Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Relações Internacionais

FERNANDA SALOMÃO FAVATO

DESAFIOS DA FORMAÇÃO DE UM REGIME INTERNACIONAL DE GOVERNANÇA DA INTERNET: Multiplicidade de atores e visões divergentes

BRASÍLIA
2020

FERNANDA SALOMÃO FAVATO

DESAFIOS DA FORMAÇÃO DE UM REGIME INTERNACIONAL DE GOVERNANÇA DA INTERNET: Multiplicidade de atores e visões divergentes

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador(a): Claudio Tadeu C. Fernandes

BRASÍLIA
2020

FERNANDA SALOMÃO FAVATO

DESAFIOS DA FORMAÇÃO DE UM REGIME INTERNACIONAL DE GOVERNANÇA DA INTERNET: Multiplicidade de atores e visões divergentes

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador(a): Claudio Tadeu C. Fernandes

Brasília, de de 2020

BANCA AVALIADORA

_____

Professor Claudio Tadeu C. Fernandes (Orientador)

_____

Professor(a) Avaliador(a)

DESAFIOS DA FORMAÇÃO DE UM REGIME INTERNACIONAL DE GOVERNANÇA DA INTERNET: Multiplicidade de atores e visões divergentes

Fernanda Salomão Favato[1]

RESUMO

Trata o presente artigo da questão envolvendo a governança da internet. Em termos mais específicos, constitui objetivo deste estudo o exame relativo à dificuldade da criação de um "regime internacional de governança" da *internet*. O artigo examinou diversos assuntos associados à questão, dentre os quais temas como a institucionalização da internet, a fragmentação da normatização da internet e a cibersegurança. Do ponto de vista metodológico, o artigo valeu-se de técnicas descritivas ao amparo do chamado neorrealismo. No tocante aos resultados e no que respeita às conclusões, o artigo demonstrou ser improvável a constituição de uma governança internacional da internet tendo em vista, especialmente, a multiplicidade de atores e seus interesses divergentes.

Palavras-chave: Internet. Governança. Fragmentação. Multilateralismo. Normatização. Cooperação. Cibersegurança. Neorrealismo. Regimes internacionais.

ABSTRACT

This article deals with the issue involving internet governance. In more specific terms, the objective of this study is to examine the difficulty of creating an "international governance regime" for the internet. The article examined several issues associated with the subject in question, among which, themes such as the institutionalization of the internet, the fragmentation of internet regulation and cybersecurity. From a methodological point of view, the article used descriptive techniques under the umbrella of the so-called neorealism. Regarding the results and the conclusions, the article demonstrated that the constitution of an international internet governance is unlikely, especially considering the multiplicity of actors and their divergent interests.

Keywords: Internet. Governance. Fragmentation. Multilateralism. Standardization. Cooperation. Cybersecurity. Neorealism. International regimes.

[1] Graduanda do curso de Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

INTRODUÇÃO

Através dos anos a *internet* se tornou o principal disseminador de informações, impulsionando a globalização e reestruturando as formas de comunicação por meio das novas fronteiras digitais. A constante evolução da tecnologia tornou nítida a dimensão do meio digital, surgindo de tal modo o aparecimento da discussão sobre a necessidade de uma legislação que delimite os campos de atuação do Estado e do setor privado e, também, a determinação dos direitos e obrigações dos cidadãos no âmbito digital.

A multiplicidade de atores e interesses no que tange à governança da *internet* cria impasses na normatização do meio e tende a afastar a possibilidade de uma governança global da *internet*. A influência americana na criação da ONG[2] que regula grande parte técnica dos fatores que envolvem a *internet* gera incômodo em diversos países que buscam mecanismos alternativos de fiscalização e regulação dos temas cibernéticos.

Com o questionamento das normas aplicáveis ao ambiente online foi se tornando claro que o a governança da *internet* não seria atribuída apenas ao aparato estatal devido à existência de instituições bem estabelecidas dentro do setor privado e na esfera da sociedade civil. Deve-se salientar que por mais que existam interesses individuais e, portanto, unilaterais, no âmbito das entidades privadas, tais como associações, empresas e ONGs de todo tipo, estas operam —todas elas— sob as leis nacionais de seus países e, em diversos casos, igualmente sob as leis de países estrangeiros (EPSTEIN, 2013). Ressalte-se, contudo, que mesmo diante do enquadramento privado de tais entidades, muitas delas têm suas atuações facilitadas pelos Estados (incentivos monetários, tarifários, subsídios, entre outros), fenômeno que exemplifica a relação de dependência entre estas instituições e seus correspondentes estados nacionais.

A evolução de tecnologias deve ser acompanhada da evolução do debate e da legitimação de suas normas. O ambiente virtual, na sua atual conjuntura, é relativamente novo e permanece em condição de permanente mudança. Do ponto de vista acadêmico, deve-se questionar como os Estados e os indivíduos podem se proteger nesse meio levando-se em consideração o aspecto transnacional da *internet*. A multiplicidade de fatores que impedem a implementação de uma legislação internacional comum deve ser estudada, de tal maneira, à luz da finalidade de progressão no que diz respeito ao

[2] *Internet Corporation for Assigned Names and Numbers* (ICANN). Mais detalhes em www.icann.org (acesso em 26/10/2019).

entendimento do próprio estabelecimento de direitos e deveres em um ambiente sem fronteiras.

Deve-se, porém, para prosseguir com a análise pertinente a este artigo, estabelecer que a noção de *internet* analisada engloba não só o meio digital como as entidades que permitem e permitiram que ela exista. Saliento, porém, que o objetivo deste artigo não é fazer análise extensa de como funciona o meio técnico e operacional da *internet*, e sim fazer uma análise básica desses aspectos que permitam a discussão sobre a fragmentação existente no cenário internacional no que diz respeito a normatização da governança da *internet* e, dessa forma, criar um ambiente online nacionalista no tocante à normatização, onde se tornará cada vez mais comum o fracionamento, de uma perspectiva global, nas normas do âmbito cibernético.

1 GOVERNANÇA: BREVES CONSIDERAÇÕES

Antes de definirmos o conceito de governança da *internet* deve-se estabelecer, primeiramente, o conceito de governança. Rosenau (1995, p.13) define governança como "*systems of rule at all levels of human activity - from the family to the international organization - in which the pursuit of goals through the exercise of control has transnational repercussion*". Em trabalho publicado por Rosenau em 1992, *Governance in the Twenty-first Century*, o autor destaca que a governança somente existirá se for extremamente eficiente, pois diferentemente do governo que pode existir mesmo sendo fraco, a governança não existirá se não funcionar efetivamente, pois criaria um espaço de caos e anarquia o que anularia a governança. Assim, governança pode ser entendido como sistema de regras que apenas será funcional se for aceito pela maioria, ou pela maioria de pessoas poderosas dentro do grupo afetado onde governança deve ser entendida como mais ampla que governo, podendo englobar tanto organizações governamentais como não-governamentais, instituições informais e a sociedade civil.

Finkelstein (1995) destaca que governança não deve ser entendida como uma instituição e sim como uma atividade; dessa forma, se a governança é exercida através de uma instituição, quer dizer apenas que a organização é a ferramenta utilizada para exercer o poder e deveres gerados pela governança. Com essa noção estabelecida deve-se seguir para identificar os atores e poderes relevantes que podem tanto formar ou influenciar as atividades de governança, como Estados, instituições, grupos de pressão, empresas, indivíduos etc. A governança da *internet*, ademais, compreende questão

vinculada ao próprio funcionamento da *internet*, incluída uma multiplicidade de variantes associadas ao desenvolvimento tecnológico, como questões políticas, econômicas, sociais e geopolíticas.

Não existe consenso no que diz respeito à definição do termo governança da *internet*, tendo em vista principalmente que: (i) o impasse existente entre o alcance das instituições e seu papel nos setores da governança; (ii) dúvida quanto à abrangência de atuação do Estado, da sociedade civil e do setor privado e seus limites nos assuntos cibernéticos; e (iii) inexistência de padronização normativa (direitos e obrigações) apta a regular tal governança. A governança da *internet* deve ser encarada como um processo coletivo contínuo com o fim de preencher a lacuna regulatória gerada pela falta de um consenso conceitual e institucional.

O termo governança da *internet*, porém, necessariamente incluiu temas de gerenciamento de assuntos relacionados à privacidade, *cybersecurity*, funcionamento de nomes de domínio, endereços IP, protocolos da internet, sistema dos servidores raiz, acesso à informação, *net neutrality*, liberdade de expressão, direitos e deveres digitais e, ainda, participação de *multistakeholders* e da sociedade civil no processo decisório e no funcionamento do sistema (SILVA, 2008; KLEINWACHTER, 2004).

Denardis (2010) afirma que o estudo de governança da *internet* deve focar nas questões que expliquem o que é permitido e existente dentro do meio digital. Neste sentido, deve-se estudar a arquitetura técnica sem ignorar as questões geopolíticas pertinentes, que expliquem a forma atual de como se utiliza a *internet*:

> Governance is usually understood as the efforts of nation states and traditional political structures to govern. Sovereign governments do perform certain Internet governance functions such as regulating computer fraud and abuse, performing antitrust oversight, and responding to Internet security threats. Sovereign governments also unfortunately use content filtering and blocking techniques for surveillance and censorship of citizens. Many other areas of Internet governance, such as Internet protocol design and coordination of critical Internet resources, have historically not been the exclusive purview of governments but of new transnational institutional forms and of private ordering. Without this qualification, the Internet governance nomenclature might incorrectly convey that this type of scholarship somehow advocates for greater government control of the Internet (DENARDIS, 2010, p. 1).

A criação de um "constitucionalismo digital" engloba iniciativas que buscam o estabelecimento de direitos políticos, normas sobre a governança digital e limitações do exercício de poder na *internet*. Tem como objetivo identificar o poder de ação e das autoridades públicas e privadas através do reconhecimento de direitos de cada um

(REDEKER; GILL; GASSER, 2018). A questão da governança da *internet* é extremamente importante pois o meio digital é instrumento transnacional e essencial da vida dos indivíduos. O intercâmbio de informações se tornou algo cotidiano. A soberania estatal, por seu turno, pode afetar diretamente o fluxo de informações.

O estudo da governança da *internet* somente por meio da análise de órgãos institucionais e suas funções no cenário internacional é limitada na medida em que desmerece o papel exercido pelo setor privado e, ainda, o poder de autorregulação do Estado. Deve-se analisar a governança da *internet* como um ambiente amplo e crescente onde as políticas que influenciam o meio ocorrem fora do discurso institucional. Deste modo, temas como a análise do controle de recursos críticos da *internet*, o design de protocolo de *internet*, os direitos de propriedade intelectual relacionados à governança da *internet*, o gerenciamento de infraestrutura e segurança do meio digital e o papel e a influência do setor privado são tópicos determinantes para a compreensão de quão amplo e quão fragmentado revela-se o âmbito da governança da *internet*.

A fim de permitir o estudo do aparato digital, cientistas da computação tendem a separar em camadas as categorias diferentes de análise da *internet*. Hill (2012, p. 13) adota o sistema de quatro camadas projetado por David Clark para explicar o funcionamento da *internet*:

> The four-layer model, like the other layering models, is generally represented as a vertical stack. At the bottom of the stack lies the "physical layer," which includes all the Ethernet wires, fiberoptic cables, DSL lines, and other hardware through which the electronic data "packets" travel. Immediately above the physical layer is the "logical layer," which encompasses the core Internet Protocols (TCP/IP), the Internet services, such as the Domain Name System (DNS), and all the applications such as the World Wide Web and e-mail. Next, situated on top of the logical layer, is the "information layer," which is comprised of all of the online content, including blogs, news, video and music that is communicated between and among users. And at the very top of the stack is the "people layer," the individuals, companies, and governments that actually participate in the Internet's growth and use.

A camada intitulada *people layer* será o foco do estudo deste artigo, pois nela se engloba a análise das políticas e agentes influentes no que tangem à governança da *internet*. Será através da análise dos diversos atores e instituições relevantes no meio da operacionalização e normatização do meio digital que será possível entender o atual cenário fragmentado.

2 INSTITUCIONALIZAÇÃO DA *INTERNET*

A projeção da *internet* tem a característica única de ter sido feita de forma que possibilitasse a expansão do meio, onde sua infraestrutura permitia o desenvolvimento de diversos tipos de formas de uso e aplicativos. A *internet* pode ser compreendida como um conglomerado de redes, protocolos, cabos de fibra, sistema de operacionalização e armazenamento que em sua essência tem como característica a existência de uma multiplicidade de atores relevantes.

O equilíbrio entre a soberania nacional e a transnacionalidade gerada pela *internet* surge como tema de debate principalmente no início dos anos 90, quando se observa o inicio da utilização do meio digital pelo meio comercial. Observam-se, porém, desde pelo menos 1990, políticas vinculadas ao fluxo de informações e aos meios de comunicação conflitantes entre os Estados do sistema internacional. A discussão sobre a necessidade de um órgão intergovernamental e novas políticas sobre o meio eram debatidas no contexto do esforço dos países em promover controle soberano no que diz respeito ao fluxo de informações. A visão liberal, por exemplo, ao englobar o meio digital, e à luz da tese que defende a menor intervenção estatal nos assuntos econômicos, acaba, por conseguinte, direcionando a *mão invisível* à *internet*.

Um dos pontos defendidos era que o crescimento do meio só foi possível devido ao aspecto fragmentado da *internet*; assim, o pouco controle que os Estados possuíam no meio foi precisamente motivo determinante de seu crescimento (KLEINWACHTER, 2004). De tal modo, a falta de uma regulamentação específica do governo, e o papel determinante do setor privado na criação e desenvolvimento da *internet*, levaram a propostas de uma governança multissetorial. Para entender o grande papel que a sociedade civil exerce no meio digital deve-se analisar o processo de criação e institucionalização da *internet*.

Observa-se que a institucionalização da *internet* tem como característica distinta o seu gerenciamento - desde a sua comercialização - ocorrendo de baixo para cima; ou seja, por indivíduos da sociedade civil. A ARPANET foi uma rede criada pela ARPA (*Advanced Research Projects Agency*) – agência criada pelo Departamento de Defesa dos EUA – na década de 60, com o intuito de idealizar um fluxo de comunicação entre computadores priorizando a comunicação com universidades e centros de pesquisas que tivessem relação direta com o Departamento de Defesa norte-americano. Em 81, a *National Science Foundation* (NSF) cria projeto intitulado CSNET com o intuito de

expandir os benefícios do programa às instituições acadêmicas e de pesquisa que não tivessem acesso via ARPANET. O sucesso foi tanto que em 84 lança-se o projeto NSFNET que permitira acesso a toda a comunidade acadêmica. Em 83 a ARPANET é dividia em duas: MILNET (com laços militares) e uma nova ARPANET (com foco para pesquisa e desenvolvimento). Observam-se, a partir daí, múltiplos projetos independentes a fim de desenvolver rede capaz de conectar computadores por todo o globo no seio das universidades (GATTO; MOREIRAS; GETSCHKO, 2009)

Jon Postel, pesquisador do *Information Science Institute* (ISI)[3], foi designado para gerenciar e criar os endereços eletrônicos de IP[4] e gerenciar o *Domain Name System* (DNS)[5] dentro do sistema da ARPANET. Depois do estabelecimento do sistema DNS, parte da operacionalização do registro de domínios foi delegada ao *Stanford Research Institute* (SRI), por meio de contrato com o Departamento de Defesa norte-americano. Com o crescimento do meio digital, a *National Science Foundation* assumiu o papel de financiadora de parte da infraestrutura do ambiente cibernético. Em 1992 subsidiou o gerenciamento de banco de dados, registros de nomes e operacionalização de diretórios. A AT&T ficaria responsável pela supervisão dos bancos de dados e a *Network Solutions, Inc.* (NSI) gerenciaria a operação de registro dos nomes de domínio (operação realizada anteriormente pelo SRI)[6] (WEINBERG, 2000). Com a expansão e a dimensão geradas pelo crescimento dessa rede de fluxo de informação, em 88 foi criada a *Internet Assigned Numbers Authority* (IANA) – através de financiamento conjunto da ISI e da DARPA – que tinha como responsabilidade principal a coordenação operacional, onde deveria atribuir os endereços de IP. Segundo Weinberg (2000 p. 13):

> Under arrangements made by various players in the domain name space through the late 1990s, NSI administered the key root server, known as the "A" root server, but policy authority over the contents of the "A" root rested with Jon Postel and IANA. It was Postel who was responsible for deciding whether a new country code domain should be added to the root zone and which entity should be responsible for

[3] Instituto pertencente à University of Southern California (USC), estabelecido em 72, para desenvolver pesquisas em assuntos relacionados a tecnologias de processamento de informações, computação e comunicação. Para mais informações acessar: https://www.isi.edu/news/story/187

[4] Cada computador funcional era atribuído à um endereço de protocolo de *Internet* (IP), que consistia em um número único de 32 btits.

[5] O Information Science Institute (ISI) foi responsável por desenvolver e implementar os servidores DNS que é capaz de mapear cada endereço de IP e traduzi-lo para endereços eletrônicos mais user-friendly como mail.google.com, etc. O nome de domínio é dividido em 3 níveis, o subdomínio (parte da frente do endereço eletrônico, exemplo, no endereço anteriormente utilizado, seria: mail), nome de domínio (do meio, no exemplo: google) e o top-level domain (na parte final, seria no exemplo o: com).

[6] Atualmente, a AT&T, a Network Solutions e as agências da National Science Foundation formam a InterNIC

> administering that domain. It was Postel and IANA who were in the end responsible for resolving disputes over the allocation of IP addresses.

Porém, a IANA era administrada de forma ambígua, onde não restavam claros os *"checks and balances"* devido ao fato de que não foi estabelecida formalmente como uma organização do Estado americano, e o papel do governo parecia se restinguir ao financiamento (PARÉ, 2003). O início dos anos 90 foi marcado por período transitório onde observou-se o caráter comercial da *internet*, surgindo novos questionamentos e demandas dos atores do sistema internacional. Observou-se o crescimento contínuo, impulsionado pela plataforma comercial no meio digital, da *World Wide Web*[7] elaborada por Tim Berners-Lee, chegando-se a mais de um milhão de nomes de domínio na *internet*.

Surge assim o primeiro movimento no sentido de assegurar nomes de domínio, juntamente com o início dos questionamentos quanto à aplicação e quanto à proteção de direitos de marcas e de direitos de autor no ambiente online. O rápido crescimento do número de adeptos com a internacionalização deixou clara a necessidade de institucionalizar os novos aspectos legais e operacionais da *internet*, principalmente no que diz respeito ao crescente número de registros de nomes de domínio. Começa assim a pró-atividade (no âmbito estatal e na esfera privada) em criarem-se forças-tarefas a fim de se debaterem assuntos relacionados à governança da *internet* (ex.: IETF - *Internet Engineering Task Force*).

Tendo em vista a crescente quantidade de registros de endereços eletrônicos e nomes de domínio, a *National Science Foundation* negocia com a NSI emenda ao acordo de contrato original, onde permitira que a NSI cobrasse anualmente taxa de US$ 50,00 de cada registro de nome de domínio ao invés de a NSF arcar com os custos (o que era o padrão).[8] Nota-se um crescente desconforto pelos usuários da *internet* não só pela taxa imposta pela NSI, mas pelo monopólio e monetização que a NSI estava exercendo no ambiente digital. Outra crítica foi a política utilizada para resolver conflitos relacionados às disputas de nomes de domínio, onde a NSI suspendia qualquer

---

[7] Foi desenhada por Tim Berners-Lee, membro da Organização Europeia para a Investigação Nuclear (CERN), para ser rede onde informações circulam na forma de URLs. Construiu-se sistema denominado ENQUIRE, desenvolvido para armazenar e reconhecer associações de informações. Possuia extenso banco de dados e vários links que conectavam os conteúdos entre si, permitindo o fluxo de informação.

[8] *NSI-NSF Cooperative Agreement No. NCR-9218742, Amendment 4, at* http://www.networksolutions.com/legal/internic/cooperative-agreement/amendment4.html (Sept. 13, 1995)

nome de domínio que recebesse uma reclamação formal de outra marca comercial, sem investigação e sem análise jurídica adequada (WEINBERG, 2000; KLEINWACHTER, 2004).

A autoridade que o governo americano exercia na operacionalização da *internet* gera questionamentos não só de outros governos soberanos como de instituições privadas e públicas. Assim, o poder americano no estabelecimento das políticas técnicas começa a gerar tensão nas relações intergovernamentais. De acordo com Epstein (2003 p. 2):

> When the question of Internet governance bubbled up as a contested issue in the late 1980s and the early 1990, neither the diverse Internet community nor the nation-states, or intergovernmental apparatus could lead Internet- policy-setting unilaterally. On the one hand, when national states started showing interest in the Internet policy debate, there were already well-established governance institutions based in the private sector, the civil society, and to a degree academia.

Postel propõe em 95 atribuir a IANA a supervisão da *Internet Society* (ISOC)[9], garantindo-se sistema de operação e gerenciamento mais abrangente e sólido. Porém, tanto o governo americano como o setor privado se oporiam a atribuir essa responsabilidade àquela organização sem fins lucrativos que, desde sua criação em 1992, atuara no sentido de facilitar o desenvolvimento operacional, de alcance, promovendo fóruns que permitiriam a multiplicidade de participantes para discutir políticas e debater a evolução do meio e dos tópicos relacionados à governança da *internet*. Fica claro que o status quo não poderia ser mantido, e os primeiros passos da normatização do meio digital tornam-se prioridade. Por iniciativa do governo americano, surge em 1997, *Working Group* a fim de discutir esses assuntos relevantes do ambiente cibernético.

> The U.S. government convened a working group, which included representatives from the White House Office of Science and Technology Policy, the National Telecommunications and Information Administration, the Patent and Trademark Office, the National Science Foundation, the Department of Defense, the Department of Justice, the Department of State, the Federal Communications Commission, and other agencies, to figure out what should be done. In July 1997, the National Telecommunications and Information Administration (NTIA) released a public request for

[9] A ISOC é dividida em diversos "working groups" que lidam com tópicos especifico relacionados ao meio digital como a Força-Tarefa de Engenharia da *Internet* (IETF), que discute e estabelece os principais protocolos da *internet* e a Diretoria de Arquitetura da *Internet* (IAB, sigla em inglês), que oferece orientação técnica com o intuito de catalisar a evolução do meio digital.

> comments regarding desirable characteristics of Internet governance and the domain name space. (WEINBERG, 2000, p. 18)

No primeiro mês de 98, o governo americano apresenta nova proposta para tornar mais eficiente o gerenciamento e operacionalização dos nomes e endereços eletrônicos: o *Green Paper*[10] é intitulado "*A Proposal to Improve Technical Management of Internet Names and Addresses*". O *Green Paper* propôs que a delegação de todo o gerenciamento relevante à operacionalização da *internet*, tais como nomes de domínio, endereços de IP e rede de servidores, fosse atribuída a uma nova organização sem fins lucrativos. A equipe que estivesse trabalhando na IANA seria transferida para a nova organização e o governo norte-americano transferiria todos as funções exercidas por qualquer vertente do governo relacionadas ao funcionamento e ao gerenciamento da *internet* e bancos de dados à nova ONG. O projeto ainda destaca a importância da legitimação da corporação e para isso sugere que seria necessário a representação, dentro da organização, dos diversos setores que possuem interesse no meio digital (WEINBERG, 2000; CANABARRO, 2014).

O *Green Paper* não agradou aos diversos setores interessados na normatização da *internet* e, por isso, quatro meses depois o governo americano lançou o *White Paper* com mudanças significativas, onde as propostas de normas apresentadas no *Green Paper* pelo governo norte-americano foram retiradas e a responsabilidade da criação de políticas relacionadas ao gerenciamento operacional do meio caberia somente à nova organização. A recepção do *White Paper* foi boa devido ao fato de que as decisões de políticas relacionadas ao meio foram deixadas para a nova corporação resolver (WEINBERG, 2000):

> The White Paper did not speak precisely to how the new corporation it described would be formed. It suggested that if the new entity were formed by "private sector Internet stakeholders," the U.S. government was prepared to recognize it by entering into agreements with it, seeking international support for it, and ensuring that it had appropriate access to databases and software controlled by NSI. In October 1998, after a series of negotiations between IANA and NSI — and more wide-ranging consultations on the interim board's composition with the U.S. government, a variety of foreign governments, Jon Postel's lawyer (a Jones, Day partner named Joe Sims), IBM, and others — Dr. Postel transmitted to the Department of Commerce documents reflecting what he described as "the consensus

[10] Green Paper é termo comumente utilizado na Grã-Bretanha e Estados Unidos para se referir a documento elaborado pelo governo sobre algum assunto politicamente relevante para que as pessoas tenham acesso a esse documento e possam discutir sobre, antes de se tomar decisões legais e políticas relacionadas ao tema. O White Paper pode ser feito após o Green Paper levando em consideração a opinião gerada, onde a proposta governamental se adapta a reação pública.

> judgment of the global Internet community as to how to form a corporation that will include the IANA function." (WEINBERG, 2000. p. 23)

Dessa forma, em 98 ocorre de fato o início da institucionalização normativa da *internet*. Como resultado das diversas negociações entre as partes técnicas, comerciais e estatais influentes no sistema digital, cria-se a "*Internet Corporation for Assigned Names and Numbers*" – ICANN (MULLER, 2002). A organização privada nasce da iniciativa do governo norte-americano, em resposta às pressões internas e externas para a normatização do sistema operacional da *internet*. A organização pode não ser vista como primeiro movimento de iniciativa global comum tendo em vista a manifesta influência norte-americana, mas inegavelmente é o primeiro mecanismo regulador de normas da *internet* no âmbito internacional.

3 TEMÁTICAS CIBERNÉTICAS QUE INFLUENCIAM DIRETAMENTE A FRAGMENTAÇÃO DA NORMATIZAÇÃO DE UMA GOVERNANÇA GLOBAL

3.1 Recursos críticos à *internet*

Recursos críticos da *internet* (CIRs) se referem não à infraestrutura física subjacente que permite o funcionamento da *internet* como cabos de fibra ótica, energia elétrica etc, e sim à infraestrutura exclusiva da *internet*, gerada pela normatização e gerenciamento histórico do ambiente cibernético, como o sistema de nomes de domínio e endereços de IP. Segundo Denardis (2011, p. 4), os endereços de IP têm importância primordial e estrutural no funcionamento da *internet*, e o números únicos de 32 bits[11] atribuídos a cada dispositivo conectado à rede permite a identificação do dispositivo utilizado:

> In 1990, the Internet standards community identified the potential depletion of addresses as a crucial design concern and the IETF recommended a new protocol, Internet Protocol version 6 (IPv6) to expand the number of available addresses. IPv6 extends the length of each address from 32 to 128 bits, supplying 2128, or 340 undecillion addresses. Despite the longstanding availability of IPv6 and for a variety of political and technical reasons, the upgrade to IPv6 has barely begun on any global scale.

[11] Protocolo da *Internet* versão 4 (IPv4).

Uma das questões fundamentais debatidas atualmente é referente à política relacionada a endereços de IP e, consequentemente, de governança da *internet* no tocante à criação do protocolo IPv6 e do gerenciamento do restante da reserva do protocolo IPv4 (DENARDIS, 2011). O crescimento exponencial da *internet* leva a um quadro tendendo a um próximo esgotamento no que diz respeito aos endereços do protocolo IPv4. Assim, coloca-se em pauta como devem ser os posicionamentos estatais e privados no que diz respeito à regulamentação do protocolo IPv4 nas suas reservas restantes e o posicionamento em relação à projeção do espaço IPv6.

O esgotamento iminente do espaço IPv4 não surtiu o efeito esperado na comunidade dos provedores dos serviços relacionados à *internet* e a transição para o protocolo IPv6 ainda permanece na sua infância. Os motivos que podem explicar a lentidão no que diz respeito a essa transição incluem: (i) a atual fragmentação do cenário da governança da *internet*; (ii) a inexistência de um órgão central que busque ativamente a implementação do IPV6; (iii) falta de qualquer tipo de ação estatal que busque a transição para o sistema IPv6 em âmbito nacional; (iv) abandono (por parte da grande maioria dos governos) da hipótese de concessão aos provedores da tarefa da transição; (v) constatação de que os sistemas IPv4 e IPv6 são interoperáveis a menos que o servidor que opera no IPv4 seja programado para se comunicar com servidores operando no IPv6 (o que é raro); e (vi) o fato de que a programação para possibilitar essa comunicação entre os servidores tende a ser cara, o que desestimula a implementação dessa transição (HILL, 2012).

Essa falta de ação e desequilíbrio na adoção e transição para a operacionalização do IPv6 entre os países gera questões importantes no que diz respeito a possível criação de dois sistemas distintos operando mutualmente com interoperação mínima. Observa-se que a Ásia (destacando o governo chinês, japonês e indiano), devido a escassez de espaço restante do sistema IPv4, a busca de um sistema apropriado que acomodasse a dimensão necessária para o uso efetivo de suas populações e se aproveitando da lacuna de gerencial existente na liderança do sistema IPv6 e seu potencial econômico, tomou a dianteira na utilização do sistema IPv6. A China priorizou a implementação do sistema IPv6 como uma das principais políticas relacionadas ao futuro da *internet*. (HILL, 2012) O domínio americano no sistema IPv4 foi um catalisador para a efetivação desse posicionamento político chinês, onde mais de US $ 200 milhões foram investidos em programas para a implementação do sistema IPv6, tem-se como grande exemplo o programa *China Next Generation Internet* (CNGI). Porém a política adotada pelos

países asiáticos em tonar a frente na adoção do IPv6 pode gerar certa fragmentação no sistema digital. Se os usuários do sistema IPv4 resistirem na transição ao novo sistema poderá ocorrer bifurcação extensa no fluxo de informação leste/oeste, além disso, se tornaria uma séria ameaça aos interesses comerciais americanos e, a fragmentação do sistema digital se tornará um perigo eminente. (HILL, 2012; CANABARRO, 2014)

Com o estabelecimento da ICANN, foram atribuídas à organização as funções de gerenciar o sistema de domínio da *internet* (DNS), regulando-se as políticas relacionadas ao sistema, endereços de IP, sistema de nomes de domínio de primeiro nível genéricos (gTLDs[1 2]) e, ainda, a coordenação do sistema de servidores-raiz.

> In addition to technical policy coordination that prevents multiple registries from attempting to deploy colliding top-level-domains (TLDs), ICANN also engages in policies that strongly resemble traditional regulation of market structure. It decides what TLDs will be made available to users, and which registrars will be permitted to offer those TLDs for sale. And it makes those decisions at least in part based on the potential registrars' willingness to offer a package of services that includes mandatory trademark arbitration. (FROOMKIN; LEMLEY, 2003, p. 1)

Deve-se destacar também, no tocante ao debate de instituições determinantes ao funcionamento da *internet* e que fazem parte da questão central da governança da *internet*, o papel fundamental da IETF (*Internet Engineering Task Force*). A IETF é responsável pela organização e gerenciamento de protocolos técnicos que permitem o fluxo de informação e a funcionalidade da arquitetura do meio digital.

> But the standards developed by the IETF are only part of a vast protocol ecosystem required to provide end-to- end interoperability for voice, video, data, and images over the Internet. For example, the World Wide Web Consortium (W3C) sets application-layer standards for the web. The International Telecommunication Union (ITU) sets Internet related standards in areas such as security and voice over the Internet. The Institute of Electrical and Electronics Engineers (IEEE) develops vital specifications such as the Ethernet LAN standards and the Wi-Fi family of standards. Countless other entities develop specifications for the technologies that collectively enable the transmission of information over the Internet: including national standards bodies such as the Standardization Administration of China (SAC); the Motion Picture Experts Group (MPEG); the Joint

[1 2] Para entender como funciona o gTLD (generic top-level domain) deve-se explicar primeiramente os TLDs (top level-domains). Um domínio de um endereço eletrônico é formado pelo nome de domínio e o TLD, onde o nome de domínio pode ser qualquer nome livre para registro e o TLD deve ser selecionado de uma lista de TLD existentes. Os TLDs são o nome de domínio mais alto na hierárquica do sistema DNS, assim, tende a ser o que aparece por último, por exemplo no endereço eletrônico www.google.com, o TLD é o .com. O gTLD é uma das categorias de TLDs e se refere a qualquer TLD que não está diretamente ligada a nenhum país específico, o mais comum gTLD existente é o .com.

> Photographic Experts Group (JPEG); and the International Organization for Standardization (ISO). (DENARDIS, 2011, p. 7)

O crescimento exponencial notado, principalmente na última década, de políticas distintas que favorecem a fragmentação do meio digital é preocupante. Notam-se políticas públicas, ação de agentes privados e interesses econômicos como contribuintes para frear a globalização e a expansão de uma rede global. A proposta da alocação das funções hoje exercidas pelo ICANN para as Nações Unidas é criticada pelos agentes defensores da *net neutrality*, pois acreditam que levaria à politização do ambiente digital de forma que prejudicaria diretamente a noção de uma *internet* livre e aberta. Porém, não levam em consideração as possíveis consequências que a manutenção do status quo podem gerar, podendo gerar atrito substancial que leve à ramificação da operacionalização do funcionamento da *internet*.

O DNS é primordial para o funcionamento mais amigável da *internet*. Opera de forma a traduzir a ordem numérica que forma o endereço de IP de cada computador em nomes de domínios mais simples como google.com. A operação de tradução necessária para esse processo tende a ocorrer sob supervisão da ICANN, onde cada nome de domínio se torna único no ambiente digital. Entretanto, é possível que um endereço de IP seja traduzido de forma que seja redirecionado a um servidor que não faça parte dos servidores sob supervisão da ICANN, fazendo com que os usuários que adentrarem aquele endereço eletrônico sejam redirecionados a outro local do que aquele esperado, CHTER, 2016). Esse tipo de redirecionamento alternativo (também conhecido como *alt roots*) é permitido pela ICANN, tendo em vista a necessidade de todo endereço de IP passar pelos servidores da ICANN não é juridicamente vinculativo.

Além disso, os *alt roots* são muitas vezes utilizados para criar redes privadas que buscam mais segurança. O problema em voga é que se pode, futuramente, expandir entre governos a ideia de se criar um sistema de *alt roots* nacional separado dos servidores da ICANN, tornando possível, deste modo, a nacionalização do sistema digital onde o contato com os servidores DNS não exista.

Hill (2012) destaca que uma das reclamações persistente de diversos países era a demora e a falta de dinamicidade do estabelecimento de ccTLDs[13] e gTLDs de

[13] O ccTLD (country code top-level domain) é uma das categorias de TLD (top-level domain) é existe apenas quando um país ou região o registram, assim, se cria um TLD de um país especifico, exemplo: ao se entrar na zara.com se entra no endereço eletrônico americano da marca, porém, se entrar na zara.com.br o usuário será direcionado a versão brasileira do site.

alfanuméricos não romanos pela ICANN, mesmo tendo esta a tecnologia necessária para tal feito desde 96 (desenvolvida pela IETF). Devido à lentidão da organização se observou, em meados de 2005-2006, a tomada de ação unilateral da China em estabelecer gTLDs em caracteres chineses; porém, para isso ser feito, os servidores desses domínios tiveram que ser configurados a servidores diferentes daqueles gerenciados pela ICANN, o que cria não só uma fragmentação do meio digital, como também sistemas que não operam entre si, criando-se de tal maneira um ambiente cibernético chinês de traço separatista.

A ação chinesa preocupou a ICANN e em 2009, em resposta, aprovou medida denominada "*IDN ccTLD Fast Track Process*":

> In response to China's experimental alternative root work, as well as to continuing pressure from other countries demanding the implementation of Internationalized Domain Names (IDNs), the ICANN Board, meeting in South Korea in October 2009, approved the "IDN ccTLD Fast Track Process" to allow countries and territories to submit requests to ICANN for ccTLDs in scripts other than those with ASCII characters, including Chinese, Arabic and Cyrillic. Subsequently, at a Singapore conference in 2011, ICANN further approved a gTLD Program to allow for the addition of IDN gTLDs into the root zone. (HILL, 2012, p. 18)

3.2 Posicionamentos polares dos atores estatais quanto à normatização do meio

Desde a implementação global da *internet* e a disseminação de seu uso, as iniciativas governamentais de regular ou estruturar aspectos da *internet* e seu conteúdo foram mínimas. Porém, com o crescimento da *internet*, começou a ficar clara a dimensão do meio e as ameaças potenciais ao Estado, tais como crimes cibernéticos, spam, golpes e a própria segurança nacional. Dessa forma, evidenciou-se que a *internet* deveria fazer parte do âmbito das políticas estatais.

A extensão do poder estatal no âmbito digital ainda não é claro. Contudo, uma das vertentes aceitas na comunidade internacional como legítima é a soberania do Estado em relação àqueles casos que envolvem proteção infantil online, crimes cibernéticos e proteção de dados. Algumas polêmicas abarcam alguns tipos de censura governamentais, incluindo censuras políticas, ataques à liberdade de expressão e restrições de conteúdo. De acordo com estudo produzido pela *OpenNet Initiative* (ONI) em 2007 (ZITTRAIN, PALFREY, 2007), já se sabia que dos quarenta países

analisados, vinte e seis praticavam algum tipo de censura no nível nacional, se destacando a China.

Temas como segurança nacional, privacidade, monitoramento do fluxo de informação e impulso econômico simultâneo à proteção dos interesses nacionais (e seus usuários) criam barreiras delimitando o espaço cibernético. Os Estados começaram a priorizar a manutenção de dados dentro das fronteiras nacionais e esse movimento é impulsionado pela descoberta da extensão da vigilância cibernética empregada pelos Estados Unidos e o alcance da espionagem do governo norte-americano (CHANDER; LE, 2015). A proteção da infraestrutura nacional crítica para o funcionamento da *internet* nos parâmetros estabelecidos pelos Estados nacionais tornou-se primordial na agenda política e a potencial vulnerabilidade existente no meio afetou os ambientes jurídicos nacionais e internacionais.

Governos notoriamente censuradores alegam que a noção construída pelo Ocidente de uma *internet* aberta e sem filtro deveria ser encarada como algo relativo e que a soberania estatal prevalece no ambiente digital, e o Estado tem direito de restringir ou modificar o fluxo de informação dentro do seu espaço nacional (MUELLER, 2011). A restrição de informação exercida pelo governo chinês inclui filtros em diversos tópicos, tais como direitos humanos, vertentes políticas oposicionistas, pornografia, minorias e, claro, movimentos pró-democracia.

Um dos principais exemplos de nacionalização da *internet* que se pode mencionar é a abordagem do governo chinês no sentido de se criar um espaço compacto sujeito às políticas nacionais. O sistema de monitoramento chinês, coloquialmente chamado de o Grande Firewall da China (GFW), é reflexo do eficiente método implementado pelo governo no âmbito digital. O sistema inclui filtragem de informações requisitos de licenciamento, controle do Estado do que pode ser compartilhado na *internet*, vigilância arbitrária e autoridade para punir ações contrária à vertente política chinesa. (MUELLER, 2011)

China e Rússia se destacam, a partir do inicio do século XXI, como atores ativos na busca do controle de políticas acerca da governança da *internet*, desafiando-se a hegemonia norte-americana na tomada de decisões e no controle dos aparatos digitais. A fim de se posicionarem na fronteira da inovação tecnológica e de lançarem a sua marca nacional, os dois países se utilizaram de empresas nacionais com grande alcance na *internet* para difundir suas respectivas políticas dentro e fora de seus territórios (BUDNITSKY; JIA, 2018). China e Rússia, respectivamente, têm como "estrelas"

nacionais as empresas Baidu e Yandex. Deve-se, porém, ressaltar não só o papel governamental ativo dentro dessas empresas, mas também a influência do setor privado nas mesmas.

As políticas nacionais russas e chinesas tendem a seguir o estatismo econômico com o envolvimento ativo do Estado na economia, onde o autoritarismo mescla-se à experiência das economias capitalistas. No início dos anos 2000, China e Rússia buscam alterar o cenário internacional hegemônico e utilizam-se de seus recursos – incluindo os meios digitais – para fortalecer suas marcas e imagens internacionalmente. O engajamento da Rússia na liderança da governança da *internet* começa em 1998, quando o país propôs resolução sobre o desenvolvimento do debate sobre a segurança internacional no campo dos meios de comunicação onde já se notava a preocupação do Estado no papel de normatização do meio digital (NOCETTI, 2015). Nos anos seguintes nota-se a união sino-russa em diversas conferências e órgãos relevantes para a discussão da governança digital, tais como a Net mundial, Fórum de Governança da *Internet* e Congresso Mundial de Tecnologia e Informação.

O interesse chinês nas políticas de governança da *internet* global começa de forma crescente a partir de 2002 onde notou-se ação unilateral de empresas privadas como a ZTE e Huawei e, a partir de 2010, observa-se ação governamental ativa na normatização do meio digital no nível internacional. A partir de 2012, percebe-se a adoção de políticas autoritárias em relação ao controle da *internet* e começa a se construir um dos maiores controles de ciberespaços e, em 2014, o Estado chinês atua ativamente para incluir a diplomacia da *internet* na agenda do país, utilizando suas empresas nacionais a implementar sua visão e valendo-se de atores empresariais locais no cenário de governança da *internet* (BUDNITSKY; JIA, 2018).

A Rússia, desde 2000, adotou políticas restritivas onde prioriza-se a segurança nacional cibernética. Porém, até início do século XXI, notou-se pouco engajamento da sociedade civil na *internet* e, consequentemente, da ação governamental. A partir de 2008, com a eleição de Dmitry Medvedev, observou-se modernização e inovação no meio digital com a criação do Centro de Inovação Skolkovo, com o objetivo de incentivar o desenvolvimento tecnológico. Porém, com a volta ao poder de Putin, em 2012, o governo efetivou dezenas de políticas restritivas que acabaram por estatizar o espaço da *internet*. Com a crise ucraniana de 2014, a deterioração das relações com o Ocidente se aprofundaram, de modo que a busca pela soberania digital tornou-se cada vez mais expressa (BUDNITSKY; JIA, 2018).

Os Estados Unidos começaram a formular políticas de segurança cibernética em 1988, com a criação da *Cyber Emergency Response Team* (CERT), equipe criada pela Universidade Carnegie Mellon e posteriormente absorvida pela *Homeland Security* devido ao alto número de invasões nos servidores existentes. Observa-se que principalmente o que diz respeito à regulamentação de políticas com o foco da segurança no meio digital tende a vir por parte do executivo norte-americano. Através dos anos, diversas diretrizes que buscavam a proteção acerca ao meio digital foram emitidas pelos presidentes Clinton, Bush e Obama. Observava-se até meados de 2009 a política americana de tentar frear o controle internacional de armas cibernéticas, pois acreditavam que poderia gerar a necessidade de criação de uma regulamentação restrita do meio digital e consequentemente reduzir o domínio tecnológico norte-americano, freando-se de tal maneira a abordagem liberal e expansionista adotada pelo governo. Porém, a partir do mandato do Obama, se nota a mudança de postura do governo americano, pois a noção da dependência estatal do governo ao âmbito digital cria receio a possível vulnerabilidade norte-americana. (SHACKELFORD; CRAIG, 2014). O *Cyber Command* (CYBERCOM) foi criado em 2009 com o objetivo de centralizar as operações cibernéticas nos EUA. Contudo, muito pouco se sabe de fato sobre as capacidades e atuação do mesmo. Deve-se ressaltar, no entanto, que uma política integral ainda não foi estabelecida pelo governo norte-americano. Até hoje se debate se a *Homeland Security* seria o órgão adequado para lidar com a temática cibernética.

3.3 Cibersegurança

Um dos grandes desafios enfrentados pela criação de políticas comuns de governança é a desconfiança gerada pelos ataques cibernéticos a mando do Estado. Um dos marcos na história para a discussão da autoridade do Estado e os direitos relacionados ao direto de privacidade e a segurança da informação, no âmbito digital, foi a revelação por Edward Snowden, em 2013, da vigilância maciça de dados pessoais pela Agência Nacional de Segurança dos Estados Unidos (NSA).

Snowden forneceu detalhes de como o governo norte-americano conseguia maximizar sua vigilância através de grandes empresas tecnológicas – *Apple*, *Google*, *Microsoft* – que permitiam o acesso de informações de milhões de cidadãos à NSA. Apresentou documentos que comprovavam que a vigilância não se restringia nacionalmente e direcionava-se a atores políticos importantes e suas comunicações

privadas. A escala dos dados obtidos pela entidade norte-americana em nome do contraterrorismo não só repercutiu mundo afora como desencadeou debates específicos relacionados aos limites existentes entre proteção de possíveis atos que venham a ameaçar a segurança nacional e o direito de privacidade dos indivíduos.

Atores que antes não pressionavam para esse novo formato de legislação que potencializa a soberania estatal em relação aos assuntos associados ao meio digital, como é o caso da União Europeia, se convertem buscando proteção contra ataques cibernéticos americanos. Nações como Rússia, Iraque e Alemanha começaram processo de pesquisa para se criar domínio virtual estritamente nacional (EICHENSEHR, 2014). Um dos fatores que freou, de certa forma, a evolução do ambiente da *internet* se tornando estritamente nacional é o resultado do processo de globalização e de seus interesses econômicos.

O Marco Civil da *internet* brasileiro foi aprovado na Câmara dos Deputados em 25 de março de 2014 em resposta aos debates levantados após a descoberta pelo mundo da extensão de vigilância por parte americana. A lei aborda questões relacionadas à privacidade, neutralidade da rede e aplicação de imposição de obrigações civis aos usuários e provedores (DATYSGELD, 2017). Conforme avaliação de Hill (2015, p. 3), não podemos deixar de destacar outros atores que inflamaram a questão da guerra cibernética:

> Various states have been accused of practicing cyber espionage or even of conducting cyber attacks. Not surprisingly, the USA accuses China (Sanger, 2013) and Russia (AP, 2011) of actively engaging in cyber attacks or at least in commercial cyber espionage. However, it is generally accepted that the USA and Israel conducted an apparently successful secret cyber attack on Iranian nuclear facilities, through the Stuxnet virus (Sanger, 2012), and that the US has invested significantly in cyber espionage (Gellman and Miller, 2013; Poulsen, 2015) and in offensive and defensive cyber capabilities (Harris, 2015).

A temática da cibersegurança é um dos principais assuntos debatidos em diversos fóruns internacionais dedicados a examinar assuntos relacionados à governança da internet, como por exemplo os eventos organizados pela *International Telecommunication Union* (ITU) (em 2007 lançou-se Agenda Global de Cibersegurança), *Internet Governance Forum* (IGF), *African Union* (em 2012 elaborou proposta de tratado em relação a crimes cibernéticos), OTAN (anualmente promove exercícios sobre a defesa do ambiente digital), *International Multilateral Partnership Against Cyber Threats* (IMPACT) e a *Shanghai Cooperation Organization* (sabe-se que

pelo menos desde 2011 discute propostas sobre a normatização cibernética) (SHACKELFORD; CRAIG, 2014).

Em 2012, na realização da WCIT-12 (*World Congress on Information Technology*), a preocupação com a proteção do espaço nacional cibernético foi destaque até mesmo antes da realização da conferência. Em documentos divulgados anteriormente ao evento, Rússia, China e Irã propuseram que a alocação de todo tipo de política acerca da internet ficasse à definição do Estado nacional. A WCIT-12 foi organizada a fim de atualizar o Regulamento Internacional de Telecomunicações (ITRs), mas acabou sendo ofuscada pela assertividade dos Estados em buscar papel ativo na normatização do meio digital. A resolução acordada entre 89 países participantes da conferência admitiu que a governança da *internet* deveria ser entendida como um processo multissetorial, mas, que o papel dos governos nacionais são importantes na construção de uma governança estável, segura e justa (SHACKELFORD; CRAIG, 2014).

A interferência russa nas eleições presidenciais americanas de 2016 exemplifica a vulnerabilidade do espaço cibernético americano e o alcance das ferramentas digitais. Em janeiro de 2017 a *Central Intelligence Agency* (CIA), a *Federal Bureau of Investigation* (FBI) e a *National Security Agency* (NSA) divulgaram que a Rússia utilizou as redes sociais para influenciar o resultado das eleições presidenciais nos EUA (MASTERS, 2018). Nota-se, porém, que atualmente as questões relacionadas à segurança no ambiente digital ofuscam qualquer tipo de discussão sobre a governança da *internet*. A cybersegurança tornou-se uma das pedras basilares na discussão sobre uma governança da *internet* global e tende a gerar mais divergências do que qualquer vertente discutida do tema. A segurança digital é difícil de seccionar-se, pois a *internet* foi criada com o intuito de transnacionalizar o espaço de forma que não só pessoas de diferentes lugares do globo possam interagir, mas que pessoas diferentes e temas distintos consigam se interligar. Um dos cenários importantes de trazer à tona na discussão sobre ciberespionagem é como a espionagem industrial pode adentrar o âmbito das relações governamentais entre nações. A prisão da diretora financeira de uma das maiores empresas de tecnologia de origem chinesa, a Huawei, por espionagem comercial, afetou diretamente as relações entre os dois países e foi fator determinante que contribuiu para o início de uma guerra comercial entre China e os EUA no ano de

2018.[14] As questões de segurança da *internet* foram levantadas e o lado americano alegou espionagem comercial exercida pelo lado chinês.

Entretanto, não foi a primeira vez que as preocupações sobre a segurança digital adentrou os discursos nacionais do Estado norte-americano. Em 2012 o parlamento dos EUA publicou relatório onde acusava duas grandes empresas chinesas, ZTE e Huawei, de serem ameaças diretas à segurança nacional americana, pois a investigação interna gerou dados que sugeriam que as empresas privadas operavam juntamente com o governo chinês para atuar não no campo comercial, mas no sentido de fornecer dados necessários para colocar o governo chinês em vantagem. Em 2014, o Departamento de Justiça dos EUA indiciou soldados chineses por espionagem comercial, que segundo o governo americano invadiram as redes de diversas empresas nacionais de forma a obterem informações confidenciais, tudo a mando governo chinês. A questão da cibersegurança nacional é única no sentido que engloba não só os interesses da nação para seus cidadãos como também pode atuar de forma ofensiva contra seus próprios cidadãos em nome da segurança nacional. Não resta claro, ademais, quais os limites justificáveis de atuação do Estado no que diz respeito à defesa nacional.

4 DISCUSSÃO SOBRE GOVERNANÇA DA *INTERNET* NO NÍVEL INTERNACIONAL

Deve-se destacar o papel da *International Telecommunication Union* (ITU), fundada em 1865 com o intuito de mediar e auxiliar a conectividade dos existentes meios de comunicação, como rádio e órbitas de satélites. Produziu a citada entidade relatório em 1983 relacionando a acessibilidade à redes de informação com o crescimento econômico. A primeira *World Telecommunication Development Conference* surge sob supervisão do ITU em 1995, estabelecendo o *Centre for Telecommunication development*, que mais tarde foi incorporado à estrutura institucional do ITU (CHRISTOU; SIMPSON, 2012)

Um marco importante para o início de regras comuns a nível global para o funcionamento eficaz frente às novas tecnologias foi o tratado "Os Regulamentos Internacionais de Telecomunicações (ITR") assinado em 1988, administrado pela ITU,

[14] USTR. 2018. Office of the United States Trade Representative. Available online: https://ustr.gov/about-us/policy-offices/press-office/press-releases/2018/june/ustr-issues-tariffs-chinese-products (accessed on 30 June 2018).

que coordena com os países todos os tipos de redes de informação e comunicação, desde fios de cobre até tecnologias de dado sem fio. Uma de suas principais funções, cumpre sublinhar, foi a estruturação de sistemas que suportassem chamadas internacionais (MULLER, 2002). Devido às novas inovações e tecnologias, em 1999 foi levantada a necessidade de uma atualização no referido tratado. Dessa forma, o pacto foi atualizado na *World Congress on Information Technology* (WCIT)[15] em 2012, a saber:

> [...] considerado um tratado global vinculante destinado a facilitar a interconexão internacional e a interoperabilidade dos serviços de informação e comunicação, bem como assegurar sua eficiência e ampla utilidade e disponibilidade pública. O tratado estabelece princípios gerais para assegurar o livre fluxo de informações em todo o mundo, promovendo acesso acessível e equitativo para todos e lançando as bases para inovação contínua e crescimento do mercado.[16]

A ITU tem papel relevante em levantar questionamentos acerca ao mundo digital. É responsável por diversos seminários, tais como o *Global Symposium for Regulators* e o *World Telecommunication/ICT Policy Forum* (WTPF), os quais fornecem plataformas para reguladores e formuladores de políticas discutirem as principais questões que envolvem a constante mudança do ambiente digital (HILL, 2015; CHRISTOU E SIMPSON, 2012). O 11 de Setembro contribuiu para a adoção da Convenção de Budapeste sobre o Cibercrime, elaborada pela Conselho Europeu em outubro de 2001. O tratado vinculativo com alcance internacional entrou em vigor em 2004 e seu texto promove a cooperação e assistência jurídica entre Estados, além de introduzir definições de termos relevantes para a normatização de leis criminais sobre CHTER, 2016)

O ICANN sempre foi questionado devido ao seu controle unilateral e tendo em vista sua relação com o governo norte-americano, resultado de uma relação contratual da organização com o Departamento de Comércio dos EUA. Além disso, com perpassar do tempo as tensões cresceram e culminaram numa série de debates a nível global sobre as políticas da *internet*, que levaram à realização da Cúpula Mundial da Sociedade da Informação (WSIS, sigla em inglês) em 2003 e 2005, patrocinada pela ONU (EPSTEIN, 2013). A *World Summit on the Information Society* (WSIS) é importante em definir e reconhecer o papel de atores não estatais na elaboração de políticas referentes à *internet*.

---

15 *World Conference on International Telecommunications (WCIT-12)*, ITU, http://www.itu.int/en/wcit-12/Pages/default.aspx

16 https://www.itu.int/pub/S-CONF-WCIT-2012/en

O ICANN, mesmo com suas ligações governamentais, sempre foi uma organização privada, e em 2000 já era claro o forte papel das instituições privadas nos assuntos relacionadas à *internet*, tendo em vista principalmente a própria arquitetura do sistema operacional da *internet* que atuava multilateralmente por meio das múltiplas fronteiras.

Um importante ponto levantado pela China e pela Rússia na cúpula citada dizia respeito à definição mais abrangente de governança da *internet*, a qual deveria compreender não só nomes de domínio e questões técnicas, incluindo as temáticas de spam e de conteúdo ilegal. Além disso, a China propôs uma nova instituição intergovernamental de supervisão que abrangeria todos os assuntos relacionados ao âmbito digital, prezando pela soberania estatal, de responsabilidade da ONU, mais especificamente a União internacional de Telecomunicação (UIT) (DATYSGELD, 2017).

Os defensores do ICANN, liderados pelos EUA, argumentavam que o sistema digital deveria ser analisado apenas levando-se em consideração as questões técnicas e por isso seria melhor administrada por uma corporação privada. Já em contraponto, outros países como a China argumentam que a *internet* deveria ser administrada sob o âmbito político e mais especificamente deveria ser administrada através de instrumentos das Nações Unidas (EPSTEIN, 2013)

A cúpula não foi capaz de resolver as divergências entre a concepção de governança da *internet*, devido à complexidade do assunto. A questão envolve fatores políticos, econômicos e técnicos em razão da dependência do sistema ao aparato técnico que é de responsabilidade do ICANN (KLEINWATCHTER, 2004; KURBALIJA, 2016). Diversos setores foram inovados e outros criados com a introdução da *internet*, sendo manifesta sua importância para todos os aspectos sociais, comercias e políticos.

Devem ser destacados, todavia, os fatores positivos da realização da WSIS, que formalizou a chamada prática do "multistakeholderism", em que "representantes de grupos de defesa do interesse público, associações empresariais e outras partes interessadas participam de deliberações políticas intergovernamentais juntamente com governos" (WSIS, 2005). Outro importante resultado da referida cúpula foi a criação de fórum multilateral global com presença do *multistakeholderism* no debate sobre assuntos referentes à governança da *internet*, o *Internet Governance Forum* (IGF), e o Grupo de Trabalho sobre Governança da *Internet* (GTGI).

Enquanto o GTGI foi fundamental em aprofundar o debate sobre *multistakeholderism*, o IGF foi formalizado para atuar na mediação de conflitos

relacionados a decisões que influenciam diretamente o funcionamento da *internet*, assim como tornou-se palco para apresentar diversos esquemas normativos. (EPSTEIN, 2013). De uma perspectiva histórica o IGF é importante no que tange à demonstração de como os princípios de governança de um sistema de informação complexo são resolvidos.

Em 2004 as Nações Unidas criaram o *United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (UN GGE), o qual foca o contexto de segurança internacional com o intuito de fortalecer a segurança dos meios de informação e de telecomunicação (SILVA, 2008). Deve-se destacar seu papel em delimitar a agenda da segurança cibernética e introduzir o principio de leis internacionais para o âmbito do mundo digital.

Inicialmente o GGE atuou como mediador das visões diferentes dos Estados, conseguindo avanços nas discussões sobre os temas propostos. Em 2011 a Índia depositou proposta para a criação de Comitê sobre Protocolo de *Internet* (CIRP) e Rússia e China depositaram proposta de Acordo de Cooperação de Xangai, o qual abordava normas para as questões debatidas referente aos direitos dos Estados no ambiente cibernético (BAJAJ, 2014). Com a elaboração do manual de Tallin[17] em 2013, se colocou em evidência a aplicabilidade da *internet* como ferramenta militar e sua importância fundamental em qualquer tipo de operação militar. Pode-se observar o seu reflexo no estabelecimento de comitê nas Nações Unidas para analisar a segurança cibernética e seu papel no campo militar.

A partir de 2014 - 2015 foi notado um claro entrave entre as partes sobre o direito inerente dos Estados, à autodefesa e à aplicabilidade do direito internacional humanitário aos conflitos cibernéticos. Esse debate se estendeu para o GGE mais atual (2016 - 2017), não sendo alcançado consenso relacionado ao tema (DAVIS GELD, 2017). Em setembro de 2011 projeto conjunto para a criação de um Código Internacional de Conduta Internacional de Segurança da Informação foi apresentado na Assembleia Geral da ONU pela China, Rússia, Tajiquistão e Uzbequistão. O texto aborda a necessidade de cooperação entre Estados para impedir o alastramento de informações que incitem de qualquer forma a instabilidade política, econômica ou social. Não se obteve, contudo, a aceitação necessária, mesmo com a revisão do texto (CHTER, 2016).

[17] Documento acadêmico elaborado a pedido da OTAN por estudiosos e especialistas da área de crimes cibernéticos que aborda a aplicabilidade do direito internacional na internet.

O papel do setor privado na possível governança da *internet* deve ser destacado, pois a origem do ambiente digital e a forma como se utiliza a *internet* hoje em dia é resultado de um dos diversos modelos testados que com o auxílio de decisões técnicas e políticas resultaram na ascensão do setor privado. A questão do modelo *multistakeholderism* é uma das questões discutidas em relação a governança da *internet* devido ao papel de organizações privadas desde a criação da própria *internet*. A definição da mesma pode ser encontrada no Parágrafo 34 da Agenda de Túnis de 2005 da WSIS:

> Uma definição funcional da governança da Internet é o desenvolvimento e a aplicação por parte dos governos, do setor privado e da sociedade civil, em seus respectivos papéis, de princípios, normas, regras, procedimentos decisórios e programas compartilhados que moldam a evolução e uso da Internet.

O modelo propõe um sistema descentralizado aonde atores privados e da sociedade civil teriam papel no processo decisório de políticas relacionadas ao ambiente da *internet*. Como já abordado, a questão formal do *multistakeholderism* na governança da *internet* teve sua origem no primeiro WSIS, porem a questão na Cúpula não surgiu de um processo multissetorial devido a configuração da primeira WSIS onde a sociedade civil era permitida apenas no inicio dos debates.

A clara conexão de múltiplos setores com a concepção e funcionamento do ambiente digital, a crescente transnacionalidade existente devido a globalização, o papel exercido pela comunidade técnica e acadêmica reforçam a necessidade de inserir esse setor nas discussões relacionadas a formalização de uma legislação referente a *internet*.

Podemos ver como exemplo do modelo *multistakeholder* de governança da *internet* a *Internet Society* (ISOC), organização sem fins lucrativos que desde sua criação em 1992, procura atuar no sentido de facilitar o desenvolvimento operacional, de alcance, promovendo fóruns que permitam a multiplicidade de participantes para discutir políticas, a evolução do meio e tópicos relacionados a governança da *internet*. A ISOC é dividida em diversos *working groups* que lidam com tópicos especifico relacionados ao meio digital como a Força-Tarefa de Engenharia da *Internet* (IETF), que discute e estabelece os principais protocolos da *internet* e a Diretoria de Arquitetura da *Internet* (IAB, sigla em inglês), que oferece orientação técnica com o intuito de catalisar a evolução do meio digital.

A *Internet Society* desenvolveu quatro pilares para o funcionamento da evolução do modelo multistakeholder: "inclusão e transparência; responsabilidade coletiva;

tomada de decisão e implementação eficazes; colaboração através de uma governança distribuída e Inter operável".[18]

5 GOVERNANÇA DA *INTERNET* NA PERSPECTIVA DO NEORREALISMO

Dada a fragmentação política atual no que diz respeito ao sistema liberal democrático, a análise neorrealista se encaixa de forma mais correta na análise de uma possível governança internacional da *internet*. O neorrealismo surge no contexto político do fim da Guerra Fria, da crise do petróleo, do crescimento das organizações internacionais, onde observa-se que a teoria realista não conseguia explicar satisfatoriamente o cenário internacional. Kenneth Waltz reformula a teoria realista, com o lançamento de seu *livro Theory of International Politics*, em 1979, reestruturando a vertente teórica original de forma a acomodar os desafios enfrentados no cenário político da época. Waltz afirma que o sistema internacional deve ser analisado de forma estrutural, sendo a anarquia a condição que orienta as relações internacionais, inexistindo poder central que consiga regular as ações estatais. Os estados interagem buscando a sua sobrevivência e a estrutura que rege o sistema internacional apenas se alterará se as grandes potências alterarem o status quo. Diz Waltz (1979, p. 145): "A distinção entre os domínios da política nacional e internacional não se encontra no uso ou não uso da força, mas nas suas diferentes estruturas."

O neorrealismo tem como principal pilar a centralidade do Estado na estrutura anárquica da política internacional e destaca como as relações de poder atuam como variável determinante para a definição dos tipos de relações existentes entre os Estados (WALTZ, 1979). A visão neorrealista sobre as organizações e regimes internacionais é determinante para entender como a teoria entende a cooperação entre Estados. As organizações internacionais não são encaradas como atores independentes e sim como mecanismos pelo qual os Estados podem-se utilizar, onde seu papel é reduzido a ferramenta estatal. As instituições são apenas reflexo das relações de poder existentes no cenário internacional que tendem a manter balança de poder existente. O neorrealismo entende o cenário internacional como anárquico onde os Estados vão agir

[18] Os objetivos ficam mais aclarados no site oficial da Internet Society. Saiba mais em: https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

de forma a maximizarem seus interesses nacionais o que, leva a poucas ocasiões de cooperação internacional a longo prazo e, quando enfrentam a possibilidade de cooperação se encontram em condição incerta e insegura tendendo a, operar sob o dilema do prisioneiro, dificultando ainda mais a cooperação entre os agentes. Importante observar que a cooperação, qualquer que seja o arranjo dado, possui limitações, inclusive estruturais e relativas à capacidade dos agentes. Neste sentido, valiosa, mais uma vez, a preleção de Waltz:

> Num sistema de auto-ajuda cada uma das unidades gasta porção de seu esforço, não a perseguir seu próprio bem, mas a arranjar os meios de se proteger dos outros. A especialização num sistema de divisão de trabalho funciona com vantagem para todos, apesar de não ser equitativa. A desigualdade na distribuição esperada do produto acrescido opera fortemente contra a extensão da divisão do trabalho a nível internacional. Quando confrontados com a possibilidade de cooperarem para ganho mútuo, os estados que se sentem inseguros devem querer saber como o ganho mútuo será dividido. São impelidos a perguntar não "Iremos ambos ganhar?", mas "Quem ganhará mais?". Se um ganho esperado é pra ser dividido, digamos, na razão de dois pra um, um estado pode usar o seu ganho desproporcional para implementar uma política virada para prejudicar ou destruir o outro. Mesmo a perspectiva de grandes ganhos absolutos para ambas as partes não invalida a sua cooperação desde que cada um tema a forma como o outro irá usar as suas crescentes capacidades. Notem que os impedimentos à colaboração podem não residir no caráter e na intenção imediata de qualquer uma das partes. Em vez disso, a condição de insegurança – no mínimo, a incerteza de um em relação às futuras intenções e acções do outro – trabalha contra a sua cooperação. (WALTZ, 1979, p. 147)

Percebe-se, assim, que a visão da teoria realista sobre acordos internacionais aproximar-se da busca pela maximização dos interesses nacionais, de forma que a cooperação ocorrerá apenas quando os interesses individuais estatais sejam atendidos. A posição estatal como entidade soberana, como o único agente político legítimo internacional, coloca em segundo plano, por conseguintes, os regimes internacionais que são, em grande medida, reflexo da manutenção de poder existente. Além do mais, a lógica da maximização dos interesses nacionais é um paradigma que não deve ser desprezado em nenhuma hipótese. Em seu emblemático modelo teórico denominado "Mapa Estrutural das Sociedades Capitalistas", Boaventura de Sousa Santos refere-se à maximização em questão como maximização da eficácia das nações no denominado espaço mundial (SANTOS, 1996).

Para que se possa compreender a fragmentação atual observada no cenário político mundial, a crise de legitimidade dos regimes internacionais e, ainda, a razão

pela qual a criação de uma governança da *internet* é improvável, deve-se entender os problemas crescentes observados desde o pós-Guerra Fria. O mundo liberal que foi desenhado desde o fim da Segunda Guerra Mundial foi construído baseado nas organizações internacionais e na busca pela institucionalização da governança internacional de forma a alterar o sistema de equilíbrio de poder que atuava como mediador das relações estatais. Com o fim da Guerra Fria, observou-se uma segunda onda de reformulação do sistema internacional, marcada pelo fim da bipolarização do cenário internacional e pela intensificação da interdependência global. Buscou-se, deste modo, a utilização das organizações internacionais como ferramentas para facilitar o intercâmbio internacional e a migração (HOOGHE; LENZ; MARKS, 2019). Porém, com a legitimação cada vez maior dos arranjos institucionais globais (ex.: normativas da OMC), observou-se que as políticas que estabeleciam as relações internacionais foram adentrando o cenário nacional de forma a afetar diretamente as políticas nacionais, o que gerou reação tardia de modo a contribuir para o crescimento do protecionismo e no atual quadro enfraquecido dos regimes internacionais.

Mearsheimer (2019) destaca que a globalização atuou de forma a erodir a ordem internacional liberal, pois contribui para a ascensão de outras economias, o que cria um mundo multipolar onde, de acordo com o próprio autor, um mundo multipolar não suporta um regime ideológico como o liberal. A ascensão da China e da Rússia põe fim à ordem unipolar americana, emergindo por conseguinte uma nova ordem internacional baseada nos princípios realistas onde o balanço de poder atuará de forma a mediar as relações econômicas e políticas e, ademais, a apontar possíveis soluções de problemas comuns ao globo. A nova ordem liberal observada no período posterior à Guerra Fria foi fundada através da expansão de instituições internacionais de modo a criar ambiente que pudesse influenciar a maioria dos Estados e suas políticas, fator fundamental para a abertura comercial desejada de forma a maximizar o livre comércio. A crise financeira de 2008, a crise do euro, o *Brexit* e a crise de refugiados são exemplos de fatores que contribuíram para a descrença do liberalismo e a ascensão de políticas nacionalistas e protecionistas, por exemplo.

CONSIDERAÇÕES FINAIS

Debater a fragmentação do ambiente digital é, em grande medida, um contrassenso, se pensarmos nos princípios de universalidade que foram utilizados na

idealização da *internet*. Contudo, ao se analisar o ambiente digital, é necessário adicionar as vertentes políticas observadas no cenário internacional atual. A retirada do Reino Unido da União Europeia, a crise dos refugiados, a sistemática saída dos EUA de diversos tratados internacionais (tais como o Acordo Transpacífico de Cooperação Econômica, o Acordo de Paris, o Acordo de Forças Nucleares de Alcance Intermediário, dentre outros), assim como a instabilidade das relações americanas junto à Organização Mundial do Comércio, as crescentes políticas protecionistas, tudo isto elucida a instabilidade atual de arranjos institucionais internacionais.

A atual fragmentação política internacional constitui derivação, segundo Mearsheimer (2019): (i) do favorecimento às organizações internacionais ao invés das políticas nacionais; (ii) da "hyperglobalization" que ocorreu pós-Guerra Fria, quando os esforços para diminuir as barreiras do comércio internacional intensificaram a interdependência global, tornando o cenário internacional mais instável e levando a crises financeiras mais recorrentemente; (iii) da limitação dos princípios basilares da ordem liberal, como a livre circulação de pessoas e a delegação de poderes a instituições internacionais, fatores que causaram fricção interna nos Estados, pois tendiam a se chocar com as crenças de soberania internacional de parte da população; e (iv) do fato de que a intensa globalização beneficiou em parte alguns Estados, causando, contudo, ao longo do tempo, problemas econômicos e políticos que provocaram o declínio da opinião favorável à ordem internacional liberal.

É precisamente neste contexto de fragmentação que deve ser situada a governança da *internet*, a qual compreenderá no futuro acordos bilaterais e, mesmo assim, de maneira muito esparsa. Entendo, por isso, que uma governança da *internet* no plano multilateral beira a impossibilidade. Há, atualmente, uma descrença em relação à capacidade de governança global das organizações internacionais, tendo em vista o atual cenário político. O extenso espectro do meio digital e os diversos atores relevantes a sua discussão criam barreiras ainda maiores no que diz respeito a uma normatização do meio. O ciberespaço foi construído de forma fragmentada onde diversos atores distintos são importantes no seu funcionamento e na sua operacionalização, de maneira que construir acordos de governança para esta área é algo ao mesmo tempo complexo e improvável.

Nota-se que a proposta inicial idealizada de se criar um espaço transfronteiriço se transformou de forma que a busca pela universalização foi substituída pela fragmentação do ambiente digital, onde se constata a existência de políticas unilaterais a

fim de filtrar o conteúdo disponível, mediante a aprovação de leis nacionais que imponham restrições em relação à privacidade, criando, assim, novas barreiras geopolíticas dentro do espaço cibernético.

Deve-se visualizar o ambiente digital além do âmbito político: o complexo ecossistema do espaço digital exige, por isso mesmo, um tipo de análise singular e específico em relação a sua regulamentação. A *internet* tem característica ímpar de estar em constante evolução, com alcance global; permite, além disso, modificações regulares promovidas por todos os seus usuários, indivíduos que a utilizam em seu potencial complexo, interligando diversos aspectos relevantes da política, economia e sociedade, criando, ao final, dificuldade no que diz respeito a sua regulamentação.

O que tem se observado é um movimento para a expansão do alcance nacional e comercial no ambiente digital de modo a proteger sua segurança e seus interesses individuais de maneira tal que a interconectividade e direitos humanos sejam deixados em segundo plano. A normatização que se observa no momento se concentra nas questões comerciais (como direitos autorais e intelectuais), na censura de conteúdos (por parte estatal e privada) e nos interesses geopolíticos. O potencial universal da *internet* tem sido constantemente freado por força de diversos fatores, em especial: (i) divergências em relação aos recursos críticos estruturais da *internet*; (ii) grande quantidade de instituições diferentes que exercem papel no funcionamento da *internet* (tais como ICANN, IETF, ITU, dentre diversos outros órgãos nacionais); (iii) posicionamentos distintos dos grandes atores estatais como China (*internet* altamente filtrada), EUA (*internet* livre) e Rússia ([19]); e (iv) priorização e preocupação com a cibersegurança nacional.

A descoberta da vigilância maciça exercida pela NSA atuou de forma a legitimar as políticas de proteção nacional no ambiente digital e incentivou a fragmentação desse local. A temática de cibersegurança é um dos maiores empecilhos na discussão de uma governança internacional da *internet* e tende a polarizar opiniões de modo que qualquer tipo de normatização no nível global seja extremamente improvável. A realidade é que para a formação de qualquer tipo de governança internacional seria necessário o apoio estatal incondicional. Devido ao atual cenário político e tendo em vista a

[19] A internet na Rússia é uma incógnita: não se sabe ao certo o nível de censura vigente no país no tocante ao uso da internet. Além disso, nos debates internacionais, a Rússia mostra-se contrária à governança compartilhada da internet.

multipolaridade observada, essa possibilidade de cooperação se afasta cada vez mais do campo das possiblidades.

Este artigo buscou analisar a diversidade de fatores que contribuem para o atual quadro fragmentado de regulamentação do meio digital. A multiplicidade de atores e interesses divergentes cria impasse no estabelecimento de uma governança da *internet* em nível global. O enfraquecimento dos organismos internacionais no cenário político internacional, os posicionamentos estatais divergentes, a quantidade de atores envolvidos na estrutura crítica da *internet* e, finalmente, as preocupações quanto à cibersegurança, evidenciam quadro fragmentado das políticas de normatização do ambiente digital.

REFERÊNCIAS

BAJAJ, K. Cyberspace: post Snowden. *Strategic Analysis*, v. 38, n. 4, p. 582-587, 2014. DOI: 10.1080/09700161.2014.918448. Acesso em: 1 maio 2020.

BUDNITSKY, S.; JIA, L. Branding Internet sovereignty: digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies, v. 21, n.* 5, p. 594–613, 2018. DOI: https://doi.org/10.1177/1367549417751151. Acesso em: 10 fev. 2020

do Rio Grande do Sul, Porto Alegre, 2014. Disponível em: https://www.lume.ufrgs.br/handle/10183/114399. Acesso em: 20 set. 2019

CHRISTOU, G.; SIMPSON, S. The influence of global internet governance institutions on the EU. *In*: COSTA, O.; JØRGENSEN, K. E. (eds.). *The influence of international institutions on the EU*: Palgrave studies in European Union politics. London: Palgrave Macmillan, 2012. p. 96-110. Disponível em: https://link.springer.com/chapter/10.1057/9780230369894_6. Acesso em: 5 mar. 2019

CHANDER, A.; LE, U. P. Data nationalism. *Emory Law Journal*, v. 64, n. 3, p. 678-739, 2015.

DATYSGELD, M. W. *O papel da governança da internet dentro da governança global:* um estudo de caso da ICANN. Repositório Institucional UNESP, 2017. Disponivel em: https://repositorio.unesp.br/bitstream/handle/11449/151066/datysgeld_mw_me_mar.pdf. Acesso em: 5 mar. 2019.

DENARDIS, L. *The emerging field of internet governance*. Yale Information Society Project Working Paper Series. 2010. DOI: http://dx.doi.org/10.2139/ssrn.1678343. Acesso em: 12 fev. 2020

World Economic Forum. Future of the Internet Initiative Whitepaper. 2016. Disponível em: www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf. Acesso em: 22 dez. 2019

EPSTEIN, D. The making of institutions of information governance: the case of the Internet Governance Forum. *Journal of Information Technology*, v. 28, n. 2, p. 137–149, 2013. DOI: doi:10.1057/jit.2013.8. Acesso em: 19 nov. 2019

EICHENSEHR, K. The cyber-law of nations. *The Georgetown Law Journal*, v. 103, p. 317, 8 Jan. 2014. Disponível em: http://ssrn.com/abstract=2447683. Acesso em: 11 jun. 2019

FINKELSTEIN, L. S. What is global governance? *Global Governance*, v. 1, n. 3, p. 367-372, 1995. Disponível em: http://www.jstor.org/stable/27800120. Acesso em: 20 out. 2019

FROOMKIN, M.; LEMLEY, M. *ICANN and Antitrust*. 2003 U ILL. L. REV. 1. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/unilllr2003&div=9&id=&page=. Acesso em: 1 fev. 2020

2009.

HILL, J. *Internet fragmentation:* highlighting the major technical, governance and diplomatic challenges for U.S. policy makers. Berkman Center Research Paper; Harvard Belfer Center for Science and International Affairs Working Paper. 2012. Disponível em: https://ssrn.com/abstract=2439486. Acesso em: 2 Fev. 2020

HILL, R. Dealing with cyber security threats: international cooperation, ITU, and WCIT. In: INTERNATIONAL CONFERENCE ON CYBER CONFLICT: ARCHITECTURES IN CYBERSPACE, 7. *Annals* ... Tallinn, 2015. p. 119-134. DOI: 10.1109/CYCON.2015.7158473. Acesso em: 8 dez. 2019

HOOGHE, L.; LENZ, T.; MARKS, G. Contested world order: the delegitimation of international governance. *Rev. Int Organ*, n. 14, p. 731–743, 2019. DOI: https://doi.org/10.1007/s11558-018-9334-3. Acesso em: 20 nov. 2019

INT'L TELCOMM. Union, Final Acts of the World Conference on International Telecommunications. 2012. [hereinafter ITU Resolutions]. Disponível em: http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf. Acesso em: 19 set. 2019

KLEINWATCHTER, W. Beyond ICANN vs ITU: how WSIS tries to enter the new territory of Internet governance. *Gazette: The International Journal for Communication Studies*, v. 66, n. 3–4, p. 233–251, 2004.

KURBALIJA, J. *An introduction to internet governance*. 7. ed. Mídia: DiploFoundation, 2016.

MASTERS, J. Russia, Trump, and the 2016 U.S. Election. *Council on Foreign Relations*, Nova York, fev. 2018. Disponível em: https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election. Acesso em: 10 jan. 2020

MCCULLAGH, D. Should the UN administer the internet?. *CNET News.com*, 30 mar. 2005. Disponível em: http://news.zdnet.co.uk/internet/0,1000000097,39193156,00.htm?r=1. Acesso em: 19 mar. 2019.

MEARSHEIMER, J. Bound to Fail: The Rise and Fall of the Liberal International Order. *International Security*, n. 43, p. 7–50, 2019. Disponível em: https://www.mitpressjournals.org/doi/full/10.1162/isec_a_00342. Acesso em: 12 jul. 2019

MUELLER, M. China and global internet governance: a tiger by the tail. *In:* DEIBERT, R.; PALFREY, J.; ROHOZINSKI, R; ZITTRAIN, J. (eds.). *Access contested:* security, identity, and resistance in Asian cyberspace. Cambridge, MA: MIT Press, 2011. p. 177–194.

NOCETTI, J. Contest and conquest: Russia and global internet governance.

International Affairs, v. 91, n. 1, p. 111–130, 2015. Disponível em: https://academic.oup.com/ia/article-abstract/91/1/111/2326827. Acesso em: 03 jan. 2020

PARE, D. J. *Internet governance in transition*. Lanham, Maryland: Rowman & Littlefield Publishers Inc., 2003.

REDEKER, D; GILL, L.; GASSER, U. Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights. *International Communication Gazette*, n. 80, p. 302–319, 2018. DOI: doi: 10.1177/1748048518757121. Acesso em: 12 nov. 2019

ROSENAU, J. N. Governance in the Twenty-first Century. *Global Governance*, v. 1, n. 1, p. 13–43, 1995.

SANTOS, Boaventura de Sousa. *Pela mão de Alice:* o social e o político na pós-modernidade. São Paulo: Cortez, 1996.

SILVA, M. *A geopolítica da rede e a governança global de internet a partir da cúpula mundial sobre a sociedade da informação*. 2008. Tese (Doutorado em Geografia Humana) - Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo, São Paulo, 2008. DOI: doi: 10.11606/T.8.2008.tde-18032009-112622. Acesso em: 03 mar. 2020

SHACKELFORD, S. J.; CRAIG, A. N. *Beyond the new 'digital divide': analyzing the evolving role of governments in internet governance and enhancing cybersecurity*, 50 STAN. J. INT'L L. 119, 2014.

USTR. *Office of the United States Trade Representative*. 2018. Available online: https://ustr.gov/about-us/policy-offices/press-office/press-releases/2018/june/ustr-issues-tariffs-chinese-products. Acesso em: 10 mar. 2020

WALTZ, Kenneth N. *Theory of international politics*. New York: McGraw-Hill, 1979.

WEINBERG, J. ICANN and the problem of legitimacy. *Duke Law Journal*, v. 50, n. 187, p. 187-260, 2000.

WSIS. World Summit on the Information Society. 2005. *Tunis Agenda for the Information Society WSIS-05/TUNIS/DOC/6* (Rev. 1). Disponível em: http://www.itu.int/wsis/doc2/tunis/off/6rev1.html. Acesso em: 1 set. 2019

ZITTRAIN, J.; PALFREY, J. *Access denied: the practice and policy of global internet filtering*. Oxford Internet Institute, Research Report No. 14, Jun. 2007. Disponível em: http://www.oii.ox.ac.uk/research/publications/RR14.pdf. Acesso em: 14 out. 2019