efeitos positivos, mas também negativos.

Entretanto, podemos dizer que a internet é inserida dentro da lógica de operação do capitalismo e, portanto, apesar da perseguição estatal, visando a

regulamentação e controle da Internet, facilmente novas restrições técnicas podem surgir. Bem como técnicas no uso de criptografia, assim como o exemplo do software Tor, que é utilizado para acesso mascarado, por meio de servidores que operam voluntariamente, manejando na forma de Internet dentro da Internet, onde passa por diversos pontos, ou seja, localidades, de forma aleatória, portanto sem rotas do tipo padrão (como são os provedores de Internet locais).

Nesse sentido, seguindo a lógica de inovação e capitalismo, podemos afirmar que as ferramentas para estas técnicas não seriam eternas, pelo contrário, estão sujeitas a mudanças a todo instante, e por esse entendimento, se o software mais utilizado atualmente deixasse de atender as necessidades dos usuários, não garantindo plena satisfação que em seu objetivo, poderia facilmente ser substituído por outro software, com provável novo paradigma a ser perseguido e assim sucessivamente.

É inevitável que ameaças se originem da rede mundial de computadores, assim que a transmissão de um dado chegue ao seu destino final, porém observamos que é preocupante aos governos, e devem os mesmos, exercer certo monitoramento e um satisfatório controle para que os usuários possam utilizar a rede.

Entretanto, houve o escândalo envolvendo o Projeto Prisma, da NSA – agência de segurança nacional dos Estados Unidos, um tipo de programa de vigilância constante e em tempo real, supostamente monitorando ligações telefônicas e atividades realizadas com cartões de créditos, além de toda movimentação realizada na Internet. Um ex-agente da NSA, revelou que o país monitora tudo o que todas pessoas fazem na internet, disse que o PRISM (Project Prism) contaria com uma colaboração das maiores companhias digitais do mundo, como Facebook, Microsoft, Apple e Google. Como prevê a matéria no The Guardian por (GREENWALD; MACASKILL; POITRAS, 2013, p.01):

> O indivíduo responsável por um dos vazamentos mais significativos da história política dos EUA é Edward Snowden, um ex-assistente técnico da CIA de 29 anos e atual funcionário da empresa de defesa Booz Allen Hamilton. Snowden trabalhou na Agência de Segurança Nacional nos últimos quatro anos como funcionário de várias empresas terceirizadas, incluindo Booz Allen e Dell. [...] Mas ele acredita que o valor da internet, juntamente com a privacidade básica, está sendo rapidamente destruído pela vigilância onipresente. “Não me vejo como um herói”, disse ele, “porque o que estou fazendo é interesse próprio: não quero viver em um mundo onde não há privacidade e, portanto, não há espaço para exploração

> intelectual e criatividade". [...] Para ele, é uma questão de princípio. "O governo concedeu a si mesmo um poder ao qual não tem direito. Não há fiscalização pública. O resultado é que pessoas como eu têm liberdade para ir além do que lhes é permitido".

Sendo assim, o anonimato na internet passa a ter um novo entendimento, sendo este, proteger-se de uma possível retaliação desequilibrada advinda do Estado. Podemos citar o caso explícito de ativistas dos Direitos Humanos, que por viverem em Estados Totalitários, para não sofrerem desforras, buscam o anonimato para utilizarem a Internet e exporem o que julgam ser necessário.

É aparente a falta do direito em áreas específicas da vasta internet, decorrente do mesmo não conseguir caminhar lado a lado com as brutais atualizações e avanços que a rede faz. Entretanto, o fato do direito não se manter atualizado não implica sua precariedade no sentido do acompanhamento, mas sim, o aumento obrigatório das atualizações tecnológicas acatarem legislações regulamentadoras alusivas ao seu uso, cabendo a verificação de riscos e proveitos para sociedade.

Estas tecnologias devem se adequar ao direito existente, isto para prevenir possíveis problemas decorrentes de sua criação, pois esses mecanismos de busca podem ir além das esferas legais, e seguindo este caminho, poderão trazer riscos aos indivíduos que não tenham a devida capacidade de se subordinam às leis que impõe o limite legal, portanto, podendo adentrar em áreas cuja classificação é maligna ao objeto ideal social.

Portanto a gravidade das ilicitudes cometidas no âmbito da Deep Web, foi preciso regulamentar esse espaço, o Brasil, em 2012, aprovou a Lei Carolina Dieckmann, que dispõe sobre a tipificação criminal de delitos informáticos, e logo a frente, em 2014, aprovou a Lei 12.965 que foi Marco Civil da Internet, e revogada tacitamente pela Lei 13.709/2018 a Lei Geral de Proteção e Dados, isto pois, enquanto o Marco Civil da Internet prévia segurança de dados apenas em ambiente online, a LGPD (Lei Geral de Proteção e Dados), criou diretrizes específicas de aplicação e segurança, detalhando os dados existentes e assegurando a movimentação dos mesmos, até mesmo offline.

Tendo em vista a possibilidade de os usuários se comunicarem com territórios em escala global, criou-se um tratado internacional, assinado por 11 países e hoje já

inclusos mais de sessenta, denominado Convenção de Budapeste. De acordo com o site do Ministério Público Federal:

> A Convenção de Budapeste tem como objetivo facilitar a cooperação internacional para combater o cibercrime. Elaborado pelo Comitê Europeu para os Problemas Criminais, com o apoio de uma comissão de especialistas, o documento lista os principais crimes cometidos por meio da rede mundial de computadores e foi o primeiro tratado internacional sobre crimes cibernéticos. A Convenção já foi assinada por mais de 60 países e é utilizada por outros cerca de 160 como orientação para as legislações locais.

Entrado em vigor em 1° de julho de 2004, ficou demonstrada a necessidade de combater tais crimes cibernéticos por toda sociedade mundial. Crimes estes tipificados na Convenção de Budapeste (2001), como infrações contra confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos, a interceptação ilegal de dados ou comunicações telemáticas, além de atentados à integridade de sistemas e produção, comercialização, obtenção ou posse de aplicativos ou códigos que permitam a prática destes crimes. Ainda assim, tipifica infrações relativas ao conteúdo como a difusão de imagens, ideias ou teorias que propaguem ou incentivem o ódio, discriminação ou a violência contra uma pessoa ou grupo de pessoas em âmbito de racismo e xenofobia, além de injúria e ameação qualificadas pelo mesmo motivo entre também outros crimes contra a humanidade.

Sendo assim, consiste na harmonização das legislações penal e processuais sobre o crime virtual, sendo considerado o único instrumento jurídico de caráter global sobre o cibercrime. Visando facilitar e fortalecer os meios disponíveis para enfrentar os crimes cibernéticos, somando com a lei do Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais.

E no mesmo viés, Castells (2007, p.203) assevera que:

> O estado não desaparece [...]. É apenas redimensionado na Era da Informação. Prolifera sob a forma de governos locais e regionais que se espalham pelo mundo com seus projetos, formam eleitorados e negociam com governos nacionais, empresas multinacionais e órgãos internacionais. A era da globalização da economia também é a era de localização da constituição política. O que os governos locais e regionais não têm em termos de poder e recursos é compensado pela flexibilidade na atuação em redes.

Apesar de haver ineficiência em diversas legislações internas, isto ocorre devido à facilidade do malfeitor em manter a conexão com diversos locais e ainda sim mascarar sua localização. A regulamentação internacional se posiciona como obstrução fortificada em valores, cultura e princípios, bem como a liberdade de expressão, interesses econômicos e política interna e externa, portanto, viabilizando a elaboração de normas em concordância de todos. Desse modo (CHAWKI; WAHABI, 2006, p.29), esclarece que:

> Persiste a necessidade de estabelecer normas globais e padrões para reger a conduta e comportamento no mundo virtual. Apesar da necessidade, as políticas nacionais e regionais podem colidir com essa normatização global. Isto exige regulamentação universal ou global considerando o impacto transnacional e arrebatador inerente do cibercrime. Apesar da dificuldade intrínseca na harmonização ou unificação de políticas criminais e penais, sendo uma manifestação de poder soberano e autoridade, as participações no ciberespaço têm instigado os Estados a trilharem por uma nova época de cooperação em matéria de direito penal e público território irregular e vacilante. [...]O objetivo principal da Convenção é harmonizar a legislação penal material e procedimento de investigação internas. Eram duas as principais preocupações dos redatores da Convenção: a primeira era assegurar que as definições fossem flexíveis a ponto de se amoldar aos novos tipos de crimes e seus métodos e a segunda era manter-se sensível aos regimes jurídicos dos Estados-nação. Estas preocupações foram especialmente desafiadoras na área de direitos humanos, porque os estados têm diferentes valores morais e culturais. Por exemplo, os países europeus têm um grau muito mais elevado de proteção da privacidade do que os Estados Unidos.

Sendo assim, considera-se necessário um consenso mundial a respeito da aceitação e aplicação das propostas legais, havendo uma concordância em relação ao uso da internet nas diversas partes do globo.

A Comunicação Social anda junto com o rol do artigo 5°, IX, da CF/88 (BRASIL 1988), portanto a liberdade de expressão da atividade intelectual, artística, científica e de comunicação, independente de censura ou licença. Devendo haver importante proteção do "meio pelo qual o direito individual constitucionalmente garantido será difundido, por intermédio dos meios de comunicação em massa" (MORAES, 2006, p.792). Bem como também cabe uma explicação do jurista Alexandre de Moraes a respeito do que são os meios de comunicação, portanto "pode-se entender meio de comunicação como toda e qualquer forma de desenvolvimento de uma informação, seja através de sons, imagens, impressos,

gestos, etc." (MORAES, 2006, p.792).

Entretanto vale destacar que a Internet é um meio de comunicação de grande potencial informativo e formador de opinião, tanto quanto rádios e televisão. Devendo ter certa atenção, não negando sua importância para a atual sociedade, além disso, necessitando de devida regulamentação dentro do território nacional.

A inviolabilidade prevista no rol de direitos fundamentais no artigo 5°, X, da CRFB/88 (BRASIL 1988), descreve os limites da liberdade de expressão e demais itens previstos no rol. Portanto, podemos afirmar que a liberdade de expressão e os demais dispositivos legais, estão sujeitos a limites descritos pela Constituição Federal, resultando em responsabilidade civil ou penal àqueles que deturparem esse direito.

Vale dizer que a insegurança em relação à privacidade gerou implicações em escala global, acarretando na fortificação do Regulamento Geral de Proteção de Dados (GDPR), um dos conjuntos de lei mais completos e com efeitos paternalistas em relação à vida on-line. Conforme matéria do Globo (GLOBO G1, 2018), exemplifica:

> É considerada como uma medida reativa a espionagem promovida pelos Estados Unidos, que foi exposta em 2013 por Edward Snowden, que permite ao usuário o direito ao esquecimento, isto é, pode solicitar que sua conta seja completamente apagada, e também ser notificado em 72 horas no caso de suas informações serem hackeadas e a coleta de dados só pode ser realizada com consentimento tácito ao usuário, essas são algumas mudanças promovidas pela medida GDPR.

Além disso, outra modificação constante é a respeito do anonimato na rede, isto devido aos discursos do politicamente correto, o que acaba privando as pessoas com ideias opostas.

E com a liberdade de expressão há também o problema do Hate Speech, traduzido como discurso de ódio. Está ligado à fixação dos limites à liberdade de expressão, pois pode estar relacionado, ou não, a manifestações de ódio, desprezo e intolerância contra grupos, além de movidas por preconceitos ligados a gênero, etnia, religião, dentre outros fatores. (SARMENTO, 2006, p.02).

No Brasil, o tema já foi abordado e discutido em decisão do Supremo Tribunal Federal, quando no caso Ellwanger (HC n° 82.424/RS, Plenário, Rel. Min. Maurício Corrêa, 2003), decidindo “que a liberdade de expressão não protege manifestações de cunho antissemita, que podem ser objeto de persecução penal pela prática do

crime de racismo". (SARMENTO, 2006, p.3). Porém, lembremos que a liberdade de expressão não existe somente para proteger opiniões que não seguem o politicamente correto, ou que estão de acordo com valores aceitos pela maioria, mas também aquelas que provocam e sensibilizam.

Os direitos humanos, em seus tratados internacionais, proíbem o discurso de ódio, por mais importante que seja a liberdade de expressão nesse âmbito, posicionamento explícito em diversos documentos internacionais, contra a proteção ao exercício abusivo desse direito. Vale apontar a claridade no artigo 4° do Pacto Internacional a respeito da discriminação racial, estabelecendo condenação a todo tipo de propagando e até organizações que se fundam em ideias ou teorias de superioridade de uma raça ou grupo de pessoas de uma cor ou origem étnica, que promovam ódio racial ou discriminação. Portanto adotam medidas que visam cessar os atos que impulsionam a discriminação ou de discriminação, estabelecendo como crime os atos de disseminação ou discriminação racial, como atos de violência ou provocações dirigidos a qualquer raça, cor, origem étnica, inclusive assistencia prestada a atividade racista. Além de deixar claro a ilegalidade, proibindo atividades onde propagam a discriminação racial, sendo puníveis a participação ou atividades destas organizações.[2]

Portando, neste caso, explícito pela discriminação racial, a primordialidade de coibição a manifestos de ódio e preconceito contra grupos raciais e étnicos, com certa ênfase a difusão de ideias que se originam através das novas tecnologias,

---

[2] Os Estados partes condenam tôda propaganda e tôdas as organizações que se inspirem em idéias ou teorias baseadas na superioridade de uma raça ou de um grupo de pessoas de uma certa côr ou de uma certa origem étnica ou que pretendem justificar ou encorajar qualquer forma de ódio e de discriminação raciais e comprometem-se a adotar imediatamente medidas positivas destinadas a eliminar qualquer incitação a uma tal discriminação, ou quaisquer atos de discriminação com êste objetivo, tendo em vista os princípios formulados na Declaração universal dos direitos do homem e os direitos expressamente enunciados no artigo 5 da presente convenção, êles se comprometem principalmente:

a) a declarar delitos puníveis por lei, qualquer difusão de idéias baseadas na superioridade ou ódio raciais, qualquer incitamento à discriminação racial, assim como quaisquer atos de violência ou provocação a tais atos, dirigidos contra qualquer raça ou qualquer grupo de pessoas de outra côr ou de outra origem étnica, como também qualquer assistência prestada a atividades racistas, inclusive seu financiamento;

b) a declarar ilegais e a proibir as organizações assim como as atividades de propaganda organizada e qualquer outro tipo de atividade de propaganda que incitar à discriminação racial e que a encorajar e a declarar delito punível por lei a participação nestas organizações ou nestas atividades.

c) a não permitir às autoridades públicas nem às instituições públicas, nacionais ou locais, o incitamento ou encorajamento à discriminação racial.

como a Internet.

Há a necessidade do debate sobre o impacto que o banimento ou a permissão das manifestações de ódio causam, para isso cabe a palavra de Sarmento (2006, p.29), sobre a busca da verdade na ideia de liberdade de expressão:

> A ideia básica da liberdade de expressão como instrumento para a obtenção da verdade parte da premissa de que, no contexto do debate livre entre pontos de vista divergentes sobre temas polêmicos, as melhores ideias prevalecerão. Sob esta perspectiva, a liberdade de expressão é vista não como um fim em si, mas como um meio para a obtenção das respostas mais adequadas para os problemas que afligem a sociedade.

Sendo assim, não se pode dizer com convicção que uma ideia está errada, pois nela pode sempre conter um fragmento de correção, pondo em exemplo as diferentes posições daqueles que são considerados equivocados pelo governo. Por mais que uma ideia esteja incorreta, proibir sua expressão publicamente seria equivocado. Pois o confronto de diferentes ideias pode fortalecer uma discussão e assim se sofisticarem, fundirem e solidificar, não se convertendo em apenas palavras.

Em ambiente de discussões de ideias, onde se busca a predisposição dos participantes de ouvir e refletir sobre os argumentos apresentados, Sarmento (2006, p.30) interpõe, dizendo que:

> Este ambiente é simplesmente inviabilizado pelo *hate speech*, que está muito mais próximo de um ataque do que de uma participação num debate de opiniões. Diante de uma manifestação de ódio, há dois comportamentos prováveis da vítima: revidar com a mesma violência, ou retirar-se da discussão, amedrontada e humilhada. Nenhum deles contribui minimamente para a busca da verdade.

Dessa forma, o pilar da liberdade de expressão deve ser mantido, não considerar que uma ideia é errada suficiente para coibi-la e suprimir. Portanto, é de extrema relevância que as expressões negativas de ódio, preconceito e intolerância, não contribuam para um debate, como também comprometem determinada discussão. Sendo assim, a busca da verdade não justifica a proteção do discurso de ódio, mas recomenda a sua proibição (SARMENTO 2006, p.31).

Contudo, podemos dizer que a liberdade de expressão é peça chave para um regime democrático, sendo assim, permite a vontade coletiva através de ideias, a expressão de pontos de vista e exposição de clamor. Sarmento (2006 p.32) conclui a

respeito:

> [...] uma democracia real pressupõe a existência de um espaço público robusto e dinâmico, em que os temas de interesse geral possam ser debatidos com franqueza e liberdade. Só assim os cidadãos podem ter acesso às informações e às idéias existentes sobre as variadas questões, o que lhes permite formarem as suas próprias opiniões sobre temas controvertidos e participarem conscientemente no autogoverno da sua comunidade política.

A restrição, portanto, deve ser estabelecida como um mecanismo para garantia da integridade do próprio discurso público, assegurando regras para o reconhecimento da igual dignidade do povo.

Entretanto, no cenário apresentado, se percebe que há uma distância entre as normas básicas de direitos humanos, visto as promulgações de tratados internacionais, com intuito de exercer a proteção da segurança nacional, violar para proteger a sociedade de uma ameaça maior. Porém, observemos que a proteção é dada à ideologia dos que exercem o poder sobre a sociedade por meio do Estado. Sendo eficaz o controle e monitoramento que visa a antecipação para um possível ataque terrorista, sendo assim, identificando a possível articulação antes da concretização do fato, porém questiona-se o fato do monitoramento de empresas executivas estrangeiras de enorme importância, onde manipulam grande valor econômico, e ainda chefes de estado em parcerias com grandes comerciais.

Todavia, momento em que se vale a vontade do Soberano, é um estado de exceção, em que se violam os direitos fundamentais de liberdade, expressão, sigilo de correspondência, informação, entre outros demais, isto por razões políticas. A exemplo dos termos estados de defesa, artigo 136, e estado de sítio, artigos 137 a 139, presente na Constituição da República Federativa do Brasil de 1988 (BRASIL, 1988).

Gilberto Bercovici (2007, p.62) explica o estado de exceção como: “o Estado suspende o direito em virtude do direito de auto-preservação”. Portanto, seria uma legitimação da alegação do estado de continuar e se manter no poder a ordem vigente.

Como visto, quando se trata de estado de exceção, os direitos fundamentais não são uma prioridade, pois o Estado confere esses direitos fundamentais conforme entendimento de que eles atuam como mecanismos que garante sua

preservação e quando sua ordem normalmente se encontra ameaçada, a exceção é permitida para retornar à normalidade.

Se discute também a respeito do vigiar e punir, como aplicado no caso NSA, e em países totalitários, diferente do Brasil, esse modo iria ferir diversos direito fundamentais previstos na Constituição Federal (BRASIL 1988), portanto os que tratam a respeito da livre manifestação de pensamento (art. 5°, IV), a livre expressão intelectual, artística, científica e de comunicação (art. 5°, IX), intimidade, vida privada, honra, imagem das pessoas (art. 5°, X), sigilo da correspondência (art. 5°, XII), acesso à informação (art. 5°, XIV) e a reunião pacífica (art. 5° XVI).

Portanto artigos estes que são atrelados a ideia da violação do indivíduo em seu aspecto mais íntimo, como prevê os incisos X e XVII citados, além da ideia de repressão ideológica onde observa-se o texto legal nos incisos IV, IX e XIV. Direitos estes que garantem aos indivíduos de quem quer que esteja no poder do Estado, tenha controle sobre a mentalidade dos cidadãos, além de que a violação torna a vida do ser em sociedade, sem privacidade e intimidade, nem se quer o benefício de não ser perturbado, todos têm o direito de fazer ou deixar de fazer algo, e portanto, um instrumento que regule isso é considerado de caráter repressivo, porquanto realiza o cerceamento a vida. A internet como ferramenta veicular de comunicação em massa, portanto barreiras e limites reforçam ainda mais a dominação ideológica, sendo assim, o seu monitoramento constante significa saber quando algo foi acessado, onde e por quem.

Sendo assim, Eduardo Magrani (2018, p.23) afirma que os dispositivos conectados diariamente irão, cada vez mais, transmitir, compartilhar e armazenar uma abundante quantidade de dados íntimos da vida do indivíduo. Sendo que a segurança e a privacidade destes usuários da rede correriam riscos com o aumento da utilização desses dispositivos e demais que futuramente entrarão neste âmbito.

O ordenamento jurídico brasileiro protege o direito à privacidade, em seu texto legal presente na Constituição da República Federativa do Brasil de 1988 (BRASIL 1988) onde diz "é livre a manifestação do pensamento, sendo vedado o anonimato" e "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral

decorrente de sua violação", texto legal presente no artigo 5°, IV e X da CRFB/88.

O direito à privacidade também é legalmente previsto, na Quarta Emenda à Constituição americana (1987), onde dispõe que:

> O direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum mandado será expedido a não ser mediante indícios de culpabilidade confirmados por juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas.

Bem como a África do Sul que adotou regulamentos específicos sobre a atividade do uso da Internet, aprovado no fim de 2013, a Lei de Proteção de Informação (Protection of Personal Information Act) rege sobre a proteção à privacidade e cria uma entidade estatal de regulação (Information Protection Regulator), que visa fiscalizar a aplicação da lei e adicionar códigos de condutas, zelando as informações, além de labutar intermediando a solicitação de dados entre entidades.

Portanto percebe-se que há uma falta de conceito legislativo, quando diz respeito à privacidade, embora alguns países como a África do Sul tenham buscado delimitar a taxativa de privacidade, em contexto global, podemos considerar um grande avanço tecnológico.

O direito à privacidade objetiva uma forma de vetar o anonimato, criando uma certa expectativa de identificar aquele que comete ato ilícito, dessa forma, acaba-se criando a lógica de que o anonimato somente é utilizado pelo indivíduo que pratica delitos. Rodotà (2013, p.12) elucida a respeito da privacidade e anonimato:

> O "homem de vidro" é a imagem que se usa para descrever um cidadão que, não tendo nada a esconder, bem pode revelar cada detalhe de sua vida, tornar-se visível por meio da verdadeira e completa descrição daquilo que é. A verdade, assim entendida, torna-se uma contínua cessão do eu para os outros, para as instituições públicas em primeiro lugar, para um algum Estado totalitário em particular. Não esquecemos a matriz nazista daquela imagem, que deu vida a um modelo adotado, depois, por todas ditaduras, reforçado pela potência tecnológica, que torna cada vez mais fácil a coleta de dados pessoais, não desdenhado nem mesmo pelas democracias todas as vezes que uma "emergência" qualquer fornece a justificativa.

Retórica essa, considerada abusiva, pois quando se fala que o bom cidadão não tem nada a esconder, confirmamos a prática de todos sabermos quando alguém dorme, come, quando cada um toma banho, se tem certos hábitos, se paga as

contas em dia. Acaba tornando-se algo perturbador, como um reality show em que as pessoas são observadas vinte e quatro horas por dia.

## CONCLUSÃO

As relações em meio a sociedade digital avançam abruptamente, a capacidade e velocidade de mensagens instantâneas a serem enviadas de um lado para outro do mundo, é praticada cada vez com maior facilidade. Dentre desse âmbito, se encontram camadas que só são acessadas mediante softwares capazes de implementar criptografia, utilizando-se de métodos eficazes para garantir pleno anonimato ao usuário.

Todavia, o excesso de anonimato e liberdade de expressão corrompe alguns dos usuários dessa rede, toda segurança atribuída dá ao entender do usuário a possibilidade de expressar-se sobre tudo, independente do certo ou errado, dentre isso, atos de violência e provocação dirigidos contra raça, cor, origem étnica, entre outros. Sendo assim se torna necessário um posicionamento legal viabilizando controlar o acesso, limitando o anonimato. Pois a rede segue em constante atualização, no momento em que focar a ferramenta utilizada, momentos após será substituída por outra que pode agir de diferentes formas para cumprir seu objetivo.

Como ocorre na Surface Web, especificamente em redes sociais, a liberdade de expressar o que pensa, o que faz e o que gostaria de fazer deriva da segurança que as pessoas sentem, por não estarem em público com as pessoas do âmbito na sociedade digital. Relaciona-se com o anonimato, visto a não obrigatoriedade de expor seus dados em um perfil na rede social. Discussões políticas, discursos de ódio, compõem muitas vezes o ambiente digital, muito mais próximos de um ataque do que uma participação em discussão.

A Deep e Dark Web, são ambientes propensos para a prática de atos ilícitos. O legislador foi competente ao impor os dispositivos legais que hoje regem a sociedade em rede. Portanto, há de relatar a respeito do avanço abrupto da tecnologia, os meios e métodos em constante otimização a ponto de fortalecer e atuar de forma mais eficaz possibilitando, em caso necessário, a substituição da ferramenta e com isso, proporcionar de forma mais eficiente sua finalidade. Restando não deficiente, mas sim, incompleta a legislação hoje imposta.

Apresentadas as ferramentas e dadas as circunstâncias, a lei 12.965 do Marco Civil da Internet contribuiu muito para o entendimento dos princípios, direitos e deveres em âmbito da rede de computadores. Além da Lei Geral de Proteção de Dados Pessoais 13.709 de 2018, criando diretrizes especificadas, aplicando mais

segurança e detalhando os dados existentes. Como também a regulamentação das empresas atuantes no país, orientando o como devem agir em relação à coleta, tratamento e compartilhamento de dados pessoais e sensíveis.

Entretanto, o estudo realizado verifica-se limitado, devido à percepção única, sendo desenvolvida a compreensão a partir de uma única parte. Sendo possível expandir em novos caminhos, possibilitando novos estudos a serem realizados com a percepção de demais estudiosos da área.

Por fim, se conclui a importância de conhecer as ferramentas tecnológicas ocultas, o valor que elas têm em relação aos direitos fundamentais, tanto no ponto positivo quando relatado, quanto no negativo. Há de frisar que a legislação brasileira que trata sobre a proteção dos dados, é de suma importância, porém há de buscar atualizações e melhorias, para que assim, acompanhe o avanço tecnológico e consequentemente esteja preparado para o que possa surgir.

Portanto há se frisar que existe alternativas de regulação presentes em todo âmbito comunicacional informático em que navegamos, apresentados da forma em que a lei amolda o próprio design da web, como no uso da inteligência artificial através de bots (robôs) para monitorar as redes sociais, regulando o discurso de ódio. Além de que há estratégias híbridas, onde combina a regulação do estado, com a auto regulação das empresas, onde o estado certificaria algumas práticas empresariais como satisfatórias para regular a web. Criando leis, no sentido estrito, de forma principiológicas, em que as regras de regulação se dão de forma administrativa, para quando surgir alguma nova prática, certa agência cria uma determinada estratégia por decreto ou resolução. Porém, formas estas expostas, somente válidas para surface web, deixando o campo não indexável à mercê de regulamentações.

**REFERÊNCIAS**

AUGÉ, M. **Não lugares:** introdução a uma antropologia da supermodernidade. Tradução Maria Lúcia Pereira. 9. ed. Campinas: Papirus, 2012. Disponível em: https://revistas.marilia.unesp.br/index.php/aurora/article/view/4711. Acesso em: 12 nov. 2021.

BECKETT, A. **The dark side of the internet**: in the deep web, Freenet software allows users complete anonymity as They share viruses, criminal contacts and child pornography. The Guardian, London, 26 nov. 2009. Disponível em: https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet. Acesso em: 12 nov. 2021.

BERCOVICI, G. E-premissas, 2007. **O Estado de exceção econômico e a periferia do capitalismo.** Disponível em: http://www.unicamp.br/nee/epremissas/pdfs/2/03.02.pdf. Acesso em: 12/04/2022.

BERGMAN, Michael K. **The Deep Web: Surfacing Hidden Value**, 2001. Disponível em: https://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main. Acesso em: 12 set. 2021.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 02 set. 2021.

BRASIL. **Lei n° 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n° 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 02 set. 2021.

BRASIL. **Lei n° 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 03 set. 2021.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm#art65. Acesso em: 03 set. 2021.

CALDERON, Bárbara. **Deep e Dark Web: a Internet Que Você Conhece É Apenas a Ponta Iceberg**. Alta Books. 2017. Disponível em: https://altabooks.com.br/produto/deep-e-dark-web/. Acesso em: 03 set. 2021.

Castells, Manuel. **Fim do Milênio**. São Paulo: Paz e Terra, 2007.

CASTELLS, Manuel. **A sociedade em rede**. A era da informação: economia, sociedade e cultura; v. 1. São Paulo: Paz e Terra, 1996. Disponível em:

https://globalizacaoeintegracaoregionalufabc.files.wordpress.com/2014/10/castells-m-a-sociedade-em-rede.pdf. Acesso em: 10 out. 2021.

CHAWKI, Mohamed; WAHABI, Mohamed**. Identity theft in cyberspace: issues and solutions**. Disponível em: https://papyrus.bib.umontreal.ca/xmlui/handle/1866/9563. Acesso em: 10/04/2022.

DUARTE, D.; MEALHA, T. 2016, **Introdução à Deep Web,** IET Working Papers Series, WPS01/2016. Disponível em: https://run.unl.pt/handle/10362/18052. Acesso em: 13 nov. 2021.

EAST, C. S. **Demystifying the Dark Web**. ItNow, v. 59, n. 1, 2017. Disponível em: https://www.researchgate.net/publication/314225204_Demystifying_the_Dark_Web. Acesso em: 12 nov. 2021.

Ferraz Júnior, T. S. (1993). **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado**. *Revista Da Faculdade De Direito, Universidade De São Paulo*, *88*, 439-459. Recuperado de https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 02/06/2022.

FULTON, C.; MCGUINESS, C. **In too deep**. Digital detectives: solving information dilemas in na on-line world. 2016, p. 95-118. Disponível em: https://www.semanticscholar.org/paper/In-Too-Deep-Fulton-McGuinness/1710dadd3c116062b2306b3a72835c58d8c3b105. Acesso em: 13 nov. 2021.

GREENWALD, G; MACASKILL, E. The Guardian, 2013. **NSA Prism Program taps in to user data of Apple, Google and others.** Diponível em: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. Acesso em: 12/04/2022.

HURLBURT, G. **Shining light on the dark web**. Computer, v. 50, n. 4, p. 100-105, 2017. Disponível em: https://www.computer.org/csdl/magazine/co/2017/04/mco2017040100/13rRUB7a14I Acesso em: 10 nov. 2021.

LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Saraiva, 2011.

MICELI, André Lima Cardoso.**TIINSIDE.** Professor da FGV alerta para os riscos da “dark web”. 2019. Disponível em: https://tiinside.com.br/20/03/2019/professor-da-fgv-alerta-para-os-riscos-da-dark-web/. Acesso em: 10 out. 2021.

Magrani, Eduardo. **A internet das coisas**. Rio de Janeiro, 2018. Disponível em: http://eduardomagrani.com/livro-internet-da-coisas-2018/. Acesso em: 14/05/2022.

Ministério Público Federal. **Crimes cibernéticos: manual prático de investigação**. São Paulo: Procuradoria da República de São Paulo: 2006. https://www2.mppa.mp.br/sistemas/gcsubsites/upload/60/ManuaL%20Pr%C3%83%C2%A1tico%20de%20Investiga%C3%83%C2%A7%C3%83%C2%A3o%20sobre%20Crimes%20de%20Inform%C3%83%C2%A1tica.PDF.

MORAES, Alexandre. **Constituição do Brasil interpretada e legislação constitucional**. 6ª ed. São Paulo: Atlas, 2006.

MONTEIRO, S. D.; FIDÊNCIO, M. V. As dobras semióticas do ciberespaço: da web visível à invisível. **TransInformação**, Campinas-SP, n. 25, v. 1, p. 35-46, jan./abr. 2013. Disponível em: https://www.scielo.br/j/tinf/a/Pk5r9yxsgkbyRWctn6Rd4GH/?lang=pt&format=pdf. Acesso em: 20 set. 2021.

PEREIRA, Leonardo. **Deep web: saiba o que acontece na parte obscura da internet**. 06 dez. 2012. Disponível em: https://olhardigital.com.br/2018/11/16/videos/deep-web-entenda-o-que-acontece no-lado-obscuro-da-internet/. Acesso em: 10 nov. 2021.

RODOTÁ, Stefano. **O direito à verdade**. Trad. Maria Celina Bodin de Moraes e Fernanda Nunes Barbosa. Civilistica.com. Rio de Janeiro, a. 2, n. 3, jul. set. 2013. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/125/95. Acesso em: 29/04/2022.

SARMENTO, Daniel. **A liberdade de expressão e o problema do hate speech**. Revista de Direito do Estado. Número 4 (outubro/dezembro) 2006, Rio de Janeiro; Renovar, 2006. Disponível em: http://professor.pucgoias.edu.br/sitedocente/admin/arquivosUpload/4888/material/a-liberdade-de-expressao-e-o-problema-do-hate-speech-daniel-sarmento.pdf. Acesso em: 24/06/2022

SHERMAN, Chris; PRICE, Gary. **The Invisible Web: Uncovering Information Sources Search Engines Can't See.** Information Today, Inc. 2001. Disponível em: https://www.amazon.com/Invisible-Web-Uncovering-Information-Sources/dp/091096551X. Acesso em: 05 ago. 2021.

SCHREIBER, Anderson. **Direitos da Personalidade**. 2. Ed. São Paulo: Atlas, 2013.

SOUZA, Carlos Affonso Pereira de **Cinco faces da Liberdade de Expressão no Marco Civil da Internet**, in: DE LUCCA, Newton, et al (Org.) Direito & Internet III – Marco Civil da Internet, Lei 12.965/2014. São Paulo: Quartier Latin, 2015.

**Tor Project**. Disponível em: https://www.torproject.org/. Acesso em: 11 nov. 2021.

VIGNOLI, R. G. **A topografia da dark web e seus não lugares**: por um estudo das dobras invisíveis do ciberespaço. 2014. Dissertação (Mestrado em Ciência da Informação) – Universidade Estadual de Londrina, Londrina 2014. Disponível em: http://www.bibliotecadigital.uel.br/document/?code=vtls000191992. Acesso em: 11 nov. 2021.

VIGNOLI, R. G.; Monteiro, S. D. **A Dark Web e seu conteúdo informacional**. Seminário de Ciência da Informação. 2015. Londrina. UEL. Disponível em:

http://www.uel.br/eventos/cinf/index.php/secin2016/secin2016/paper/viewFile/266/186. Acesso em: 11 nov. 2021.