

XXV ENCONTRO NACIONAL DO CONPEDI - BRASÍLIA/DF

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

JOSÉ RENATO GAZIERO CELLA

CINTHIA O. A. FREITAS

Todos os direitos reservados e protegidos.

Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI

Presidente - Prof. Dr. Raymundo Juliano Feitosa – UNICAP

Vice-presidente Sul - Prof. Dr. Ingo Wolfgang Sarlet – PUC - RS

Vice-presidente Sudeste - Prof. Dr. João Marcelo de Lima Assafim – UCAM

Vice-presidente Nordeste - Profa. Dra. Maria dos Remédios Fontes Silva – UFRN

Vice-presidente Norte/Centro - Profa. Dra. Julia Maurmann Ximenes – IDP

Secretário Executivo - Prof. Dr. Orides Mezzaroba – UFSC

Secretário Adjunto - Prof. Dr. Felipe Chiarello de Souza Pinto – Mackenzie

Representante Discente – Doutoranda Vivian de Almeida Gregori Torres – USP

Conselho Fiscal:

Prof. Msc. Caio Augusto Souza Lara – ESDH

Prof. Dr. José Querino Tavares Neto – UFG/PUC PR

Profa. Dra. Samyra Haydêe Dal Farra Napolini Sanches – UNINOVE

Prof. Dr. Lucas Gonçalves da Silva – UFS (suplente)

Prof. Dr. Fernando Antonio de Carvalho Dantas – UFG (suplente)

Secretarias:

Relações Institucionais – Ministro José Barroso Filho – IDP

Prof. Dr. Liton Lanes Pilau Sobrinho – UPF

Educação Jurídica – Prof. Dr. Horácio Wanderlei Rodrigues – IMED/ABEDI

Eventos – Prof. Dr. Antônio Carlos Diniz Murta – FUMEC

Prof. Dr. Jose Luiz Quadros de Magalhaes – UFMG

Profa. Dra. Monica Herman Salem Caggiano – USP

Prof. Dr. Valter Moura do Carmo – UNIMAR

Profa. Dra. Viviane Coêlho de Séllos Knoerr – UNICURITIBA

Comunicação – Prof. Dr. Matheus Felipe de Castro – UNOESC

D598

Direito, governança e novas tecnologias [Recurso eletrônico on-line] organização CONPEDI /UnB/UCB/IDP/ UDF;
Coordenadores: Cinthia O. A. Freitas, José Renato Gaziero Cella – Florianópolis: CONPEDI, 2016.

Inclui bibliografia

ISBN: 978-85-5505-177-7

Modo de acesso: www.conpedi.org.br em publicações

Tema: DIREITO E DESIGUALDADES: Diagnósticos e Perspectivas para um Brasil Justo.

1. Direito – Estudo e ensino (Pós-graduação) – Brasil – Encontros. 2. Governança. 3. Novas Tecnologias.
I. Encontro Nacional do CONPEDI (25. : 2016 : Brasília, DF).

CDU: 34



CONPEDI

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito

Florianópolis – Santa Catarina – SC
www.conpedi.org.br

XXV ENCONTRO NACIONAL DO CONPEDI - BRASÍLIA/DF

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

Apresentação

No XXV Encontro Nacional do CONPEDI, realizado de 06 a 09 de julho de 2016, que teve lugar na Universidade de Brasília - UnB, e que foi organizado pelo Curso de Pós-Graduação em Direito - Mestrado e Doutorado, da UnB - Universidade de Brasília; pela Universidade Católica de Brasília - UCB; pelo Centro Universitário do Distrito Federal - UDF; e pelo Instituto Brasiliense do Direito Público - IDP, o Grupo de Trabalho - GT “Direito, Governança e Novas Tecnologias” se destacou no evento não apenas pela qualidade dos trabalhos apresentados, mas pelo numeroso público, composto por pesquisadores-expositores e interessados, que deixou a sala AT085 (onde o grupo se reuniu) repleta até o término das atividades. Foram apresentados 14 artigos objeto de um intenso debate presidido pelos coordenadores e acompanhado pela participação instigante do público presente.

Esse fato demonstra a inquietude que os temas tratados no GT despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em Direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõem a enfrentar os desafios que as novas tecnologias impõem ao Direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva, os coordenadores do grupo de trabalho dividiram os artigos em blocos, que se congregam nesta coletânea.

A proteção à privacidade foi o pano de fundo do primeiro bloco de trabalhos apresentados. O direito à privacidade e a proteção de dados pessoais encontraram destaque no enfrentamento de temas como “zonas de convergência e conflito no que se refere aos direitos à privacidade e proteção de dados”, “relações trabalhistas e o direito fundamental à autodeterminação informativa”, a “proteção jurídica dos dados pessoais na Internet”, “captação e proteção de dados pessoais no Brasil”, e “privacidade do consumidor e captura de dados pessoais pelo fornecedor nos contratos eletrônicos”.

Os aspectos gerais da sociedade da informação foram objeto do segundo bloco de trabalhos que versaram sobre a “crise da soberania estatal e a Internet como instrumento ora de dominação ora de emancipação social no contexto da globalização do século XXI”, “banalização do exibicionismo e cultura do ódio na sociedade digital em função da agilidade de troca de informações”, “direito de acesso ao mundo virtual na sociedade informacional”, “regulamentação da Internet e a sua relação com o Estado nas sociedades contemporâneas”, “o acesso à Internet como bem essencial e o projeto do Facebook Internet.Org” e, finalmente,

discutiu-se sobre “crise na informação, questionando se os dados e informações digitais constituem-se em verdadeiro patrimônio economicamente aferível e proveitoso ao seu originador”.

As discussões acerca da democracia eletrônica congregaram temas como “efemeridade e liquidez das informações num contexto de redes sociais e computação em nuvem”, “tecnologias de informação como ferramentas de luta por direitos fundamentais”, “a tecnologia e o direito à informação como contribuintes para o exercício da democracia e o meio ambiente” e “movimentos sociais, crimes e cidadania no contexto da sociedade em rede”, descortinando o terceiro bloco de artigos apresentados no grupo de trabalho.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema “direito, governança e novas tecnologias”. Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em Direito brasileira, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. José Renato Gaziero Cella

Profa. Dra. Cinthia Obladen de Almendra Freitas

**REFLEXÃO SOBRE A RELAÇÃO ENTRE A INTERNET E O ESTADO NAS
SOCIEDADES CONTEMPORÂNEAS: A IMPORTÂNCIA DE UMA
REGULAMENTAÇÃO QUE COMPREENDA A DINÂMICA DO
DESENVOLVIMENTO TECNOLÓGICO E VALORIZE OS DIREITOS
FUNDAMENTAIS**

**REFLECTION ABOUT THE RELATION BETWEEN INTERNET AND STATE IN
CONTEMPORARY SOCIETIES: THE IMPORTANCE OF A PROPER
REGULATION THAT COMPREHENDS THE DYNAMIC OF TECHNOLOGICAL
DEVELOPMENT AND APPRECIATES FUNDAMENTAL RIGHTS**

**Matheus Fernando de Arruda e Silva ¹
Rui Decio Martins ²**

Resumo

O artigo faz uma reflexão, de caráter transdisciplinar e linha de raciocínio hipotético-dedutiva, sobre a relação entre a Internet e o Estado nas sociedades contemporâneas. O objetivo é demonstrar que a Internet não é simplesmente um meio de divulgação da informação em massa e necessita uma devida regulamentação, tendo em vista a dinâmica do desenvolvimento tecnológico e foco na valorização dos Direitos Fundamentais, previstos tanto no ordenamento jurídico interno como internacional, de modo a evitar uma regulamentação que possa configurar uma acepção de estado de exceção, admitindo-se a violação dos direitos dos usuários em prol da soberania estatal.

Palavras-chave: Estado, Internet, Direitos fundamentais

Abstract/Resumen/Résumé

The article makes a reflection, of transdisciplinary character and hypothetic-deductive reasoning line, about the relation between Internet and State in contemporary societies. The objective is to demonstrate that the Internet is not a simply mean of mass dissemination of information and needs a proper regulation, in view of the dynamics of technological development and emphasis on appreciating the Fundamental Rights, already provided in both the domestic and international legal system, in a way to avoid a regulation that can configure a meaning of exception state that admits the violation of the users' rights on behalf of State sovereignty.

Keywords/Palabras-claves/Mots-clés: State, Internet, Fundamental rights

¹ Mestrando em Direito pela Universidade Metodista de Piracicaba - Unimep. MBA em Gerência de Projetos pelo Centro Universitário Salesiano de São Paulo, 2015. Bacharel em Relações Internacionais pela FACAMP, 2013

² Coordenador e Professor Titular do Programa de Mestrado da UNIMEP. Doutor em Direito pela PUC/SP, 2003. Mestre em Direito pela USP, 1999. Graduado pela Faculdade de Direito da USP, 1982

1 Introdução

Nos últimos anos, com foco especial ao período que compreende o final dos anos 70 e a década de 80, deu-se início ao que ficou popularmente conhecido como globalização, termo esse, conforme apontado por Chesnais (1996, p. 23), como sendo de origem das escolas de administração de empresa norte-americanas (Harvard, Columbia, Stanford, etc). Ainda segundo Chesnais (1996, p. 23), o adjetivo global presente em globalização visava passar a mensagem de que não importava mais o local físico (lugar) onde se possam gerar lucros (valorizar o capital) porque os obstáculos de outrora foram superados, conforme expresso na seguinte passagem:

Em matéria de administração de empresas, o termo [global] era utilizado tendo como destinatários os grandes grupos, para passar a seguinte mensagem: em todo lugar onde se possa gerar lucros, os obstáculos à expansão das atividades de vocês foram levantados, graças à liberalização e à desregulamentação; a telemática e os satélites de comunicações colocam em suas mãos formidáveis instrumentos de comunicação e controle; reorganizem-se e reformulem, em consequência, suas estratégias internacionais.

A partir da passagem de Chesnais (1996), é possível observar que há uma estreita relação entre o capital e a tecnologia. Essa relação se configura da seguinte forma: a tecnologia passa a ser um instrumento para a comunicação e o controle, o que a torna em um mecanismo para a valorização do capital. Assim, para a atual ordem capitalista contemporânea, um grupo especial de tecnologias passam a ter uma relevada importância: as tecnologias de informação e comunicação (TIC).

Nesse artigo parte-se da hipótese de que é o Capital o principal responsável por uma série de problemas que assolam o universo da Internet (a exemplo de tráfico de drogas, pornografia infantil, etc), e não a Internet propriamente dita. Diante disso, o principal objetivo desse trabalho é demonstrar o porquê de a Internet (a qual pode ser inserida dentro do campo das TIC) não poder ser tratada como um meio de comunicação qualquer por parte do Estado em qualquer uma de suas esferas e, conseqüentemente, o porquê de ser necessário uma regulamentação que leve em consideração o entendimento sobre o seu devido funcionamento dentro das sociedades capitalistas contemporâneas. Esse objetivo decorre da hipótese de que a não compreensão pode levar a decisões equivocadas oriundas de uma má-percepção, com reflexos nos três poderes, e que, em casos extremados podem inclusive, conflagrar uma experiência de estado de exceção em Estados Democráticos de Direito.

Em caráter secundário, o presente trabalho buscou mostrar como a Internet, em que pese a sua origem e o papel enquanto mecanismo de valorização capital, possui uma real capacidade de valorização positiva dos Direitos Fundamentais (individuais, coletivos e difusos), previstos tanto no ordenamento jurídico interno (Constituição Federal) como internacional (Convenções e Tratados Internacionais), o que por sua vez, busca reforçar a importância de uma devida regulamentação capaz de valorizar o papel positivo da Internet.

De modo a se alcançar os objetivos ora elencados, o presente artigo pode ser classificado como teórico, com recorte temporal transversal, o qual leva em consideração o período do surgimento da Internet até os dias atuais e com material bibliográfico e documental transdisciplinar (enfoque entre as áreas de economia e direito). Essas escolhas metodológicas foram feitas não para realizar um esgotamento teórico, mas de modo a permitir uma fundamentação que possa dar ensejo à uma reflexão e debate na área de Direito referente a importância de uma regulamentação que tenha em vista a dinâmica do desenvolvimento tecnológico e foco na valorização dos Direitos Fundamentais.

Diante do exposto, esse artigo está dividido em três partes. Na primeira é realizada uma abordagem histórico-técnica sobre Internet e Inovação, que é considerado o pilar da hipótese ora elencada. Na segunda é abordada a relação entre a Internet, o Estado e os Direitos Fundamentais. Já a terceira parte compreende as diversas vertentes da Internet. Por fim, nas considerações finais é realizada a síntese desse trabalho.

2 Abordagem histórico-técnica sobre Internet e Inovação

Joseph Schumpeter (1961, p. 110), em sua obra denominada “Capitalismo, Socialismo e Democracia”, afirmou que as sociedades tipicamente capitalistas operam em uma espécie de processo de destruição criadora, o qual se constitui enquanto um “processo de mutação industrial que revoluciona incessantemente a estrutura econômica a partir de dentro, destruindo incessantemente o antigo e criando elementos novos”. Assim, é a partir desse processo que os agentes que estão inseridos dentro da lógica capitalistas devem se adaptar para sobreviver.

Ao se adaptar o agente passa a ficar inserido dentro de uma lógica de reprodução social pautada na inovação. As inovações poderão dar origem a novos bens de consumo, métodos de produção ou transporte, mercados, ou ainda formas de organização industrial criadas pela empresa capitalista (SCHUMPETER, 1961, p. 110). Nesse sentido, a constante produção de inovação é o que irá se constituir enquanto força motriz do capitalismo.

Observa ainda Schumpeter (1961) que o processo de destruição criadora deve ser compreendido dentro de um longo período de tempo e que somente pode ser devidamente analisado dentro desse contexto. Disso é possível afirmar que o processo de destruição seria lento uma vez levaria um período considerável de tempo para a destruição e criação das estruturas existentes. No entanto, como dentro dessa lógica a concorrência ocorre por meio da inovação e esta, por sua vez, deve ser cada vez mais constante, no capitalismo os processos de destruição criadora a partir de dado momento tenderiam a ocorrer com cada vez mais frequência.

Na atual fase do capitalismo, um tipo específico de tecnologia passou a ser o cerne das transformações: as tecnologias de informação e comunicação (TIC). Conforme aborda Castells (2000, p. 68) em sua obra “A sociedade em rede”:

O cerne da transformação que estamos vivendo na revolução atual refere-se às tecnologias da informação, processamento e comunicação. A tecnologia da informação é para esta revolução o que as novas fontes de energia foram para as revoluções industriais sucessivas, do motor a vapor à eletricidade, aos combustíveis fósseis e até mesmo à energia nuclear, visto que a geração e distribuição de energia foi o elemento principal na base da sociedade industrial.

A transformação a qual se refere o autor vai se caracterizar pela penetração desse rol específico de tecnologias nas mais diversas esferas da vida humana. Em sua obra “A Condição Humana”, Hannah Arendt (2010) aborda que as relações sociais ao longo do tempo passaram a ficar cada vez menores e como o termo global passou a dar uma noção de tamanho cada vez mais indeterminado. Nesse sentido, as próprias TIC atuam como instrumentos que reafirmam o questionamento do que é global. Hoje, devido a tecnologia como satélites e cabos intercontinentais de fibra ótica, é possível se comunicar com pessoas nas mais diversas localidades, mesmo que isso inclua ambientes remotos geograficamente. Com o avançar da tecnologia, a tendência é que mesmo lugares remotos possam em determinado momento serem alcançados em períodos cada vez mais reduzidos.

Como forma de visualizar o rápido avanço técnico da microeletrônica, uma formulação em especial merece destaque: “A lei de Moore”. Moore (Cf. INTEL, 2015), um dos co-fundadores da Intel, fabricante de chips estadunidenses, em 1965 elaborou o que ficou conhecido como “Lei de Moore”. De acordo com ela, o número de transistores dos chips aumentaria de forma exponencial a cada dois anos (aproximadamente entre 18 e 24 meses) a um determinado preço. Essencialmente, quanto maior o número de transistores maior o desempenho do chip. Esse aumento no número de transistores por sua vez, é acompanhado do

processo de miniaturização dos transistores. Se nos primórdios da informática os computadores ocupavam andares inteiros de edifícios, hoje não é de se admirar que um processador de um smartphone consiga ter muito mais performance e capacidade para a realização de cálculos.

A internet é fruto direto do desenvolvimento tecnológico. A sua origem histórica, conforme apontado por Castells (2000, p. 82), resulta do trabalho da ARPA – Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos que criou para fins estratégicos-militares uma rede de comunicação independente de centros de comando e controle, ou seja descentralizada, e que permitisse o fluxo informacional independente do ponto da rede que se encontrassem as partes interessadas.

Ainda de acordo com Castells (2000, p. 83), a ARPANET, nome dado a essa primeira rede de computadores, entrou em operação em 1º de setembro de 1969 e era aberta aos centros de pesquisa que colaboravam com o Departamento de Defesa dos Estados Unidos, ou seja, sua utilização inicial foi para fins acadêmicos-militares. Posteriormente houve a divisão da rede, sendo uma dedicada a fins acadêmicos (ARPANET) e outra exclusivamente para fins militares (MILNET). As diversas redes isoladas que surgiam passaram a ter como espinha dorsal a ARPANET. Esse entrelaçamento de redes passou a ser chamar ARPA-INTERNET e, posteriormente, INTERNET.

A ARPANET foi encerrada em 28 de fevereiro de 1990 e foi substituída pela NSFNET (uma das diversas redes que surgiram), porém essa também viria a ser encerrada em abril de 1995. Esse foi o primeiro passo para a Internet se constituir enquanto elemento privatizado. Sobre isso, afirma Castells (2000, p. 83):

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.

Em outras palavras, a Internet passou a ser regida por diversos entes, cada qual com algum tipo de responsabilidade. Isso se deve ao fato de a Internet ser basicamente composta por uma série de acordos e contratos multilaterais que regem a interconexão das redes. Cada *Internet Service Provider* (ISP), ou simplesmente provedor de internet (que é quem fornece o acesso à internet) possui acordo de interconexão com outro ISP, que por sua vez, possui acordo com outro ISP, e assim sucessivamente. Para se chegar a determinado endereço a

informação precisará percorrer as redes nas quais os ISP realizaram acordos multilaterais para a troca de tráfego.

Cabe ainda mencionar que cada ISP fornece a seus usuários uma identificação única na rede, o denominado endereço IP (*Internet Protocol*) (STALLINGS, 2005, 68). O endereço IP por sua vez, é fornecido aos ISP por meio de uma entidade que os administra. A nível mundial, quem originalmente administrava os endereços IP era o *Internet Assigned Numbers Authority* (IANA), porém atualmente, parte¹ das funções do IANA foram incorporadas pelo ICANN (*Internet Corporation for Assigned Names and Numbers*). Para o Brasil, a solicitação dos endereços cabe ao LACNIC (*Latin America and Caribbean Network Informatrion Centre*), localizado no Uruguai, e que coopera com o IANA para a alocação de endereços IP na região da América Latina e Caribe. Além do LACNIC existem outros organismos que realizam essa função nas outras regiões do mundo: APNIC (*Asia Pacific Network Information Centre*) para a região da Ásia e Pacífico, ARIN (*American Registry for Internet Numbers*) para os Estados Unidos e Canadá, RIPE NCC (*Réseaux IP Européens Network Coordination Centre*) para a região da Europa e do Oriente-médio e AFRINIC (*African Network Information Centre*) para a região da África. Todas essas entidades são denominadas entidades de registros regionais da Internet, as quais operam em cooperação ao IANA e ICANN.

Os domínios (ou *domains* no termo em inglês) atuam como um mecanismo de alocar um determinado nome a um endereço IP em específico. Essa conversão irá ocorrer por meio de servidores de sistema de nome domínio (*domain name system servers* ou simplesmente servidores DNS). No Brasil, quem opera os servidores de nome de domínio raiz do país, isso é, a autoridade competente para o fornecimento dos domínios “.br” é a entidade “Registro.br”, a qual sincroniza suas informações com os outros servidores de raízes DNS espalhados pelo mundo.

Assim, para um usuário ter um domínio “exemplo.com.br” ele deve ter um servidor de domínio interno que identifique qual o IP de internet atrelado a esse domínio. Por sua vez, o endereço IP do servidor DNS do usuário deverá estar registrado no Registro.br, o qual se encarrega de transmitir essas informações ao servidor raíze principal. Então, para um usuário

¹ Para maiores informações sobre as funções do IANA cabe a leitura do documento intitulado “Funções da Iana: o básico”. Cf. IANA. **Funções da Iana: o básico**. Disponível em < <https://www.icann.org/en/system/files/files/functions-basics-08apr14-pt.pdf> >. Acesso em 10 de fev. 2016.

acessar esse domínio (“exemplo.com.br”), o servidor de domínio do ISP desse usuário irá consultar um dos servidores DNS raiz espalhados pelo mundo².

Diante dessa breve exposição histórico-técnica é possível observar que a Internet, embora aparente funcionar de forma anárquica, isso é, sem um Estado principal que atue como controlador, está sujeita ao controle e monitoramento dos diversos países que a ela estão conectados. Isso permite a esses países a possibilidade de aplicar restrições contra ISPs, o que vai contra a concepção originária da Internet de garantir que uma informação alcance outra parte da rede e consequentemente, prejudica a utilização plena da mesma por parte dos usuários.

3 Internet, Estado e Direitos Fundamentais

A Internet é uma tecnologia e como tal adveio de uma inovação. Essa inovação está atrelada a necessidade de se transmitir uma determinada informação de um ponto ao outro. Ao se garantir que a informação chegue em determinado local, a informação consegue cumprir o seu papel: informar. A velocidade das informações e o alcance que a Internet propiciou superaram os meios de transmissão de informação tradicionais. Isso faz com que a propagação da informação possa ser tanto positiva como negativa.

O controle pleno da Internet, o Estado impor aquilo que pode e o que não pode, independentemente de sua justificativa, mais do que se constituir enquanto mera forma de censura, é uma violação aos direitos fundamentais individuais, coletivos e difusos. O Estado passa a assumir um discurso patriarcal para proteger os seus cidadãos quando na verdade o que se está promovendo é um mecanismo para a sua própria sobrevivência, o que é naturalmente contrário à concepção de Estado Democrático de Direito onde o que se deve prevalecer é a vontade da população e não a de seus governantes.

Todavia, cabe observar que a própria Internet está inserida dentro da lógica de operação do capitalismo e consequentemente, em sua lógica de inovação. Isso significa que apesar dos esforços dos Estados em realizarem o controle da Internet, formas de superar as restrições técnicas que forem impostas podem surgir. Esse é o caso do uso de técnicas avançadas que combinam o uso de criptografia e redes virtuais privadas, a exemplo do

² Cabe observar que os ISP costumam adotar a prática de cache de DNS, isso é, armazenar localmente a informação de identificação de qual domínio corresponde a determinado endereço IP em seus próprios servidores. Esse armazenamento tende a ser atualizado de tempos em tempos, e não a cada requisição individual, como forma de poupar recursos da rede e oferecer uma melhor experiência aos seus usuários por meio de um tempo de latência reduzido (quanto maior a distância física entre o usuário e o servidor DNS, em teoria, maior seria o tempo que o usuário levaria para acessar determinada página).

software “Tor³”, o qual permite acessar, por meio de servidores operados por voluntários, uma espécie de “Internet dentro da Internet”, isso é, acessar diferentes localidades sem utilizar as rotas padrões dos provedores de Internet locais.

Cabe lembrar que dado o ritmo de inovações do capitalismo, não é certo afirmar que as ferramentas e técnicas hoje empregadas para garantir a anonimato na Internet são eternas e imutáveis. Novas técnicas estão sujeitas a existirem a todo instante. A título de exemplificação, supondo que o *software* utilizado no exemplo anterior deixe de atender de forma satisfatória sua finalidade de garantir anonimato, não há o que impeça outro *software* de substituí-lo. Mais ainda, esse novo *software* seria o novo paradigma a ser perseguido, e assim sucessivamente.

As redes descentralizadas dentro da Internet, que utilizam tecnologia *peer-to-peer*⁴ (ponto a ponto) em detrimento de conexão direta, abrem possibilidades para a utilização cada vez mais anônima da rede, especialmente por conta da criptografia dos dados, ou seja, uma vez que os dados estão criptografados é necessário primeiro decodificá-los para somente então conseguir identificar qual o seu conteúdo. Essa é uma operação que consome tempo e recursos, embora não necessariamente impossível de ser realizada, a exemplo⁵ do caso de produtoras de conteúdo que processam usuários por transferirem ilegalmente da internet e compartilharem, por meio de aplicativos *peer-to-peer*, conteúdo protegido pelas leis de *copyright*.

As tecnologias de monitoramento e controle são inevitavelmente uma ameaça à concepção originária da Internet de garantir que um dado transmitido chegue a seu destino, reflexo esse de a Internet ter surgido para fins militares. No entanto, o que se observa e que deve ser motivo de real preocupação dado o seu impacto, é o posicionamento dos governos de exercerem monitoramento e controle cada vez maior daquilo que os usuários realizam na rede.

³ Segundo descrição disponível no próprio website do *software*, isso é possível graças a uma série de tuneis, os quais dificultam a identificação do acesso originário a determinado local da Internet (seja em um IP direto ou em um domínio). Em outras palavras, o Tor funciona como um mecanismo que permite um maior de caráter de anonimato dentro da Internet já que dificulta a identificação do endereço IP original. Uma vez que o IP não é identificado não é possível descobrir quem cometeu o ato.

⁴ *Peer-to-peer* (termo original em inglês) consiste em uma modalidade de conexão ponto-a-ponto; isso é, descentralizada da ótica cliente-servidor tradicional.

⁵ Conforme a notícia de Franklin (2015, online), uma produtora norte-americana processou usuários do aplicativo Popcorn Time por terem assistido a um filme protegido por leis de *copyright*. Esse aplicativo utiliza conexões do tipo *peer-to-peer* para transmitir conteúdo audiovisual via streaming. Dessa forma, ao mesmo tempo em que o usuário assiste (realiza o *download* para o seu dispositivo informático particular) ao conteúdo ele mesmo envia esse conteúdo (promove o *upload*, ou seja, compartilha) para outros usuários da rede do tipo *peer-to-peer* que utilizam o aplicativo Popcorn Time. No entanto, cabe observar que tal aplicativo utiliza mecanismos para ocultação dos usuários, ou seja, isso significa que de algum modo foi possível por parte da produtora descobrir a identificação dos usuários.

O escândalo relacionado ao *Project Prism* (Projeto Prisma) da *North American Security Agency* (NSA – agência de segurança nacional dos Estados Unidos), ferramenta utilizada pela agência ora referida para coletar dados de usuários com o propósito de “proteger a segurança nacional”, reforçou a questão do anonimato dentro da rede. Isso se deve ao fato de que foram colocados no mesmo lado da moeda tanto pessoas comuns quanto indivíduos perigosos à sociedade (terroristas). O problema é que tal ação não se aplica exclusivamente ao monitoramento de terroristas, mas sim a qualquer tipo de indivíduo sem distinção, conforme noticiado por Edward Snowden, o agente responsável pelo vazamento de informações sobre o monitoramento da NSA (Cf. GREENWALD; MACASKILL, 2013).

O estar anônimo na Internet passa então a ter novo significado: se proteger de uma eventual represália desproporcional advinda do Estado. É esse o caso típico dos ativistas de Direitos Humanos que, com medo justificado de sofrer represálias de Estados Totalitários, buscam formas de ficarem anônimos ao utilizarem a Internet.

No cenário exposto há um claro afastamento das normas básicas de direitos humanos, nas quais os Estados assinam e promulgam tratados internacionais, usando como discurso que o que realmente estão exercendo é a “proteção da segurança nacional”, ou seja, que eles estão violando apenas para proteger a sociedade de uma ameaça maior. Tal concepção é uma falácia porque o que está sendo protegida em verdade é a ideologia daqueles que exercem o poder sobre a sociedade por meio do Estado. Admite-se a possibilidade de o monitoramento e o controle realmente prevenirem a ocorrência de um ataque terrorista, ou seja, identificando uma suposta articulação antes da concretização do fato concreto, mas é de se questionar o que se dizer quando do monitoramento de executivos de empresas transnacionais estrangeiras de grande valor econômico ou ainda no caso dos chefes de estado de importantes parceiros comerciais.

Monitorar para vigiar e punir é a conflagração prática do estado de exceção: violam-se os direitos fundamentais de liberdade, expressão, sigilo de correspondência, informação, etc, para fazer valer a vontade do Soberano. Assim, esse estado de exceção se deve a razões políticas, não se configurando dentro de uma acepção estritamente jurídica-constitucional do termo, a exemplo dos termos estados de defesa, art. 136, e estado de sítio, arts. 137 ao 139, empregados na Constituição Brasileira de 1988 (BRASIL, 1988).

A acepção de estado de exceção fica evidenciada na abordagem de Gilberto Bercovici (2007, p. 62), segundo o qual “o Estado suspende o direito em virtude do direito de auto-preservação”. Em outras palavras, o estado de exceção é a validação da razão do estado de continuar a existir, ou seja, de manter no poder a ordem vigente. Essa lógica perversa é o

que admite os ISP monitorarem aquilo que seus usuários fazem quando inseridos dentro de suas redes, e repassar essas informações ao Estado (conflagração política da exceção) ou outras entidades que atendam o interesse do capital, como exemplo das entidades de proteção dos direitos autorais que fecham acordos com os ISP e contam com apoio legal (conflagração econômica da exceção).

Os direitos fundamentais não são exceção quando se trata da configuração de estado de exceção, já que continuam na posição de direitos inseridos dentro do ordenamento jurídico interno do Estado. Na normalidade, o Estado concede os direitos fundamentais porque compreende que os mesmos atuam enquanto um mecanismo de garantir sua preservação. Porém, se a ordem normal está ameaçada, a exceção é permitida para se voltar à normalidade, mesmo que isso inclua a suspensão desses direitos.

Com base na Constituição Brasileira de 1988, é possível afirmar que a prática de monitoramento da Internet para vigiar e punir, a exemplo do praticado pelos Estados Unidos (caso NSA) e China, feriria um extenso rol de direitos fundamentais (BRASIL 1988), dentre os quais: a livre manifestação de pensamento (art. 5º, IV); livre expressão intelectual, artística, científica e comunicação (art. 5º, IX); intimidade, vida privada, honra, imagem das pessoas (art. 5º, X); sigilo da correspondência (art. 5º, XII); acesso a informação (art. 5º, XIV) e reunião pacífica (art. XVI).

A livre manifestação de pensamento e de expressão e o acesso a informação (art. 5º, IV, IX e XIV) estão atrelados à ideia de repressão ideológica, ou seja, reprimir aquele que pensa de forma diferente daquele que está no poder do Estado. O indivíduo não informado é o indivíduo alienado, não esclarecido em uma concepção kantiana (Cf. KANT, 2015), gado, e como gado segue a manada. Isso garante a quem estiver no poder do Estado o controle sobre a mentalidade dos indivíduos e consequentemente, a possibilidade de se perpetuar no poder. A Internet é um veículo para comunicação em massa por excelência, as difusões das informações ocorrem em tempo recorde logo, controlar o que é disposto a todos na Internet é de pleno interesse da classe política.

Intimidade, vida privada, honra, imagem e sigilo de correspondência (art. 5º X e XVII) estão atrelados à violação do indivíduo em seu aspecto mais íntimo. Essa violação torna a vida do indivíduo um livro aberto a todos que tiverem acesso, ou seja, não lhe resta mais as benesses da privacidade e intimidade, tão pouco o benefício de não ser perturbado. Saber o que os indivíduos fazem ou deixam de fazer é um instrumento de notório caráter repressivo se caracterizando enquanto cerceamento da vida. São limites e barreiras impostos que reforçam ainda mais a dominação ideológica. Com o monitoramento da Internet isso

implica em saber o que foi acessado, onde foi acessado, quando foi acessado e com quem se comunicou ou se identifica ideologicamente. Em outras palavras, é uma lógica deturpada que, para o indivíduo não criar provas contra si mesmo, ele deve ser totalmente transparente.

A reunião pacífica pode ser entendida, dentro da Internet, como sendo a participação em fóruns de discussão e salas online de bate-papo. O monitoramento dessas atividades restringe a troca de informação e limita o impacto da comunicação. Ao se impedir a formação de grupos, impede-se o indivíduo de difundir informação, em especial aquela contra o regime político ideológico.

Também no plano internacional a defesa desses direitos fundamentais relacionados ao uso e acesso à Internet pode ser invocada. E assim o faremos numa ordem cronológica dos diversos instrumentos de *ius gens*.

A Carta das Nações Unidas, de 26 de junho de 1945, embora não trate o assunto diretamente, prevê em seu artigo 1º, § 3º, que são propósitos das Nações Unidas “conseguir uma cooperação internacional para resolver os problemas internacionais de caráter econômico, social, cultural ou humanitário, e para promover e **estimular o respeito aos direitos humanos e às liberdades fundamentais** para todos, sem distinção de raça, sexo, língua ou religião” (grifo nosso).

Na Carta da OEA – Organização dos Estados Americanos, de 30 de abril de 1948, o tema vem previsto de forma genérica já no artigo 2º. O artigo 12 estipula que não se pode restringir os direitos fundamentais **de maneira alguma** (grifo nosso). Na sequência, o artigo 38 prevê a difusão entre os seus Estados “dos benefícios da ciência e da tecnologia, promovendo, de acordo com os tratados vigentes e as leis nacionais, o intercâmbio e o aproveitamento dos conhecimentos científicos e técnicos”. Os Estados Membros deverão dar importância capital dos “seus planos de desenvolvimento, ao estímulo da educação, da ciência, da tecnologia e da cultura, orientadas no sentido do melhoramento integral da pessoa humana e como fundamento da democracia, da justiça social e do progresso”. Por fim, o artigo 51 propugna pelo desenvolvimento da ciência e da tecnologia e de “programas de difusão e divulgação” para adequá-las ao seu desenvolvimento integral.

No mesmo contexto de criação da OEA, e na mesma data, veio a público a Declaração Americana de Direitos e Deveres do Homem, que em vários dispositivos trata o tema deste trabalho: no Artigo IV, temos a liberdade de opinião e de expressão, além da difusão pensamento por qualquer meio e aqui, é obvio, inclui-se a Internet. Pelo Artigo V resguarda-se a inviolabilidade da vida privada e familiar. O Artigo X reza sobre a inviolabilidade da correspondência e garante sua circulação. O Artigo XII garante a toda

pessoa o direito à educação “para melhorar o seu nível de vida e poder ser útil à sociedade”. Qualquer restrição abusiva ao acesso à tecnologia propiciada pela Internet fere esse direito. No artigo seguinte, toda pessoa “tem o direito (...) de ser protegida em seus interesses morais e materiais, no que se refere às invenções, obras literárias, científicas ou artísticas de sua autoria”.

Alguns meses depois de publicada a citada Declaração, foi a vez da ONU trazer sua inestimável contribuição para a proteção dos Direitos Humanos, com a edição da Declaração Universal dos Direitos Humanos, em 10 de dezembro de 1948. A defesa de certos direitos correlacionados ao tema deste artigo vem prevista em vários dispositivos, a começar pelo Artigo XII que versa sobre a defesa do direito à inviolabilidade de correspondência e à vida privada. A liberdade de pensamento, consciência e religião encontra guarida no Artigo XVIII. O artigo XIX prevê que “toda pessoa tem direito à liberdade de opinião e expressão; esse direito inclui a liberdade de, sem interferências, ter opinião e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras”. O Artigo XXVI cuida de que “a instrução técnico-profissional será acessível a todos”. O próximo artigo resguarda o acesso à cultura e à participação “do progresso científico e de seus benefícios”.

No ano de 1966, dois grandes pactos referentes aos direitos humanos foram editados no âmbito da ONU: o Pacto Internacional sobre Direitos Civis e Políticos, e o Pacto Internacional dos Direitos Econômicos, Sociais e Culturais.

Pelo primeiro, as liberdades de pensamento, de consciência, e de religião estão previstas no Artigo 18; a liberdade de expressão e de opinião encontra amparo no Artigo 19. O desfrute do “progresso científico e suas aplicações” estão no Artigo 15.

Seguindo nossa ordem temporal, a Convenção Americana sobre Direitos Humanos, de 1969, mais popularmente conhecida como Pacto de San José da Costa Rica, em seu Artigo 12 garante o direito à liberdade de consciência e de religião e, no artigo seguinte, a liberdade de pensamento e de expressão.

4 Demistificando diversas vertentes da Internet

Cabe agora distinguir três vertentes da Internet: *web*, *deep web* e *dark web*. Essa classificação não é oficial e tão pouco doutrinária. O objetivo dessa classificação é apenas para fins didáticos-explicativos de modo a facilitar a compreensão do leitor. Reconhecem-se ainda outras classificações possíveis, a exemplo daquelas que foram sintetizadas e apresentadas por Monteiro e Fidencio (2013, p. 43), a saber: *Web* visível, *Web* invisível, *Web*

opaca, *Web* privada, *Web* proprietária, *Web* oculta, *Dark web* e *Dark net*, sendo que estas últimas podem ser alocadas dado o caráter de ilicitude envolvido dentro da classificação única de *Dark web* e as demais na formulação de *Deep web*.

Web seria a parte plenamente visível, disponível pelos motores de busca. É a Internet que está disponível ao abrir o navegador. Não existe nenhuma espécie de barreira para a acessar. Os sites que estão disponíveis possuem seu conteúdo plenamente mapeado pelos motores de busca, ou seja, é a Internet que todos os usuários, iniciantes ou avançados, acessam em seu dia-a-dia. Artigos acadêmicos, bem como os de revistas, tendem a utilizar também a nomenclatura *Surface web* para se referir a essa web em específico, ou seja, ela é tratada como a Internet superficial ou ainda “porção plenamente visível”.

Deep web, ou *web* profunda em tradução livre, é a parte não visível da Internet. As barreiras para acesso podem incluir registros, convites, *softwares* específicos (a exemplo de websites “.onion” acessados pelo *software* Tor), dentre outros itens possíveis. É o caso de websites que estão parcialmente mapeados pelos motores de busca, mas que para acessar de forma plena é necessário um registro. Isso se deve ao fato de o administrador do site não ter interesse em realizar sua plena publicação ou ainda chamar a atenção de autoridades governamentais ou não. Sítios privados, nos quais seja necessária alguma forma de autenticação para acesso, ainda que para fins lícitos (a exemplo de comunidades virtuais e fóruns discussão), nos quais seja necessária algum tipo de aprovação por parte do administrador do sítio para poder ter o acesso pleno, também podem ser enquadrados nessa classificação, já que o que está oculto é o conteúdo e não o domínio em si.

Dark web, por sua vez, seria uma espécie de lado negro da Internet. As barreiras são ainda mais complexas do que as empregadas na *Deep web*, já que o seu uso é corriqueiramente associado a atividades ilícitas (a exemplo de comércio de drogas). Por conta disso, é óbvio que os métodos de acesso envolvem tecnologias avançadas e complexas, como uso extensivo de redes virtuais privadas e criptografia.

É possível argumentar que esses três termos seriam apenas um só: *web*. Isso não deixa de ser verdade, uma vez que todos fazem parte da Internet. Outra argumentação possível é que *Deep web* e *Dark web* são na verdade a mesma coisa, isso é *Deep web*, ou seja, a parte não plenamente visível da Internet em que o acesso via motores de busca e navegadores web tradicionais são difíceis ou impossíveis. Essa segunda argumentação não deixa de ter sentido lógico uma vez que barreiras são necessárias para acessar o conteúdo desses locais.

No entanto, as simplificações de tais abordagens apresentam uma falha conceitual: não há distinção com relação a qualidade do conteúdo presente e consequentemente, dos motivos que justificam as barreiras empregadas para o acesso. Esse problema ideológico-conceitual não se apresenta se realizada essa classificação didática.

O motivo de justificar a qualidade é de fácil compreensão: a *Deep web* pode contribuir para a efetiva proteção dos direitos humanos, o que abarca direitos fundamentais coletivos e difusos, a exemplo do caso ora exemplificado da utilização da *Deep web* para divulgação de informações que ocorrem em Estados Totalitários. Além disso, restringir quem pode acessar o conteúdo promove ainda a possibilidade de se garantir valer a privacidade e a intimidade dos indivíduos na rede: não é porque coloca uma informação como disponível na Internet que todos os indivíduos do mundo devam ter direito pleno de acesso àquela informação. Os limites dos direitos fundamentais são os próprios direitos fundamentais, logo o direito à privacidade e a intimidade do indivíduo estão em pé de igualdade com o de acesso à informação, logo o direito de acesso à informação não deve se sobressair a ele.

As técnicas empregadas na *Deep web* e *Dark web*, cujo o foco é o anonimato, dificultam a ação do Estado, uma vez que só é possível punir seja o usuário que acesse seja o fornecedor do conteúdo em si, se for possível identificar qual a respectiva responsabilidade das partes envolvidas. O anonimato perfeito, em teoria, impede a identificação do responsável logo, se não sabe quem comete o ilícito não há como punir pois não há o sujeito ativo, na forma de um indivíduo ou de um grupo de pessoas, o que é uma base do Direito Penal.

Apesar desse aspecto negativo da tecnologia, isso é, de sua utilização para a realização de atos e condutas criminosas, o que deve ser perseguido não é a tecnologia. Ao se combater uma determinada tecnologia, dada a lógica de inovação, outra tecnologia surgirá, ou seja, é uma medida paliativa e de resultado duvidoso pois só terá efeito até o surgimento do substituto. Nesse sentido parece mais sensato buscar soluções diretamente no mundo real, em vez de reprimir uma tecnologia em si, ou seja, centralizar os esforços nos motivos que levaram ao surgimento da *Dark web*, e cortar as suas verdadeiras raízes.

Embora o Estado seja dotado de recursos e mecanismos coercitivos, a tecnologia apresenta uma característica única: a evolução por meio da destruição criadora. É aqui que se encaixa a ideia da concorrência schumpeteriana, na qual a concorrência se dá pela capacidade de inovação. Quando se descobre uma brecha para quebrar o anonimato, outra tecnologia pode surgir e substituí-la. Mais ainda, a própria tecnologia já existente pode ser aprimorada e dificultar ainda mais a ação por parte do Estado. A exemplo de tal situação, basta observar a

evolução dos algoritmos criptográficos, os quais constantemente são mais difíceis de serem quebrados.

Monteiro e Fidencio (2013, p. 40) apontam que dado o mecanismo de indexação de conteúdo dos mecanismos de busca, nem todo o tipo de conteúdo é facilmente indexado. Isso se deve ao fator tecnológico envolvido. Nem todas as extensões e formatos de arquivo que possuem conteúdo textual, conseguem ser devidamente indexados para que haja a associação com termo buscado. No entanto, a própria tendência da evolução tecnológica faz que com o tempo mais arquivos e páginas passem a ser efetivamente indexados, tornando-se visíveis a mecanismos de busca tradicionais. Nesse sentido, esse conteúdo que hoje está disposto em porção não visível da *Web* passaria⁶ para a parte visível. Segundo Bergman *apud* Becket (2009, online), no final dos 90 a *Deep web* seria entre duas e três vezes maior que a *Web* normal. Nos dias de hoje, mensurar a dimensão real da *Deep web* seria uma difícil tarefa por dois motivos: (1) com o aumento de usuários da rede e avanço tecnológico, o usuário comum passou a ser também produtor de conteúdo, ou seja, aumentou o conteúdo tanto da porção visível como da não visível da *Web* e (2) a dificuldade de mensurar a quantidade de conteúdo hoje existente. Por conta dessas características, dimensionar com exatidão pode ser considerada uma tarefa meramente utópica, embora não impossível.

Combater as operações ilícitas da *Dark web* é uma razão aparentemente nobre e honrada por parte do Estado. No entanto, o mesmo resultado do esforço para o desenvolvimento tecnológico para combater a estrutura perversa da *Dark web* pode ser empregada para minar o uso positivo da *Deep web*. Assim se conflagra a grande questão da sociedade na Internet: a ponderação de anonimato vs segurança.

Bautista Luzardo (Cf. 2015), estabelece em seu artigo a relação entre a *Deep web* e o desejo. Mas a abordagem⁷ da autora não leva em consideração uma diferença básica entre *Deep web* e *Dark web*, então, de modo a sanar essa questão para a lógica desse artigo, deve-se compreender a questão da ilicitude e desejo apresentado pela autora dentro da ótica da *Dark web*, e não da *Deep web*. A abordagem da autora permite identificar que a ilicitude dos atos

⁶ Por exemplo, atualmente (2016), o Google, reconhecido motor de busca, consegue identificar termo presentes em arquivos em formato “.pdf” e lista-os nas páginas de resultados de pesquisa, já outros motores de buscas não necessariamente oferecem esse tipo de suporte uma vez que a tecnologia deles deve ser capaz de não apenas identificar as palavras no arquivo “.pdf” como também conseguir reconhecer a referência do documento dentro do servidor web que rastreia o *website*.

⁷ Dentre as obras contemporâneas, essa apresenta um dos melhores caminhos ao identificar no capital uma das causas dos problemas da Internet. No entanto, ao se focar excessivamente na questão dos crimes motivados pelo desejo, é feito o reducionismo de aceitar que o simples fato de determinado conteúdo estar criptografado, requisitar senha, o qualquer outro elemento impeditivo para o livre acesso, seja para cometer tais ato ilícito de motivação pecuniária. Por conta disso, foi feito nesse artigo, por diversas vezes, a separação básica de conceitos

praticados na *Dark web* possuem a exploração dos desejos, a tentativa de se obter o que não é facilmente alcançável dentro de uma perspectiva crítica às sociedades capitalistas.

Da relação entre *Dark web* e desejo, explorada por Bautista Luzardo (2015), é possível identificar um elemento em específico que norteia a ilegalidade da *Dark web*: o capital. A ilegalidade, aquilo que está na *Dark web*, drogas, pornografia, etc, são desejos construídos dado a lógica do capital. A ilegalidade dá dinheiro, seduz, vicia, e, por conta disso, o Estado teria a nobre tarefa de combater-la. Em verdade, a *Dark web* é uma contra resposta àquilo que o Estado já combate no mundo real, se constituindo então em um nicho de mercado a ser explorado. É possível afirmar que a *Dark web* é fruto dos próprios Estados nacionais, os quais falharam em proteger os indivíduos da lógica perversa do capital.

5 Considerações finais

A Web é fruto direto do desenvolvimento tecnológico, originalmente para atender finalidades militares, que prezavam a redundância de transporte de informações de modo que para que uma informação saísse do ponto A pudesse realmente chegar ao seu destino no ponto B independente da rota utilizada. Com o avançar de seu desenvolvimento novos atores passaram a fazer uso da rede, a exemplo da comunidade acadêmica e civil, o que mudou a sua função social.

Considerando a sua estrutura, é possível afirmar que o Estado consiga realizar determinado tipo de intervenção nas redes que estejam localizadas dentro de seus territórios, tal como a intervenção direta em ISPs para bloquear o acesso a determinado *website*. No entanto, mesmo que ocorra essa intervenção, ela não ocorre de forma plena dado que o próprio avançar tecnológico pode levar à utilização de novas tecnologias que permitam burlar e/ou ainda dificultar a intervenção estatal.

A vigilância e o controle da rede atende a interesses de classes políticas para se perpetuarem no poder com base no controle da informação. Nesse sentido, a utilização da própria tecnologia como forma de burlar e/ou dificultar a intervenção estatal pode ser considerada positiva para garantir a proteção de direitos fundamentais individuais, coletivos e difusos, os quais devem estar acima de interesses de classes políticas dominantes.

Apesar desse aspecto positivo do uso da tecnologia, é de se observar que um certo lado obscuro da Internet merece destaque, a denominada *Dark web*, já que a mesma se aproveita desse mesmo tipo de tecnologia que pode preservar e valorizar os direitos fundamentais individuais, coletivos e difusos para transgredi-los.

A regulamentação da Internet deve ser capaz de valorizar positivamente os direitos fundamentais, mesmo que para isso seja necessário lançar mão da segurança nacional. Do contrário, a própria regulamentação vem a configurar uma aceção de estado de exceção, admitindo-se a violação dos direitos em prol da soberania estatal.

Os avanços tecnológicos fornecem a sociedade mecanismos de valorizar os direitos fundamentais individuais, coletivos e difusos, logo a restrição total por parte dos Estados em combater as ferramentas é inútil, já que ao se eliminar uma, dado a lógica do processo de destruição criadora, outra poderá assumir o seu lugar.

Propõem-se ao Estado a não realização de medidas paliativas, isso é, aquelas que não consideram a Internet com suas particularidades e que a tratam como se fosse um meio de comunicação qualquer (a exemplo de jornais e revistas). Essas medidas refletem a falta de esclarecimento, logo são ineficazes ao que se propõem. O resultado inicial pode ser positivo, mas de lógica a ser superada por alguma outra tecnologia. Assim, o verdadeiro inimigo a ser combatido pelo Estado não é a Internet e seus usuários, mas o próprio capital, já que ele é capaz de se utilizar da grande rede de computadores de forma perversa para conseguir a sua auto-valorização e disso decorrer as diversas ilicitudes exemplificadas na vertente da *Dark Web*.

6 Referências bibliográficas

ARENDT, H. **A condição humana**. 11. Ed. Rio de Janeiro: Forense Universitária, 2010.

BAUTISTA LUZARDO, D. M. DEEP WEB: APROXIMACIONES A LA CIBER IRRESPONSABILIDAD. *rev.latinoam.bioet.*, Bogotá , v. 15, n. 1, Jan. 2015. Disponível em < http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1657-47022015000100003&lng=en&nrm=iso >. Acesso em 21. out. 2015.

BECKETT, A. *The Guardian*, 2009. **The dark side of the internet**. Disponível em < <http://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet> >. Acesso em 22. out. 2015.

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 21 Out. 2015.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado, 1988. Disponível em <

http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm >. Acesso em 22. out. 2015.

CARTA das Nações Unidas. 26 de junho de 1945. Disponível em < http://www.planalto.gov.br/ccivil_03/decreto/1930-1949/d19841.htm >. Acesso em 21 fev. 2016

CARTA da Organização dos Estados Americanos. 30 de abril de 1948. Disponível em < <http://www2.camara.leg.br/legin/fed/decret/1950-1959/decreto-30544-14-fevereiro-1952-340000-publicacaooriginal-1-pe.html> >. Acesso em 21. fev. 2016.

CASTELLS, M. **A Sociedade em Rede** (vol 1). Trad. Roneide Venancio Majer com a colaboração de Klauss Brandini Gerhardt. 8. Ed. São Paulo: Paz e Terra, 2000.

CHESNAIS, F. **A mundialização do capital**. São Paulo: Xamã, 1996.

DECLARAÇÃO Americana dos Direitos e Deveres do Homem. Abril de 1948. Disponível em < https://www.cidh.oas.org/basicos/portugues/b.Declaracao_Americana.htm >. Acesso em 15. jan. 2016.

DECLARAÇÃO Universal dos Direitos Humanos. 10 de dezembro de 1948. Disponível em < <http://unesdoc.unesco.org/images/0013/001394/139423por.pdf> >. Acesso em 21. fev. 2016.

FRANKLIN, L. *Revista Exame*, 2015. **Produtora processa usuários por assistirem filme do Pierce Brosnan via Popcorn Time**. Disponível em < <http://exame.abril.com.br/tecnologia/noticias/produtora-processa-usuarios-por-assistirem-filme-do-pierce-brosnan-via-popcorn-time> <. Acesso em 15 de jan. 2016

GREENWALD, G; MACASKILL, E. *The Guardian*, 2013. **NSA Prism program taps in to user data of Apple, Google and others**. Disponível em < <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> >. Acesso em 10 Jun. 2015.

INTEL. **Moore's Law and Intel Innovation**. Disponível em < <http://www.intel.com/content/www/us/en/history/museum-gordon-moore-law.html> >. Acesso em 21. Out. 2015.

KANT, I. **Resposta à pergunta: o que é esclarecimento?**. Trad. Luiz Paulo Rouanet. Disponível em < http://www.uesb.br/eventos/emkant/texto_II.pdf >. Acesso em 21. Out. 2015.

MONTEIRO, S. D.; FIDENCIO, M. V. As dobras semióticas do ciberespaço: da web visível à invisível. **Transinformação**, Campinas, v. 25, n. 1, p. 35-46, Abr. 2013. Disponível em < http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-

37862013000100004&lng=en&nrm=iso >. Acesso em 21. out. 2015.
<http://dx.doi.org/10.1590/S0103-37862013000100004>.

PACTO Internacional dos Direitos Econômicos, Sociais e Culturais. 19 de dezembro de 1966. Disponível em < http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D0591.htm >. Acesso em 21. fev. 2016

PACTO Internacional sobre Direitos Civis e Políticos. 16 de dezembro de 1966. Disponível em < http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm >. Acesso em 21. fev. 2016.

PACTO de San José da Costa Rica. 22 de novembro de 1969. Disponível em < http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/anexo/and678-92.pdf >. Acesso em 21. fev. 2016

SCHUMPETER, J. **Capitalismo, Socialismo e Democracia**. Rio de Janeiro: Editora Fundo de Cultura, 1961.

STALLINGS, W. **Redes e Sistemas de Comunicação de Dados: Teoria e aplicações corporativas**. 5. Ed. Rio de Janeiro: Elsevier, 2005.