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

GEORGIA MARIA VASCONCELOS PFEILSTICKER RIBAS

O MUNDO CIBERNÉTICO: a Governança na World Wide Web e o Impacto nas Relações Internacionais.

BRASÍLIA – DF
2020

GEORGIA MARIA VASCONCELOS PFEILSTICKER RIBAS

O MUNDO CIBERNÉTICO: a Governança na World Wide Web e o Impacto nas Relações Internacionais.

Monografia apresentada 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: Prof. Msc. Lucas Soares Portela.

BRASÍLIA – DF
2020

GEORGIA MARIA VASCONCELOS PFEILSTICKER RIBAS

O MUNDO CIBERNÉTICO: a Governança na World Wide Web e o Impacto nas Relações Internacionais.

Monografia apresentada 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: Prof. Msc. Lucas Soares Portela.

BRASÍLIA, 06 DE JUNHO DE 2020

BANCA EXAMINADORA

Professor Orientador
Lucas Soares Portela

Professor Avaliador
Oscar Medeiros Filho

A todas as pessoas que amo e admiro, e que me apoiaram neste caminho do conhecimento.

AGRADECIMENTOS

Agradeço primeiramente a minha família, em especial, minha avó Norma Ilse Pfeilsticker Ribas que, em seus 92 anos, me deu todo o apoio para a realização dessa etapa em minha vida. Agradeço ainda aos meus amigos e colegas de classe que me fizeram companhia em momentos difíceis durante os quatro anos de estudos e que estiveram torcendo por mim durante todo esse tempo.

Também agradeço os meus colegas de trabalho, em especial, Meu ex-Coordenador e agora amigo e colega de trabalho Gustavo Sousa Torres, por me proporcionar a oportunidade de fazer parte de uma Assessoria Internacional com uma brilhante equipe, que me ensinou e me apoiou durantes os anos da graduação.

Agradeço a todos os professores do Curso de Relações Internacionais da Faculdade de Ciências Jurídicas e Sociais do Centro Universitário de Brasília, pelo incrível esforço e por compartilharem seus conhecimentos. Agradeço imensamente ao meu Orientador, Professor Lucas Soares Portela, pela paciência, por ser um professor/orientador/pai/amigo, pelas oportunidades de crescimento intelectual no decorrer dos anos de estudo e pelo incentivo ao projeto de pesquisa. E por fim, agradeço aos meus padrinhos Nilson Dias Martins dos Santos Júnior e Monica Rossyna Lopes e Vasconcelos dos Santos por desde o momento em que nasci sempre estiveram ao meu lado independente da situação, amo vocês como todo o meu coração.

Meus sinceros agradecimentos a todos, por deixarem uma pequena, mas significativa marca no meu livro da vida.

“Você não pode esperar que outra pessoa aja. Eu estava procurando por líderes, mas percebi que liderança é ser o primeiro a agir.”

— Edward Snowden

“The work of a generation is beginning here”.

— Edward Snowden

Resumo

Essa monografia tem como objetivo maior defender o porquê estudar as Relações Internacionais no Meio Cibernético (CiberRI), um campo internacionalista, cujo o objeto de estudo é o impacto no mundo cibernético e nas relações internacionais, tendo como marco histórico a criação da ARPANET no final dos anos 60. Assim, a literatura envolve, os autores clássicos das Relações Internacionais, passando brevemente pela Ciência da Computação e Tecnologia da informação. O presente trabalho divide-se em três partes. A primeira parte faz um aparato histórico da criação da internet em si, fazendo uma análise relacionando as teorias de RI, com uma possível teoria cibernética. A segunda parte é discutida de forma a apresentar a problemática da securitização do espaço cibernético, e a apresentação do regime internacional e governança no mesmo âmbito. Por fim, o último capítulo apresenta dois casos práticos o caso Facebook + Cambridge Analytica e o caso Edward Snowden + Wikileaks, ajudando dessa forma a contextualizar alguns acontecimentos ciber internacionais. Esse estudo segue tanto o uso de métodos qualitativos quanto quantitativos, tais como pesquisa bibliográfica e documental e análise de reportagens, entre outros.

Palavras-chave: Ciberespaço. Relações Internacionais Cibernéticas. Securitização. Governança.

Abstract

This undergraduate thesis has the main purpose of advocating on why study International Relations in the Cybernetic Environment (CiberIR), an internationalist field, whose object of study is the impact on the cyber world in the international relations. As a historic milestone is the creation of ARPANET in the late 60s. Therefore, the literature involves the classic authors of international relations, passing quickly through Computer Science and Information Technology. The present work is divided into three parts. The first part makes a brief history of the creation of internet itself, making an analysis related to the theories of IR, with a possible cybernetic theory. The second part is discussed in order to present the problem of securitization of the cyberspace, and a presentation of the international regime and governance in the same scope. Finally, the last chapter presents two practical cases, the case of Facebook + Cambridge Analytica and, the case of Edward Snowden + Wikileaks, as a result helping to contextualize some international events. This follows both the use of qualitative and quantitative methods, such as bibliographic and documentary research and analysis of reports, among others.

Key-words: Cyberspace. International Cyber Relations Securitization. Governance.

SUMÁRIO

INTRODUÇÃO

Este trabalho de pesquisa exibirá o fenômeno tecnológico da Internet, a forma com que a tecnologia evoluiu nas últimas décadas, o procedimento histórico que deu origem ao regime global para a sua governança e respectiva pauta temática que atrai o interesse para as relações internacionais. A criação da World Wide Web em 1989 e o avanço das tecnologias da informação no final do século XX, criaram o espaço cibernético como o conhecemos hoje. Essa evolução não foi só dentro do espaço virtual, mas também, na forma em como os Estados interagem no meio internacional.

Os mesmos estão intervindo mais nas dinâmicas do ciberespaço com a elaboração de estratégias de defesa, segurança e inteligência cibernética devido ao surgimento de novas tecnologias. A presente monografia argumenta as novas possibilidades de ameaças à segurança nas relações internacionais que vem se espalhando no ciberespaço pela ação de indivíduos, organizações e Estados Nações. Nesse aspecto, a justificativa científica para a realização desse trabalho é que o tema possui grande relevância para o campo de estudo das Relações Internacionais e possui pouca bibliografia no Brasil. O objetivo geral é fazer uma análise sobre a política de cooperação entre estados e o regime internacional bem como mostrar a importância que a governança na internet tem dentro do sistema internacional e assim, compreender a importância da cibersegurança, e ciberdefesa (Estados, Organizações Internacionais e indivíduos).

Não se pode isolar o meio cibernético ou a internet dos seus efeitos sobre a forma com que as nações interagem e definem regras de coexistência no meio internacional. As variáveis que permitiram o aparecimento da Internet e suas consequências políticas, jurídicas, econômicas e socioculturais não foram totalmente exploradas dentro do ponto de vista das relações internacionais. As ordenações institucionais que possuem o propósito de administrar o funcionamento das redes em escala global direcionam para a existência de mecanismos de governança que não se encaixam em moldes tradicionais do regime que coordena as relações entre os Atores no Sistema Internacional.

A presente pesquisa pode ser caracterizada enquanto seu recorte metodológico com natureza descritiva, explicativa e exploratória quanto aos fins e um estudo qualitativo quanto aos meios. Foi utilizado o método dedutivo, isto é, partindo do geral para o

particular, primeiro foi feito uma análise da história e criação do meio cibernético e depois estudou-se os casos práticos do Facebook + Cambridge Analytica e o caso Snowden + Wikileaks.

Com base nestas discussões teóricas e subsidiadas por esses procedimentos metodológicos, a presente monografia está estruturada por meio de uma lógica dedutiva em três capítulos, partindo de marcos históricos-teóricos, até se chegar a uma análise empírica de um estudo de caso. A base da monografia conta fontes primárias (reportagens em jornais e revistas, documentação governamental sobre o assunto e dados quantitativos) e fonte secundária (artigos e livros científicos e gráficos disponíveis sobre o assunto).

No primeiro capítulo, é apresentado o delinear histórico da criação da Internet, e sua delimitação de espaço, sendo diferenciado do espaço geográfico. Suas características também são apontadas, como temporalidade, fisicalidade, permeação, fluidez, participação, atribuição e responsabilidade. Ainda no primeiro capítulo é apresentado a instauração da internet no Brasil, e sua instauração em 1975, durante o governo de Ernesto Geisel; a importância de estudar o espaço cibernético nas Relações Internacionais, observando o movimento de institucionalização sobre a temática; e finalmente ao final do capítulo são apresentados os aparatos teóricos de Relações Internacionais, como o Neorrealismo e o Construtivismo, e suas relações com o ciberespaço.

O segundo capítulo é apresentado, a securitização no espaço cibernético, com o aumento em ataques e sequestros cibernéticos observou-se uma tendência do tema no mundo. A problemática da segurança multidimensional e a definição do mesmo são apresentadas neste capítulo juntamente ao regime da governança no meio cibernético e nas relações internacionais, a reestruturação do setor de defesa e o estabelecimento da política de segurança da informação no brasil.

No último capítulo são apresentados os recursos de poder no século XXI, onde no mundo atual encontramos grandes transnacionais das Tecnologias da Informação e Comunicação, que possuem uma maior parte dos recursos tecnológicos. Obtendo um grande poder sobre os padrões de comportamento e de consumo. Além disso, são apresentados neste capítulo o caso de vazamento de dados da empresa Facebook junto a Cambrite Alalyitica, que gerou uma grande repercussão e preocupação sobre a utilização indevida de dados dos usuários tanto na plataforma como fora dela. Não poderia ficar de

fora dessa abordagem o famoso caso do Edward Snowden e do site Wikileaks, que publicou em seu site uma enorme quantidade de arquivos e informações secretos do governo dos Estados Unidos.

1 ASPECTOS TEÓRICOS E HISTÓRICO DO ESPAÇO CIBERNÉTICO

O Espaço Cibernético é criado através do espaço-tempo onde há oscilações com movimentos digitais; com inúmeros comandos, linhas de códigos, que representam fatos relacionados à comunicação, informação e tecnologia. Esse enorme "mundo" é formado por uma espécie de teia de informações que se vincula ao tempo, pois existe um período em relação ao envio e a chegada das informações.

A concepção newtoniana sobre o tempo é considerada uma unidade linear independente do espaço. Já a teoria da relatividade de Albert Einstein afirma que as grandezas de tempo e espaço formam juntos uma unidade cósmica indissociável. Em 1915, a teoria da relatividade geral mudou a concepção geométrica de espaço, deixando de ser tridimensional para ser quadrimensional.

Assim o espaço e o tempo deixam de ser concepções independentes para formarem "um objeto quadrimensional chamado Espaço-Tempo" (Hawking, 1995, p.40). A característica abstrata e a enorme dimensão do espaço cibernético dificultam a compreensão de seu tamanho. Por ser algo intangível, a mensuração desse ambiente se torna mais complexa do que aquela realizada nos demais espaços geográficos.

O espaço cibernético é extremamente amplo onde não há delimitações. Seu limite é o próprio imaginário humano e capacidade de projetá-la em inovação tecnológica. A constituição, o tratamento, transmissão e a acumulação desse enorme volume de dados acontecem sem delimitação de fronteiras e a informação hoje está disponível literalmente em qualquer lugar, basta com que o indivíduo tenha acesso a uma rede e um aparelho celular.

O espaço cibernético apresenta alguns aspectos bem diferentes do demais espaço geográfico, seja terrestre marítimo ou aéreo, que são consideramos como concretos. Já o

espaço cibernético é considerado por muitos estudiosos como um ambiente abstrato sendo um produto do imaginário humano.

Quadro 1.1 - Características do espaço cibernético

Características	Significância
Temporalidade	Modifica a nossa noção de tempo, a torna mais instantânea, devido a velocidade da troca de informação;
Fisicalidade	Através do espaço cibernético é possível ultrapassar as barreiras geográficas sem sair do seu local;
Permeação	É possível se infiltrar em fronteiras e jurisdições;
Fluidez	Está em constante alteração;
Participação	Devido ao fato de aumentar a possibilidade de ativismos políticos;
Atribuição	Em alguns casos, como a Dark Web, é difícil identificar os atores responsáveis;
Responsabilidade	Conectada, especialmente, com a sexta característica, devido à dificuldade, em alguns casos, de conectar o crime com o responsável, possibilita evitar mecanismos de responsabilidade.

Fonte: Arthur C. Maziero e Danielle J. Ayres Pinto,2018.

Desde seus primórdios, os seres humanos modificam o espaço geográficos conforme a necessidades e interesses que vão surgindo, em um processo chamado de "territorialização" (RAFFESTIN, 1993). Dessa forma, os espaços são moldados em territórios conforme o contexto histórico e social de cada povo, mesmo que em um ambiente virtual como no caso do espaço cibernético. Assim, por ser uma criação humana, o espaço cibernético foi explorado como uma ferramenta de grande importância desde sua constituição, controlado satélites, radares marinhos até mesmo trilhos do metrô.

O processo de territorialização, conforme Raffestin (1993) também pode ser utilizado como um instrumento político, de controle e de poder. Nessa perspectiva, o espaço cibernético foi ampliado dentro de sua territorialização sendo atualmente distinto do próprio conceito de Internet, pois inclui não somente a rede conectada de computadores, mas qualquer grupo de equipamento que armazenam e trocam informações (CLARKE, 2010). Assim, pode-se inferir que o espaço cibernético é mais amplo do que a própria

Internet, pois engloba também as intranets[1] e qualquer sistema que guardar informações, que são os principais recursos de poder desse espaço geográfico.

1.1 Histórico do Espaço cibernético

As primeiras fases da criação do que hoje chamamos de internet começou em 1960 no Estados Unidos da América, especificamente no Instituto de Tecnologia de Massachusetts (MIT) (KNIGHT, 2014). Os pesquisadores do MIT procuraram desenvolver uma espécie de comunicação através de "pacotes"[2] entre alguns computadores. O conceito de computadores em redes conectados por roteamento de pacotes em vez de comutação por circuitos foi desenvolvido por Joseph Carl Robnett Licklider, do MIT, em agosto de 1962 (KNIGHT, 2014).

A ideia de pacotes de dados foi desenvolvida por Licklider. Por meio dessa criação, seria possível identificar a origem do dado até o ponto de chegada, permitindo o envio da informação de um local a outro. Naquela época, Licklider era o primeiro gerente do programa de pesquisa de computação da Defense Advanced Research Projects Agency (DARPA), conhecido atualmente como ARPA (KNIGHT, 2014).

Um segundo pioneiro, mas não menos importante para o desenvolvimento da internet, foi Paul Baran, que trabalhou como pesquisador financiado pela Força Aérea Americana na RAND Corporation na Califórnia (KNIGHT, 2014). Seu trabalho consistia em desenvolver um sistema que garantisse a resiliência da Força Aérea Americana após um ataque nuclear. A pesquisa de Baran consistia em criar uma comunicação descentralizado que em tese permitiria os militares de manter o comando e controles de aeronaves junto a mísseis nucleares mesmo depois de um ataque nuclear. Também considerado como um dos pais da internet, Vincent Cerf que hoje é Vice- Presidente da Google explica o papel de Baran:

> Baran articulou a utilidade de empacotamento, embora tenha chamado as unidades como "Blocos de mensagem", Seu sistema nunca foi construído. No entanto seu trabalho foi notado pelos especialistas de desenharam a ARPANET depois da conclusão do seu desenho básico. Enquanto eu estava dirigindo o programa da Internet tive como objetivo torná-la

[1] Redes privadas de computadores
[2] Conjunto de dados ou sequência de dados estruturados em uma unidade digital chamada pacote.

> resistente a um ataque nuclear e, além disso, demonstrou sua capacidade de autorecuperação em cooperação com o Comando Aéreo Estratégico, utilizando rádios aéreos de comunicação por pacotes. Então, as ideias de Baran encontraram terra fértil na Internet, ainda que não na ARPANET. (KNIGHT, 2014, p. 18).

A comunicação por pacotes possibilitou a criação da ARPANET, através de pesquisas do Departamento de Defesa dos EUA. Tornando-se operacional em 1969, quando quatro computadores foram conectados. Esse projeto não foi projetado para uso militar, mas sim para compartilhar recursos de comunicação entre universidades com o apoio de pesquisas do Pentágono. Eram elas a Universidade da Califórnia em Los Angeles, através de seu centro do desenvolvimento do "software"; o Stanford Research Institute; a Universidade da Califórnia em Santa Bárbara e a Universidade de Utah, todos beneficiários de contratos com a ARPA (KNIGHT, 2014).

Em seguida houve a criação do TPC/IP[3] que viabilizou a arquitetura aberta de comunicações em rede, permitindo assim a interconexão entre rede de computadores onde quer que estejam localizados. Novas pesquisas para o pentágono conseguiram estender o conceito de pacotes de redes para rádio terrestre e satélite, que acabaram sendo interconectadas a ARPANET (KNIGHT, 2014).

Depois de 1980, a Internet começou a se disseminar em um ritmo muito alto; conectando redes locais, microcomputadores e estações de trabalho. Em 1986, a ARPANET foi conectada a uma nova rede acadêmica a National Science Foundation Network - NSFNET, assim desativando a ARPANET em 1990.

Já na Europa, outro grande avanço aconteceu, na Organização Europeia para Pesquisas Nucleares (CERN). Em 1089, Tim Berners-Lee, físico e cientista da computação, propôs o uso de hipertextos de uma forma distribuída, que basicamente seria um conjunto de documentos armazenados em locais distintos interligados entre si por meio de pontos não hierárquicos que estão vinculados uns aos outros (KNIGHT, 2014). Esses então documentos poderiam ser resgatados usando uma plataforma de navegação; o que possibilitaria o uso em massa da internet. Dessa forma Berners-Lee inventou e implementou a internet com o conceito de hipertexto, que hoje conhecemos com *World Wide Web*.

---

[3] Transmission Control Protocol/Internet Protocol.

Outra criação que contribuiu para o que conhecemos como espaço cibernético hoje foi o sistema binário. A codificação das letras do alfabeto em uma sequência de dígitos binários foi devidamente aperfeiçoada pelo filósofo inglês Francis Bacon, em 1605. Segundo Bacon, qualquer "objeto" poderia ser codificado. Após meio século, o filósofo alemão Gottfried Leibniz criou o sistema binário a partir de numerais[4], como conhecemos hoje.

A partir de códigos criados através do sistema binário, os computadores realizam o processamento de dados, sendo que cada numeral, representa um *bit*[5]. Sem eles não seria possível fazer a leitura das informações enviadas.

Após o surgimento das diferentes redes, surgiu um novo tipo de conflito, a "Guerra de Protocolos" (KNIGHT, 2014). Essa disputa surgiu entre o desenvolvimento da comunicação baseada no TCP/IP. Com parcerias internacionais cada vez mais frequentes e com o surgimento de novas políticas industriais e tecnológicas houve a necessidade da criação de uma única linguagem para que todos os envolvidos pudessem interpretar e entender as informações utilizadas.

Assim foi criado o chamado *Hypertext Markup Language* (HTML), um tipo de código básico utilizado para a viabilização da comunicação na Internet. Em 1993, houve um grande avanço tecnológico com a introdução de um dos primeiros navegadores gráficos que possuía uma ampla divulgação chamado de "Mosaic", que foi desenvolvido pelo National Center for supercomputing Applications (NCSA) da Universidade de Illinois nos Estados Unidos. Aquele momento abria a Internet ao público em geral.

Existiu também a formação do *Hypertext Transfer Protocol* (HTTP), o protocolo primordial que estabelece conexões de internet em todo o mundo. Esse aperfeiçoamento também permitiu a origem do primeiro navegador de internet, o *WorldWideWeb* (WWW), em 1990. Embora as grandes inovações tenham acontecido principalmente nos Estados Unidos, cada região do globo apresenta sua própria história de integração e territorialização do espaço cibernético, inclusive no Brasil.

1.2 A Internet no Brasil

[4] Sistema que usa como padrão de comunicação sequências formadas pelos numerais 0 e 1.
[5] Bit é um dado, que pode ser utilizado em conjunto para formar informações.

A Internet foi instalada no Brasil em 1975, durante o Governo de Ernesto Geisel. O então Ministério de Comunicações determinou que a Embratel seria responsável pela implementação e expansão da Rede Nacional de Transmissão de Dados. No início da década de 80, houve um grande interesse no país pela temática telecomunicação e computação. Esse enorme interesse refletiu-se em muitas conferências e programas de pesquisa.

Em 1979, a Agência de Telecomunicações Brasileiras anunciou um projeto para criar a Rede Latina Americana de Computadores (REDLAC). O objetivo era desenvolver pesquisas em comunicação de pacotes, redes locais e interligação de redes (KNIGHT, 2014, p.21). Naquela época, a criação de políticas públicas e incentivo a pesquisa durante o governo militar de Geisel (1975 a 1979) inicialmente foi elaborado pelo II Plano Nacional de Desenvolvimento

Essas políticas industriais procuraram desenvolver a indústria nacional de insumos e componentes eletrônicos. Isso geraria uma autonomia tecnológica assim como uma indústria de equipamentos eletrônicos. No mesmo período, em 1978, com o apoio e condecoração da UNESCO, o *Intergovernmental Bureau for Informatics dos EUA* foi criado por 35 países, incluindo o Brasil. Esse *Bureau* promoveu a Informática nos países em desenvolvimento, incluindo também a criação de uma legislação de fluxos dos dados transfronteiriços (KNIGHT, 2014).

A posição Brasileira foi defendida pelo Tenente Coronel Joubert Brizida, Secretário Executivo da Secretaria Especial de Informática, durante a primeira Conferência Internacional sobre Fluxos de Dados Transfronteiriços que foi realizada em Roma, em junho de 1980. Durante seu discurso o Tenente Coronel falou que "O país que não se preocupa com o controle das informações estratégicas que utiliza corre risco de se tornar intoleravelmente dependente, através das telecomunicações, dos interesses de derivados grupos políticos e econômicos fora de suas fronteiras" (COMSCORE, 2013).

1.3 Uma Teoria sobre o Espaço Cibernético?

A chamada "Teoria Cibernética" foi criada por um matemático estadunidense chamado Norbert Wiener, entre 1943 e 1949. Durante alguns anos Wiener trabalhou no MIT, onde estudou física probabilística e focou no estudo do movimento das partículas elementares em líquido, fenômeno conhecido como movimento browniano. Na segunda guerra, Wiemer trabalhou para o governo norte americano com problemas matemáticos para desenvolver uma arma que seria capaz de atingir alvos móveis, que contribuiria com o desenvolvimento dos sistemas de uma mira automática, que ajudou a criar a Teoria Cibernética[6].

A contribuição de Wiener não foi a constituição de hardware, mas sim a criação de um "recinto" onde computadores e autômatos fossem desenvolvidos. A epistemologia da palavra cibernética que provém do grego significa Timoneiro ou piloto. Em seu estudo Wiener percebeu que para que um computador o funcionasse deveria controlar suas próprias atividades. Um exemplo de sistema de autocontrole utilizado por Wiener é o termostato, que através da temperatura de um lugar específico onde se encontra regula sozinho a temperatura para mais quente ou frio.

A teoria cibernética pode ser vista por muitos como uma "super ciência" ou a ciência das ciências. Ela estimulou o estudo e pesquisas em áreas dos sistemas de controle e sistemas que trabalham com a informação. Um dos pontos de partida gerados pela Teoria da Cibernética nas mais diversas perspectivas do conhecimento é a possibilidade de reduzir todo fenômeno ou processo estudado à noção e ou a sua transmissão. A cibernética levou a alteração do homem em um conjunto crescente de atividades, gerando a autonomia de serviços que antes eram exercidos particularmente pelo homem.

É perceptível que as premissas do estudo da Cibernética possam ser aplicadas em vários campos da vida humana, principalmente quando se trata de comunicação e troca de informações. No que tange às relações internacionais, desde o final do século XX a temática do ciberespaço já se incorporou a agenda de muitos Estados e Organizações Internacionais. Especialmente no que tange à temática da segurança internacional, mediante do que se convencionou chamar de "segurança cibernética".

[6] A Cibernética é o estudo de autocontrole encontrado em sistemas estáveis, sejam eles biológicos, elétricos ou mecânicos. No início a Cibernética focava apenas na criação de máquinas auto reguláveis semelhantes ou comportamento do ser humano.

Parte dessa temática emergente já se refere a alguns Estados, como os Estados Unidos, China e Rússia, sendo verdadeiras potências cibernéticas. Eles se destacam por serem capazes de produzir armas cibernéticas em um contexto de uma guerra cibernética e de defesa cibernética. Isso evidencia o que Nye Jr chama de poder cibernético.

Pelo o fato do campo do ciberespaço ser multidisciplinar, o mesmo reivindica espaço nas demais ciências sociais, como por meio das Relações Internacionais. Na Era da Informação, a informação é poder, o ciberespaço como um novo espaço de interação social é a manifestação para as diversas formas de dominação, tornando-se uma fonte de exercício e difusão de poder. Por este viés, afirma-se que o objeto das Relações Internacionais no espaço cibernético são as próprias relações de poder através da detenção de informações neste ambiente.

A criação da tecnologia digital, da internet e de recursos como a realidade virtual passou a interferir na cognição humana. Da mesma forma, conflitos de interesses seguem também a evolução tecnológica, havendo a necessidade de se criar regulamentos para gerir as relações sociais e políticas no espaço cibernético. Assim, pode-se inferir que a informação que circula são recursos desse território, sendo o usuário o operador deste recurso, não sendo parte constitutiva desse território.

Atualmente, muito se tem falado sobre a equiparação do espaço cibernético a um espaço geográfico, delimitação de fronteira, soberania de Estado, controle governamental e disputa de poderes (PORTELA, 2016). Em meio a tantas colocações, a resposta do que é o espaço cibernético pode ser apontada pela Geografia, mais especificamente pela Geopolítica, conforme Gonzales e Portela (2017).

A relevância do espaço cibernético para o Estado tem uma relação direta com seu poder e soberania, concepções que estão relacionados ao espaço. Sendo o espaço cibernético um tabuleiro de xadrez onde há uma vasta disputa de poderes, que avidamente tem crescido e impactado na geopolítica do mundo, seu domínio é uma ferramenta desejada. Tornando assim, o estudo do espaço cibernético algo extremamente necessário para que se possa entender as relações de poder entre os Estados dentro desse meio, pois o ciberespaço é uma extensão do sistema social e político.

Com o crescimento da importância da questão cibernética para a disciplina das Relações Internacionais, é necessário discutir conceitos essenciais para melhor

compreender os problemas atuais. Nesse campo científico observa-se um movimento de institucionalização sobre tal temática nas principais universidades do mundo, sem se esquecer da crescente quantidade de publicações científicas nesta área (PORTELA, 2016).

Isso deve-se, em grande parte, ao aspecto securitário que envolve este ambiente, a Segurança Cibernética, a ponto da comunidade gnosiológica de RI falar, até mesmo, em termos como, arma cibernética, defesa cibernética, guerra cibernetica, Guerra Fria cibernética, poder cibernético e potências cibernéticas. O descobrimento mais importante, à luz do valorativo de pesquisa, diz respeito à criação e ao reconhecimento do subcampo de Relações Internacionais Cibernéticas (CiberRI) em RI.

Ausência de uma teoria das Relações Internacionais para o espaço cibernético se dá por ser um objeto de estudo relativamente novo em comparação com o estudo das relações internacionais que por exemplo no ano de 2019 completou 100 anos. Além de ser uma disciplina nova, por ser uma temática intensamente técnica para desenvolver-se uma teoria cibernética nas reações internacionais deve-se haver pelo menos um conhecimento básico sobre tecnologia da informação, informática e comunicação digital.

1.4 Espaço cibernético a luz das teorias de Relações Internacionais

O subcampo internacionalista de Relações Internacionais Cibernéticas (CiberRI), que aqui se defende, não paira apenas no mundo das ideias; este subcampo também ganha vida mediante sua aplicação no meio empírico. Em outras palavras, teoria e prática se juntam, à luz de elementos teóricos de Relações Internacionais, conforme explicado por Gills Vilar-Lopes (2017).

Interpretar o poder neste novo domínio, com novas características, à luz das teorias das Relações Internacionais torna-se imprescindível. Dentre as diversas tentativas de entender as dinâmicas das relações internacionais existem três teorias que podem ser aplicadas ao ciberespaço na tentativa de entendê-lo: Neorrealismo, ou Realismo Estrutural; Neo-institucionalismo; e, Construtivismo.

O Realismo Estrutural é uma das teorias mais estudadas e utilizadas na área das Relações Internacionais. Também uma das mais coesas, pois os seus representantes utilizam das mesmas premissas em seus estudos, resguardado algumas variações. Nesta

corrente teórica, o Estado é entendido como o único e/ou principal ator das relações internacionais. Essa teoria foi a primeira a interpretar as relações internacionais como um sistema, considerado pelos teóricos como o terceiro nível de análise.

Segundo Waltz (1979) este sistema internacional é baseado em três pilares: a autoajuda, a anarquia e o dilema de segurança. Com o objetivo de melhor entender e prever os acontecimentos, a teoria em si faz algumas generalizações. A principal delas explica que dentro do ambiente anárquico, onde não há a possibilidade de confiança entre atores, o objetivo máximo dos Estados é sobreviver neste meio e acumular o maior poder possível, resguardando cada vez mais sua sobrevivência, em uma relação correlata.

Ainda sobre essa corrente teórica, seus dois principais autores são Kenneth Waltz, como explanado acima, e John Mearsheimer. Através dos dois é possível perceber dois entendimentos sobre poder que se complementam, sendo que os poderes são as capacidades dos atores dentro do sistema, as quais são atribuídos aos mesmos (WALTZ, 1979). Além disso, o poder pode ser medido através da comparação entres os atores.

De maneira a complementar o pensando de Waltz (1979), Mearsheimer dispõem a ideia de que o poder possui duas dimensões: o poder potencial e o poder real. O poder potencial é baseado na população e o nível de riqueza que o Estado possui. Por sua vez, o poder real baseia-se na capacidade militar, podendo dessa forma ser medido de uma forma mais concreta do que o poder potencial.

A corrente teórica neoliberal, tal qual a Neorrealista compreende o Estado como um ator racional e o principal, mas não o único, nas relações internacionais. Além disso, também compreende o sistema como anárquico. Porém, diferentemente da corrente anterior, foca seus estudos no papel exercido pelas instituições, oficiais e oficiosas, em um sistema internacional, no qual os atores, a partir do século XX, são cada vez mais interdependentes. (STERLING-FOLKER, 2013).

A interdependência entre atores ou Estados no cenário internacional ocorre quando há efeitos de custo recíproco, pois, ela diminui a autonomia de cada ator. Dessa forma, independentemente da decisão, sempre haverá custos e não há garantias de que os benefícios superam os malefícios. Nesse sentido a realidade é percebida através da ideia da interdependência complexa.

Esta teoria possui três características: os canais múltiplos que conectam a sociedade, incluído os atores não estatais; a multiplicidade dos problemas tratados nas agendas das relações interestatais e a não existência de uma hierarquia consistente e clara entre os assuntos; por último, a força militar não é empregada entre estados dentro da interdependência complexa (KEOHANE; NYE JR, 2011). O poder é aqui pensado através da relação com o outro, com a capacidade do ator "A" em fazer com que o ator "B" faça algo que do contrário ele não faria:

Quadro 1.2 – Faces do poder relacional segundo Nye

PRIMEIRA FACE: A usa ameaças ou recompensas para alterar o comportamento de B em relação às preferências iniciais e estratégias. B sabe disso e sente o efeito do poder de A.
SEGUNDA FACE: A controla a agenda de ações de maneira a limitar as escolhas de estratégia de B. B pode ou talvez não saiba disso e esteja ciente do poder de A.
TERCEIRA FACE: A ajuda a criar e moldar as crenças, percepções e preferências básicas de B. Talvez B não esteja ciente ou perceba o efeito do poder de A.

Fonte: NYE JR (2012, p.36)

Além disso, nessa teoria de Nye Jr (2012), o poder é dividido entre *hard power* e *soft power*. O primeiro refere-se à capacidade de impor suas exigências através de meios coercitivos, militares ou econômicos. O segundo refere-se à capacidade de "A" conseguir o que deseja através da atração e não coerção, ou seja, moldar a visão de "B", para que ele também compartilha do mesmo desejo.

A partir deste conceito e para melhor entender seu papel na interdependência, é necessário dividir as relações de poder em duas dimensões: sensibilidade e vulnerabilidade. Isto é, em um mundo da interdependência complexa todos são sensíveis às escolhas do outro. Entretanto, uns são mais vulneráveis devido à falta de alternativa para mudar aquele cenário político.

Por sua vez, a teoria construtivista dentro do campo das Relações Internacionais possui alguns pontos que convergem com outras vertentes dentro do construtivismo. Essas vertentes estudam como os objetos e práticas, especialmente os entendidos como naturais,

foram construídos numa interação agente e estrutura (FEARON; WENDT, 2002) sendo dessa forma que todos retratam o mundo como "*intersubjectively and collectively meaningful structures and processes*"[7] (ADLER, 2013, p. 121).

Assim, as relações internacionais são concebidas como socialmente construídas, permeadas de valores sociais e normas que regulamentam essa relação. Dessa forma, não são apenas resultados da ação de um indivíduo, mas do conjunto de atores que compõe o sistema internacional.

Algumas características do Construtivismo são de importante destaque. A primeira é a atenção especial dada ao papel das ideias na construção da vida social, estas para obterem alguma relevância social necessitam ser transformadas em práticas. A segunda característica é que o construtivismo não toma os agentes ou sujeitos como dados e, portanto, é de seu interesse demonstrar como eles foram construídos (FEARON; WENDT, 2002).

Por entender que o mundo social é construído pelos indivíduos, a concepção de poder para os construtivistas não pode estar focada apenas nas capacidades materiais, pois estas apenas só ganham sentido a partir da socialização dos atores (GUZZINI, 2013).

Percebendo a complexidade que as relações internacionais ganham dentro do cibernético bastante complexos, as teorias abordadas podem ser aplicadas para compreender os "problemas" e efeitos desse ambiente no cenário internacional. De acordo com a teoria neorrealista a concepção de poder é pensada e medida através das capacidades de cada Estado, ou seja, a de exercer o poder através da coação do outro ator.

A dificuldade de se entender o poder cibernético é que ter poder nesse ambiente não necessariamente indica a existência de mais recursos, como por exemplo armas cibernéticas. A teoria apenas considera como principais atores as grandes potências. Havendo, portanto, uma dificuldade dos Neorrealistas em compreenderem o movimento de transferência de poder dentro do meio cibernético, pois se comparado com o mundo físico, o surgimento e a capacidade de ação dos atores estatais ou não-estatais no mundo cibernético é muito maior.

Já na teoria neoliberal entende-se o conceito de poder de uma maneira mais ampla, dividindo o poder em *hard power* e *soft power*, não apenas considerando seus

[7] Estruturas e processos intersubjetivamente e coletivamente significativos [tradução nossa]

aspectos material, mas trazendo para análise as instituições e atores não estatais diferente da teoria realista. Assim, essas características possibilitam entender melhor os efeitos do poder cibernético nas relações internacionais. Por exemplo, através dos conceitos de *hard power* e *soft power* é possível compreender as ações de grupos terroristas, que não ou quase não utilizam o espaço cibernético para ataques diretos, mas sim de maneira efetiva e constante para exercer o *soft power*, principalmente nos processos de convencimento de novos membros para compor o grupo (NYE JR, 2012).

Através da ideia de interdependência complexa, que o espaço cibernético expandiu o grau de interações entre os atores, em suas duas abstrações, sensibilidade e vulnerabilidade. É possível pensar como o poder cibernético aumenta o que é sensível entre os Estados e ao mesmo tempo auxilia a diminuir os aspectos vulneráveis de cada um dos Estados menores perante os maiores. Isso se dá devido ao desenvolvimento de tecnologias próprias e não permanecer refém das mudanças tecnológicas nas grandes potências (MAZIERO, 2018, p. 09).

Por fim, mas não menos importante, a concepção que possui uma maior amplitude pertence a teoria construtivista. A teoria não apenas pensa que a relação de poder entre os agentes é algo relacional, mas algo que decorre da socialização dos atores e de suas identidades. Através dessa teoria é possível entender a questão cibernética nas relações entre os agentes estatais, na criação de instituições e nas organizações que se responsabilizam por esta questão. O Construtivismo também demonstra que o meio cibernético e sua segurança são assuntos de caráter nacional.

Logo, os assuntos cibernéticos podem dentro do construtivismo serem considerados dinâmicos, de ações ofensivas ou defensivas. Se transformando em um novo espaço de poder para o ator estatal, com influência também de atores não estatais. Constata-se dessa forma que a teoria construtivista seja talvez a melhor para analisar esse novo espaço, onde há a interação das dinâmicas de poder no sistema internacional e a influência de atores não-estatais, desde setor privado até a figura do próprio indivíduo.

2 SECURITIZAÇÃO DO ESPAÇO CIBERNÉTICO

Com o enorme aumento em ataques e sequestros cibernéticos no mundo, observou-se um movimento de securitização do tema no mundo, promovendo diversos debates que envolveram países e organizações internacionais. Dentre as diversas, podemos citar Organizações como a Aliança para a Segurança das Nações Unidas e a Prosperidade da América do Norte (ASPAN), a Aliança do Tratado do Atlântico Norte (OTAN), a Organização para Cooperação de Xangai (OCX) e a própria Organização das Nações Unidas.

Essa preocupação veio crescendo de uma forma exponencial principalmente depois dos muitos acontecimentos como a ciberguerra entre a Rússia e a Estônia, em 2007 e o conflito cibernético entre a Rússia e a Geórgia, em 2008. Esses dois casos são uns dos mais conhecidos mundialmente, pois geraram uma grande repercussão mundialmente abrindo uma nova série de debates que até então pouco se falava.

Os ataques cibernéticos da Rússia à Estônia, em 2007, e à Geórgia, em 2008, contribuíram para a inserção do tema de segurança cibernética na agenda internacional (LOBATO & KENKEL, 2015). Ainda, em 2010, outro ataque mobilizou os países, um vírus chamado Stuxnet foi instalado nas instalações nucleares iranianas, tendo como objetivo danificar as centrífugas do programa nuclear iraniano (LOBATO & KENKEL, 2015).

A partir desses eventos muitos países começaram a debater sobre segurança cibernética e a grande necessidade de se desenvolver as estruturas e instituições defesa cibernética.

A fim de evitar futuros ataques muitos países iniciaram abordagens para encontrar soluções sejam elas multilaterais em cooperação, formulando políticas e legislações que protejam as nações e seus indivíduos de ataques cibernéticos.

Joseph Nye Jr (2010) divide os atores do espaço cibernético em três categorias: governos, organizações com redes altamente estruturadas e indivíduos. Destaca também que o baixo custo de se cometer um ataque cibernético é um fator permissivo para que pequenos Estados e atores não estatais tenham um papel significativo nesse ambiente.

Nye Jr (2010) também comenta sobre a dificuldade de afirmar que determinado Estado é dominante no espaço cibernético, como alguns o são no mar ou no ar, pois mesmo aqueles Estados que tenham consideráveis recursos de *soft* e *hard power*, estão lidando com novos atores e com novos desafios inerentes ao espaço cibernético.

Ademais, mesmo que alguns países possuem leis nacionais que tipificam o crime, ainda não há um tratado internacional abrangente que lide com os crimes e criminosos atuantes no espaço cibernético. Trata-se de um entrave a este tipo de punição, pois, na maioria das vezes, os ataques cibernéticos são provenientes de outros Estados, e a inexistência de um tratado desse tipo dificulta a punição aos respectivos criminosos (KRAMER, 2009).

O maior tratado internacional feito acerca do tema foi a Convenção de Budapeste, que foi elaborada em 2001, no âmbito do Conselho da Europa. Dos países da América do Sul, somente a Argentina e o Chile ratificarem este tratado, porém, apesar de não ser tão abrangente, ele reconhece a importância da cooperação internacional na luta contra os crimes cibernéticos (CONVENÇÃO DE BUDAPESTE, 2001).

A importância da segurança do espaço cibernético é embasado na proteção das infraestruturas críticas nacionais, pois um ataque de grandes proporções poderia fazer com que informações detalhadas sobre planos militares acabasse em posse de grupos ou Estados inimigos, debilitando as estratégias do Exército, além de poder causar o bloqueio de dados bancários e interferir na bolsa de valores. Sistemas de transporte e de saúde também poderiam entrar em colapso ao serem violados em um ataque (MIRANDA, 2009).

Cabe ressaltar ainda, que de acordo com Meyer (2016), a maior parte das infraestruturas do espaço cibernético pertencem ao setor privado, fato esse que reitera a importância da cooperação entre esses dois setores.

A segurança cibernética tem como fundamento geral garantir a segurança pública no espaço cibernético, tentado proteger o espaço cibernético contra os ilícitos nacionais e internacionais e evitando que os atores que utilizam este espaço tenham seus dados violados ou disseminados por criminosos que neste espaço atuam. Carvalho (2011) define a segurança cibernética como

> A proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes

> de comunicações e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. Também abrange a interação com órgãos públicos e privados envolvidos no funcionamento das infraestruturas críticas nacionais, especialmente os órgãos da Administração Pública Federal (APF) (CARVALHO, 2011, p. 10).

Já a defesa cibernética está no âmbito das relações entre os Estados, envolvendo o poder cibernético e a guerra cibernética. O Ministério da Defesa do Brasil a define como:

> Conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente. No contexto do preparo e emprego operacional, tais ações caracterizam a Guerra Cibernética (BRASIL, 2010 apud CARVALHO, 2011, p. 18).

Devido às vulnerabilidades inerentes ao espaço cibernético – facilidade e baixo custo de se realizar um ataque cibernético a qualquer um de seus atores; dificuldade de imputar um ataque cibernético; facilidade de realizar um ataque sob garantia de anonimato; falta de regulamentação deste bem comum – e por se tratar de uma ameaça existencial, alguns Estados têm optado pela securitização desse espaço.

Assim sendo, alguns Estados têm buscado lidar com ataques cibernéticos de diversas maneiras, a partir da cooperação internacional, instituições, estabelecimento de políticas, para que, dessa forma, possa ser assegurado o bem-estar dos usuários, a segurança nacional.

2.1 A problemática da segurança multidimensional

O conceito de Segurança Multidimensional foi definitivamente estabelecido na Conferência Especial sobre Segurança realizada na Cidade do México em 2003. Durante a conferência, o conceito de Segurança Multidimensional ajudou a entender como essa nova modalidade de guerra, como a ciberguerra, tem ganhado projeção entre os Estados.

O espaço cibernético é um teatro de guerra caracterizado pela (in)segurança multidimensional, uma vez que a mesma possui tanto um caráter de ameaça tradicional interestatal quanto de nova ameaça. (RAMOS ,2015). Tendo em vista, que com a

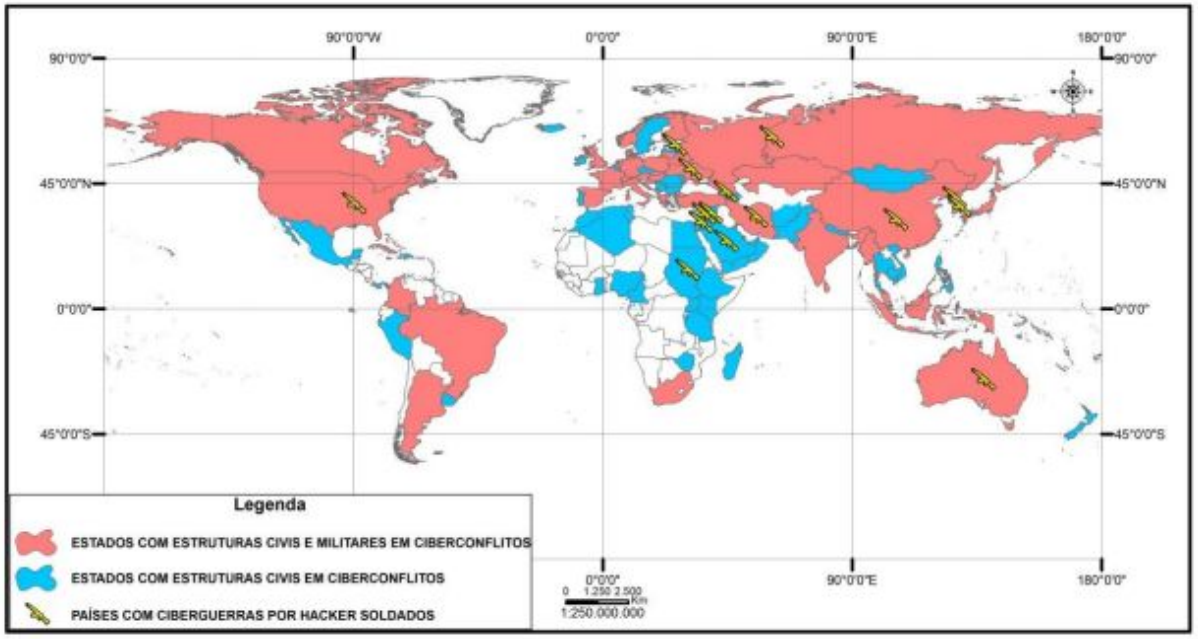
intensificação da globalização, não só os Estados e Organizações Internacionais tornam-se alvos, mas os próprios indivíduos e empresas, a ciberguerra trata-se de uma questão de insegurança do sistema mundial como um todo.

A perspectiva de segurança multidimensional obtém relevância à medida que elucida porque a segurança cibernética antes de ser puramente e exclusivamente de uma ótica internacionalista, passa a ser então visualizada dentro de uma agenda multidimensional, com reverberação em agendas securitárias tênues de natureza civil e militar. (DAVID, 2001).

O grande dilema da segurança é que o mesmo possui multidimensional, trazendo junto a ele uma diversidade de arenas e atores com fronteiras nem sempre convergentes. Percebe-se esse dilema em dois pontos, o primeiro sendo a indefinição de fronteiras dentro do espaço cibernético, separando o nacional do internacional, e o segundo sendo a indefinição de quais estruturas estatais atuariam no espaço cibernético, se seria m as estruturas civis, de segurança pública, ou as estruturas militares, de defesa.

Com base na análise de cyber conflitos, na identificação e categorização de sua natureza e *stakeholders* envolvidos, mostra-se a possibilidade de uma apreensão da espacialização dos campos de poder dos ciber conflitos, de uma forma, a mostrar, tanto as forças descentralizadas dos ataques cibernéticos, quanto as forças centralizadas, dos meios civis e militares, conforme podemos vislumbrar:

Figura 2.1 - Estruturas Civis e Militares da ciberguerra



Fonte: SENHORAS,2014.

A existência de estruturas civis e militares com ações realizadas principalmente por hackers soldados como observado nos Estados Unidos, Rússia, China, Coréia do Sul, Coréia do Norte, Austrália, Estônia, Geórgia, Ucrânia, entre outros países gera ainda mais instabilidade no sistema internacional, pois dessa forma torna-se mais difícil o Estado ter controle sobre os ataques cibernéticos.

2.2 A Governança nas Relações Internacionais

Há um regime de governança da Internet no plano internacional que vem sendo moldado nas quatro últimas décadas. Esse evolui conforme interesses de atores que, em contexto de competição tecnológica global, apresentam um diferencial de poder oriundo do conhecimento de que dispõem sobre novos padrões tecnológicos e de sua capacidade relativa de acompanhar e influir na própria evolução de tais padrões.

Por exemplo, o uso da língua inglesa como o padrão adotado para endereçamento dos sítios eletrônicos em escala global constituiria fator a preservar as vantagens iniciais

dos Estados Unidos como "*first movers*" (CRUZ, 2006, p. 21). Esse tipo de diferencial habilitaria alguns atores a compreender melhor que outros as implicações políticas e econômicas resultantes do regime em formação e, consequentemente, influir na definição das regras e na escolha dos padrões globalmente aplicáveis.

No intuito de delimitar a governança da Internet, faz-se necessário dar atenção ao significado e à extensão do termo governança e aos motivos do seu uso para designar o conjunto de mecanismos relacionados à gestão da Internet no plano global.

James Rosenau (2000) faz distinção entre governança e governo. Afirma que governo sugere um conjunto de atividades sustentadas por autoridade formal e poder de implementar decisões tomadas em determinado contexto político-institucional. Governança, por sua vez, estaria relacionada a atividades apoiadas em objetivos comuns, que podem ou não derivar de responsabilidades formais, porém não dependem do exercício de poder coercitivo para serem aceitas. Nessa perspectiva, o conceito de governança englobaria o de governo, mas a ele não se limitaria, abrangendo também um conjunto de decisões tomadas por atores não governamentais, aceitas e tacitamente seguidas pela maioria.

No contexto da difusão de poder numa economia globalizada, a emergência de novos atores internacionais, tais como empresas transnacionais e entidades não governamentais de atuação global, tenderia a limitar o exercício da soberania estatal. Essa diluição de poder não daria vazão, pelo menos em horizonte previsível, ao surgimento de governo global (STRANGE, 1996, p. 184), tendo em conta a resistência dos Estados nacionais em abrir mão do controle sobre três processos essenciais: o monopólio do uso da força, o poder de coletar tributos e a exclusividade em determinar o que é lícito e o que é criminoso.

A teoria dos regimes oferece instrumental que auxilia a compreender o modo pelo qual a Internet é gerida em escala global. Trata-se de averiguar se os mecanismos existentes para a governança da Internet constituem ou não um regime internacional próprio, tal como entendido pela doutrina. Para responder a essa questão, cabe, inicialmente, delimitar os conceitos de governança da Internet e de regime internacional, para então qualificar o tipo de relação existente entre ambos e os efeitos dela decorrentes.

O Grupo de Trabalho sobre Governança da Internet (GTGI), criado pelo Secretário-Geral das Nações Unidas em cumprimento a mandato a ele atribuído na primeira fase da Cúpula Mundial sobre Sociedade da Informação (CMSI), realizada em Genebra, de 10 a 12 de dezembro de 2003, produziu a seguinte definição para governança da Internet:

> Governança da Internet é o desenvolvimento e aplicação por governos, setor privado e sociedade civil, em seus respectivos papéis, de princípios comuns, normas, regras, processos decisórios e programas que moldam a evolução e o uso da Internet. (CMSI, 2003, p. 79).

A Teoria dos Regimes apresenta diversas acepções para o significado da expressão regime internacional. Robert Keohane (1989, p. 4), expoente da corrente neoliberal das relações internacionais, propõe que "regimes são instituições com regras explícitas, acordadas por governos, relacionadas a um conjunto particular de temas em relações internacionais." (KEOHANE, 1989). Nessa acepção, os Estados seriam o centro de qualquer regime internacional, na medida em que regimes somente poderiam derivar de acordo intergovernamental que os constituísse. A definição exclui a possibilidade de regimes formados espontaneamente, fora dos cânones das relações intergovernamentais, por atores outros que não os Estados.

Tendo em conta a ausência de uma instituição fundada em tratado e constituída com mandato para atuar no conjunto de temas afetos à Internet, não se poderia falar, segundo essa vertente teórica, em regime internacional para a sua governança (LUCERO, 2011)

Ao cotejar essa formulação com a definição de governança da Internet elaborada pelo GTGI e endossada pela CMSI, torna-se aparente que Krasner (1983) ofereceu inspiração para a linguagem empregada naquela construção (LUTERO, 2011, p. 79). Vale notar que na definição desse autor não há qualquer limitação seja ela categórica ou não, quanto à participação de atores não estatais na construção do regime.

A definição de governança da Internet explicita quais seriam os atores do regime, ao mencionar governos, setor privado e sociedade civil, em seus respectivos papéis. A história da internet, o modo em que funciona e a maneira de como seus protocolos

evoluíram, revela ter existido participação de vários segmentos da sociedade, sendo eles indivíduos e grupos de pesquisa, organizações militares, empresas privadas, associações civis, agências estatais reguladoras, entre muitos outros. O fato de que a internet funciona em uma escala global é a confirmação empírica da existência de um mecanismo implícito de coordenação, em torno do qual convergiriam a s expectativas desses diferentes autores. (LUCERO, 2011).

Krasner (1983) não condiciona a existência de regime à presença de organizações formais. Na sua concepção regimes seriam um conjunto de princípios, normas e regras juntamente a processos decisórios, todos eles são expressões usadas na concepção e definição de governança na internet. Ele apresenta a seguintes definições para princípios, normas, regras e processos decisórios:

> Princípios são valores de fato, causação e integridade. Normas são padrões de comportamento definidos em termos de direitos e obrigações. Regras são prescrições ou prescrições específicas para ação. Processos decisórios são práticas vigentes para formular e implementar escolhas coletivas. (KRASNER, 1983, p.02).

A característica da internet de operar em escala global, de modo contínuo e ininterrupto, demonstra que, a despeito das críticas e dificuldades oriundas da interação dos participantes do regime, estes têm acatados suas normas e regras, fazendo com que o regime cumpra com o propósito de manter e operar uma rede interligada em escala global (LUCERO, 2011). Dessa forma pode-se concluir que a governança na internet é operada com base em regimes internacionais efetivo e robusto, no qual estão presentes todos os elementos da definição proposta por Krasner (1983). Tal regime possui um alto grau de complexidade, tamanha é sua efetividade e robustez que nem mesmo uma cúpula mundial foi capaz de alterar substancialmente as bases e pressupostos de seu funcionamento.

2.3 Defesa e estabelecimento da política de segurança da informação no Brasil

No caso do Brasil, com o início da Internet comercial em 1993 (World Wide Web), a interconectividade deixou de ser restrita às redes acadêmicas, ganhando escala e propulsão. Neste contexto, a criação do Comitê Gestor da Internet (CGI.br), em 1995,

ofereceu um espaço favorável não só para o desenvolvimento de políticas e de um diálogo multissetorial referente aos desdobramentos da Internet no país, mas também para a elaboração de novas estruturas pertencentes a essa governança.

As preocupações com os riscos de segurança que emergiram com a rápida expansão da internet comercial e com a necessidade de manter uma infraestrutura resiliente e operacional levaram à criação de dois órgãos dedicados ao assunto: o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) e o Núcleo de Coordenação do Ponto BR (NIC.Br).

O CERT.br foi criado em 1997 a partir de um estudo encomendado pelo CGI.br para o estabelecimento de uma "coordenadoria de segurança de redes". Já o NIC.br foi criado, em 2003, para implementar as decisões do CGI.br e, em 2005, passou a administrar o registro de nomes sob o domínio ".br". (LOBATO, 2018)

Após a criação do Comitê Gestor da Segurança da Informação, em 2000 foi estabelecido um sistema hierárquico de tomada de decisões federais, partindo da Presidência da República, no nível estratégico, e se ramificando até o nível operacional, a exemplo de forças-tarefa dentro da Polícia Federal e do Centro de Defesa Institucional da Presidência da República (GSI-PR) que presta assistência à presidência em temas de defesa e segurança, além de coordenar as atividades de inteligência federal e segurança da informação, por meio da Agência Brasileira de Inteligência (ABIN) (LOBATO, 2018).

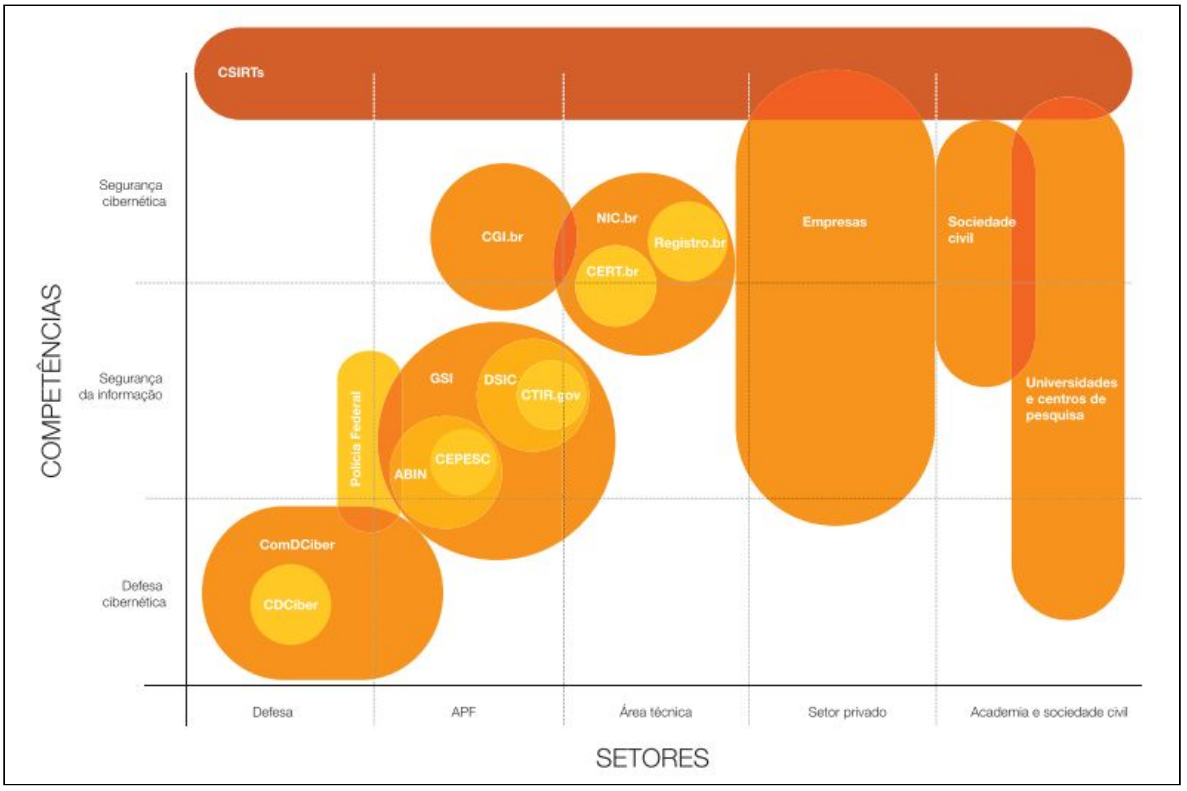
No âmbito do Ministério da Defesa (MD), a Estratégia Nacional de Defesa (END), lançada em 2008 e atualizada em 2012, reconhece o espaço cibernético, ao lado dos setores nuclear e espacial, como um dos três principais setores estratégicos para a defesa e segurança nacionais. A END se destaca como parte de um processo político-estratégico de estruturação e desenvolvimento tecnológico no setor militar com o intuito de promover maior cooperação entre as Forças Armadas, e responsabiliza o Exército pela coordenação e integração de programas relativos ao setor cibernético.

Em 2016, estabeleceu-se o Comando de Defesa Cibernética (ComDCiber), composto por representantes do Exército, da Marinha e da Aeronáutica. O órgão foi encarregado de "planejar, orientar, coordenar e controlar as atividades operativas, doutrinárias, de desenvolvimento e de capacitação no âmbito do Sistema Militar de Defesa Cibernética". Trata-se de um comando operacional conjunto que se insere na estrutura

regimental do Exército Brasileiro, junto ao Estado-Maior Conjunto, chefiado pela Marinha, e o Departamento de Gestão e Estratégia, chefiado pela Aeronáutica.

Nesse sentido, a criação do ComDCiber marca uma maior integração entre as Forças Armadas, além de colocar em evidência um processo de fortalecimento das capacidades do Centro de Defesa Cibernética (CDCiber), conforme previsto na revisão da END, em 2012 e sintetizada a seguir:

Figura 2.2 Estrutura da Governança da Segurança Cibernética no Brasil



Fonte: LOBATO, 2018, p. 09.

Conforme detalhado, a institucionalização da segurança cibernética no país engloba órgãos técnicos, de natureza governamental, que contribuem para o desenvolvimento de políticas, normas e práticas diferentes, porém intrinsecamente relacionadas. A figura 2 retrata o panorama mais geral da estrutura da governança da segurança cibernética no Brasil, tendo em vista a participação desses diferentes setores. Ela nos permite identificar os principais grupos e temas pertencentes a essa estrutura, mostrando também que a segurança cibernética é preocupação compartilhada por uma

vasta gama de atores, e que sua governança deve incluir a ampliação da colaboração entre eles no que tange à formulação de políticas integradas.

2.4 Desafios para a Defesa e Segurança Cibernética

Tanto no mundo, quanto no Brasil, há muitas instituições que lidam com a segurança e defesa cibernética, por esse motivo, a abordagem utilizada por elas, muitas vezes, transpassa a característica técnico-operacional, o que acaba refletindo no nível político e jurídico dos Estados. Essa diversificação criou uma série de desafios e oportunidades para cooperação e coordenação no meio cibernético.

Cabe ressaltar que a segurança cibernético se distingue do conceito de defesa cibernética em alguns países, como o próprio Brasil. O primeiro conceito está associado às mesmas fronteiras da segurança pública tradicional (MEDEIROS FILHO, 2014). Enquanto o segundo termo, conforme Oscar Medeiros Filho (2014) está vinculada às questões de guerra. Assim, conforme esse autor, as delimitações da segurança e defesa cibernética está vinculado com a ameaça que se debate.

Ainda sobre esses dois conceitos, há pelo menos quatro desafios que merecem destaque (LOBATO, 2018): (i) o risco de excessiva securitização e de uma acentuada militarização da segurança cibernética; (ii) o risco de exclusão de atores não-estatais da governança da segurança cibernética, desde a definição de prioridades até a elaboração e implementação de políticas; (iii) a preferência, cada vez maior, por soluções que buscam o bloqueio de aplicações, remoção de conteúdo e criminalização de comportamentos na Internet; e (iv) problemas de coordenação e a transferência de tecnologia.

Os riscos da securitização e militarização é fruto de “megaeventos” no Brasil, a criação de órgãos especializados vinculados às forças armadas evidencia o esforço para lidar questões de segurança cibernética a partir da aplicação das competências de órgãos de aparato militar e de Inteligência do Estado. Esses esforços resultaram em uma maior alocação de recursos para combater ameaças, Terrorismo, Guerra cibernética e a Sabotagem industrial.

A ausência de canais para inclusão de atores não-estatais no processo de elaboração de políticas também resulta de processos de securitização e militarização, que acabam retirando da esfera do debate público determinados assuntos avaliados como estratégicos para o país.

Com isso, o processo de elaboração de políticas sobre o tema se torna mais restrito aos órgãos de segurança e inteligência. O tratamento e resposta a ameaças por meio de uma lógica de securitização, reacende o trade-off normativo entre a segurança e o respeito a liberdades e direitos fundamentais, colocando-os em polos opostos, ao invés de encará-los como princípios que devem caminhar conjuntamente no processo de elaboração de políticas para a segurança cibernética.

Diante desse contexto, representantes da academia e a sociedade civil chamaram a atenção para a importância da inclusão do multissetorial às diretrizes, a estruturação de órgãos pertencentes ao regime nacional de segurança cibernética, e para o processo de elaboração de políticas para o setor. (LOBATO, 2018).

Notou-se, também, uma tendência a responder aos desafios de segurança pelas vias do bloqueio, remoção de conteúdo e criminalização. A aprovação de leis que autoriza o bloqueio de aplicativos e websites, além da tentativa de criminalizar uma série de condutas, crimes autorais e o acesso indevido a computadores e sistemas, foram motivadas pela dificuldade e/ou imparcialidade de acessar dados criptografados de redes sociais e aplicativos de mensagens. Essas categorias de episódios contribuíram para elevar a tensão entre, de um lado, a abordagem com foco na criminalização de condutas e, do outro, aquelas com foco na proteção de direitos e garantias legais na internet.

Os desafios da coordenação são evidentes no âmbito da administração pública brasileira, em virtude da escassez de mecanismos que são efetivos de governança da segurança da informação e comunicação, somando a isso, encontra-se a dificuldade dos atores no meio internacional de “transferir conhecimento e tecnologia” uns para os outros, onde no cenário em que vivemos é algo improvável de se acontecer, pelo simples fato de que esse ato de transferência possa abalar a estratégia e defesa de um país em relação a uma nação “amiga” ou não.

3 INFORMAÇÃO, RECURSO DO PODER DO SÉCULO XXI

No mundo atual existem grandes empresas transnacionais das Tecnologias da Informação e Comunicação que aglomeram grande parte dos recursos do poder cibernético, como dados computacional, inovação. Também administram algoritmos que permitem expandir e manter grandes bases de usuários, que por si só geram continuamente uma imensa quantidade de informações.

Essas informações permitem que se tenha um conhecimento sobre padrões de comportamento e de consumo, essenciais não apenas para o comércio, mas também para o Estado, que buscam obter algum tipo de controle sobre determinada população. Como reiteram os estudiosos Ávila e Pinheiro (2014, p. 85) "O domínio da informação é elemento base da construção de poder na contemporaneidade". Essa gigantesca quantidade de dados é coletada e armazenada a partir de vários dispositivos a que a sociedade está submetida na maior parte do tempo, através de seus dispositivos móveis, TV a cabo e satélite, computadores, consoles de videogame entre muitos outros.

O constante uso dessas ferramentas tecnológicas que estão dispostas no dia-a-dia da maior parte da população gera uma quantidade muito maior de dados, sejam elas fotos, mensagens instantâneas, e-mails, vídeos, serviços de localização, transações financeiras, notícias entre incontáveis outros atos, que facilmente influenciam os mercados de consumo, esse fato influências esses mercados desde os primórdios da web.

Deste modo, os dados coletados revelam o conhecimento da conduta de indivíduos e torna-se um ativo de poder das companhias que obtêm e centralizam todas essas informações. Ao mesmo tempo em que os usuários desfrutam de uma "certa liberdade" online, com uma considerável capacidade de expressão, criação e autonomia, por consequência inevitavelmente acabam entregando toda essa gama de informações às poucas empresas que exercem o domínio sobre esse fluxo de dados. Podemos equivaler esse processo ao que Castells (2011) identificou, como a forma pela qual a liberdade se converteu em *commodity* mediante os serviços de computação em nuvem.

Na contemporaneidade, há um cenário coordenado por grandes corporações que operam globalmente na internet, como a Apple, Amazon, Google, Facebook e Microsoft que se tornaram responsáveis pelo enorme acúmulo dos dados e informações de grande

parte da população mundial. Não se desconsidera nesse caso a situação específica da China na qual sofre enorme censura do governo e o mesmo impõe inúmeras normas para que empresas ocidentais como a Facebook opere no país.

Essas organizações são centrais no ciberespaço e apresentam forte aglomeração dos recursos de poder. A concentração desses recursos, faz com que a capacidade de atrair fundos financeiros aumente exponencialmente gerando novas tecnologias agregando ainda mais dados e ampliando sua base de usuários. São exemplos a compra do Youtube pela Google e a compra do Instagram pelo Facebook.

3.1 Facebook e o caso Cambridge Analytica.

Em 2018, o escândalo de vazamento de dados começou com uma reportagem do jornal americano *The New York Times e The Guardian*, que expuseram o compartilhamento indevido de dados de usuários do Facebook com a empresa de consultoria Cambridge Analytica. Inicialmente, o número era de 50 milhões de usuários. Agora, no ano de 2020 novos dados do próprio Facebook indicam que a quantidade de pessoas afetadas foi ainda maior, até 87 milhões de informações pessoais dos usuários foram parar nas mãos da empresa, indevidamente.

A empresa obteve acesso a essas informações através do lançamento de um aplicativo de teste psicológico. Aqueles usuários do Facebook que participaram do programa acabaram, sem necessariamente saber que estavam entregando informações, à Cambridge Analytica. Não apenas suas informações, mas os dados referentes a todos os amigos do perfil.

As informações foram obtidas a partir do teste de personalidade aparentemente inofensivo, disponibilizado gratuitamente aos usuários da rede social em 2014. Segundo o criador, o pesquisador Aleksandr Kogan, o método de análise aplicado ao teste era capaz de traçar o perfil de qualquer pessoa rapidamente a partir de informações como páginas curtidas e postagens realizadas na plataforma. O escândalo gerou uma onda negativa contra o Facebook sob questionamento pela proliferação de notícias falsas nas eleições americanas de 2016. A empresa entrou na mira de autoridades nos Estados Unidos e no Reino Unido.

O deputado britânico Damian Collins convocou o CEO do Facebook, Mark Zuckerberg, para depor diante de um comitê legislativo. As autoridades trabalharam para conseguir um mandado de busca e apreensão para entrar na sede da Cambridge Analytica e recolher material que ajudassem a elucidar o caso.

A Cambridge Analytica é uma empresa de análise de dados que trabalhou com o time responsável para campanha do republicano Donald Trump nas eleições de 2016, nos Estados Unidos. Na Europa a empresa foi contratada pelo grupo que promovia o Brexit, fenômeno da saída do Reino Unido da União Europeia. A empresa é propriedade do bilionário do mercado financeiro Robert Mercer e era presidida, à época, por Steve Bannon, então principal assessor de Trump.

> A empresa teria comprado acesso a informações pessoais de usuários do Facebook e usado esses dados para criar um sistema que permitiu predizer e influenciar as escolhas dos eleitores nas urnas, criando uma campanha digital hiper segmentada para clientes como Trump, segundo a investigação dos jornais. *The Guardian e The New York Times*. (Revista BBC, 2018, on-line)

A mesma assumiu a culpa perante a corte em 2019, de ter adquirido dados sem a permissão dos usuários, porém alegou que não houve uso indevido dos mesmos. O vazamento de perfis no Facebook teria ocorrido por conta de uma política flexível do Facebook com relação à entrega de informações de perfis a aplicativos de terceiros na rede social. Entre 2007 e 2014, a empresa de Mark Zuckerberg ofereceu livremente dados de usuários a desenvolvedores de apps.

Já no Brasil, a empresa Cambridge Analytica já estaria em negociações com candidatos a governos estaduais e ao senado para as eleições de 2018. A empresa iria operar no país em parceria com a agência brasileira Ponte Estratégia, mas o acordo foi suspenso logo após os artigos publicados no New York Times e no Observer of London.

A suspensão da parceria da Cambridge Analytica no Brasil acontece também em meio a um inquérito instaurado pelo Ministério Público do Distrito Federal para apurar se o Facebook compartilhou dados de usuários brasileiros com a consultoria britânica. Ainda não se sabe se a Cambridge Analytica tem presença no Brasil com outros parceiros além da agência Ponte Estratégia.

Segundo o especialista Renato Opice Blum:

> O Brasil é muito atraente para uso de dados visando marketing, seja pela característica interativa do Brasileiro, ou mesmo porque é um bom mercado. Fake news e dados funcionam muito aqui, pois circula com intensidade e as pessoas acreditam muito. Aqui já tem fake news há duas eleições. No mercado de comunicação, já houve caso envolvendo agências sem tanta preocupação com sigilo, e tivemos de rever como é um assunto que traz responsabilidades para agências e seus funcionários. Os executivos e analistas recebem, afinal, não só bancos de dados, mas também informações sensíveis, contratos específicos, materiais que demandam criptografia. Nos casos de marketing, portanto, a responsabilidade é agravada, pois comunicação lida com estratégias mais arrojadas. (BLUM, 2018, online)

Importante notar aqui, o interesse do setor privado em matéria de governança na Internet, não é uniforme tendo em conta as variedades de modelos de negócios possíveis no meio cibernético e a diversidade dos setores produtivos que dele participam (KURBALIJA,2008). As empresas de gestão de conteúdo como a Google, Yahoo, Facebook, eBay entre outras possuem crescente presença no processo de governança, são empresas cujo o modelo de negócios surgiu e depende exclusivamente da internet, para a qual desenvolvem aplicações de gestão de conteúdos com alto grau de inovação e agregação de valor.

Joseph Nye Jr (2011) chega a afirmar que a Internet está proporcionando a todo tempo consequências nas esferas pública, privada e até mesmo individual, argumentando que os Estados poderão se tornar menos fundamentais na vida das pessoas por causa da Internet e dos novos padrões de comunidade e governança. Acontecimentos como a manipulação de dados do Facebook feito pela empresa de consultoria Cambridge Analytica, em 2016, para beneficiar a campanha de Donald Trump colocam em dúvida a ideia de Nye (2011), pois as dificuldades de regulação, seja estatal ou via algum organismo internacional, facilitou que tal prática ocorresse. Neste sentido, Rafael Ávila e Marta Pinheiro (2014) indicam que há uma relação de interdependência entre as entidades estatais e não-estatais para com o uso da rede mundial de telecomunicações, estando o Estado em uma posição de constante pressão destas tecnologias de informação e comunicação.

3.2 Caso Snowden + Wikileaks

Uma característica importante do espaço cibernético é a maior introdução e a maior delegação de poder de novos atores, devido ao progressivo barateamento dos meios de acesso ao ciberespaço, especialmente nos Estados Unidos e na Europa (CHOUCRI, 2014). Tais atores, que podem ser naturalmente identificados na Internet ou operar de forma anônima, podem influenciar nos níveis de assimetria de poder existentes. É o caso de atores de inferior poder relativo, como cibercriminosos que adentram sistemas computacionais de indivíduos, empresas e órgãos estatais, ou como o surgimento do Wikileaks, organização responsável por uma plataforma de publicação na Internet de documentos sigilosos de grandes empresas e Estados, na tentativa de trazer maior transparência de informações ao público.(MARIANO, 2018).

O caso Snowden ajuda a compreender as relações entre Estado, sociedade e poder cibernético. Em 2013, Edward Snowden, então analista da Agência de Segurança Nacional dos Estados Unidos (NSA), revelou como seu país espionava seus cidadãos e os de outros países, entre eles o Brasil, incluindo chefes de Estado, através da Internet e de escutas telefônicas. Naquele instante o indivíduo anônimo se modifica aceleradamente em um ator internacional em condição do seu entendimento sobre a execução das tecnologias digitais que operava e de sua situação privilegiada em relação ao acesso aos dados e informações sigilosas.

O WikiLeaks é uma organização transnacional sem fins lucrativos, localizada na Suécia, que posta, em sua página on-line, publicações de fontes anônimas, documentos, fotos, informações confidenciais, vazadas de governos ou empresas, sobre assuntos sensíveis ou até confidenciais. A página foi arquitetada com base em vários pacotes de programas (*software*), *Freenet*, *Tor* e *PGP (Pretty Good Privacy)* incluindo a *MediaWiki.*

A página anunciada em dezembro de 2006, governada pelo The Sunshine Press, em meados de novembro de 2007, 1,2 milhão de documentos estavam disponíveis. Seu principal porta-voz e editor é o australiano Julian Assange, ciberativista e jornalista. Em 2010, entretanto, essa organização começou a postar uma série de telegramas sensíveis de natureza secreta na rede.

Parte dessas publicações exaltaram alguns atores, como os Estados Unidos, contra as ações do Wikileaks, pois comprometem as atividades desses países (CASTELLS, 2010). Naquele ano, o Wikileaks passou a ter como objetivo o “combate, pela publicidade, de más

condutas governamentais e não governamentais, de variável gravidade, da hipocrisia a crimes de guerra" (LAFER, 2011).

A publicação de uma enorme quantidade de documentos secretos, revelou a dimensão da negociação entre Estados. Ao demonstrar como os países agiam e pensavam em suas negociações, o Wikileaks utilizou de documentos oficiais. Dessa forma, ele evidenciou atividades legais dos Estados, mas que estavam sendo realizadas sem pudor e respeitos aos demais atores.

No caso de Edward Snowden, por outro lado, as suas revelações demonstraram o lado obscuro das coletas de informações por parte dos Estados centrais. De acordo com Luke Harding (2014), Snowden revelou os acessos clandestinos às informações eletrônicas de outros Estados. As principais revelações dadas por Snowden diz respeito, principalmente, aos países do "Five Eyes Group" e o sistema de vigilância mantido por eles, o ECHELON (HARDIND, 2014).

Além dos acessos a informações não autorizadas, outras características que chamaram a atenção do mundo sobre a espionagem estadunidense e de aliados sobre o mundo era a quantidade de informação monitorada, incluindo de pessoas "inocentes". Gerando, uma forma de protestos ao redor do mundo, pedindo uma maior privacidade na internet, onde os dados e informações ali dispostos, não poderiam ser usados ou vendidos de formas indevidas, seja por empresas e ou estados. Foram apresentadas por mais de 80 instituições e ONGs americanas campanhas para protestar contra o programa de vigilância online.

As organizações, American Civil Liberties Union (ACLU), a fundação World Wide Web, Mozilla, e o Greenpeace colocaram no ar o site *Stopwatching.us* ("Parem de nos vigiar", em tradução livre) e pediram ao Congresso que divulgassem mais elementos sobre o vasto programa de vigilância.

Após o vazamento, o general Keith Alexander, chefe da Agência de Segurança Nacional, apontou que a revelação dos programas de vigilância da inteligência dos EUA causou "dano irreversível" à segurança nacional e ajudou os "inimigos da América". Assim, a implementação de novas medidas de segurança foram anunciadas de segurança para impedir o vazamento de informações.

> O Estado norte-americano, detendo recursos como conhecimento, algoritmos, poder computacional e infraestrutura informacional, lançou-se sobre dois deles que estavam fortemente concentrados nas duas transnacionais de tecnologia, os dados e as bases de usuários. Não ficou claro se essas empresas cooperaram com o Estado ou também foram vítimas dessa interceptação de dados, mas o fato é que esse tipo de coleta realizada por algoritmos também pode favorecer governos, a fim de conhecer melhor seus cidadãos, controlar e influenciar comportamentos, independente do nível de abertura política dos países. (MARIANO, 2018, p. 222).

A noção que se tem de algoritmos é de fácil percepção hoje devido às várias plataformas que podemos acessar diariamente. Basta ver que a Netflix possui um catálogo exposto diferente para cada assinante, pois seu algoritmo de recomendação é personalizado. Esse fenômeno é chamado por alguns autores de "cultura algorítmica": o uso de processos computacionais para classificar, hierarquizar pessoas, objetos, idéias e lugares, além de hábitos de conduta, expressões e pensamentos que aparecem durante o processo (STRIPHAS, 2012).

Toda essa coleta de informações se torna cada vez mais útil e precisa graças aos algoritmos presentes nas plataformas digitais que utilizamos, como o Facebook ou o Instagram. Eles selecionam e organizam as informações, no caso das redes sociais, para criar, por exemplo, a *timeline* (feed de postagens) e todo o conteúdo que cada usuário verá. O ambiente virtual é, portanto, personalizado exclusivamente para cada usuário, com base nos seus gostos, nos seus *likes* (curtidas), nas suas atividades registradas, ver um filme, participar de um evento, etc. Diante dessa tendência, parece normal que se questione quem tem controle sobre esses processos e como esses algoritmos são construídos e para qual finalidade. Questionar e conhecer o funcionamento dos algoritmos, assim como eles se disseminam, é muito importante nos dias atuais, embora alguns setores sejam contrários a divulgar esse tipo de informação, pois os algoritmos em si seriam um tipo de segredo industrial.

3.3 Panorama Internacional da Lei Geral de Proteção de Dados Pessoais - LGPD

Um dos motivos que inspiraram o surgimento e criação de regulamentações sobre a proteção de dados e informações pessoais, foi o grande fluxo de dados digitais

internacionais, viabilizado pelo avanço tecnológico e a globalização. na Europa, após escândalos de espionagem e divulgação de dados de clientes envolvendo Cambridge Analytica e Facebook gerou uma grande discussão que culminou na *General Data Protection Regulation* (GPDR) que regulamenta no âmbito da União Europeia a segurança de dados. Dessa maneira, surgiu uma necessidade de reforçar e resgatar o compromisso das instituições para com os indivíduos, na qual a sociedade digital, na qual a proteção de dados e a garantia de um direito fundamental, como o da privacidade é necessária.

Dessa forma, desde os anos 90, vem sendo debatido em diversos lugares do mundo para uma melhor governança dos dados pessoais. A liderança sobre a temática surgiu na União Europeia, sobre a chefia de um partido intitulado *The Greens*, que consolidou-se na promulgação do Regulamento Geral de Proteção de Dados (GDPR), número 679, aprovado em 27 de abril de 2016, tendo como principal objetivo abordar a proteção da pessoa física no que tange o tratamento de dados pessoais e a livre circulação desses dados (*Free data flow*), o regulamento trouxe um prazo de dois anos para a implementação de penalidades.

Assim, por sua vez, causando uma espécie de "efeito dominó", visando que os demais países e empresas que buscassem manter alguma relação comercial com a UE deveriam também ter uma legislação de igual ou superior nível que a GDPR. Segundo o preâmbulo 2 e 13 do GDPR, os objetivos são: 1) Contribuir para a realização de um espaço de liberdade, segurança, justiça de uma união econômica. 2) Assegurar um nível base de proteção da pessoa física no âmbito da União e evitar que divergências criem obstáculos à livre circulação de dados pessoais no mercado interno. 3) Garantir a segurança jurídica e transparente aos envolvidos no tratamento de dados pessoais. 4) Impor obrigações e iguais responsabilidades aos controladores e processadores que possuem essas informações e assegurem um controle coerente de tratamento de dados. 5) Possibilitar uma cooperação entre as autoridades de controle de diferentes Estados-Membros.

Coloca-se aqui em evidência que a proteção da pessoa física no que tange ao tratamento de dados pessoais é um Direito Fundamental, atestado por inúmeras legislações em diversos países. Na Europa, já se encontrava previsto na Carta dos Direitos Fundamentais da União Europeia e no Tratado que organiza o funcionamento do mesmo; os efeitos da GDPR são principalmente, mas não exclusivamente, políticos, econômicos e

sociais. Apenas trata-se de mais uma regulamentação que surgiu dentro dessa linha de pensamento, em que se busca trazer mecanismos de controle para equilibrar as relações em um cenário digital sem fronteiras. No Brasil, havia uma previsão no Marco Civil da Internet e na Lei do Cadastro Positivo, porém a temática ainda era difusa e sem objetividade. Foi nessa linha, que uma nova legislação foi criada, ou seja, padronizou e normalizou o que seriam os atributos qualitativos de proteção de dados; essa padronização sendo a Lei Nº 13.709/2018, conhecida como a Lei Geral de Proteção de Dados Pessoais - LGDP.

A LGDP está dividida em 10 capítulos, com 65 artigos, bem menor do que a sua referência europeia, que possui 11 capítulos, com 99 artigos; Em análise, a especialista Patricia Peck Pinheiro, doutora em Direito Internacional, relata que: " A versão nacional é mais enxuta e em alguns aspectos deixou margem para a interpretação mais ampla, trazendo alguns pontos de insegurança jurídica por permitir espaço a subjetividade onde deveria ser mais assertiva". Inicialmente, na criação da lei, houve um veto presidencial em relação à criação da Autoridade Nacional de Proteção de Dados Pessoais (ANPD), que logo foi alterada pela MP Nº 869/2018 e pela lei aprovada um ano depois a Lei Nº 13.853/2019; Na época em que estava sendo elaborada, o veto a criação da ANPD, foi bastante discutida pois sem o órgão haveria uma lacuna inicial na estrutura do projeto de implementação da nova regulamentação, além de não permitir que o Brasil fosse reconhecido pela União Europeia, pois um dos requisitos para reconhecimento era a existência de uma autoridade nacional de fiscalização independente, que não apenas prejudicaria a aplicação e fiscalização das medidas propostas, mas criaria um entrave nas relações comerciais entre Brasil e União Europeia.

Por fim, a LGPD regulamenta a forma como serão tratados os dados pessoais no Brasil. As empresas dos setores público e privado deverão alinhar as práticas de coleta, utilização, tratamento e armazenamento dos dados pessoais, evitando que empresas e até o estado fiquem cada vez mais vulneráveis à espionagem ou de ataques de Hackers como evidenciado as divulgações de áudios de empresas e dos principais poderes do Brasil. A lei está prevista a entrar em vigor no próximo ano de 2021, e é notório que se deve discutir sobre a adaptabilidade da tecnologia da informação a LGPD o que acaba trazendo

como consequência uma insegurança jurídica de como se dará a aplicabilidade da lei e que atitudes devem ser tomadas visando o cumprimento da lei.

CONSIDERAÇÕES FINAIS

A internet e o espaço cibernético podem ser apresentado como um fenômeno tecnológico, que embora seja constituída como uma ferramenta pode apresentar atualmente um processo de construção de um regime global da governança da Internet. Essa surgiu nos Estados Unidos, no final dos anos 60, mas atualmente apresenta uma estrutura mais ampla e complexa, que abarca toda a dinâmica social do mundo, e consequentemente também das relações internacionais. A existência de acordos, tratados e estruturas internacionais comprova a existência desse regime global.

A criação dessa ferramenta acompanhou também a evolução política e os movimentos do poder nas relações internacionais. Isso impactou também na forma que a internet passou a ser usada no mundo. Sendo criada dentro de instituições civis de caráter científico, suas engrenagens também foram aplicadas no contexto da segurança internacional, não no sentido estrito, mas na amplitude do que é a disputa de poder no mundo. Assim, ficou patente depois dessa pesquisa, que o espaço cibernético floresceu no contexto das estruturas hegemônicas de poder ao final do século XX.

Apesar disso, o fato de ter nascido em território estadunidense, permite que esse país ainda exerce muita influência sobre a governança global da Internet. Os padrões técnicos e protocolos foram desenvolvidos nos Estados Unidos, o centro do sistema econômico e político do pós-guerra fria. Impuseram-se sobre os demais atores estatais os protocolos e regras para o uso do espaço cibernético no século XX.

Isso foi resultado do processo bem-sucedido de alianças entre as instituições de pesquisas e a área estratégica do Estado norte-americano, que acabou assimilando a importância do desenvolvimento tecnológico como elemento de poder no cenário internacional. Tais alianças encontrariam apoio no interesse comercial de empresas tecnológicas, que eventualmente beneficiaram-se do ambiente inovador para criação e expansão de mercado.

Embora tenha sido notado um movimento em prol do que se chamou de governança global da Internet, não há tratado nem Organizações Internacionais que forneça uma base ou referência institucional definida para o regime de gestão da Internet. Logo, esse regime resulta da ação de governos, do setor privado, da sociedade civil e de

organizações internacionais, de comunidades técnicas e principalmente dos usuários, sempre em um processo de interação ininterrupta que delineia a evolução e o uso da internet em todo o mundo, e que podemos melhor caracterizá-lo usando o termo "governança".

A soma das interações dos mais diversos entes que contribuíram para o nascimento da internet tem contribuído para mantê-la em contínuo funcionamento. A pauta da Governança da Internet, contempla recorte histórico de surgimento e evolução da tecnologia e confirma a existência do mesmo, que tende a afastar-se da concepção clássica multilateral com base em Organizações internacionais integradas por governos/Estados. Afinal, a concentração de poder nesse ambiente, somado com a difusão de poder para atores não estatais, demanda uma configuração distinta de governança, que nesse caso, surgiu de forma natural.

Por mais que não possa ser compreendido como uma estrutura clássica, a governança da Internet pode ser enquadrada dentro de um espectro teórico. Por exemplo, no que se refere a autoridade formal, embora essa seja ausente ou inexistência, há princípios, normas, regras e processos decisórios específicos de um regime clássico, que nesse aspecto se mostra efetivo e vigoroso. Ainda assim, tentativas de criação de instâncias decisórias intergovernamental para o regime no meio cibernético chegaram a ser suscitadas em maior nível político. Entretanto, não houveram alterações substanciais ao modelo vigente nos dias atuais.

Assim, apesar de já considerarmos a existência de uma governança global, o regime internacional para a Internet continua em plena construção. Essa realidade impõe a diplomacia um desafio de adaptação em torno do regime vigente, tanto para identificar, sugerir e avançar pautas e temas de interesse nacional, quanto para influir na evolução institucional desse regime.

A atual fase das relações internacionais é singular não somente por causa das mudanças sistêmicas, provocadas pelo processo de transformação na distribuição do poder mundial, mas principalmente pela aceleração e ampliação da interconectividade das sociedades e entre diferentes sociedades. São estabelecidas um conjunto de novas tecnologias digitais que pendem à universalização o que simultaneamente intensificam,

importantes mudanças no padrão de interação social e, portanto, alterando a forma como as relações de poder são estabelecidas.

Diante disso e do seu caráter tecnológico, que sempre tende a evoluir, espera-se uma constante mudança do espaço cibernético para satisfazer as necessidades das relações internacional. Essas estão sendo marcadas, nos últimos anos, tanto pelo aumento do número de atores com capacidade real de influência a política internacional, inclusive atores não-estatais, quanto pelo aumento de acontecimentos que revelam crises e instabilidades política nos Estados, na diplomacia e nas instituições Internacionais. Fatos como a revelação das informações sigilosas pelo Wikileaks, a vitória de Donald Trump no processo eleitoral norte-americano e o plebiscito britânico que decidiu o Brexit, são exemplos importantes de como a política nacional e internacional tem se modificado, com grau maior ou menor de influência de atores por meio do espaço cibernético.

Ademais, é natural que os países procurem utilizar a tecnologia da internet em favor dos objetivos de desenvolvimento de sua sociedade. O regime brasileiro para a governança da internet, por exemplo, foi construído a partir de experiências com a gestão de recursos com a colaboração dos setores acadêmicos, não governamental e governamental. O Brasil desenvolveu um modelo de gestão aberto com a participação equilibrada de diversos setores, coordenados pelo Comitê-Gestor da Internet. Essa estrutura permitiu que ao Brasil propor legitimidade e substância à sua participação internacional.

Por fim, ao tratar do meio cibernético nas relações internacionais, entende-se que o sistema internacional é instigado pelas transformações provenientes das capacidades cibernéticas dos atores internacionais, sendo uma ameaça potencial à segurança nacional e a ordem internacional tal como a conhecemos.

REFERÊNCIAS BIBLIOGRÁFICAS

ADLER, Emanuel. **Constructivism in International Relations**: Sources, Contributions, and Debates. In: CARLSNAES, Walter; RISSE, Thomas; SIMMONS, Beth A.. Handbook of International Relations. 2. ed. London: Sage Publications Ltd, 2013

AGOSTINELLI, Joice. **A importância da lei geral de proteção de dados pessoais no ambiente online**. Ética Encontro de iniciação científica. ISSN 21. 768498, v. 14, n. 14, 2018

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016] BRASIL.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018, **dispõe sobre a proteção de dados pessoais e altera** a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

BOFF, S. O; BORGES, V. F **A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil**. Revista Sequência, [s. l.], v. 35, n. 68, p. 109-127, 2014.

BUZAN, Barry; HANSEN, Lene. **A evolução dos Estudos de Segurança Internacional.** Tradução: Flávio Lira. São Paulo: Ed. Unesp, 2012.

BUZAN, Barry; WÆVER, Ole. **Regions and powers**: the structure of international security.
Cambridge: Cambridge University Press, 2003.

CASTRO, Thales. **Elementos de política internacional**: redefinições e perspectivas. Curitiba: Juruá Editora, 2005.

COELHO, Amanda Carmen Bezerra Coêlho. **A lei geral de proteção de dados pessoais brasileira como meio de efetivação dos direitos da personalidade**. 2019.

CLARKE, Richard A. **Cyber War**: the next threat to national security and what to do about
it. New York: HarperCollins Publishers, 2012

COMSCORE. **2013 Brazil Digital Future in Focus**. Relatório Anual. Comscore, inc. 2013.

DE CARVALHO, P.S.M. **O Setor Cibernético nas Forças Armadas Brasileiras**. In: Desafios Estratégicos para a Segurança e Defesa Cibernética. 1a. Ed. Brasília: Presidência da República, 2011, pp. 13-34.

FEARON; WENDT, Alexander. **Rationalism v. constructivism**: a skeptical view. In: CARLNAES, W.; RISSE, T. SIMMONS, B. A Handbook of International Relations. London: SAGE Publications, 2002.

GONZALES, Selma Lúcia de M; PORTELA, Lucas Soares. **A Geopolítica do Espaço Cibernético Sul-Americano:** (In) Conformação de Políticas de Segurança e Defesa Cibernética? Revista Austral, v.7, n.14. Rio Grande do Sul: UFRGS, 2018.

GUZZINI, Stefano. **The Concept of Power**: a Constructivist Analysis. Millennium: Journal of International Studies, [s.l.], v. 33, n. 3, p.495-521, jun. 2005.

GUZZINI, Stefano. **Power, Realism and Constructivism**. Abingdon: Routledge, 2013.

HARE, Forrest. **Borders in Cyberspace:** Can Sovereignty Adapt to the Challenges of Cyber
Security? In CZOSSECK, Christian; GEERS, Kenneth. The Virtual Battlefield: Perspectives
on Cyber Warfare. Cryptology and Information Security Series, Vol. 3. Estonia: CCDCOE, 2009.

HAWKING.Stephen. **Buracos Negros, Universos-bebês e Outros Ensaios.** Rio de Janeiro. 1995.

KEOHANE; NYE JR, 2011. **O futuro do poder**. Trad. LOPES, Magda. São Paulo: Benvirá 2012.

KEOHANE, Robert. **International Institutions and State Power**: Essays in International Relations Theory. Boulder: Westview Press, 1989

KNIGHT, Peter T. **A Internet no Brasil**: Origens, Estratégia, Desenvolvimento e Governança. Indiana: AuthorHouse, 2014.

LOBATO, Cruz Luiza. **Uma Estratégia para a Governança da Segurança Cibernética no Brasil**. Série: Segurança Cibernética e Liberdades digitais. Instituto Igarapé. Setembro 2018.

LOPES, Gills Vilar. **Relações Internacionais Cibernéticas (CiberRI):** O Impacto dos Estudos Estratégicos sobre o Ciberespaço nas Relações Internacionais. Congresso Latino Americano de Ciência Política. Montevidéu: Alacip, 2017.

LUCERO, Everton. **Governança da Internet**: aspectos da formação de um regime global. Brasília: FUNAG, 2011.

MAZIERO, Arthur C; PINTO, Danielle J. Ayres. P**oder Cibernético e o espaço Internacional**: uma Perspectiva a partir das Teorias das Relações Internacionais. Segurança Internacional, Estudos Estratégicos e Política de Defesa. (2018)

MEARSHEIMER, John J.. **The Tragedy of Great Power Politics**. New York: W. W, Norton & Company, 2001.

MEDEIROS FILHO, Oscar. **"Em busca de ordem cibernética internacional**". In Segurança e Defesa Cibernética: da fronteira física aos muros virtuais, organized by Oscar Medeiros Filho, Walfredo B. Ferreira Neto and Selma Lúcia de Moura Gonzalez. Coleção I - Defesa e Fronteiras Cibernéticas Pernambuco: Editora UFPE, 2014.

NYE JR, Joseph S. **O futuro do poder**. São Paulo: Benvirá, 2012.

PINHEIRO. Patricia Peck. **Proteção dos Dados Pessoais: Comentários à Lei Nº 13.709/2018 (LGPD).** ed. 2. São Paulo. Saraiva educação. 2020.

PORTELA, Lucas Soares. **Agenda de Pesquisa sobre o Espaço Cibernético nas Relações Internacionais**. Revista Brasileira de Estudos de Defesa, v. 3, nº 1. Santa Catarina: ABED, 2016

RAFFESTIN, Claude. **Por uma Geografia do Poder**. Paris: Ed. Ática, 1993.

SENHORAS, E. M. **Mapas de ciber conflitos no mundo:** relatório de pesquisa organizado para Congresso Acadêmico de Defesa Nacional. Boa Vista: UFRR, 2014.

STERLING-FOLKER, **Making Sense of International Relations Theory**, Second edition. 2013.

UNODC. **The use of the Internet for terrorist purposes**. New York: United Nations, 2012.

WALTZ, Kenneth N. **Foreword: thoughts about assaying theories**. In: ELMAN, Colin; ELMAN, Miriam F. (Ed.). Progress in International Relations Theory: appraising the field. Cambridge, MA: MIT Press, 2003.

_____. **Teoria das Relações Internacionais**. Tradução de: Maria Luísa F. Gayo. Lisboa: Gradiva, 2002.

WALTZ, Kenneth N.. **Theory of International Politic**s. Reading: Addison-wesley Publishing Company, 1979.

ZANATTA, R. **A Proteção de Dados entre Leis, Códigos e Programação: os limites do Marco Civil da Internet.** Em: De Lucca, N., Simão Filho, A., Lima, C. Direito e Internet III: Marco Civil da Internet. São Paulo: Quartier Latin, p. 447-470, 2015.