UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
UNIVERSIDADE ESTADUAL DE CAMPINAS
PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

PROGRAMA DE PÓS-GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS
SANTIAGO DANTAS – UNESP, UNICAMP E PUC-SP

CAMILA GOMES DE ASSIS

A política de segurança cibernética norte-americana: estado e empresas de tecnologia na sociedade do Big data

São Paulo
2020

CAMILA GOMES DE ASSIS

A política de segurança cibernética norte-americana: estado e empresas de tecnologia na sociedade do Big data

Dissertação apresentada ao Programa de Pós-graduação em Relações Internacionais San Tiago Dantas da Universidade Estadual Paulista "Júlio de Mesquita Filho" (Unesp), da Universidade Estadual de Campinas (Unicamp) e da Pontifícia Universidade Católica de São Paulo (PUC-SP), como exigência para obtenção do título de Mestre em Relações Internacionais, na área de concentração "Paz, Defesa e Segurança Internacional".
Orientador: Tullo Vigevani
Co-orientador: Laís Forti Thomaz

São Paulo
2020

Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Políticas Públicas e Relações Internacionais – Biblioteca
Graziela Helena Jackyman de Oliveira – CRB 8/8635

Assis, Camila Gomes de.
A848 A política de segurança cibernética norte-americana : estado e empresas de tecnologia na sociedade do Big data / Camila Gomes de Assis. – São Paulo, 2020.
91 f. : il. ; 30 cm.

Orientador: Tullo Vigevani.
Co-orientadora: Laís Forti Thomaz.

Dissertação (Mestrado em Relações Internacionais) – UNESP/UNICAMP/PUC-SP, Programa de Pós-Graduação em Relações Internacionais San Tiago Dantas, São Paulo, 2020.

1. Tecnologia e relações internacionais. 2. Ciberespaço – Aspectos políticos. 2. Internet – Aspectos políticos – Estados Unidos. I. Título.

CDD 327.10285

CAMILA GOMES DE ASSIS

A política de segurança cibernética norte-americana: estado e empresas de tecnologia na sociedade do Big data

Dissertação apresentada ao Programa de Pós-graduação em Relações Internacionais San Tiago Dantas da Universidade Estadual Paulista "Júlio de Mesquita Filho" (Unesp), da Universidade Estadual de Campinas (Unicamp) e da Pontifícia Universidade Católica de São Paulo (PUC-SP), como exigência para obtenção do título de Mestre em Relações Internacionais, na área de concentração "Paz, Defesa e Segurança Internacional".
Orientador: Tullo Vigevani
Co-orientador: Laís Forti Thomaz

BANCA EXAMINADORA

_____

Prof. Dr. Tullo Vigevani (Universidade Estadual Paulista "Júlio de Mesquita Filho")

_____

Prof. Dr. Samuel Alves Soares (Universidade Estadual Paulista "Júlio de Mesquita Filho")

_____

Prof. Dr. Alcides Eduardo dos Reis Peron (Universidade de São Paulo)

São Paulo, 07 de fevereiro de 2020.

A Carminha, minha amada avó *[in memoriam]*.

AGRADECIMENTOS

Aos meus pais, Maria e Wladimir, que com amor sempre acreditaram em mim e em minhas escolhas, nunca medindo esforços para me ajudar a atingir meus objetivos.

Aos meus avós, Almerindo e Carminha, pelo exemplo de força e sabedoria. Faço um agradecimento especial a minha avó, Carminha da Silva Gomes, que sempre destacou a relevância dos estudos e da necessidade de aprendizado. Hoje sinto dolorosamente sua falta e gostaria de lhe dizer pessoalmente, muito obrigada.

Ao meu orientador, professor Tullo Vigevani, pelos valiosos conselhos acadêmicos, pela sua compreensão e suporte durante toda a trajetória deste mestrado.

A minha co-orientadora Laís Forti Thomaz pela sua constante prestatividade e compreensão.

A Karina Gomes de Assis, minha irmã, amiga e primeira professora. Com você aprendi as primeiras letras, o pensamento crítico e a vontade de aprender. Obrigada por seguir ao meu lado em cada passo que dou em direção ao meu amadurecimento.

Ao professor Carlos Gustavo Poggio pela sua valiosa contribuição em minha qualificação.

Aos professores Alcides Eduardo dos Reis Peron, a quem agradeço também pela participação em minha qualificação com sugestões e correções profícuas, e Samuel Alves Soares que prontamente aceitaram participar das bancas de defesa desta dissertação. Aproveito para reiterar ao Professor Samuel meu especial agradecimento pela sua participação em minha trajetória acadêmica sendo um exemplo de comprometimento e conhecimento no trabalho que exerce.

À professora Suzeley Kalil Mathias com quem iniciei minha carreira acadêmica e com quem sempre pude contar nessa trajetória.

Ao professor Gills Vilar Lopes grande pesquisador da área e que gentilmente se dispôs a ler o esboço mais inicial deste trabalho e fazer suas considerações.

Aos meus colegas, pelas excelentes trocas.

Ao Marcel, meu companheiro, com quem partilho todas as vitórias e derrotas. Obrigada pela sua existência em minha vida, a tornando uma experiência única, mais repleta de sabedoria e alegria.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

RESUMO

Nesta dissertação analisamos a institucionalização de políticas de segurança cibernética baseadas na prática de compartilhamento de dados entre setor público e privado nos Estados Unidos. Abordamos como a interação entre atores público e privados durante o processo de formulação dessas políticas incorpora dois propósitos distintos. Primeiro, a manutenção de uma lógica de mercado baseada na vigilância e dominada pelo monopólio norte-americano no setor das tecnologias da informação e comunicação, representados pelos grandes monopólios provedores de serviço de internet e *Big Techs*, com especial destaque para o intitulado GAFA (Google, Apple, Facebook e Amazon). Segundo, pelo interesse do governo norte-americano em se utilizar do setor privado - e da legitimidade que este possui em captar dados pessoais -, para reordenar suas políticas de inteligência e torná-las mais eficientes para atender aos objetivos de segurança nacional na sociedade do Big Data. Enquanto estudo exploratório essa pesquisa procura compreender a relação entre os interesses do setor público norte-americano e de atores privados na promoção de uma sociedade de vigilância. Posicionamento que reverbera na política de poder norte-americana, gerando impacto internacional.

Palavras-chave: Segurança Cibernética. Big Tech. Big Data. Setor Público. Setor Privado. Vigilância. Internet. Compartilhamento de Dados. Estados Unidos.

.

ABSTRACT

This dissertation analyzes the institutionalization of cybersecurity policies based on the practice of data sharing between the public and private sectors in the United States. We examine how the interaction between public and private actors during the process of formulating these policies incorporates two distinct purposes. First, the maintenance of market logic based on surveillance and dominated by the American monopoly in the sector of information and communication technologies, represented by the large monopolies on Internet service providers and Big Techs, with special emphasis on the so-called GAFA (Google, Apple, Facebook and Amazon). Secondly, according to the interest of the American government in using the private sector - and the legitimacy that it has in capturing personal data -, to reorder its intelligence policies and make them more efficient to meet national security objectives in society of Big Data. As an exploratory study, this research seeks to understand the relationship between the interests of the North American public sector and private actors in promoting a surveillance society. Positioning that reverberates in the North American power policy, generating international impact.

Keywords: Cybersecurity. Big Tech, Big Data. Data Sharing. Internet. Public Sector. Private Sector. Surveillance. United States.

RESUMEN

Esta disertación analiza la institucionalización de las políticas de ciberseguridad basadas en la práctica del intercambio de datos entre los sectores público y privado en los Estados Unidos. Examinamos cómo la interacción entre actores públicos y privados durante el proceso de formulación de estas políticas incorpora dos propósitos distintos. Primero, el mantenimiento de la lógica de mercado basada en la vigilancia y dominada por el monopolio estadounidense en el sector de las tecnologías de la información y la comunicación, representada por los grandes monopolios de los proveedores de servicios de Internet y Big Techs, con especial énfasis en el llamado GAFA (Google, Apple, Facebook y Amazon). En segundo lugar, de acuerdo con el interés del gobierno estadounidense en utilizar el sector privado, y la legitimidad que tiene para capturar datos personales, para reordenar sus políticas de inteligencia y hacerlas más eficientes para cumplir con los objetivos de seguridad nacional en la sociedad de Big Data. Como estudio exploratorio, esta investigación busca comprender la relación entre los intereses del sector público norteamericano y los actores privados en la promoción de una sociedad de vigilancia. Posicionamiento que repercute en la política del poder norteamericano, generando impacto internacional.

Palabras clave: Ciberseguridad. Big Tech, Big Data. Sector público. Sector privado. Vigilancia. Internet. Compartir datos.

SUMÁRIO

1 INTRODUÇÃO

Nesta dissertação analisamos a institucionalização de políticas de segurança cibernética baseadas na prática de compartilhamento de dados entre setor público e privado nos Estados Unidos. Abordamos como a interação entre atores públicos e privados durante o processo de formulação dessas políticas incorpora dois propósitos distintos. Primeiro, a manutenção de uma lógica de mercado baseada na vigilância e dominada pelo monopólio norte-americano no setor das tecnologias da informação e comunicações, representado pelo intitulado GAFA (Google, Apple, Facebook e Amazon). E, segundo, o interesse do governo norte-americano em se utilizar do setor privado - e da legitimidade que este possui em captar dados pessoais para reordenar suas políticas de inteligência e torná-las mais eficientes, atendendo os objetivos de segurança nacional na sociedade do Big Data. Enquanto estudo exploratório procuramos compreender a relação entre os interesses do setor público norte-americano e de atores privados em promover uma sociedade de vigilância. Posicionamento que reverbera na política de poder norte-americana, gerando impacto internacional.

O surgimento de tecnologias digitais transformou a Internet em um elemento central para política global. Neste novo cenário, o ambiente digital e os dados que nele circulam passaram a ser compreendidos como aspecto central ao poder político e econômico de atores públicos e privados. Isso porque Estados, bem como os mercados, passaram a identificar na captação massiva de dados um elemento chave para o seu desenvolvimento e progresso, o que acaba por transformar a lógica de poder que opera no sistema internacional (POWERS; JABLONSKI, 2015; WEST, 2017).

Observa-se, portanto, que o ritmo acelerado das mudanças tecnológicas e a maneira como as sociedades respondem ao mundo digital afeta os interesses de atores estatais e não estatais. A vigilância, enquanto prática, precede a criação da Internet, contudo nas últimas décadas, graças à consolidação desta inovação disruptiva, a vigilância se expandiu e se aprofundou enormemente, passando a ser conduzida com uma intensidade sem precedentes e em níveis até então nunca vistos (BALL; WEBSTER, 2003;LYON, 2007).

Os atentados de 11 de setembro de 2001 aprofundaram o processo de securitização em torno da *"guerra ao terror"* nos Estados Unido, aumentando o poder de ação repressiva do Estado e da utilização de meios excepcionais para a promoção da segurança (MOTTA, 2014). Esse episódio foi responsável por alinhar atores, organizações, debates e pontos de vista em diferentes áreas da vida pública, seja no campo político, econômico ou acadêmico, em direção à aceitação da vigilância como prática legítima à promoção da segurança nacional.

Neste contexto, os governos passaram a reivindicar o direito de monitorar as atividades de seus cidadãos e de cidadãos estrangeiros em ambiente *online*, respaldados pelo discurso de garantia da aplicação da lei e da proteção à segurança nacional, baseados em uma estratégia de previsão e predição pautada, dentre outros fatores, no acúmulo massivo de informações com o objetivo de produzir inteligência para se adiantar a ataques terroristas.

Tinha início nos Estados Unidos o que autores como Elliot Cohen (2010) definem como uma cultura de controle baseada na lógica de vigilância e na ideia de que a preservação da segurança demanda, em certo nível, abrir mão de liberdades civis, como por exemplo o direito à privacidade. Desde o início da administração Bush em 2001, o Estado de direito foi severamente comprometido pela aprovação de leis que flexibilizavam direitos civis em nome da segurança nacional. A legislação mais emblemática deste período é o Ato Patriótico (*Patriot Act*) que institucionalizava uma vigilância em massa e sem mandado das comunicações eletrônicas de americanos e estrangeiros sem a necessidade de supervisão judicial (COHEN, 2010; LYON, 2007). Essa legislação abria precedente para que a vigilância atingisse não apenas a rotina daqueles que se apresentam como uma ameaça em potencial ao Estado, mas a todos, pois, a estratégia de predição e antecipação repousava sobre uma capacidade de vigilância massiva.

Essa lógica baseada no controle e na obtenção crescente de informações não demoraria a ter efeito na instituição de uma nova forma de mercado, especializado em extrair e comercializar informações pessoais e previsões sobre comportamentos. Nas palavras da autora Shoshana Zuboff (2019), os ataques terroristas de 11 de setembro empurraram a comunidade de inteligência para uma curva de demanda desconhecida, baseada em um requerimento massivo de informações que não era capaz de ser atendido pelas estruturas tecnológicas em posse do governo. Segundo a autora, no final do ano de 2001, a comunidade de inteligência, liderada, sobretudo, pela *Central Intelligence Agency* (CIA) e pela *National Security Agency* (NSA), entoando o lema de "domínio sobre a informação", mobilizou centenas de bilhões de dólares que seriam aplicados no setor privado para patrocinar tecnologias especializadas na captação, armazenamento e processamento de dados. Este contexto foi favorável ao surgimento do que seria descrito pela autora Shoshana Zuboff (2019) como capitalismo de vigilância, um novo gênero de capitalismo centrado na monetização de dados pessoais adquiridos por vigilância. Esse conceito e termos correlatos como capitalismo "dadocêntrico", descrevem a nova lógica econômica em ascensão baseada não apenas na comercialização de dados, mas na rentabilização de tecnologias capazes de aprimorar a sua capacidade de coleta, armazenamento e processamento tornando-se evidente a intersecção entre o capital e o Estado neoliberal para

promover uma crescente sociedade de vigilância em ambiente digital (BALL; SNIDER, 2013; WEST, 2017; ZUBOFF, 2019).

O segundo capítulo, intitulado "*A sociedade do Big Data e as transformações estruturais no valor da informação*", aborda as implicações da mudança tecnológica para a sociedade na era do Big Data. Avalia-se como atores públicos e privados reformularam seus interesses e sua lógica de poder diante do surgimento de uma sociedade marcada pela permeabilidade do ambiente digital em todas as esferas da vida cotidiana. Pondera-se que tanto a lógica estratégica dos Estados como a lógica do mundo dos negócios têm crescentemente se apoiado no caráter preditivo e prescritivo do mundo digital convergindo a mesma lógica vigilância.

A evolução desse mercado acabou por conectar intimamente a vigilância estatal ao poder das grandes empresas digitais. Se havia dúvidas sobre essa dependência, os vazamentos promovidos pelo ex-funcionário da NSA, Edward Snowden, em 2013, sobre um esquema de vigilância interno e internacional praticados pela agência de inteligência norte-americana findaram com qualquer ceticismo sobre essa prática. Documentos disponibilizados por Snowden e divulgados no jornal *The Washington Post*[1] expuseram que a maior agência de inteligência do mundo pegava carona nas redes, ferramentas e técnicas de empresas provedoras de serviços de internet como a Verizon[2], ou grandes *Big Techs* como Google, Facebook, Apple, dentre outros. Tais revelações demonstraram uma convergência, entendida aqui como intencional, entre as prioridades militares e corporativas dos Estados Unidos em desenvolver tecnologias responsáveis por moldar e vigiar nosso cotidiano.

A intersecção entre o campo dos negócios, o Estado e atores militares no desenvolvimento e governança da Internet compõe na estrutura norte-americana um "complexo industrial informacional" (BALL; SNIDER, 2013; POWERS; JABLONSKI, 2015; ZUBOFF, 2019), que em uma referência ao conceito cunhado pelo presidente Eisenhower em 1961[3], deseja descrever a intersecção dos interesses públicos e privados em ampliar a sensação de insegurança

---

1 Cf. Gellman e Soltani (2013).

2 A Verizon Communications Inc. é uma holding estadunidense especializada em telecomunicações.

3 Cunhado pelo ex-presidente norte americano, Dwight D. Eisenhower em seu discurso de despedida da presidência dos Estados Unidos, o conceito de complexo industrial militar descreve o relacionamento político instituído entre as forças armadas do governo nacional e a industrial a fim de obter para o setor privado a aprovação política para pesquisa, desenvolvimento e produção de tecnologia de característica militar, ao mesmo tempo em que alimentava a máquina de guerra norte-americana. A colaboração e interseção dos interesses entre governo, militares e empresários na manutenção de um estado de guerra permanente permitia aos Estados Unidos alimentar a indústria bélica, lucrando com o discurso de promoção à segurança nacional. Na sociedade do Big Data essa lógica seria replicada de maneira que o relacionamento político entre esses mesmo atores se estabeleceria com o proposito de obter a mesma categoria de validação ao setor privado só que neste caso para realizar de pesquisa, desenvolvimento e produção de tecnologia voltada à vigilância, preservando a lucrativa lógica do capitalismo "dadocêntrico", ao mesmo tempo em que alimenta a máquina de inteligência estadunidense.

relacionado ao ambiente cibernético e, portanto, a necessidade de intensificar a vigilância em ambiente digital, validando essa atividade mediante ações legais e incentivo ao desenvolvimento de pesquisas e do mercado especializado na captação de dados (BALL; SNIDER, 2013; MCCHESNEY, 2013). Uma variedade de outros autores empregam conceitos correlatos para descrever esta mesma lógica. Complexo militar digital (MCCHESNEY, 2013), complexo de vigilância governamental corporativo (EDWARDS, 2014), complexo industrial da Internet (FLYVERBON; DEIBERT; MATTEN, 2017) e rede de informações industrial militar (COHEN, 2010) são exemplos de outras denominações utilizadas para se referir à esta mesma lógica.

No terceiro capítulo, intitulado "*Histórias Cruzadas: como Estado e empresas norte-americanas construíram a sociedade do Big Data*", abordamos, mediante análise histórica, como as políticas governamentais norte-americanas se interseccionaram aos interesses do setor privado para conformar o que hoje definimos como sociedade do Big Data. Traçando uma linha que vai desde a criação da Internet até a administração Bush (2001-2008), debatemos como o domínio do setor privado sobre a infraestrutura da internet e dos dados que nela circulam ocorreu com apoio governamental. O estudo realizado permitiu levantar importantes variáveis durante esse processo como, por exemplo, o relevante papel desempenhado pelas agências de inteligência como grandes investidoras de capital de risco em pesquisas dedicadas a ampliar a capacidade do governo norte-americano em coletar, armazenar e processar dados, incorrendo no surgimento de uma nova categoria de empresas, *Big Techs*, e uma nova lógica de mercado, o capitalismo de vigilância, instituindo o que seria descrito como um complexo industrial informacional ou complexo industrial de vigilância nos Estados Unidos. Além disso, o capítulo aborda como as transformações ocorridas no pós 11 de setembro de 2001, período em que o discurso securitizador em torno da *"guerra ao terror"* flexibilizou a privacidade em nome da segurança nacional, permitiu que um arcabouço legal em torno da vigilância fosse instituído, incentivando, por sua vez, um aumento nos investimentos em tecnologias capazes de recolher informações em massa fossem amplamente financiadas. O capítulo encerra com pequenas considerações sobre como o alinhamento entre setor público e privado na política interna norte-americana para a instituição de uma lógica de vigilância se associou à uma política externa que possibilitou ao país dominar a infraestrutura global da Internet. A instituição do que seria descrito por McChesney (2013) como cartel global da internet fazendo com que regulamentos e decisões judiciais tomadas a nível nacional tenham efeitos extraterritoriais.

As disputas internacionais neste campo temático reverberam, não apenas na tentativa dos demais Estados Nação em alavancarem seu mercado nacional em tecnologia digital, mas também na instituição por parte desses países de legislações que busquem restringir a capacidade de

empresas norte-americanas em captar informações em seu território. O exemplo mais notório dessa política foi a instituição do novo Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia, criada em 2016, revogando a obsoleta Diretiva de Proteção de Dados Pessoais de 1995. Esse novo regulamento estabelecia cláusulas e exigências relativas à forma como são tratadas as informações pessoais na União Europeia, determinando que aqueles responsáveis pelo tratamento dos dados pessoais devem declarar qualquer recolha de dados, bem como a finalidade do processamento de dados que venham a realizar, quanto tempo os dados permanecerão armazenados em seus bancos de dados e se esses dados foram compartilhados com terceiros fora da União Europeia (UNIAO EUROPEIA, 2016). Esse regulamento é aplicável a todas as empresas que operam no Espaço Econômico Europeu, independente do seu país de origem, se estendendo, naturalmente, às empresas norte-americanas.

A guerra comercial e tecnológica que hoje se estabelece em torno do mercado digital, além de vinculada a um desejo de ampliar o poder econômico dos Estados também está ligada aos princípios estratégicos de sua política de poder (REARDON, 2019; IGNATIUS, 2019). A busca pela nacionalização dos serviços de internet, portanto, conduziria a um processo de balcanização da internet, ou seja a fragmentação de um sistema de rede unitário e sua transformação em enclaves separados, o que, em uma perspectiva geral, prejudicaria os interesses dos grandes monopólios do setor de tecnologias de informação e comunicação, em sua totalidade norte-americanos, que diante dessa realidade se veriam compelidos a dividir uma fatia de mercado.

Preservar sua soberania no cenário político atual perpassa, portanto, a necessidade de garantir seus ativos digitais nacionais, sendo parte da estratégia de poder de grandes Estados incentivar o desenvolvimento de empresas provedoras de serviços de internet e *Big Tech*s nacionais, em uma tentativa de refrear o domínio norte-americano sobre essas infraestruturas. Para o governo norte-americano, por sua vez, manter seu poder no cenário internacional significa manter sua primazia nesse mercado. A arquitetura da Internet foi moldada conforme o interesse do governo norte americano, responsável por impor às demais nações um padrão de governança da internet, uma ideologia de rede e um monopólio de empresas de internet responsáveis por operarem essa infraestrutura (MCCHESNEY, 2013). A hegemonia norte-americana neste mercado concedeu ao país vantagens, pois além de fortalecer seu poder material, permitiu ao governo estadunidense deter as principais empresas relacionadas ao mercado da internet sob sua jurisdição, obtendo acesso à maior variedade de dados em circulação em todo mundo, um dos principais recursos de poder da geopolítica contemporânea.

Assim, diante dessas considerações, não podemos deixar de entender o ciberespaço como uma arena geopolítica onde os Estados competem entre si, mas que também estão sendo

desafiados pelo setor privado. O espaço cibernético [4] além de caracterizar-se como um novo domínio onde a guerra pode ser operacionalizada, também se apresenta como uma nova fonte de inteligência para o Estado além de comportar-se como um espaço fundamental à interação social e ao desenvolvimento econômico. Os interesses circunscritos nesse domínio são múltiplos fator que reverbera inclusive quando avaliamos as políticas de poder e de segurança voltadas ao ambiente digital.

Como destaca Germano (2014) a natureza híbrida do ciberespaço responsável por interseccionar os ambientes político, civil e militar, a partir de uma mesma estrutura tecnológica, gera uma dificuldade em institucionalizar políticas, inclusive de segurança, visto que qualquer ação empreendida dentro dessa esfera acaba tendo efeitos no campo dos negócios, no campo estratégico e social, adentrando a área de interesses de atores públicos e privados. Mesmo quando esses atores parecem se alimentar de uma mesma lógica, que no caso da sociedade do Big Data parece ser definida pela captação massiva de dados, eles podem divergir opiniões em como melhor regulamentar este domínio (GERMANO, 2014). Hodiernamente, uma das discussões centrais em torno do ambiente cibernético está na definição do equilíbrio entre privacidade e segurança.

Portanto, a disputa assídua pela primazia em estabelecer normas e padrões de governança na internet, com o objetivo de preservar sua capacidade de adquirir a maior quantidade de dados possíveis, tem sido elemento de disputa não somente entre atores estatais, mas também entre atores públicos e privados. Esses atores privados possuem interesses específicos estritamente vinculados à manutenção da lógica econômica que operam, orientados pelo objetivo central de proteger e alavancar seus lucros. Seus interesses específicos podem convergir ou distanciar-se do posicionamento do governo.

Em decorrência do poder que acumulam, uma vez que são os principais detentores das infraestruturas críticas e dos dados, essas empresas adquirem um novo *status* de poder econômico, político e social, pois se transformaram em atores centrais para a aplicação da lei e da segurança nacional, sendo categorizadas por Rozenshtein (2018) como "intermediários de vigilância", ou seja, entidades que ficam entre as agências de aplicação de lei e as informações

[4] A literatura dedica à definição de espaço cibernético é diversa. Em termos técnicos o ciberespaço, ou espaço cibernético, pode ser definido como um ambiente composto por (i) um hardware, formado pelas máquinas e redes que compõem sua infraestrutura e (ii) um software, composto pelo conjunto de informações em circulação nesse domínio como dados e mídia, sendo definido como "um conjunto de redes e sistemas de comunicação interligados entre si de forma direta ou indireta" (FERREIRA NETO, p. 70, 2014). A internet é apenas uma parte que compõe o ciberespaço.

pessoais do público, tornando-se responsáveis por 'decidir quão fácil ou difícil' será o acesso a essas informações pelas autoridades públicas.

Embora existam normas para a solicitação de informações por parte dos governos aos setores privados, os intitulados intermediários de vigilância mantêm um elevado grau de discrição na avaliação crítica da legalidade dessas solicitações. Essas empresas são responsáveis por decisões que têm grandes consequências para a privacidade dos indivíduos e para a segurança dos Estados (COOPERATION..., 2018). Deste modo, legislações e regulamentações relacionadas à promoção da segurança e privacidade no ciberespaço são um importante termômetro para avaliar não apenas o posicionamento de atores públicos, mas também, de atores privados sobre a promoção da vigilância.

Identificamos que as legislações CISPA (*Cyber Intelligence Sharing and Protect Act*[5]*)* e CISA (*Cybersecurity Information Sharing Act*[6]*),* tramitadas no congresso norte-americano durante a administração Obama, são fundamentais para melhor compreender a relação que se estabelece entre as grandes empresas de internet nos Estados Unidos, o governo federal e as estruturas de inteligência norte-americanas quando debate-se vigilância na era do Big Data, e portanto, a relação equacional entre privacidade e segurança ao avaliarmos as políticas para o ambiente digital.

Inseridas no congresso norte-americano como legislações de segurança cibernética, tais legislações passaram a ser enquadradas por grupos opositores como projetos de lei de cibervigilância, uma vez que ambos buscavam ampliar o compartilhamento de informações entre setor público e privado para fins de segurança, ao mesmo tempo em que conferiam ao setor privado proteção de responsabilidade contra possíveis processos relacionados à invasão de privacidade. Essas disposições associadas a um texto pouco claro, justificavam sua fama violadora. Apesar da forte oposição a esses projetos de lei, em parte exacerbada pelo momento político delicado vivido após as declarações de Edward Snowden em 2013, a CISPA e a CISA receberam apoio de importantes atores do setor privado.

Um estudo exploratório feito no capítulo quatro dessa dissertação *"O governo Obama: o difícil equilíbrio entre privacidade e segurança na ciberespaço"* permite avaliar como legislações de segurança cibernética podem se converter em legislações de cibervigilância, mascarando a intenção de atores governamentais. Este estudo exploratório possibilita ainda identificar o papel e a força do setor privado no interior dessa lógica, além de assinalar a

[5] Cf. U.S.Government (2011)
[6] Cf. U.S.Government (2015b, 2015c)

presença de disputas inter burocráticas entre as agências norte-americanas para coordenar as políticas nesse domínio, considerada uma variável interveniente nesse processo, pois tal disputa abriria espaço para um maior poder de barganha pelo setor privado.

Judith Germano (2014) pontua que uma das dificuldades para a padronização da dinâmica relacional entre setor público e privado, em termos de segurança cibernética, está exatamente no fato de que “diferentes órgãos do governo têm papéis e interesses conflitantes" (GERMANO, 2014, p. 1). Deste modo, o espaço a ser ocupado pelo setor privado parece também depender da disputa política estabelecida entre as diferentes agências, órgãos e departamentos bem como da intenção política que cada uma dessas estruturas poderá nutrir em relação às questões de segurança cibernética e a definição do setor privado enquanto parceiro. No que se refere à essa temática destaca-se o embate entre o Departamento de Segurança Interno (*Department of Homeland Security - DHS*) e a NSA. Para discutir tais questões, esta dissertação opta pela reconstrução histórica fundamentada na exploração de algumas fontes primárias (e.g. documentos oficiais, legislações, *hearings*) e fontes secundárias.

Por fim, sem a pretensão de esgotar o tema, algumas conclusões são pontuadas com o objetivo de instituir um plano de fundo para que uma agenda de pesquisa futura seja desenvolvida. Uma breve consideração sobre as decisões políticas tomadas durante a administração Trump, ainda em curso, parecer corroborar com os debates levantados nessa dissertação, qual seja, que a interação entre atores público-privados durante o processo de decisão entre segurança e privacidade no domínio digital incorpora dois propósitos distintos. Primeiro, a manutenção de uma lógica de mercado baseada na vigilância e dominada pelo monopólio norte-americano no setor das tecnologias da informação e comunicação. E, segundo o interesse do governo norte-americano em se utilizar do setor privado - e da legitimidade que este possui em captar dados pessoais para reordenar suas políticas de inteligência e torná-las mais eficientes. Um exemplo mais significativo da continuidade dessa tendência, para além da tentativa de aprovação da legislação CISPA e CISA, foi a instituição do *USA Cloud Act* em 2018, que permite que autoridades federais norte-americanas obriguem as empresas de tecnologia baseadas nos Estados Unidos, por meio de mandato ou intimação, a fornecer dados armazenados em seus servidores, independente, se esses dados se encontram armazenados nos Estados Unidos ou no Exterior. Essa legislação manifesta-se como uma clara intenção do governo norte-americano em contornar as questões de territorialidade que podem se apresentam como um impeditivo ao governo norte-americano obter acessos aos dados, utilizando-se do fato de que as principais empresas de internet são empresas de capital norte-americano.

2 A SOCIEDADE DO BIG DATA E AS TRANSFORMAÇÕES ESTRUTURAIS NO VALOR DA INFORMAÇÃO

> *A informação será para o século XXI o que o petróleo e o gás foram para o início do século XX. Ela irá alimentar o poder econômico e político*. (GOLDSTEIN, 1994 apud JABLONSKI; POWERS, 2015, p. 75).

Em um movimento de quase total digitalização da vida social, a produção de dados se transformou em um elemento central para as práticas política, econômica e social. A constante modernização das NTICs (Novas Tecnologias de Informação e Comunicação) alterou a variedade, o volume e a velocidade com que as informações são produzidas, armazenadas e processadas, promovendo a classificada "Data Revolution". Tal conceito passou a ser utilizado para descrever o novo estágio atingido pela Sociedade da Informação, onde o amplo alcance e a permeabilidade das tecnologias digitais à vida cotidiana tornaram-se responsáveis por produzir uma quantidade massiva de dados classificados como Big Data (KITCHIN, 2014; ZUBOFF, 2019).

Na contemporaneidade, praticamente tudo é convertido em dados: o click em uma página Web, a quantidade de acessos a uma conta de e-mail, o histórico de buscas no Google, dados de mobilidade captados via gps e até mesmo os registros de compras feitos através de cartões de crédito. Existem inúmeros fornecedores de big data: consumidores, governos, organizações, ONGs ou qualquer indivíduo ou entidade que de algum modo exerça atividade em ambiente digital (FLYVERBOM; DEIBERT; MATTEN, 2017). Em tal contexto, o dado que é inicialmente uma entidade puramente matemática, gerada a partir de qualquer movimentação em ambiente online, converte-se em um instrumento político e de valor econômico agregado após o emprego cognitivo para transformá-los em informação útil (KITCHIN, 2014; RUPERT; ISIN; BIGO, 2017; WEST, 2017; ZUBOFF, 2019).

Nas palavras de Michael Palmer, vice-presidente executivo da ANA (*Association of National Advertisers*) "Os dados são como petróleo bruto. São valiosos, mas se não refinados, não podem ser usados de verdade", sendo necessário, portanto, analisá-los para que tenham valor" (ARTHUR, 2012). Esse processo de conversão do dado em informação útil, com valor político e econômico agregado, é intitulado de data mining ou, em português, mineração de dados. O *data mining* consiste em explorar grandes quantidades de dados à procura de padrões consistentes. Esse processo demanda a filtragem e armazenamento da maior quantidade de dados

que se puder realizar somado ao emprego de tecnologia capaz de converter estes dados em informação inteligível (FLYVERBOM; DEIBERT; MATTEN, 2017).

Vive-se hoje dentro de uma realidade marcada pela geração intensa de informações em potencial, de modo que o processamento de dados se transforma no principal instrumento das práticas políticas, econômicas e militares. Zuboff (2019) argumenta que o "Big Data" não é uma tecnologia ou um efeito tecnológico inevitável, mas se origina no social, comportando-se como um catalisador de interesses políticos e comerciais específicos. A sociedade do Big Data é produto de duas racionalidades: a governamental e a dos negócios que se valem de uma mesma lógica: "promover vigilância para atender seus objetivos" derivando, portanto de um propósito de ampliação do conhecimento (BALL; WEBSTER, 2003; KITCHIN, 2014)

O Big Data carrega consigo forte valor preditivo, característica positiva tanto do ponto de vista político-estratégico como comercial. O processo de mineração de dados, ou *data mining*, fornece *insights* sobre comportamentos e motivações humanas, tendências sociais, mudanças ambientais, dentre outras informações necessárias à predição, previsão e antecipação, gerando entusiasmos tanto sobre os setores empresariais que se utilizam dessas informações para prever e antecipar gostos, preferências e desejos dos consumidores, quanto aos setores político-estratégico-militares do Estado que se valem dessas informações para construir inteligência e dar continuidade à operações militares e estratégicas. Pois, de acordo com David Lyon (2015, p.150) , "os mesmos dados são cada vez mais usados para diferentes propósitos [...] dados comerciais podem receber novos significados no domínio da segurança, sendo combinados e conectados de maneiras novas". Portanto, dentro da sociedade do Big Data, políticas governamentais e negócios parecem ser atraídos pela intensificação das práticas de "vigilância", ou em outros termos, pela progressiva necessidade de ampliação da captação e armazenamento de dados, informações e, logo, de conhecimento.

Neste capítulo, descrevemos como atores públicos e privados reformularam suas políticas de poder e suas estratégias, sejam essas econômicas e comerciais no caso dos atores privados, ou estratégico-militares no caso das entidades estatais diante do surgimento de uma sociedade marcada pela permeabilidade do ambiente digital em todas as esferas da vida cotidiana. Buscamos debater também a crescente hibridação entre atores públicos e privados no campo da vigilância, questionando até que ponto esses dois interesses não se encontram interseccionados (TRÉGUER, 2019). Diante de tais reflexões, as intituladas empresas privadas ligadas às NTICs adquirem um status central, atuando como intermediárias para a execução da vigilância (ROZENSHTEIN, 2018). Esses parâmetros são fundamentais para avaliar as políticas de compartilhamento de dados dentro da segurança cibernética, pois é a partir da convergência entre

essas duas lógicas, e da aproximação ou distanciamento do interesse desses dois atores, que se institucionaliza, nos Estados Unidos, políticas voltadas à regulamentação do ciberespaço, sejam políticas de privacidade de dados ou segurança cibernética.

2.1 Novas dimensões estratégicas no poder da informação

A centralidade da informação ao poder não é um elemento novo. Os trabalhos clássicos de Sun Tzu e Clausewitz já mencionavam a relevância da informação enquanto elemento central às operações táticas e estratégicas dos Estados. Hodiernamente, a era informacional intensificou a capacidade de coleta de grandes quantidades de dados e ampliou o alcance e a velocidade da transmissão dessas informações. Diante dessa nova realidade, o valor da informação permaneceu relevante, contudo, o ambiente foi alterado, e, portanto, a lógica de atuação dos atores foi modificada, demandando readequações à ação estratégica do Estado.

O amplo processo de informatização gerado pela evolução das tecnologias de informação e comunicação, dentre elas a internet, passou a ser percebido como fundamental à construção de vantagens militares, especialmente, a partir do crescimento da indústria de software nos Estados Unidos (POWERS; JABLONSKI, 2015). Na década de 1980, surgiu o conceito de Revolução dos Assuntos Militares (RAM) utilizado para descrever o aparecimento de tecnologias disruptivas responsáveis por tornar obsoletos os conceitos e capacidades militares existentes, exigindo uma reavaliação por parte dos tomadores de decisão, e do *establishment* militar de como, com quais instrumentos e por quem a guerra seria travada (BROSE, 2019). As novas tecnologias, em ascensão, marcaram um processo de transição da lógica de guerra mecanizada, característica da era industrial, para a intitulada guerra de informação descrita como uma guerra de decisão e controle centrada no conhecimento. O slogan da guerra sofreu uma alteração gradual, substituindo o lema “preservar-se e aniquilar o inimigo”, para “preservar-se e controlar o oponente” (POWERS; JABLONSKI, 2015).

Essa possibilidade de controle encontrava-se diretamente vinculada à ampliação da capacidade de aquisição de conhecimento, resultado do surgimento de tecnologias que expandiam a produção, transmissão e processamento de informações. Surgia um desejo crescente em avançar com a integração da inteligência avançada, sendo fundamental, na visão dos pensadores da RMA desenvolver um conceito que até então havia sido pouco articulado, sendo este o conceito de Guerra Informacional, ou *Information Warfare*, descrito como a capacidade de degradar ou até paralisar o comando, controle, comunicação e inteligência (C^3I) do oponente. Como enfatiza Myrian Dunn Calvety (2007, 2012), rapidamente os pensadores militares norte-

americanos começaram a escrever sobre essa temática, visão que foi popularizada fora dos círculos militares por autores como Alvin Toffler.

Como observou o Secretário de Defesa norte americano William Perry, em 5 de maio de 1994:

> Vivemos em um era que é movida pela informação. É uma era que Alvin Toffler chamou de Terceira Onda. A capacidade de adquirir e comunicar grandes volumes de informação em tempo real, o poder da computação para analisar essas informações rapidamente e a existência dos sistemas de controle para passar essa análise para vários usuários simultaneamente – são avanços tecnológicos que estão mudando a face da guerra e como nos preparamos para enfrentá-la (U.S. GOVERNMENT, 1996, p. 52, tradução nossa)

Nesse contexto, conceitos diversos surgiram para categorizar essas novas formas de conflito, sem que se chegasse a um consenso sobre sua definição. Entretanto, pode-se argumentar que o aspecto comum entre eles era a ideia de substituição das armas físicas pela supremacia em liderar a revolução da informação (NYE JR; OWENS, 1996).

Em termos concretos, a guerra do Golfo inaugurou a percepção de que a capacidade de "ver o espaço de batalha" se transformava na chave para a vitória. Nesse sentido, o principal objetivo das forças armadas converteu-se em dominar o espectro da informação e obter a intitulada superioridade informacional (*information superiority*) definida pela capacidade de coletar, processar e disseminar um fluxo ininterrupto de informações ao mesmo tempo em que nega essa mesma capacidade a um adversário (CAVELTY, 2007, 2012; U.S. GOVERNMENT, 1996).

Autores como Arquilla e Ronfeldt (1997) dedicaram-se a analisar o impacto das tecnologias de informação e comunicação dentro da lógica de disputa pelo poder internacional. Em grande medida, os autores argumentam que a revolução da informação provocou mudanças tanto em como as sociedades poderiam entrar em conflito, bem como, no modo mediante o qual suas forças armadas poderiam entrar em guerra.

Os conceitos de *netwa*r e *cyberwar* foram cunhados para definir ambas as situações. O conceito de *Cyberwar* era definido como o ato de interromper, se não destruir, os sistemas de informação e comunicação do adversário (ARQUILLA; RONFELDT, 1997, 2001). Esta era apenas uma das faces da nova lógica de conflito que se estabelecia dentro de uma sociedade governada pela centralidade das novas tecnologias de informação e comunicação. A outra face da moeda era representada pela *Netwar*, entendida como a prática de secretamente "perturbar, danificar ou modificar o que uma população alvo sabe ou pensa que sabe sobre o mundo ao seu redor" (ARQUILLA; RONFELDT, 1997, p. 28, tradução nossa). A *Netwar* incorpora diplomacia, propaganda, campanhas psicológicas, interferência na mídia local, infiltração de

redes e bancos de dados de computadores, dentre outras práticas. O grande diferencial entre estas duas formas de conflito, está no fato de que o primeiro visa diretamente a infraestrutura dos sistemas de informação, o segundo visa percepções sociais a serem atingidas através destes meios digitais.

Apesar da centralidade conferida às tecnologias de informação no contexto da revolução dos assuntos militares, os tomadores de decisão e estudiosos do período acabam por compreender essa nova tecnologia da mesma maneira que compreendiam tecnologias criadas em momentos anteriores, ignorando a importância e particularidades que tais tecnologias implicam para a disputa de poder na seara internacional (CARR, 2016). De acordo com a autora Madeline Carr (2016), a literatura da época ignora aspectos únicos e importantes desta tecnologia emergente responsáveis por impactar em seu relacionamento com o poder nas Relações Internacionais. Dentre os fatores negligenciados inclui-se a forte permeabilidade dessa tecnologia na sociedade civil, responsável por ampliar a gama de interesses políticos em discussão neste domínio.

Segundo Calvety e Brunner (2016), a *Information Warfare* não limita-se, portanto, a um conflito militar. A intitulada guerra de informação visa toda a infraestrutura de informação de um adversário durante todo o continuum do período de paz ao de guerra. Os autores Powers e Jablonski (2015) caracterizam a "guerra cibernética", ou *cyberwar* não apenas como uma extensão da estratégia militar e do conflito para o ambiente em rede, mas também como a disputa dos Estados em alavancar seus sistemas de informação para fins de poder político, econômico e social. Diante dessa constatação os autores propõem uma perspectiva mais ampla do que viria a se constituir de fato uma guerra cibernética. A intitulada guerra cibernética, conceito que tem ganhado expressividade no século XXI, refere-se à utilização de redes digitais para fins geopolíticos, seja promover ataques contra os sistemas eletrônicos de outros Estados-Nação, ou utilizar as redes interligadas, como a Internet, para promover a agenda econômica e militar de um Estado, o que inclui utilizar a internet para moldar as opiniões políticas, os hábitos de consumo, os valores culturais e sociais de uma população, bem como a percepção da internet como um instrumento fundamental para a captação de informações valiosas que podem vir a servir aos propósitos de inteligência do Estado.

Libicki (2007) argumenta que as evoluções técnicas e as mudanças nas práticas de comunicação e informação nos últimos vinte anos tornaram necessária a adição do dado (*data*) como uma variável de ajuste dentro das considerações sobre o conceito de guerra informacional. Na visão do autor, quando o conceito surgiu a guerra de informação era definida pela centralidade das TICs na segurança nacional, contudo, no tempo presente, o próprio conceito de

NTICs tem se tornado obsoleto devendo ser substituídos por dados e tecnologias de dados. Essa transformação se deve à, já mencionada, expansão do volume de informações disponíveis, ampliação que decorre da crescente utilização de tecnologias digitais somada ao surgimento de uma nova variedade de objetos e organismos interconectados e inteligentes, conformando a intitulada internet das coisas.

Os dados, portanto, têm se comportado crescentemente como um ativo estratégico e tático fundamental ao campo de batalha, sendo úteis para as práticas de inteligência, vigilância e reconhecimento. Como destaca Rosenweig (2013), os governos têm crescentemente recolhido e armazenado tais dados para que esses possam ser convertidos em inteligência. Isso porque a inteligência muitas vezes se manifesta como a primeira tática de defesa, em especial em um ambiente ontologicamente marcado pela insegurança devido suas características. Nesse sentido, construir poder estatal, hodiernamente, dependente da captação massiva de dados (WOLOSZYN, 2016).

2.2 Novas dimensões econômicas no poder da informação

2.2.1 O capitalismo de vigilância

A ampliação na produção de dados transformou também o ramo dos negócios. A mediação computacional de praticamente todas as esferas da vida humana transformou o cotidiano em matéria prima para um novo mercado baseado na venda de previsões comportamentais sobre os consumidores e na construção de mercados personalizados (WEST, 2017). As duas estratégias que haviam mudado a lógica de operação do Estado dentro da sociedade do Big Data – previsão e antecipação - também estavam presentes no campo econômico, sendo difícil afirmar, com certeza, qual havia servido de modelo para a outra.

Essa nova lógica de acumulação de capital, baseada na monetização de dados comportamentais, foi definida pela autora Shoshana Zuboff (2014) como capitalismo de vigilância, uma variante extrativa do capitalismo de informação5, responsável por direcionar o setor privado rumo a um projeto de vigilância lucrativo, transformando os dados na mais nova e lucrativa commodity comercial do século XXI (ZUBOFF,2019). Modelo de negócios também categorizado como capitalismo de dados.

Segundo Zuboff (2019), a análise de dados massivos, o Big Data, começou como uma maneira de reduzir a incerteza dentro do contexto produtivo. A automação permitia que as máquinas informassem aos gestores sobre o processo produtivo, permitindo que sua atividade se

tornasse mais transparente e que o conhecimento gerado fosse capaz de oferecer informações necessárias para aprimorar e/ou controlar com mais precisão a produção.

A vigilância se realizava, em um primeiro momento, dentro do ambiente de trabalho. Contudo, o rápido desenvolvimento tecnológico fez com que o foco mudasse, e silenciosamente, se convertesse para a monetização comercial do conhecimento sobre comportamentos, bem como a utilização desse conhecimento comportamental para influenciar e moldar o mercado e o fluxo de receita futuros.

De acordo com West (2017), o capitalismo de dados moderno, como hoje o conhecemos, iniciou-se em meados dos anos 1990, antecedendo inclusive a bolha das ponto.com, período marcado por uma mudança tecnológica e econômica para a indústria nascente da Internet, em que passou-se a compreender a Internet não apenas como um mercado para a venda de mercadorias (*e-commerce*), mas também como um espaço que permite a produção e colheita de dados dos usuários, insumo que passou a ser gradativamente compreendido com um produto de alto valor agregado e adquirido mediante a observância da vida cotidiana.

O conceito de capitalismo de vigilância se define nas palavras da autora Shoshana Zuboff, criadora dessa terminologia, como:

> 1.Uma nova ordem econômica que reivindica a experiência humana como matéria-prima para práticas comerciais ocultas de extração, previsão e vendas; 2. Uma lógica econômica parasitária na qual a produção de bens e serviços está subordinada a uma nova arquitetura global de modificação comportamental. 3. Uma mutação desonesta de capitalismo marcado por concentrações de riqueza, conhecimento e poder sem precedentes na história humana; 4. A estrutura fundamental de uma economia de vigilância; 5. Ameaça significativa à natureza humana no século XXI assim como o capitalismo industrial foi para o mundo natural no século XIX e XX; 6. A origem de um novo poder instrumental que afirma domínio sobre a sociedade e apresenta desafios surpreendentes para a democracia de mercado; 7. Um movimento que visa impor uma nova ordem coletiva com base na certeza total; 8. Uma expropriação de direitos humanos críticos que é melhor entendida como um golpe de cima: uma derrubada da soberania do povo (ZUBOFF, 2019, p. 8, tradução nossa).

Para Zuboff (2019, p.92), a primeira empresa a identificar na lógica anteriormente descrita a oportunidade de geração de capital foi a empresa Google. Inc. O modelo de negócios adotado por essa corporação serviu como ponto de partida para a codificação de uma nova e poderosa lógica de acumulação de capital. A empresa compreendeu que vender produtos ou serviços online, como por exemplo a venda extensão de arquivos que poderiam ser enviados por e-mail gerava menos lucro do que comercializar dados e previsões sobre o comportamento de seus usuários para o mercado.

A capitalização da vida social se estabelece, especialmente, via dados de escape, ou em inglês *exhaust data*, definidos como o subproduto das informações resultantes de todas as nossas

atividades digitais, como sites visitados, links clicados, passagem de mouse, curtidas no Facebook, páginas visualizadas, tempo de permanência e localidade em que essas visualizações haviam sido realizadas.

Esses dados são responsáveis por construir uma trilha de comportamento do usuário na Internet, de modo que quando submetidos a processos de matematização como *data mining* ou *data analitics*, fornecem perfis de comportamento e preferências dos usuários, comportando-se como a pedra filosofal da era digital, transformando qualquer dado (data) em ouro ou em outras palavras convertendo uma série de dados brutos em matéria prima algorítmica altamente lucrativa.

Segundo Rosenzweig (2013), a ascensão e consolidação dessa lógica econômica foram possíveis apenas graças às transformações tecnológicas, que ampliaram a portabilidade e conectividade dos meios de comunicação, bem como a vinculação de praticamente todos os objetos e sistemas a meios digitais – conformando o intitulado fenômeno: internet das coisas ou *Internet Of Things* (IOT)[7]. Essas evoluções tecnológicas impactam diretamente na permeabilidade dos sistemas digitais na vida cotidiana, elevando exponencialmente a captação e análise de dados pessoais e informações sobre um indivíduo ou organização, fenômeno nomeado pelo autor de *data surveillance*. A mediação computacional tornou o mundo visível, cognoscível e compartilhável de uma maneira até então não apreciada. As inovações tecnológicas relacionadas ao armazenamento de informações também desempenharam relevante papel na consolidação desse novo mercado. A crescente diminuição no custo de armazenamento de dados, graças à computação em nuvem, conformou um importante capítulo dentro dessa nova lógica econômica, devido à possibilidade de criação de um imenso banco de dados que pode ser consultado a qualquer instante, sem gerar custos absurdos (GANDY, 2003). Como destaca Vicente Mosco (2016, p. 13, tradução nossa), "a nuvem e o big data são mecanismos que potencializam o capitalismo informacional, ao mesmo tempo em que permitem um modo de saber cada vez mais dominante". A comoditização de dados introduz uma lógica que atravessa as dimensões econômicas, políticas e sociais.

Essa é uma lógica que tende a se perpetuar e intensificar, graças aos interesses de atores públicos e privados em sua manutenção. Schneier (2015) e Zuboff (2019) colocam em evidência que a conversão de dados em insumo para geração de receita, apresentando-se como um ativo de alta lucratividade tem gerado pressões econômicas, mas também políticas, crescentes em direção

[7] A semântica dessa expressão remete à ideia de uma rede mundial de objetos interconectados e unicamente endereçáveis, baseado em protocolos de comunicação padrão.

à intensificação da conexão e monitoramento online (SCHNEIER, 2015; ZUBOFF, 2019). Como pontua Vincent Mosco (2016, p. 19, tradução nossa), "juntamente com o capitalismo de vigilância está o estado de vigilância que, como expuseram as revelações feitas por Edward Snowden, têm acesso quase completo aos dados armazenados na nuvem e fornecidos pela Internet e outras redes eletrônicas". Não sendo, portanto, inesperado que atores de todos os tipos, inclusive os Estados, estejam cada vez mais preocupados com as implicações de segurança que essa nova lógica econômica e social impõe.

A prática de vigilância, hodiernamente em voga, não foi atualizada de maneira ocasional, mas derivou de ações políticas e interesses econômicos fortemente coordenados, e, portanto, intencionais, liderados pelo governo norte-americano. Como será explorado no próximo capítulo, as agências de inteligência norte-americanas, com especial destaque para CIA (*Central Intelligence Agency*), desempenharam um papel central no incentivo do desenvolvimento de tecnologias de uso comercial mas que ao mesmo tempo mostravam-se capazes de suprir as necessidades das agências de inteligência em coletar, armazenar e processar dados com maior eficiência.

Ademais, a universalização da vigilância e o incentivo ao desenvolvimento das tecnologias de comunicação, como os computadores e tecnologia digital, a exemplo da internet, responsáveis por instituir as bases do capitalismo de vigilância, estiveram diretamente associadas a três tendências em desenvolvimento nos Estados Unidos no pós segunda guerra mundial, sendo essas (1) a instituição do complexo industrial militar; (2) a ascensão de uma lógica econômica fortemente baseada no marketing corporativo e nas mídias, centrado na Madison Avenue e, por fim (3) a financeirização. Tendências estabelecidas com o objetivo de incentivar a continuidade do crescimento da economia norte-americana no pós-segunda guerra, mas que gradativamente se tornaram a base da política e econômica do país (FOSTER; MCCHESNEY, 2014).

Como muito bem destacaram Foster e McChesney (2014), esses três pilares da economia norte-americana identificariam na vigilância digital uma oportunidade de elevar seus ganhos, havendo inúmeras justificativas para que representantes desses três setores apoiassem a sociedade de vigilância praticando lobby e interferindo politicamente em legislações que de algum modo venham a regulamentar essa prática. Nesta pesquisa, iremos focar em explorar como a lógica circunscrita em torno do complexo industrial militar se estruturou e tornou-se responsável por alavancar a vigilância digital.

3 HISTÓRIAS CRUZADAS: COMO ESTADO E EMPRESAS NORTE-AMERICANAS CONSTRUÍRAM A SOCIEDADE DO BIG DATA

Nesse capítulo abordamos, mediante análise histórica, como as políticas governamentais norte-americanas se interseccionaram aos interesses do setor privado para conformar o que hoje definimos como sociedade do Big Data.

Traçando uma linha que vai desde a criação da Internet até a administração Bush (2001-2008), debatemos como o domínio do setor privado sobre a infraestrutura da internet e dos dados que nela circulam ocorreu com apoio governamental. Argumenta-se que, embora a Internet tenha tido início como um projeto da ARPA (*Advanced Research Projects Agency*) - agência de estudos avançados do Pentágono-(BLOCK, 2008, p.175), a partir dos anos 1990, o Estado norte-americano iniciou um percurso de aproximação ao setor privado, colaborando, sobretudo, para o fortalecimento das estratégias comerciais das empresas norte-americanas voltadas ao desenvolvimento de tecnologia capazes de atender às demandas civis e militares, resultado de uma política característica do governo Clinton.

O estudo realizado permitiu levantar importantes variáveis durante esse processo como, por exemplo, o relevante papel desempenhado pelas agências de inteligência como grandes investidoras de capital de risco em pesquisas dedicadas a ampliar a capacidade do governo norte-americano em coletar, armazenar e processar dados, incorrendo no surgimento de uma nova categoria de empresas, *Big Techs*, e uma nova lógica de mercado, o capitalismo de vigilância, instituindo o que seria descrito como um complexo industrial informacional ou complexo industrial de vigilância nos Estados Unidos.

Além disso, o capítulo aborda como as transformações ocorridas no pós 11 de setembro de 2001, período em que o discurso securitizador em torno da "*guerra ao terror"* flexibilizou a privacidade em nome da segurança nacional, permitiu que um arcabouço legal em torno da vigilância fosse instituído, incentivando, por sua vez, um aumento nos investimentos em tecnologias capazes de recolher informações em massa fossem amplamente financiadas. Nesse contexto, foi criado o *Total Information Awarreness* (TIA), precursor da lógica de captação de informação em massa.

O capítulo encerra com pequenas considerações sobre como o alinhamento entre setor público e privado na política interna norte-americana para a instituição de uma lógica de vigilância se associou a uma política externa que possibilitou ao país dominar a infraestrutura global da Internet. Nesse sentido, exploram-se alguns aspectos políticos do que seria descrito por

McChesney (2013) como cartel global da internet, especialmente os potenciais efeitos transfronteiriços de regulamentos e decisões judiciais tomadas a nível nacional.

3.1 Redes de comunicação interativa: um empreendimento acadêmico-militar com consequências econômicas

As novas tecnologias de informação e comunicação (NTICs), fatores estruturantes da internet e do ciberespaço, surgiram na época da Guerra Fria. O projeto ARPANET, rede precursora da Internet, foi desenvolvida pelo *Information Processing Techniques Office (IPTO)* vinculado à ARPA (*Advanced Research Projects Agency*), agência criada em 1957, associada ao Departamento de Defesa, responsável por desenvolver inovações disruptivas e de risco capazes de se contrapor a possíveis ameaças científico-tecnológicas (e, por conseguinte, militares) concebidas pela União Soviética (BLOCK, 2008, p.175; MOWERY, 1994).

O conflito bipolar foi caracterizado por um expressivo embate científico e tecnológico entre os dois países. A corrida pelo desenvolvimento tecnológico e inovativo retroalimentava as disputas estabelecidas no campo ideológico, político e militar, comportando-se como uma importante interface da estratégia norte-americana para expressar o seu poder no cenário internacional. Em termos históricos, os Estados Unidos vistos como a nação mais capaz de desenvolver tecnologias e indústrias inovativas do que qualquer outro Estado Nação. Deste modo, o lançamento do satélite soviético Sputnik, em 1957, foi percebido como um golpe auferido contra o protagonismo norte-americano e seu *status* de prestígio e liderança no cenário internacional (ABBATE, 2000; CARR, 2016; CASTELLS, 2005).

Portanto, a criação da ARPANet, em momento imediatamente posterior a este acontecimento, cumpria, dentre outros, o propósito de resgatar a crença no poder inovativo norte-americano. Para além do valor simbólico deste empreendimento científico, havia também uma justificativa estratégico-operacional. Abbate (2000) argumenta que a criação da ARPANet atendia um propósito muito específico à Guerra Fria, qual seja estabelecer um sistema de comunicações militar mais seguro contra ataques nucleares, permitindo aos Estados Unidos preservar sua capacidade de comunicação e resposta.

Os sistemas de comunicação até então existentes, como o telefone e o telégrafo, estavam baseados em uma arquitetura extremamente vulnerável conhecida como “modelo de raios”. Esse tipo de arquitetura contava com a existência de uma estrutura central para a qual todas as informações eram direcionadas e posteriormente encaminhadas aos seus destinatários pretendidos. Especulava-se à época que caso ocorresse um ataque nuclear em solo norte-

americano, a administração governamental perderia toda sua comunicação e capacidade de resposta pois um ataque inviabilizaria todo o fluxo informacional (ABBATE, 2000; CARR, 2016)

Diante de tal constatação, a *Rand Corporation*, em 1960, começou a desenvolver uma proposta de rede alternativa baseada fundamentalmente na descentralização e flexibilidade do modelo de comunicação. Intitulado de "teia de aranha", esse modelo dispunha de uma estrutura ramificada. Dentro dessa arquitetura os pacotes de dados seriam programados para encontrar a rota mais rápida possível para seu destino, de maneira que a falha de um roteador não culminaria na total paralisação do sistema, mas resultaria na circulação dos pacotes de informação através de um caminho alternativo. Essa estrutura ramificada possibilitava que nenhuma parte desta rede fosse completamente dependente da existência de outra parte. Uma rede experimental deste tipo foi financiada pela DARPA, sendo ela a ARPANET (CARR, 2016).

Essa nova "estrutura" criada para o compartilhamento de informações recebeu o nome de comunicação interativa que passaria por evoluções crescentes ao longo dos anos. Inicialmente essa rede foi implementada em quatro universidades durante o ano de 1969, o objetivo era que pesquisadores de qualquer uma dessas universidades pudessem compartilhar informações e operar qualquer uma das outras máquinas conectadas a este sistema de modo remoto. Já na década de 70 uma expansão para 200 computadores foi realizada.

Um dos principais desafios enfrentados à época pelos projetistas era encontrar uma forma de transição de uma rede unitária como a ARPANet para um sistema que pudesse incorporar uma variedade de redes pertencentes e operadas por organizações e entidades independentes e diversas. A alternativa técnica encontrada foi a criação de um protocolo comum a ser compartilhado por todas as redes candidatas a se juntarem a este mesmo sistema. Uma mesma "linguagem" deveria ser falada por todos aqueles que desejassem se juntar a esta rede. Os cientistas da ARPA, trabalhando em estreita colaboração com especialistas de Stanford, desenvolveram, em 1974, essa linguagem comum que ficaria conhecida como protocolo de controle de transmissão/ protocolo da Internet, ou em sigla TCP/IP (MOWERY, 1994). O desenvolvimento do TCP/IP marcou uma etapa crucial no desenvolvimento da conexão em rede, estimulado por uma percepção de que a arquitetura da internet deveria ser aberta. Embora o ano de 1974 tenha marcado o início do TCP/IP, seriam necessários vários anos de modificações e reformulação antes de ser competido e adotado universalmente da maneira como hoje o compreendemos.

Não demorou para atores da política norte-americana identificarem o potencial dessa nova tecnologia para os Estados Unidos. Representado inicialmente por um pequeno grupo de

políticos (em sua maioria, democratas que acreditavam que cada vez mais a tecnologia informacional seria parte fundamental a consolidação do poder norte-americano), um grupo intitulado “Democratas-Atari” passou a enfatizar a necessidade de uma participação mais ativa do setor privado no desenvolvimento de tais tecnologias (POWERS; JABLONSKI, 2015).

O senador, e, posteriormente, vice-presidente, Albert Gore Jr, membro do partido democrata é a grande figura representativa deste contexto político. Albert Gore Jr, ou também conhecido como Al Gore, teve um impacto político fundamental no desenvolvimento da Internet e da tecnologia web no país (CARR, 2016, p. 50). Gore argumentava que a tecnologia informática seria essencial para o futuro do poder norte-americano, crença essa que era afirmada em seus escritos e na sua prática política.

Em nota lançada pela Revista de Computação Acadêmica em novembro de 1989, Al Gore à época Senador pelo Tennesse, destacou que a garantia de competitividade dos Estados Unidos no próximo século dependia do desenvolvimento da computação de alto desempenho. Isso porque os supercomputadores transformariam a maneira mediante a qual os Estados Unidos pensam e fazem negócios, sendo necessário um aumento imediato do acesso a redes de alta velocidade, bem como a participação do setor privado nessas redes.

Buscando atingir tal objetivo Al Gore propôs em 1989 o projeto de lei *“High Performance Computing and Communication Act* (HCCA) promulgado como lei pública em dezembro de 1991. Essa lei especificava que inicialmente a infraestrutura da Internet deveria ser apoiada fiscalmente e administrada pelo governo federal através da *National Science Foundation* (NSF), esta era contudo uma medida provisória, devendo ser extinto o envolvimento do NSF quando as redes comerciais pudessem atender às necessidades de rede dos pesquisadores norte-americanos (U.S. GOVERNMENT, 1991).

Segundo Gore, patrocinador deste projeto, em um primeiro momento o governo federal teria que assumir a liderança deste empreendimento a fim de garantir as necessidades norte-americanas diante dessas novas tecnologias, além de apresentar ao setor privado o potencial de uma economia baseada na tecnologia informacional em rede (CARR, 2016, p. 51 apud GORE, 1989). Deste modo, se as empresas ainda não estavam interessadas em construir as redes que os Estados Unidos precisavam, o governo federal deveria atrair essa participação.

Dentre as disposições contidas nesta legislação constava a necessidade de promover maior colaboração entre o governo, laboratórios federais, indústria, centros de computação de alto desempenho e universidades. Fruto dessa colaboração, a lei HCPA forneceu financiamento à *National Center for Supercomputaing Applications* vinculado a Universidade de Illinois, onde Marc Andreessen, criou em 1993 o navegador *Web Mosaic* considerado como “o trampolim

tecnológico para a internet comercial". Um navegador de *web* é um aplicativo de *software* que facilita o contato entre usuários e informações dentro do sistema de internet, inovação que, segundo as palavras de seu criador, não teria acontecido caso tivesse sido relegada às mãos do setor privado (CARR, 2016, p.57-58).

O surgimento do navegador *Mosaic* colocava em evidência o potencial da Web para a publicação e comércio, e, portanto, o surgimento, da internet como um veículo de entretenimento. Até sua invenção, as páginas online eram baseadas praticamente em texto. Os softwares utilizados para acessar esse conteúdo eram também bastante confusos, o que limitava seu uso aos profissionais que detinham conhecimento técnico. Isto posto, o navegador *Mosaic* revolucionava, em especial, visualmente, os seus antecessores criando um interesse público por gerar conteúdo para a web o que aumentava a quantidade de sites na rede. Portanto, na segunda metade da década de 90, a Internet já era uma entidade muito diferente do que era no início daquela década, passando de um empreendimento acadêmico/militar, que até então havia gerado pouco interesse fora das comunidades militares e de pesquisa, para uma rede privatizada e aberta ao tráfego comercial, tendo sido rapidamente transformada em uma esfera privada de mercados fechados e monopolistas, liderado por empresas norte-americanas (CARR, 2016).

Essa transformação se deve a modificação da visão de poder pelos formuladores de política norte-americanos justificável pelo surgimento de um novo conjunto de variáveis que passaram a conduzir a política norte-americana. Estando incluída entre elas a defesa pela minimização do governo e a ascensão a relevância do poder econômico derivado de um paradigma político definido pelo liberalismo e força do livre mercado (CHRISTOPHER, 1993 apud CARR, 2016; LAKE, 1993). Lógica que seria intensificada na administração Clinton-Gore.

3.2 A era Clinton: quando o capitalismo encontra a Internet

A vitória de Clinton e Al Gore na eleição presidencial de 1992 transformou a Internet de ferramenta de uso exclusivo de pesquisadores militares e acadêmicos em um componente fundamental à infraestrutura crítica nacional norte-americana, bem como em um empreendimento econômico de alto valor agregado.

A Internet foi incorporada pela diretriz geral da política econômica do pós guerra-fria, baseada no livre comércio, na abertura comercial e no potencial dos dividendos da paz (CARR, 2016). Nesse contexto um conjunto de políticas foram estabelecidas para gerenciar a transição da Internet de uma rede financiada e operada pelo governo, restrita à pesquisa e educação, para uma rede privada e amplamente acessível e aberta à atividade comercial. Como parte dessa estratégia,

o governo Clinton lançou, logo após as eleições, a *High Perfomance Computing and Communications Initiative* (HPCCI), fundamentada no anteriormente mencionado projeto de lei HPCA elaborado pelo agora vice-presidente Al Gore (CARR, 2016). Essa iniciativa comprometia um maior volume de recursos federais para apoiar o setor de informação e tecnologia, prometendo ampliar o poder competitivo norte-americano. Em 1995, três anos após seu lançamento, a iniciativa tinha um orçamento anual de US$ 1,1 bilhão. (POWERS; JABLONSKI, 2015). O HPCCI era supervisionado pelo President's Council of Advisors on Science and Technology (PCAST), uma equipe de especialistas acadêmicos e do setor privado, dentre eles o vice-presidente sênior da AT&T, uma das principais companhias americanas de telecomunicações. Esse conselho consultivo considerava essencial a comunicação ativa entre o governo e a indústria para a evolução desse mercado. Mediante parcerias público-privadas, o HPCCI conduzia a "transformação da sociedade [americana] através das tecnologias de informação" (POWERS; JABLONSKI, 2015).

A perceptível relevância desse setor à economia norte-americana fez com que em 1993, o HCCA e o HPCCI fossem sintetizados na principal iniciativa de política econômica do governo Clinton, intitulada *Technology for America's Economic Growth* que se comprometia a instituir o equilíbrio de 50/50 na alocação de financiamento federal em pesquisa e desenvolvimento para as áreas de defesa e não defesa. Surgia um novo compromisso com o desenvolvimento tecnológico especialmente centrado no desenvolvimento de uma Infraestrutura Nacional de Informação, as intituladas "superestradas da informação". Essa política parecia se comprometer ainda a impulsionar os principais laboratórios de pesquisa federais a instituírem parcerias comerciais, exigindo que entre 10% e 20% de seus orçamentos fossem alocados para formar novas *joint ventures,* isto é, um acordo para realização de projeto de realização econômica com o setor privado (POWERS; JABLONSKI, 2015). Essa nova política estabelecia uma agenda para tornar a computação de alto desempenho mais acessível.

Para alcançar esse objetivo o governo delineou cinco princípios que serviriam de base para a sua futura política de tecnologia da informação. Esses eram: (i) encorajar o investimento do setor privado, (ii) promover a concorrência, (iii) fornecer acesso aberto à rede para todos os provedores de informações e usuários, (iv) assegurar o serviço universal e, por fim, (v) criar um ambiente regulatório flexível capaz de acompanhar as rápidas mudanças tecnológicas e de mercado (CLINTON; GORE JR, 1993). Havia um amplo interesse do governo em trabalhar com a indústria para desenvolver tecnologias (softwares, computadores e equipamentos de comunicações), pois, como destaca o documento lançado à época:

> "[...]o acesso eficiente à informação está se tornando crítico para todas as partes da economia americana. Bancos, seguradoras, empresas de manufatura e muitas outras operações de negócios agora dependem de links de comunicação de alta velocidade [...] Acelerar a introdução de um sistema de comunicação eficiente e de alta velocidade tem o mesmo efeito no desenvolvimento econômico e social dos EUA do que o investimento público nas ferrovias obteve no século XIX. Fornecendo uma ferramenta crítica em torno da qual muitas oportunidades novas de negócios poderiam se desenvolver (CLINTON; GORE JR, 1993, p. 16-17)

Essas políticas refletiam uma mudança de posicionamento do governo em financiar pesquisa nos Estados Unidos. Se durante a Guerra Fria o modelo industrial era altamente especializado, servindo a um pequeno grupo, uma vez que o incentivo era destinado a pesquisas militares com pouco potencial spin-off, o governo Clinton redirecionou esse financiamento para o incentivo de pesquisas genéricas, cujo efeitos poderiam ser sentidos em todos os setores. Dentro dessa nova lógica, a ARPA ajustou seu foco rapidamente e passou a investir pesado em pesquisas em tecnologias de comunicação que possuíssem um duplo potencial de utilização (POWERS; JABLONSKI, 2015).

Como resgatam os autores Powers e Jablonski (2015), a busca pelo adensamento do crescimento econômico e a segurança nacional passaram a se interseccionar no incentivo dado ao governo para o desenvolvimento das TICs. Resgatando o testemunho do diretor da ARPA à época, Gary L. Denman, para o congresso norte-americano, ficava manifesto que:

> [. . .] Nossa missão [da ARPA] é fazer a transição para uma indústria nacional crescente e integrada capaz de fornecer os sistemas militares mais avançados e acessíveis, e os produtos comerciais mais competitivos. Estamos tentando simultaneamente incentivar dois elementos que se apoiam mutualmente: estimular o crescimento econômico e aproximar as indústrias de defesa e comercial (DENMAN, 1993 apud POWERS; JABLONSKI, 2015, p. 59).

Lançada em 1993, a *Defense Reinvestement and Conversion Initiative* (DRCI) complementava as políticas focadas em redirecionar os recursos federais para além das pesquisas militares. A DRCI traçava um plano de conversão econômica destinado a redirecionar a receita que havia, em períodos anteriores, servido exclusivamente ao financiamento das atividades de Defesa para atividades focadas no incentivo ao desenvolvimento do progresso econômico, vinte quatro bilhões de dólares foram reservado para esse propósito. Essa política fazia parte da percepção crescente de que as necessidades de defesa poderiam ser crescentemente supridas por produtos e tecnologias comerciais (POWERS; JABLOSNKI, 2015).

O incentivo financeiro concedido pela administração Clinton foi acompanhado do gradual estabelecimento de um ambiente regulatório favorável ao chamamento do setor privado a investir na construção do sistema nacional de telecomunicações de alta velocidade que o país

necessitava. A flexibilização regulatória, como a remoção da lei de propriedade de mídia cruzada, regulamento que impedia os proprietários de telefones, cabos e jornais de possuírem e investirem em qualquer uma das outras indústrias de mídia foram estratégias utilizadas pelo governo federal para "limpar da estrada" os destroços de regulamentações obsoletas que impediam o livre fluxo de ideias e comércio (POWERS; JABLONSKI, 2015)

Uma postura mais rígida também foi adotada pelo governo para impelir o setor privado a investir nessa infraestrutura, como por exemplo, a promulgação da Política de Utilização Aceitável (*Acceptable Use Policy* - AUP) elaborada pela NSF. Essa política determinava que o tráfego de rede deveria se restringir à "pesquisa e educação", proibindo a atividade comercial através dessas redes. A comercialização pela Internet estaria condicionada à privatização da infraestrutura da internet, o que em termos práticos significa dizer que o setor privado poderia utilizar essas redes para fins comerciais apenas quando assumisse a sua administração.

Apesar de a Internet ter sido transformada de um serviço público para um setor capitalista na década de 90, foi apenas em 1995 que essa tecnologia foi totalmente e formalmente delegada ao domínio privado, abrindo-se para os negócios.

Os esforços internos em desenvolver e liderar esse mercado foram acompanhados por um posicionamento internacional semelhante. Em discurso realizado na primeira Conferência Mundial de Desenvolvimento das Telecomunicações (*International Telecommunication Union* - ITU), Gore, então vice-presidente, pediu aos governos que priorizassem as cinco diretrizes políticas focadas no incentivo ao desenvolvimento de tecnologias da informação, que ele e o presidente Clinton haviam delineado para a política interna norte americana meses antes. Demandava-se, portanto, indiretamente que o mundo adotasse o modelo de regulamentação de telecomunicações dos Estados Unidos. Como resultado foi elaborada a Declaração de Buenos Aires sobre o desenvolvimento global de telecomunicações para o século XXI lançada em 1995. Essa declaração estabelecia que o desenvolvimento das telecomunicações de informação e comunicação deveriam ser promovida pela liberalização, pelo investimento privado e a competição, colocando, portanto, os princípios do livre mercado como centrais ao desenvolvimento internacional da infraestrutura da internet (POWERS; JABLONKSI, 2015).

Na mesma ocasião foi lançado o projeto *Global Information Infrastructure* (GII) – cujo objetivo era conectar o mundo mediante a desregulamentação do setor de telecomunicações, remoção de proteções comerciais e um aumento no investimento direto estrangeiro por empresas e instituições ocidentais na infraestrutura de comunicação global.

Para Powers e Jablonski (2015), os esforços empreendidos para criar uma Internet universal baseada nas preferências legais, políticas e sociais ocidentais foram movidas por

motivações econômicas e geopolíticas norte-americanas, os tomadores de decisão à época no poder acreditavam que a Internet, uma vez comercializada e privatizada, tinha o potencial de gerar crescimento econômico capaz de sustentar o poder dos Estados Unidos. Portanto, a convite do governo norte-americano a Internet foi fagocitada pelo capitalismo, estando submetida à todas as características estruturantes do processo de acumulação de capital tipicamente norte-americano: o capitalismo monopolista, a lógica das grandes corporações e a interferência da elite do poder (MCCHESNEY, 2013).

3.3 O boom das ponto.com: surgimento da *In-Q-Tel* e o complexo industrial militar informacional

A política instituída na administração Clinton obteve resultados. A área de negócios relacionada ao meio tecnológico passou a crescer exponencialmente em decorrência da percepção de lucro certo atrelado às novas empresas baseadas na Internet categorizadas como empresas ponto.com. A combinação entre o rápido aumento do preço das ações dessas empresas, a confiança de mercado em lucros futuros e a especulação em ações individuais levou ao estouro da bolha especulativa nos anos 2000. O episódio ficou conhecido com bolha da Internet ou bolha das empresas ponto.com, culminando em uma retirada imediata do capital de risco do Vale do Silício.

Contudo, enquanto muitos ficaram consternados com a rapidez com que o setor de tecnologia havia desmoronado, um novo ator vislumbrou a situação como uma oportunidade, sendo este ator a *Central Intelligence Agency (*CIA*)*. Em 1999, a CIA criou uma empresa de capital de risco inicialmente nomeada *de In-Q-It* e posteriormente renomeada para *In-Q-Tel*, cuja missão era investir em *startups* alinhadas com as necessidades de inteligência da agência (LEVINE, 2018; POWERS; JABLONSKI, 2015; ZUBOFF, 2019). A agência percebeu que não poderia acompanhar o ritmo de inovação estabelecido pelo setor privado, e inverteu sua estratégia decidindo não apenas tornar-se comprador de TI, mas também um investidor central dessa tecnologia. A *In-Q-Tel* buscava, portanto, explorar a inovação explosiva e criativa do setor de TI concentrado no Vale do Silício. Em 1997, George Tenet, diretor da CIA declarou "A CIA precisa nadar no Vale", referindo-se, a necessidade desta agência de inteligência dominar as novas tecnologias que surgiam no vale do Silício. Dados levantados apontam que a *In-Q-Tel* financiou mais de 180 empresas e forneceu pelo menos 280 soluções de tecnologia para a comunidade de inteligência.

A instituição dessa empresa de capital de risco caracterizava na percepção dos autores Powers e Jablonski (2015) uma mudança significativa dos esforços até então empreendidos pelo governo para explorar a engenhosidade do setor privado para fins de inteligência. Iniciativas anteriores já haviam explorado esse mercado, contudo, a partir de uma estratégia divergente.

A agência *Advanced Research and Development Activity (*ARDA*),* criada em 1998, tinha a função de avaliar propostas e financiar pesquisas de alto risco e alto retorno projetadas para alavancar tecnologias de ponta focadas em resolver alguns dos problemas mais críticos da Comunidade de Inteligência, com foco especial nas áreas de mineração de dados, processamento de vídeo e computação quântica. A ARDA foi fundada por George J.Tenet à época diretor da CIA e em 1997 a necessidade das agências de inteligência se conectaram com as tecnologias do Vale do Silício. Essa agência atuava, por sua vez, mediante o padrão de concessões e contratos, assistindo a todos os serviços de inteligência do país, incluindo a CIA e o *Federal Bureau of Investigation* (FBI). Seu orçamento fazia parte do Programa Nacional de Inteligência Estrangeira, sendo de caráter confidencial. Uma reportagem lançada pelo New York Times em, um ex-funcionário mencionou que essa agência gastou cerca de US$ 100 milhões em 2003. Utilizando como suporte a sede da NSA, a ARDA, posteriormente seria convertertida no *Disruptive Technology Office* (DTO) mantendo um perfil discreto, financiando de modo silencioso as pesquisas de interesse para a comunidade de inteligência (CAVELTY, 2016; COHEN, 2010)

Um empreendimento ainda mais antigo focado em aproximar atores públicos e privados para incentivar o desenvolvimento de tecnologias capazes de ampliar a capacidade das agências de inteligência nacionais norte-americanas foi a criação do *Highlands Forum* em meados da década de 90. Descrito como uma rede interdisciplinar informal patrocinada pelo Governo Federal e composta por atores chave da indústria, academia e governo, o *Highlands Forum* apoiava o desenvolvimento de políticas e estratégias governamentais de alto nível, especialmente vinculadas à discussão de temáticas na área de “informação, ciência e tecnologia”. (POWER; JABLONSKI, 2015; ZUBOFF, 2019).

Oficialmente criada em 1997 por Richard O Neill, esta iniciativa era descrita como uma ponte entre o Pentágono e as poderosas elites americanas localizadas fora do ciclo militar, em especial os líderes comerciais do Vale do Silício, comportando-se como um espaço de *networking* onde autoridades militares e de inteligência se comunicam com membros da indústria de alta tecnologia, autoridades eleitas, acadêmicos de elite, executivos corporativos e empreiteiros de defesa. Em palestra proferida na Universidade de Harvard, em 2001, O Neill relatou que já em 1994, os formuladores de política norte-americanos se preocupavam-se em

compreender como o conflito poderia surgir em um ambiente marcado pela centralidade da informação, sendo, portanto, o papel principal do *Highland Forum* observar como a informação, e as tecnologias a ela relacionadas, transformariam os cenários futuros de conflito, indicando, qual a melhor estratégia e a política a ser adotada pelo Departamento de Defesa (*Deparment of Defense* - DoD) nesse contexto (COHEN, 2010).

O grupo exercia o papel de um laboratório de ideias do Pentágono (CAVELTY, 2016; COHEN, 2010; POWERS; JABLONSKI, 2015; ZUBOFF, 2019). Os principais tópicos tratados eram (i) segurança e conflito na era da informação, (ii) ciência do futuro, tecnologia e ambiente informacional, (iii) tecnologia informacional e interações da indústria e governo, (iii) proteção das redes de informação, (iv) transformação: mudança organizacional, inovação e estratégia. Essa iniciativa tinha como principal objetivo possibilitar ao Pentágono criar relações duradouras com o poder corporativo, instituindo um ambiente de influência bidirecional, onde empreiteiros privados poderiam influenciar a formulação de políticas, ao mesmo tempo em que o Pentágono torna-se capaz de influenciar o que está acontecendo, e portanto, sendo produzido no setor privado.

A criação da *In-Q-Tel* ia na mesma direção dessas duas iniciativas, qual seja, preencher a lacuna das necessidades tecnológicas da comunidade através do setor privado. Contudo, operando sobre uma lógica distinta e inovadora, através do investimento direto, a criação de *joint ventures*, doação de fundos, tudo de maneira independente da aprovação e da autorização da CIA. Dois critérios guiavam os investimentos realizados pela In-Q-Tel, estes deveriam trabalhar de maneira não classificada e as tecnologias deveriam ter potencial econômico, seguindo a política iniciada durante o governo Clinton. As principais áreas de investimento eram segurança da informação, uso da Internet, arquiteturas de distribuição como métodos para interagir com sistemas personalizados, mecanismos para permitir que aplicativos diferentes interajam, manipulação automática de dados arquivados e conectividade em ampla variedade de ambientes, e por fim, geração de conhecimento como tecnologia de mineração de dados.

A presença da *In-Q-Tel* era bem vista pelo setor privado, em parte, esse bom relacionamento se deve, na percepção de Powers e Jablonski (2015) à porta giratória entre os dois setores. Para além de tal fato, a *In-Q-Tel* comportava-se como um investidor mais prático em comparação a outras empresas de capital de risco, oferecendo sugestões diretas e sistemáticas sobre os produtos em desenvolvimento, além de ter a capacidade de conectar empresas de tecnologia a problemas do mundo real - por meio de seu enorme aparato de inteligência, permitindo que os empreendimentos apoiados pelo seu capital se beneficiassem de pesquisas de campo que de outro modo seriam extremamente caras, e, em muitos casos impossíveis.

Nas palavras de Powers e Jablonski (2015, p.69, tradução nossa) “a *In-Q-Tel* conseguiu tirar proveito de uma época em que o Vale do Silício usava muletas e os investidores estavam receosos em perder bilhões dentro de um mercado jovem e imprevisível”. Outras empresas de capital de risco passaram a perceber a *In-Q-Tel* como um lançador de tendências. O sucesso do empreendimento da CIA serviu de inspiração para outras agências governamentais norte-americanas interessadas em explorar e promover pesquisas inovadoras através do setor privado, dentre elas, o próprio DoD que lançou em 2006 o *Defense Venture Catalyst Initiative* (DeVenCI), projeto responsável por conectar capitalistas de risco do setor privado, projetos de pesquisa e funcionário do regimento militar. Havendo uma inegável presença do governo e dos valores da comunidade de inteligência norte-americana no Vale do Silício (MCBRIDE, 2011).

Este relacionamento próximo e co-dependente cultivado entre o governo dos Estados Unidos e as empresas envolvidas na produção, armazenamento, processamento e distribuição de dados, definidas de maneira geral como indústria da informação instituiu as bases do que seria descrito pelos autores Powers e Jablonski (2015) como o complexo industrial de informacional. Ao que parece, esta é uma referência direta ao conceito de complexo industrial militar cunhado nos anos 60 pelo presidente norte-americano Eisenhower para descrever a colaboração e interseção dos interesses entre governo, militares e empresários na manutenção de um estado de guerra permanente responsável por alimentar a indústria bélica nos Estados Unidos, lucrando com o discurso de promoção à segurança nacional.

Uma variedade de outros autores empregam conceitos correlatos para descrever esta mesma lógica. Complexo militar digital (MCCHESNEY, 2013), complexo de vigilância governamental corporativo (EDWARDS, 2014), complexo industrial da Internet (FLYVERBON; DEIBERT; MATTEN, 2017) e rede de informações industrial militar (COHEN, 2010) são exemplos de outras denominações utilizadas para se referir à esta mesma lógica, qual seja, a interseção do capital e do Estado neoliberal na promoção do surgimento e crescimento de tecnologias voltadas à captação, armazenamento e processamento de informação. Essa lógica estabelecida pelo boom das *ponto.com*, transformando o governo, mais especificamente as agências de inteligência, no principal responsável em investir em tecnologias digitais, se fortaleceria e com os acontecimentos de 11 de setembro, se intensificam os gastos em inteligência (ZUBOFF, 2019). A Internet seria adotada pelas forças militares e pelas agências de segurança nacional que rapidamente perceberiam que a vigilância pode ser feita por computadores e não por seres humanos (NAUGHTON, 2016).

Segundo McChesney (2013), a relação entre o governo e o por ele intitulado “cartel” das ISPs e gigantes digitais era complementar e íntima. Para as agências de segurança nacional as

vantagens dessas parcerias eram claras, o setor privado permitia ao governo realizar vigilância e inteligência doméstica fora da estrutura imposta pelo Congresso, marcado por ordens judiciais. Ademais, o alcance global dessas grandes corporações fornecia aos Estados Unidos acesso a uma quantidade de dados inimaginável e também extraordinários. O status social adquirido pelas grandes corporações de Internet norte-americanas, transformando suas plataformas quase em um recurso vital, as tornavam capazes de obter acesso à categorias de informação até então não imagináveis. Observa-se, deste modo, que a associação com o setor privado também é vantajosa em termos de legitimidade. O recolhimento e o armazenamento de informações pessoais pelo setor privado têm maior aceitabilidade do que quando essas práticas são realizadas pelo governo. Isso deriva de uma precondição imposta pelo mercado do capitalismo de vigilância (SKINNER, 2013 apud BERNAL, 2016, p. 250).

Dentro desse novo mercado, a privacidade se comporta como uma moeda de troca não sendo compreendida como um fim em si mesmo, mas um meio necessário para um bem supostamente maior: o acesso a uma variedade de produtos online considerados socialmente fundamentais. A GAFA, vale lembrar, acrônimo utilizado para se referir às empresas Google, Apple, Facebook e Amazon, construiu um ideário coletivo onde renunciar voluntariamente aos direitos a proteção dos dados pessoais confere acesso a uma série de produtos online. Portanto, diferente da vigilância estatal, a vigilância corporativa é percebida de maneira inofensiva, como uma moeda de troca necessária a obtenção de recursos valiosos (MCCHESNEY, 2013).

Essa relação não se manteria, se não fosse mutuamente vantajosa, isto posto, os grandes gigantes da Internet se beneficiam com a alta lucratividade da venda de seus serviços de dados ao governo, ao incentivo dado pelos setores militares ao desenvolvimento de tecnologias de uso dual e que, portanto, pode ser explorada comercialmente, exemplos são, as hoje mundialmente conhecidas plataformas Google Earth e Google Maps que derivaram de incentivos de pesquisa militar posteriormente compradas pelo capital privado[8]. Além disso, essas grandes corporações possuem vantajosos subsídios do governo e a complacência desse ator para instituir legislações e marcos regulatórios favoráveis a manutenção de seus negócios. Na esfera internacional, os Estados Unidos são um agressivo defensor de livre-mercado, em parte porque o domínio dessas empresas no mercado mundial significa o domínio norte-americano sobre os dados em circulação no mundo. Ademais, o governo é como uma força policial privada para essas empresas, pois, desenvolvem políticas que pretendem proteger a propriedade intelectual dos Estados Unidos

[8] Em 2004 a empresa Google.Inc adquiriu a empresa de mapeamento por satélite Keyhole que serviu de espinha dorsal ao projeto Google Earth, Google Maps e o aplicativo Street View Project. A empresa *Keyhole* havia sido patrocinada pela empresa de capital de risco da CIA, *In-Q-Tel.* Cf. Powers e Jablonski (2015).

através da defesa de suas patentes e direitos autorais. Nesse sentido, o curso racional para essas empresas, mesmo que não estejam diretamente envolvidas com as agências militares e de segurança nacional, é cooperar com o Estado de segurança nacional, e porque não dizer, de vigilância estabelecido. (MCCHESNEY, 2013).

Isto posto, para que essa lógica continue operando é necessário que o governo mantenha essa relação vantajosa, pois, como estas instituições estão baseadas na maximização dos lucros, não há dúvidas de que a venda de ferramentas de vigilância e dados para outras nações se apresentem como uma alternativa. Nessa toada, a avaliação da política interna norte-americana, é de extrema relevância, pois, nos permite compreender o jogo de poder entre as grandes corporações de internet e o poder norte-americano. Esse relacionamento tem impacto direto na expressão do poder internacional dos Estados Unidos. Nas palavras de McChesney (2013, p.164, tradução nossa): "o domínio da Internet pelas mãos do monopólio, bem como o surgimento de uma estrutura em nuvem que liga toda a internet, é perfeita ao governo. Este precisa lidar apenas com um pequeno grupo de gigantes para efetivar seu controle sobre a Internet".

Dando continuidade às reflexões acima manifestas nos dedicaremos agora a compreender como a ascensão de um estado de máxima alerta à preservação da segurança nacional, criada pelos atentados de 11 de setembro, reverberaram na relação anteriormente descrita baseada na instituição de um complexo informacional industrial cada vez mais direcionado à vigilância, possibilitado não apenas pelo incentivo ao desenvolvimento de pesquisas e tecnologias voltadas a essa prática, mas também pautada na instituição de um campo legal propício ao seu florescimento.

3.4 A era Bush: o combate ao terrorismo e a intensificação da cibervigiliância

Os atentados de 11 de setembro promoveram mudanças significativas na política norte-americana. O discurso de securitização em torno da *"guerra ao terror"* criou um cenário de exceção responsável por restringir no âmbito interno os direitos fundamentais dos cidadãos norte-americanos em nome da segurança nacional. O contexto de exceção transformava medidas excepcionais em medidas jurídicas, um claro exemplo foi a legalidade conferida à vigilância sistemática praticada, inclusive, sobre os cidadãos norte-americanos solapando seu direito à privacidade garantida pela quarta emenda da Constituição dos Estados Unidos (MCADAMS, 2005).

Internacionalmente, o estado de exceção se fez manifestar através das guerras preventivas, baseadas na reformulação ou ampliação da busca por uma invulnerabilidade em

termos de segurança. A base estratégica dessa nova política estava pautada na lógica de prevenção e de antecipação da ocorrência de eventos perturbadores, o que recaí, impreterivelmente, em uma inteligência cada vez mais eficaz. A inteligência passou a adquirir um caráter "acionável", exigindo que uma quantidade indefinida de informações fosse captada e armazenada para que pudessem ser utilizadas de maneira oportuna (GANDY, 2012, p. 125). A captação de informações de maneira direcionada, focada em alvos unitários, parecia não mais contemplar os objetivos estratégicos do novo século muito menos as diretrizes do poder norte-americano. Nesse sentido, as guerras preventivas foram seguidas pela instalação e propagação de um novo aparato de segurança em aeroportos, em zonas de fronteira, nas grandes metrópoles mundiais. Tecnologias como câmeras, detecção biométrica, mapeamento e monitoramento através de satélites com o poder de registrar imagens para controles territoriais e populacionais passaram a ser amplamente difundidas (MCADAMS, 2015; POWERS; JABLONSKI, 2015).

Historicamente, a prática de vigilância estrangeira era prevista constitucionalmente pelo ordenamento jurídico norte-americano através da *Foreign Intelligence Surveillance Act* (FISA) aprovada em 1978. Essa lei federal estabelecia os procedimentos para a vigilância física e eletrônica praticada pelo governo norte-americano durante o processo de coleta de informações de governos e agentes de poder estrangeiro. Sob a regulamentação da FISA, a atividade de inteligência dos Estados Unidos era regulada pelo Tribunal de Vigilância de Inteligência Estrangeira (*Foreign Intelligence Surveillance Court* - FISC) responsável por supervisionar e autorizar os pedidos de mandado de vigilância por parte das agências policiais e de inteligências federais criando, no ideário político e social norte-americano, um maior equilíbrio entre a política de inteligência norte-americana e o princípio de respeito à privacidade.

Com a evolução do discurso securitizador em torno do combate ao terrorismo, a legislação FISA passou a ser percebida como limitada, uma vez que a necessidade de instituição de um tribunal para julgar a pertinência das ações de vigilância manifestava-se como um impedimento à garantia de resultados positivos no campo da inteligência. O governo e as agências de inteligência norte-americanas voltaram-se, no pós 11 de setembro de 2001, a uma necessidade crescente da captação de toda e qualquer informação disponível com a maior rapidez possível, o congresso procurou remover o "muro" que a FISA impunha à exequibilidade dessa prática. O resultado disso foi a atribuição de legitimidade à uma série de mecanismos legais capazes de ampliar a vigilância, sendo a legislação *"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism",* mais popularmente conhecida como *Patriot Act*, ou em português, Ato Patriótico, o grande representante legal da

nova política interna e externa de vigilância inaugurada após o 11 de setembro nos Estados Unidos.

Sobre o *U.S Patriot Act*, George W. Bush afirma:

> Esta nova lei que assino hoje [U.S Patriot Act] **permitirá a vigilância de todas as comunicações usadas por terroristas incluindo e-mails, Internet e telefones celulares**. A partir de hoje, poderemos enfrentar melhor os desafios tecnológicos impostos por essa proliferação da tecnologia das comunicações. O povo americano precisa saber que **estamos coletando muita informação** e estamos gastando muito tempo tentando reunir o máximo de inteligência possível para perseguir cada pista, para percorrer cada dica para que possamos manter a América segura. E isso está acontecendo (PRESIDENT…, 2001, tradução nossa, grifo nosso).

Assinado em 26 de outubro de 2001, o *Patriot Act* representa uma somatória de leis que ampliava o poder de ação das agências federais e órgãos de inteligência norte-americanos em relação à investigação e à vigilância de atores estrangeiros e nacionais. A seção 215 do *Patriot Act* modifica a mencionada legislação FISA, que exigia que o único objetivo da vigilância das comunicações eletrônicas dos Estados Unidos fosse estrangeiro. O *Patriot Act* criou um filtro muito menos rigoroso permitindo que as agências governamentais coletassem informações de inteligência estrangeira de cidadãos americanos e não americanos, além de excluir a necessidade da instituição de um julgamento de pertinência antes da prática de captação de informações como era previamente estabelecido (PETRELLA, 2014).

O *Patriot Act* não deixou de identificar o potencial das redes digitais aos seus propósitos de vigilância e controle. Até o 11 de setembro de 2001, as regras que regiam a vigilância digital encontravam-se em um limbo legislativo. Segundo Powers e Jablonski (2015), o interesse urgente do governo norte-americano em obter acesso à maior quantidade de informações possíveis rapidamente extravasou para as redes de comunicação vinculadas à Internet. Evidências de que os terroristas do 11 de setembro haviam usado a Internet para reservar as passagens aéreas, aprender sobre o aeroporto, realizar pesquisas sobre aplicação inicial de pesticidas, além de terem realizado centenas de trocas de e-mails em inglês, árabe e urdo[9], contendo informações sobre o ataque, levaram o governo norte-americano a compreender o papel vital da Internet, e portanto, a necessidade de intensificar o debate sobre o monitoramento governamental e a necessidade do compartilhamento de informação entre os divergentes órgãos de polícia e inteligência do governo norte-americano. Diante desse cenário, uma preocupação em identificar padrões de comportamentos de usuários da internet se intensificou dentro das

[9] Língua indo-europeia da família indo-ariana que se formou sob influência persa, turca e árabe no sul da Ásia durante a época do sultanato de Deli e do Império Mongol.

áreas de tecnologia da informação das comunidades de inteligência e contraterrorismo dos Estados Unidos.

Deste modo, após os ataques terroristas, o governo Bush e suas agências de inteligência entraram em *hiperdrive*, buscando adquirir qualquer e toda informação que pudesse potencialmente ajudar a prevenir ataques terroristas, resultando em uma verdadeira massificação das práticas de cibervigilância e ciberespionagem no século XXI (GUNDALINI; TOMIZAWA, 2013, p. 33; WOLOSZYN, 2016)

Em termos legais, a seção 216 do *Patriot Act* ratificava um comportamento mais permissivo à coleta de metadados de telefonia e de comunicação em rede ao tornar a "lei de registro" ou, em inglês, *"pen register"* aplicável a dispositivos que rastreiam "informações de discagem, roteamento, endereçamento ou sinalização". A referida lei de registro permitia, em sua versão original, que o governo demandasse das empresas de telefonia que operavam nos EUA registros detalhados de chamadas contendo informações sobre a data, hora, local, duração e interlocutores envolvidos, desde que existisse uma "suspeita razoável e articulável" de que tais informações serviriam para identificar um grupo terrorista estrangeiro. Como destaca Petrella (2014), o *Patriot Act* ampliou o escopo dessa legislação, passando a registrar os IPs (*Internet Protocol*), os protocolos de comunicação usados entre todas as máquinas em rede para encaminhamento dos dados. A aplicação da lei de registros passará a permitir, portanto, que os agentes da lei obtenham autorização inclusive para monitorar o uso de e-mail de um suspeito.

O uso da lei de registro para vigilância na Internet é especialmente problemático, pois o resultado de sua aplicação se manifesta de modo muito diferente de quando utilizado para monitor as atividades por telefone (WELLS, 2003). Isso se deve às próprias características da Internet. Quando uma pessoa faz uma ligação telefônica, o conteúdo da comunicação é separável dos dados transacionais usados para conectar-se a outro telefone. A Internet funciona, por sua vez, de maneira contrária usando uma tecnologia conhecida como comutação de pacotes. Essa tecnologia divide os dados em pequenos pacotes de informações que são transferidos e remontados na ordem correta no computador designado a receber a mensagem. Isto posto, esse tipo de tecnologia não permite que a lei de registro cumpra seu fundamento central, qual seja, separar os dados transacionais do conteúdo das informações trocadas. Deste modo, uma agência de aplicação de lei que utilize a lógica da lei de registros para monitorar o uso de um endereço de e-mail por um indivíduo suspeito, acabaria por receber os dados transacionais e os dados de conteúdo desse indivíduo (WELLS, 2003).

Nas palavras de Wells (2003):

> O *Patriot Act* dos EUA transformou a lei de registros de uma ferramenta passiva de vigilância em um instrumento intrusivo mediante o qual investigadores do governo poderiam expor detalhes particulares das atividades de uma pessoa na internet antes que haja uma causa provável de que pessoa esteja conectada a atividades criminosas ou terroristas (WELLS, 2003, p. 53, tradução nossa).

Outras disposições polêmicas presentes no *Patriot Act* impactavam a privacidade em ambiente online, inclusive legalizando a instituição de programas que posteriormente seriam expostos pelas declarações de Edward Snowden como sinônimo de uma vigilância indiscriminada. Por exemplo, o *Patriot Act* autorizava o FBI implementar o programa *Carnivore*, um sistema de computador que poderia ser conectado a um provedor de serviços de internet e acessado remotamente por um link. Esse programa poderia ser configurado para interceptar e gravar comunicações digitais com objetivo de combater ameaças terroristas. O mecanismo de funcionamento deste programa gerava, no entanto, preocupações sobre a capacidade deste *software* ser suficientemente preciso e capaz de evitar que o monitoramento da atividade de atores suspeitos levasse a interceptação de informações de outros usuários, interferindo, portanto, na sua privacidade e promovendo, deste modo um recolhimento massivo de informações (DEVRIES, 2003, p. 294-95).

Para além do *Patriot Act*, a instituição de um arcabouço legal capaz de construir um terreno fértil à prática de vigilância se estendeu ao longo dos dois mandatos da administração Bush. Em 2005, o jornal New York Times lançou um artigo intitulado *"Bush Lets U.S Spy on Callers Without Courts"* tornando público que meses após os ataques de 11 de setembro, o presidente Bush havia secretamente autorizou a NSA a espionar americanos e outras pessoas localizadas nos Estados Unidos sem a necessidade uma aprovação prévia obtida através de mandado aprovado em tribunal, como exigia os casos de espionagem doméstica (RISEN; LICHTBLAU, 2005).

Mesmo após declarações de violação foram aprovadas duas legislações que flexibilizavam, ao invés de restringir as práticas de captação de informações, sendo estas a *Protect America Act de 2007* e as emendas instituídas à legislação FISA em 2008, legislação intitulada *FISA Amendments Act of 2008* (FAA).

O *Protect America Act* em *2007* promulgada como lei em 5 de agosto de 2007 pelo Presidente Bush é uma emenda feita a legislação FISA. Essa lei removia o requisito de mandato para vigilância governamental de alvos estrangeiros que "se acreditava" estarem localizados fora dos Estados Unidos, além de permitir que empresas americanas cooperassem com as atividades de inteligência, fornecendo ao governo informações ou assistência, sem a necessidade de notificar seus clientes ou assinantes, permitindo, ainda, que os atores privados que cooperassem

com o governo fossem compensados. As ferramentas fornecidas pela *Protect America Act* expiravam, no entanto, em 16 de fevereiro de 2008. Nesse contexto, o congresso aprovou em 2008 a FAA, um novo conjunto de emendas a já mencionada legislação FISA.

Dentre as alterações realizadas instituía-se uma extensão das informações que poderiam ser captadas, diminuindo a necessidade de descrições detalhadas da natureza das informações ou do objeto visado pela atividade de vigilância. Além das flexibilizações da prática vigilância sob um americano localizado fora dos Estados Unidos. A nova emenda estabelecia que a vigilância sem mandato nesses casos passaria de 7 dias para 48 horas, se a corte da FISA fosse notificada e recebesse uma solicitação assinada por funcionários específicos vinculados ao setor de inteligência, autorizando este ato. A FAA é descrita como a base legal para os programas de vigilância divulgados por Edward Snowden em 2013, incluindo o PRISM. A FAA é descrita como a base legal para os programas de vigilância divulgados por Edward Snowden em 2013.

As disposições contidas na lei também apresentam pontos positivos ao setor privado. Como praticamente toda a infraestrutura de comunicações nos EUA pertencia ou era operada por atores privados, como permanece sendo no presente, o governo não poderia deixar de considerar uma parceria robusta com esses atores, criando uma cláusula benéfica aos interesses dos intitulados intermediários de vigilância nesta lei. A FAA previa, portanto, a concessão de imunidade às empresas (liberdade de responsabilidade) caso contribuíssem com o governo, criando uma barreira para várias ações judiciais destinadas a expor e impedir os supostos abusos de poder e atividades ilegais do governo federal.

Ficava estabelecido que:

> Nenhuma causa de ação caberá em qualquer tribunal contra qualquer provedor de serviço de comunicação eletrônica por fornecer qualquer informação, instalações ou assistência de acordo com [uma ordem / solicitação / diretiva emitida pelo Procurador Geral ou o Diretor da Inteligência Nacional [28] (U.S. GOVERNMENT, 2008, tradução nossa).

Essa disposição se demonstrou altamente vantajosa a empresas como a AT&T que haviam sido alvo de uma variedade de processos após enunciadas como cúmplice da vigilância sem mandato praticada pela NSA. Como destaca Elliot Cohen (2010), já a partir de 2002 a AT & T que à essa época já dispunha de serviços baseado na Web, o intitulado *worldnet* - concordou em fornecer à NSA acesso completo à sua infraestrutura de telecomunicação global, redirecionando o tráfego de Internet do usuário para equipamentos de mineração de dados. No período mencionado foi firmado um acordo entre a NSA e a AT&T para a instalação do *Narus* STA 64000 – um analisador de tráfego de dados que coletava informações de uso da rede em tempo real e produzia análise. Esse analisador ficava instalado no canal de mensagens, ou seja,

na nuvem do provedor de Internet, ao invés de se conectarem a cada roteador ou provedor (COHEN, 2010). A NSA obtinha acesso a uma quantidade massiva de informações.

A FAA permitia que, portanto, que a agência de inteligência nacional continuasse a cooperar com o setor privado, contudo, respaldada por parâmetros legais. Ao mesmo tempo as disposições contidas na lei possibilitavam que os atores privados cooperassem sem medo de violar acordos de usuários e ir contra a "Lei de Comunicações" estabelecida em 1934. Respaldadas legalmente as três maiores empresas de telecomunicações dos EUA, AT&T, Comcast e Verizon continuaram a compartilhar dados de chamadas com a NSA (COHEN, 2010).

As flexibilizações na capacidade legal de praticar vigilância pelo governo foi acompanhada pela ausência de uma evolução das leis de proteção à privacidade no ambiente digital. Em retrospectiva histórica, em 2000, a *Federal Trade Commission (FTC)*, havia concluído que a autorregulação das políticas de privacidade pelas empresas provedoras de serviços e produtos de internet não seria suficiente para proteger os consumidores em ambiente digital decidindo propor uma legislação federal para regulamentar a privacidade on-line. Rapidamente essa iniciativa foi solapada pelos acontecimentos do 11 de setembro, responsável por ordenar o foco predominante da privacidade para a segurança. Essa nova ênfase fez com que o congresso norte-americano perdesse o interesse em regulamentar a utilização da informação adquirida em ambiente online no setor privado, pois este se apresentava com um potente aliado aos serviços de inteligência nacionais (ZUBOFF, 2019).

O abandono em instituir uma regulamentação de privacidade mais rígida em ambiente online criou, nas palavras da autora Shoshana Zuboff (2019), um terreno fértil ao crescimento e consolidação do capitalismo de vigilância. Para Zuboff (2019), caso a regulamentação proposta pela FTC tivesse sido levada adiante, teria imposto restrições que caso traduzidas em lei transformariam os pressupostos básicos à operacionalização do capitalismo de vigilância em práticas ilegais ou pelo menos sujeitas a avaliação e contestação pública. Apesar de não nos debruçarmos na avaliação deste arcabouço legal, dedicado às políticas de privacidade em ambiente online, desejamos destacar que mesmo os Estados Unidos sendo uma das nações mais tecnologicamente desenvolvidas e digitalmente conectadas, bem como detentoras dos principais monopólios da internet, pouco evoluiu na institucionalização de uma política interna para proteção à privacidade de dados, ou adquiriu protagonismo internacional na discussão sobre essa temática.

No país, a proteção da privacidade em ambiente online, em nível federal, continua sendo enquadrada em legislações instituídas em um contexto político, social, econômico e tecnológico completamente diverso, incorrendo em inadequações que mais mascaravam a aquisição de

informação de maneira indevida do que protegem a privacidade do usuário. Nesse sentido, apesar de algumas disposições legais favoráveis a uma vigilância mais agressiva tenham expirado, como é o caso, das disposições contidas no *Patriot Act*, não podemos dizer que uma evolução significativa foi obtida na proteção da privacidade do indivíduo em detrimento da segurança quando debatemos o ciberespaço, essa questão será melhor explorado no capítulo 4. Por hora, desejamos destacar como a administração Bush instituído um terreno legal, onde

3.4.1 *Total Information Awareness* (TIA): a precursora tecnológica da vigilância em massa

Desde que o intitulado ataque terrorista de 11 de setembro de 2001 foi compreendido como resultado de uma falha na capacidade do governo norte-americano em captar informações e produzir inteligência, a solução encontrada foi garantir que o governo norte-americano nunca mais faltasse com esse conhecimento, ocorrendo uma natural vinculação entre o poder e a capacidade de estabelecer uma vigilância sem precedentes.

A vigilância havia sido assegurada por mecanismos legais, contudo, ainda era necessário ampliar a capacidade tecnológica dos Estados Unidos em fomentar essa prática. Revelado ao mundo em 2002, o intitulado *Total Information Awareness* (TIA) foi um projeto desenvolvido pelo *Information Awareness Office* (IAO), vinculado a DARPA, cujo objetivo era revolucionar a capacidade dos EUA de detectar, classificar e identificar terroristas – possibilitando que os EUA tomassem medidas oportunas para antecipar e derrotar com sucesso os atos terroristas (BALL; WEBSTER, 2003; GOLDENBERG, 2002).

Tecnicamente, o TIA era um metaprograma projetado para agregar sinais gerados por meio de outros programas executados pelo IAO, estando dentre suas funções realizar pesquisas, analisar informações, minerar dados, traduzir o conteúdo e reconhecer padrões para o desenvolvimento de modelos descritivos e preditivos capazes de antever ataques terroristas. Esse programa foi incorporado no orçamento norte-americano no ano de 2003 e previa a participação de cerca de nove entidades governamentais norte-americanas, dentre elas a NSA. Até maio do referido ano ele operou sob esse título, sendo renomeado, posteriormente para *Terrorism Information Awareness*.

Rapidamente, o projeto TIA levantou preocupações relacionadas ao desrespeito à privacidade. À época, a ACLU categorizou esse programa como um “arrastão virtual” uma vez que exigia que o governo coletasse o máximo de informações possíveis sobre todos, mantendo essas informações armazenadas em grandes bancos de dados. A pressão fez com que o programa fosse formalmente suspenso. Contudo, o software de mineração de dados desenvolvidos no

contexto dessa iniciativa foi adotado por outras agências governamentais. Em termos práticos, e não mais legais, o projeto TIA continuaria em desenvolvimento, agora financiado pelo orçamento classificado e tendo sido dissolvido em vários componentes, estes em sua maioria transferidos para o controle gerencial da NSA.

Em artigo lançado pelo jornal *New York Times* em 2012, com base nas informações disponibilizadas por Snowden, tornou-se de conhecimento público que o legado do *Total Information Awareness* continuou florescendo na NSA (HARRIS, 2012). Para além da incorporação da lógica de operação do programa TIA em outras agências do governo norte-americano, a lógica instada por esse projeto foi delegada à operacionalização pelo setor privado. De acordo com os autores Foster e McChesney (2014), os observadores mais atentos da política norte-americana facilmente perceberam que diante da pressão exercida pelo congresso a DARPA e a NSA deslocaram o programa para a iniciativa privada.

Expedições secretas ao Vale do Silício em busca de novas tecnologias de *data mining* e *data warehousing* passaram a ser realizadas. A promessa econômica da tecnologia do Big Data passou a integrar o vale do silício com força. As grandes corporações tornaram-se responsáveis por alimentar o formalmente extinto projeto TIA, mediante a captação de uma diversidade de informações como histórico de compras com cartão de crédito, registros médicos, registros bancários, informações de passagens aéreas, aluguel de carros dentre outros. O governo, para explorar seus enormes bancos de dados, passou a realizar contratos com essas empresas. A lógica de excepcionalismo baseado, dentre outros, princípios, na ampliação da vigilância permitiu que um número considerável de empresas de TICs lucrassem com contratos governamentais, sobretudo na área de inteligência, situação que foi favorecida pela já mencionada revogação de medidas mais restritivas de proteção de privacidade na Internet (FOSTER; MCCHESNEY, 2014).

Nesse contexto, empresas especializadas nesse mercado como a *ChoicePoint*, a *Oracle Corporation* e grandes corporações da Internet descritas como repositórios de informações pessoais, como as empresas *Google. Inc e Facebook.Inc* encontraram um nicho muito favorável ao seu crescimento. A intersecção entre a lógica do capitalismo de vigilância e o estado de vigilância já manifesto em momentos anteriores, criava raízes mais profundas. A anteriormente mencionada empresa *ChoicePoint.Inc* desempenhou um papel de extrema relevância para a efetivação desse objetivo durante o governo Bush. Essa empresa, especializada em uma *data warehousing*, foi capaz de alavancar sua receita de mercado com base na comercialização de dados pessoais de milhões de cidadãos norte-americanos (COHEN, 2010).

Diferente da lógica empregada pela empresa *Google.Inc*, a *Choice Point* obtinha os dados que comercializava através de uma variedade de entidades governamentais como, por exemplo, registros de previdência ou mediante compra de dados de outras entidades privadas a exemplo de empresas especializadas em sistemas de pagamentos. Essa empresa não mascarava o tipo de negócio que desempenhava, comportando-se como verdadeira empreiteira de vigilância, o que na visão de Eliot Cohen (2010) é menos problemático e violador do direito à privacidade do que aquela que se estabelece quando avaliamos a parceria do governo como empresas como *Google.Inc*.

Empresas que seguem o modelo de negócios do Google estão pautadas no capitalismo de vigilância, ou seja, apesar de serem conhecidas pelos serviços gratuitos que disponibilizam, como por exemplo, mídia social, mecanismos de buscas, provedor de e-mail, elas obtém receita mediante comercialização dos dados gerados a partir da interação dos usuários com seus serviços. Dito isso, uma amplitude de usuários que se utilizam do mecanismo de buscas do Google não obtendo plena consciência de que seus registros de pesquisa e, portanto, suas preferências pessoais, estariam sendo armazenados e comoditizados pela empresa. No caso dessas empresas, apesar de possuírem um *front-end*[10] totalmente diverso dos programas de vigilância colocados em prática pelo governo, aparentando serem totalmente inofensivas, o *back-end*[11] é extremamente semelhante a programas como TIA.

Em audiência realizada em abril de 2018 no Congresso norte-americano a Senadora Democrata Maria Cantwell abordou a semelhança entre o projeto TIA e a coleta de informações privadas realizadas, hodiernamente, pelas grandes corporações de Internet. Sua reflexão foi realizada em ocasião à audiência feita com o dono da empresa Facebook.Inc, Mark Zuckerberg, após as acusações auferidas a ocasião do episódio da Cambridge Analytic, levantando a reflexão sobre como as grandes corporações hodiernamente acumulam um nível de poder que os americanos negaram à DARPA.

Nas palavras de Newton Lee (2014), as empresas privadas e a onipresença das redes sociais como Facebook, Google, Twitter e Youtube estão criando tecnologias e infraestruturas necessárias para colocar em prática, através de mecanismos civis, a proposta de projeto desenvolvido pela DARPA em 2002. Reconhecimento facial, rastreamento de localização, aplicativos sociais com rastreamento GPS e mineração de dados são alguns elementos chaves

[10] Trata-se da interface da página web que interage diretamente com o usuário.
[11] Trata-se da parte secundária referente às linguagens de programação e comandos que formam a base de dados responsável por criar uma página web.

para a efetividade de um programa com as características do TIA. Havendo um claro entrelaçamento entre tecnologias militares e civis.

Dentre outros fatores, essas parcerias e/ou troca de experiências entre setor público e privado apenas se concretizaram em decorrência do ativo mecanismo de portas giratórias existentes entre o *establishment* de inteligência e os contratantes do setor privado (COHEN, 2010; POWERS; JABLONSKI, 2019; ZUBOFF, 2019). A empresa ChoicePoint.Inc, por exemplo, mantinha uma ativa porta giratória com antigos, e em breve contratados funcionários da administração Bush. Seu quadro de executivos ou sócios associados incluíam o Secretário de Estado Adjunto, o Vice-Diretor da Agência de Segurança Nacional, o Diretor de Contra Terrorismo e Contra Inteligência e o Procurador Geral Adjunto e autor da Lei Patriótica dos Estados Unidos, Viet Dinh. Com a empresa Google. Inc não era diferente.

Um grande número de ex funcionários do governo se juntariam à empresa Google.Inc após anos de serviços prestados. A título de exemplo Rob Painter, ex diretor de avaliação tecnologia da *In-Q-Tel* deixaria em 2004 a CIA para se tornar gerente federal sênior da empresa Google. Inc. Em 2010, Jared Cohen, ex- consultor da Secretaria de Estado Hillary Clinton e um dos principais elaboradores da doutrina de liberdade da Internet do Departamento de Defesa, diretriz da política externa para Internet durante o governo Obama, deixaria sua função para se tornar diretor de ideias do Google. Em 2012, a diretora da DARPA, Regina Dugan, deixaria seu cargo para se tornar chefe de projetos especiais em informação e poder nesta empresa.

O mesmo era verdade para o movimento contrário onde ex-funcionários do Google deixavam a empresa para ocupar cargos importantes no governo. Andrew McLaughlin deixou o cargo de especialista em políticas do Google para servir com vice-diretor de tecnologia na Casa Branca durante a administração Obama. Segundo dados levantados pelo *Tech Transparency Project* (TTP), de 2006 a 2016, um total de 197 funcionários do Governo norte-americano, onde se inclui ex-membros da Casa Branca, agências administrativas, agências independentes, congresso e campanhas, foram para a empresa *Google.Inc* e empresas relacionadas. Em comparação, 61 portas giratórias foram identificadas no sentido oposto (i.e. do *Google.Inc* para o governo norte-americano). No que se refere especificamente à relação entre a Casa Branca e a empresa *Google.Inc*, um total de 53 portas giratórios foram estabelecidas, contabilizando 22 ex-funcionários da Casa Branca que deixaram o governo para trabalhar no Google e 31 Executivos do Google (ou empresas relacionadas que ingressar na Casa Branca ou foram nomeados para conselhos consultivos federais (TECH TRANSPARENCY PROJECT, 2016).

A avaliação das portas giratórias entre a empresa *Google.Inc* e o governo norte-americano, apesar de manifestar-se como uma pequena amostragem, deixa a clara a presença da

lógica de porta giratórias entre essas duas categorias de atores, havendo uma clara troca de interesses e fluxo de influência.

3.4.2 O financiamento da liberdade na Internet no tempo da vigilância

Ao mesmo tempo em que implementavam políticas destinadas a facilitar e legitimar a obtenção de informações pelo governo, como relatado no tópico anterior, o Governo Bush herdou do governo Clinton sua política em prol da liberdade de Internet ao redor do mundo. Em 2006, o Departamento de Estado norte-americano, liderado pela então Secretária de Estado, Condolezza Rice, estabeleceu a *Global Internet Freedom Task Force* (GIFT), iniciativa cuja função primária era "monitorar e responder às ameaças à liberdade de expressão na internet" (U.S. GOVERNMENT, 2006). Essa força de trabalho tinha como objetivo maximizar a liberdade de expressão e o livre fluxo de informações e ideais, minimizar o sucesso dos regimes repressivos na prática de censura e silenciamento do debate legítimo além de promover o acesso à informação e ideias pela Internet.

Desde seu lançamento, a GIFT desenvolveu uma robusta estratégia global responsável por expandir as fronteiras da liberdade na Internet, consequentemente ampliando o acesso a essas redes. A estratégia do GIFT era organizada em torno de três prioridades: monitoramento, resposta e expansão do acesso à internet (U.S. GOVERNMENT, 2006). Defender a liberdade de internet significava monitorar como os países em todo o mundo tem se comportado diante dessa questão, mas também construir respostas como, por exemplo, atuando em coordenação com parceiros internacionais, expandindo os compromissos de liberdade na Internet em organizações multilaterais, reportando diretamente aos governos estrangeiros sobre os graves incidentes de repressão cometidos e também trabalhando conjuntamente com *stakeholders* – indústrias de tecnologia, organizações não governamentais (ONGs) e outras partes interessadas em um processo destinado a desenvolver princípios compartilhados para orientar as atividades do setor privado em economias restritivas.

Incorporada a essa política estava a promoção do acesso expandido à Internet e a disponibilidade de tecnologias de informação e comunicação em países em desenvolvimento, o que interessava fortemente o setor privado. Uma variedade de programas do governo dos Estados Unidos, incluindo projetos da USAID e do *Telecommunications Leadership Program* e parcerias público-privadas como a *Digital Freedom Initiative*, atendiam a esse objetivo (POWERS; JABLONSKI, 2015). No ano de 2004, registrou-se um gasto de cerca de US$ 250 milhões do governo norte americano em projetos que incluem o fornecimento de infraestrutura de

telecomunicações, acesso à Internet, hardware de computadores. O programa contava, deste modo, com um fundo de doações. Um montante de cerca de US$ 500.000 era disponibilizado para propostas e abordagens de ponta para combater a censura na Internet em países que buscam restringir os direitos humanos básicos, incluindo a liberdade de expressão. (POWERS; JABLONSKI, 2015).

Nas palavras de Goldsmith (2018), a administração Bush tornava o governo norte-americano aberto a prática de pagar e promover "tecnologias da liberdade". O Governo Bush estava pagando caro para desenvolver uma iniciativa diplomática de alto perfil capaz de moldar a internet e, ao disseminar seus tradicionais valores de proteção à democracia e aos direitos humanos, criar uma lógica totalmente fértil à expansão dos seus grandes monopólios de tecnologia, ao mesmo tempo em que internamente buscava flexibilizar a política que permitia que esses monopólios lhe concedessem acesso indiscriminado aos seus bancos de dados. A administração Obama daria continuidade a essa política, mediante a instituição do intitulado *21st Century Statecraft* seguindo, com as devidas transformações, um direcionamento político iniciado ainda na administração Clinton, e perpetuada no governo Bush, qual seja, o constante compromisso com a expansão da Internet aberta, permitindo que as grandes corporações e a infraestrutura norte-americana atinjam um alcance crescentemente global.

Esta doutrina pontua que o crescimento acelerado da disponibilidade e do poder das tecnologias de informação é responsável por transformar as relações internacionais, bem como, as condições para o governo no século XXI. O crescimento contínuo das redes de comunicação permitiu que as nações abrissem novos mercados, desenvolvessem novas políticas tecnológicas e criassem novas estratégias para reagir a formas disruptivas de ameaças.

A então Secretária de Estado Hillary Clinton enfatizou que até o presente momento uma só tecnologia não tinha gerado uma mudança de paradigma simultânea no campo do comércio, das comunicações pessoais e da mídia em massa, criando um ambiente complexo no interior do qual as principais estruturas da sociedade convergem em uma única infraestrutura comum não existindo, nas palavras da Secretária de Estado uma internet econômica, uma internet social e uma internet política, mas, apenas uma internet fazendo com que quem detenha o poder sobre sua estrutura adquira um poder até então não imaginável (POWERS; JABLONSKI, 2015).

Diante da relevância deste domínio, Hillary Clinton defendeu ativamente a necessidade da preservação de uma Internet Livre, apoiando na liberdade de expressão, no direito à privacidade e a garantia de conectividades.

Em trecho de seu discurso Clinton afirma que:

> [...] as modernas redes de informação e as tecnologias que elas suportam podem ser aproveitadas para o bem ou para o mal. As mesmas redes que ajudam a organizar movimentos pela liberdade também permitem que a Al Qaeda vomite o ódio e incite à violência contra os inocentes. E tecnologias com o potencial de abrir o acesso ao governo e promover a transparência também podem ser sequestradas pelos governos para acabar com a dissensão e negar os direitos humanos. (DICKINSON, 2010, tradução nossa).

Ainda nesse contexto, Hillary Clinton pontua que "Por conta própria, as novas tecnologias não tomam partido na luta pela liberdade e pelo progresso, mas os Estados Unidos o fazem" (DICKINSON, 2010, tradução nossa), enfatizando que a política norte-americana do século XXI se volta para o exterior em prol da defesa de uma única Internet, onde toda a humanidade tenha acesso igual ao conhecimento e ideias.

Observa-se, deste modo, que a batalha pela liberdade na Internet, ou Internet aberta, tem sido definida como uma questão sensível dentro das discussões sobre segurança cibernética, e, portanto, segurança nacional. Singer e Friedman (2014) argumentam que essa temática tem se transformado inclusive em um objeto de embate dentro da seara internacional, uma vez que diferentes Estados nutrem percepções distintas sobre essa questão. Países como a China, veem a censura e a restrição a conteúdo online como mecanismos estratégicos para sua política de segurança nacional. Deste modo, algumas tecnologias, como, por exemplo, mídias de comunicação social, foram categorizadas pela China e seus aliados em fóruns internacionais como ferramentas para ataques cibernéticos. Como pontuamos ainda no início dessa dissertação a associação entre a atuação das empresas norte-americanas, em especial grandes empresas de telecomunicações como o Google é visto por uma variedade de Estados, dentre eles a China, como uma ameaça à sua soberania nacional, permeando as discussões já mencionadas sobre soberania digital e autonomia digital.

Diante desse cenário as discussões sobre internet aberta e liberdade na internet se transformam em uma questão importante dentro das relações internacionais, apresentando-se de maneira associada a outros debates de fundamental relevância, como por exemplo, a respeito da proteção da soberania versus autoritarismo, manutenção da segurança nacional e a instrumentalização das grandes corporações de Internet em mecanismos de vigilância estatal.

Os Estados Unidos destacam-se pelo seu posicionamento em prol de uma Internet aberta. Como enfatizado em secções anteriores as primeiras iniciativas empreendidas nesta direção foram realizadas ainda durante a administração Clinton, quando duas diretrizes se consolidaram centrais à política externa norte-americana para internet, quais sejam, (i) a defesa de uma atitude pouco reguladora do Estado no processo de desenvolvimento das estruturas da Internet priorizando a atuação do setor privado em seu desenvolvimento e (ii) a garantia de liberdade de

expressão, criando um espaço onde as ideias pudessem ser expressas incluso aquelas que carregavam o *american way of life* no ambiente global (GOLDSMITH, 2018). Esse projeto impreterivelmente se associava ao aumento da riqueza das empresas norte-americanas e de seu alcance global que para além de conferir poder econômico, ampliava a capacidade estratégica e geopolítica nos Estados Unidos ao formar um cartel da internet composto quase que exclusivamente por empresas norte-americanas.

O domínio sob este mercado hoje significa o domínio sobre os dados que circulam ao redor do mundo, sendo esses um dos principais recursos de poder da geopolítica atual. Como pudemos vislumbrar, o posicionamento da administração Obama, pelo menos em relação à sua política externa para internet, se manteve similar a de seus antecessores estando baseada na alavancagem de seu setor privado de internet a partir da promoção dos valores de liberdade e democracia associados a essa tecnologia.

4 GOVERNO OBAMA: O DIFÍCIL EQUILÍBRIO ENTRE PRIVACIDADE E SEGURANÇA NO CIBERESPAÇO

Apesar de ter assumido a presidência dos Estados Unidos durante um período de convulsão política, em decorrência da crise do subprime e da manutenção de uma *"guerra ao terror"* em duas frentes (Iraque e Afeganistão), a administração Obama não negligenciou a política cibernética. Na realidade, seu governo foi o primeiro a construir um arcabouço legal em torno das questões cibernéticas enquanto problema independente de segurança nacional. Até então a pauta de segurança cibernética havia sido inserida nos Estados Unidos de maneira associada a outros debates centrais, como por exemplo, a proteção da infraestrutura crítica no governo Clinton e o combate ao terrorismo no governo Bush.

Como prova de seu comprometimento com essa temática, o presidente Barack Obama, em momento imediatamente posterior à sua posse, demandou ao Conselho de Segurança Nacional (NSC) e ao Conselho de Segurança Interna (CSI) uma revisão das principais diretrizes da política de segurança cibernética dos EUA, ou seja, do chamado projeto *Comprehensive National Cybersecurity Initiative* (CNCI), lançado em janeiro de 2008 pelo presidente Bush[12]. Essa revisão deveria ser inicialmente cumprida em 60 dias, contudo, foram gastos 90 dias para a conclusão da tarefa. O objetivo era estabelecer uma nova abordagem para o tratamento das questões cibernéticas, através de uma estratégia *top-down*, de cima para baixo, fortemente coordenada pelo governo federal. Nas palavras de Obama:

> A partir de agora, nossa infraestrutura digital – as redes e os computadores que dependemos todos os dias – será tratada como deveria: como um ativo nacional estratégico" [..] "proteger esta infraestrutura será uma prioridade de segurança, vamos garantir que essas redes sejam seguras, confiáveis e resistentes. Vamos deter, prevenir, detectar e defender contra-ataques e recuperar rapidamente de qualquer interrupção ou dano" (TEXT... 2019).

Os resultados obtidos foram publicados em maio de 2009 em documento intitulado *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure.* documento responsável por instituir que o "status quo não era mais aceitável" (U.S. GOVERNMENT, 2014) para lidar com essas questões, sendo fundamental e inevitável uma revisão nas estruturas políticas e na distribuição de responsabilidades na coordenação de políticas para defesa e segurança do ciberespaço. Diante dessa necessidade de reformulação, o

[12] Essa iniciativa descreve as metas de segurança cibernética dos Estados Unidos, instituindo inclusive o papel de uma variedade de agências na operacionalização de políticas no ciberespaço, como por exemplo, o papel do Departamento de Segurança Interna, o Escritório de Gerenciamento e Orçamento e a Agência de Segurança Nacional.

documento sinalizava a pretensão da Casa Branca em encarregar-se em primeira instância da segurança cibernética. Essa pretensão teria consequências práticas como, por exemplo, a criação em 29 de maio 2009 de uma posição na Casa Branca de Coordenador de Segurança Cibernética, popularmente conhecido como CyberCzar. Howard Schmidt – ex-executivo da Microsoft, assumiu o cargo em dezembro do mesmo ano, seguindo a tendência de portas-giratórias entre as grandes corporações de internet e o governo norte-americano, a essa altura já conhecida na política dos Estados Unidos (PHILLIPS, 2009).

Apesar de puxar para si a responsabilidade de coordenar e orientar as políticas de segurança cibernética, o documento reforçava a impossibilidade de lidar sozinho com essa problemática, reforçando, deste modo, a importância de colaboração com outros setores da sociedade civil, inclusa uma ativa participação do setor privado. Era intenção primária do presidente Barack Obama, ao publicar sua Estratégia de Segurança Cibernética, alardear o papel e liderança do setor privado para a instituição de uma política de segurança cibernética verdadeiramente eficiente mantendo, deste modo, uma postura iniciada em outras administrações (Clinton e Bush) que colocavam as parcerias público-privadas como o *hub* da promoção da segurança no ciberespaço (CARR, 2016).

Em discurso proferido Obama pontuou:

> Nós fortaleceremos as parcerias público-privadas que são críticas para este empreendimento. A grande maioria de nossas infraestruturas críticas informacionais pertencem e são operadas pelo setor privado. Então deixe-me ser muito claro: meu governo não ditará normas de segurança para empresas privadas. Pelo contrário, vamos colaborar com a indústria para encontrar soluções tecnológicas que garantam a nossa segurança e promovam nossa prosperidade (U.S. GOVERNMENT, 2009)

Contudo, segundo Coldebella e White (2010) antes de ser possível institucionalizar um programa de segurança cibernética bem sucedido a administração Obama deveria confrontar e resolver dois problemas classificados como espinhosos sendo o primeiro um problema burocrático – isto é, a dificuldade em definir quem se tornaria o responsável final perante o Presidente e o público pela implementação efetiva e legal do programa de segurança cibernética e o segundo referia-se a uma questão de legitimidade, ou seja, quais ferramentas técnicas "o povo americano" se mostraria confortável em ver o governo implementando. Sem uma discussão franca sobre limites, o público poderia justificadamente relutar em apoiar o programa. Esses fatores exerceriam interferência direta no equilíbrio a ser instituído entre privacidade e segurança quando se debate políticas para o ciberespaço.

Segundo Mitchell (2018), Obama estava claramente intrigado com este desafio e ciente do estado perigoso do campo de disputa referente a essa temática. O Departamento de Segurança

Interna – instituído na administração anterior – e a Agência de Segurança Nacional realizavam, na descrição do autor um verdadeiro cabo de guerra na tentativa de obter maior controle sobre a política cibernética. Apesar do DHS ter sido definido, em 2007, através do *Homeland Security Presidential Directive 23 (HSPD23)* e da *National Security Presidential Directive 54 (NSPD/54)* como o principal órgão responsável pela coordenação de todos os ativos de cibersegurança dos Estados Unidos, tanto nos setores federal quanto privado, sua escolha era questionada dentro e fora do governo, argumentando-se que as funções delegadas ao DHS melhor se encaixariam à comunidade de inteligência, dada a alta expertise da NSA defender as redes de alta tecnologia dos Estados, ou ainda que essas funções deveriam ser desempenhadas pelo DoD ou pela Casa Branca (COLDEBELLA; WHITE, 2010).

O 11 de setembro, intensificaria a disputa entre o DHS e a NSA pela coordenação das práticas de segurança cibernética, em especial no tocante à questão de quem seria a grande receptora das informações compartilhadas pelo setor privado para fins de segurança cibernética. A comunidade de inteligência tinha amplo interesse na administração do ciberespaço, visto que, o mesmo é fonte inesgotável de inteligência. Nas considerações de Nojeim e Laperruque (2015), é importante que a responsabilidade da coordenação das políticas de segurança cibernética, incluso a prática de compartilhamento de dados, estivesse atribuída ao Departamento de Segurança Interna ao invés de uma agência de inteligência como a NSA ou uma agência militar , como o DoD pois, o DHS, por tratar-se de uma agência civil, dispõe de mecanismos de controle e supervisão mais adequados em casos de violação à privacidade enquanto que agências como a NSA operam longe dos olhos do público.

O reconhecimento e aceitação dessa autoridade não apenas pelos atores governamentais como também privados tornava-se cada vez mais urgente. Somente após essa definição seria possível estabelecer as diretrizes da necessária parceria com o setor privado, bem como evoluir, na institucionalização de práticas consideradas de fundamental relevância ao alcance de uma segurança cibernética mais efetiva, como por exemplo, a definição das diretrizes da prática compartilhamento de informações entre setor público e privado para fins de segurança cibernética.

Essas discussões chegaram também ao congresso. Os legisladores norte-americanos, diante dos ataques cibernéticos que se adensavam durante a administração Obama, com especial destaque para o ataque feito à empresa Sony Pictures[13], concordavam que reformas abrangentes

[13] Em resposta ao lançamento do filme "a Entrevista" que retrata uma paródia do governante norte-coreano, Kim Jong Un, um grupo de hackers invadiu os sistemas de computador do entretenimento da Sony Pictures em outubro de 2014, roubando enormes quantidades de documentos confidenciais do estúdio de Hollywood e os

eram necessárias para proteger tanto os sistemas de informação privados quanto os governamentais, no entanto, divergências sérias sobre os detalhes dessas políticas se apresentavam em decorrência da existência de um congresso muito fragmentado (KOMINSKY, 2014). Dentre os pontos de embate e divergência de opiniões se destacam as discussões sobre o papel do governo federal na implementação de políticas de cibersegurança, a já mencionada responsabilidade e as capacidades do DHS no tocante a essa temática, o papel do setor privado enquanto parceiro e as diretrizes de compartilhamento de informação entre o setor público e privado para fins de segurança cibernética.

Na medida em que as ameaças e a tecnologia evoluíram em sofisticação e amplitude, as propostas legislativas do Congresso se tornavam mais desatualizadas. A necessidade de proteger um sistema que em sua maioria está sob posse do setor privado e que comporta-se não apenas como infraestrutura crítica fundamental às atividades estratégicas do Estado, mas também como um espaço de troca e interação social, fez emergir questionamentos de como uma agenda legislativa e regulamentar nos Estados Unidos deveria negociar entre segurança e privacidade (SIVAN-SEVILLA, 2017). Novamente enfatizamos que a decisão dessas questões no âmbito político nacional norte-americano tem efeitos transnacionais. As características impostas pelo próprio ambiente digital, associado ao protagonismo que os Estados Unidos dispõem quando avaliamos a infraestrutura e o mercado global da Internet, fazem com que a institucionalização de práticas que regulamentem a relação do governo norte-americano com seus grandes monopólios de Internet tenham impacto internacional em decorrência do alcance global de suas empresas.

Deste modo, a promoção da segurança cibernética se manifesta como um dilema de segurança multidimensional e multifacetado que se estende além do Estado e de sua interação com outras entidades estatais, incluindo ponderações que envolvem também a relação Estado e setor privado e Estado e sociedade civil, sempre levando-se em consideração o impacto internacional de decisões nacionais. Nesse sentido, compreender como os governos gerenciam os riscos no ciberespaço demanda analisar como a escolha entre segurança e privacidade está sendo feita pelo setor público, e como o setor privado tem se posicionamento diante dessas questões, avaliando o impacto internacional de escolhas realizadas a nível interno.

A sociedade do Big Data, como discutido no primeiro capítulo, trouxe modificações ao valor econômico da informação, onde uma nova categoria de atores privados passou a gerar

---

publicaram on-line nas semanas seguintes – expondo-os a todos, desde possíveis cibercriminosos a jornalistas que estudavam os documentos e relatavam tudo, desde os detalhes de produções recentes de filmes até a extensão dos dados dos funcionários vulneráveis na Internet. Cf. Peterson (2014).

receita mediante a comercialização de dados pessoais, fazendo com que qualquer legislação voltada a regulação, mesmo que tangencial, da prática de captação, armazenamento e disponibilização de dados passasse a angariar o interesse direto desses atores.

Uma variedade de leis que impactam a privacidade e a cibersegurança passaram a ser incluídas no congresso dos Estados Unidos, antes mesmo das declarações de Edward Snowden. Dentre elas, incluímos a *Cyber Intelligence Sharing and Protection Act* (CISPA) aprovada na Câmara pela primeira vez em abril de 2012. Esse projeto de lei e objeto de estudo deste trabalho, possibilitaria o compartilhamento voluntário de informações entre o governo e as empresas privadas da Internet, gerando preocupação nas organizações defensoras da liberdade civil em ambiente online que identificavam em seu texto imprecisões que poderiam incorrer na violação ao direito de privacidade, não somente de cidadãos norte-americanos, mas também em uma perspectiva global. Dentre suas disposições previstas está a concessão de proteção de responsabilidade às empresas que venham compartilhar informações com o governo norte-americano. A legislação CISPA foi escolhida como objeto de análise nesta pesquisa exatamente por ser uma legislação de segurança cibernética que suscita a necessidade de ponderação entre privacidade e segurança. Essa legislação mobilizou a atenção de grandes empresas de internet, elevando os gastos de lobby do setor de internet. A título ilustrativo no primeiro trimestre de 2013, um total de 192 organizações registraram prática de lobby na legislação CISPA, apresentando o quinto valor mais alto em comparação a qualquer outro projeto de lei no mesmo trimestre (VENDITUOLI, 2013).

Durante sua tentativa de aprovação no congresso norte-americano que se seguiu de 2011 a 2015, ressurgindo mesmo quando se acreditava que a legislação havia sido completamente derrotada, a legislação CISPA esbarrou nas declarações de Edward Snowden responsáveis por impactar diretamente no posicionamento de governos e mercados a respeito da equação entre privacidade e segurança em ambiente online. A tentativa, por sua vez, de institucionalizar a prática de compartilhamento de informações entre setor público e privado não se limitou a Câmara dos Deputados, encontrando espaço também no Senado, onde foi inserida a *Cybersecurity Information Sharing Act*, mais uma vez tendo como autores do projeto de lei representantes da comunidade de inteligência. Contudo, será apenas em 2015 que uma vitória nessa direção seria obtida, o que conduz aos seguintes questionamentos: o que mudou? Quais foram os fatores intervenientes? Qual é a participação do setor privado? Os próximos tópicos têm como objetivo esclarecer essas questões.

4.1 *Snowdenleaks*: a segurança cibernética no centro da arena internacional

As denúncias realizadas em 2013 pelo ex-funcionário da *Central Intelligence Agency* (CIA) e da *National Security Agency* (NSA), Edward Snowden, afetaram diretamente como o Governo Obama lidaria com as questões cibernéticas. A revelação de que os Estados Unidos operavam um esquema de vigilância interno e internacional com o apoio das grandes empresas provedoras de serviço de internet norte-americanas colocou em tela a forte dependência da comunidade de inteligência norte-americana em relação à infraestrutura e aos sistemas de comunicação do setor privado, bem como gerou forte desconfiança da comunidade internacional em relação à neutralidade das principais empresas provedoras de serviços de internet norte-americanas.

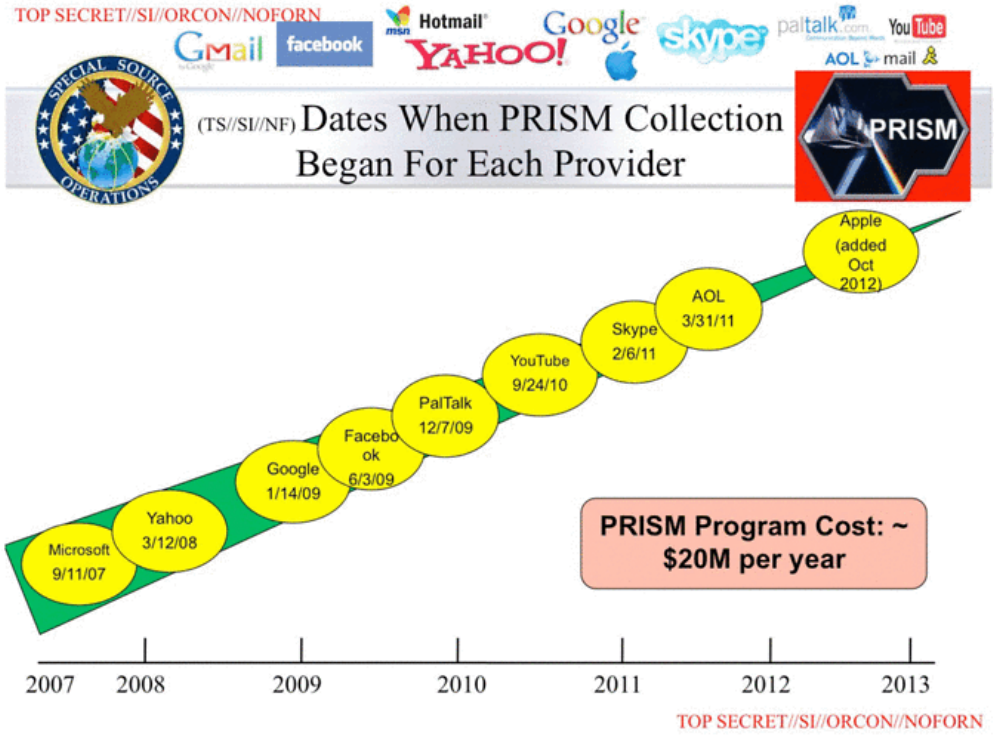
Como esclarece Simcox (2015), as revelações chocaram muito mais pela denúncia de forte colaboração e envolvimento de importantes *players* da Internet global, como as empresas Apple, Google e Facebook, do que pela existência de um esquema de vigilância interno e internacional operacionalizado pela NSA, ainda que fosse contestável e que esteja até o presente momento pouco esclarecido até que ponto esse setor realmente contribuiu com a exequibilidade dessa prática.

De acordo com os documentos publicizados a vigilância realizada pela NSA se estabelecia através da intercepção de dados em trânsito ou mediante a parceria com o setor privado. Dependendo, neste segundo caso, da complacência desse setor para sua efetivação. A intitulada coleta por *Upstream* se refere ao primeiro caso, residindo na intercepção de dados através das redes de cabo de fibra óptica intitulados *"backbones* da internet", em uma definição simplificado, cabos que transportam as informações referentes a dados de telefone e internet do destinatário ao receptor. Esse tipo de coleta ocorre durante o processo de transmissão e se estabelece através da inserção de interceptores ao cabo de fibra óptica, permitindo a captação das informações que estão em circulação. Em linhas gerais, a realização desta prática não demanda complacência ou conhecimento do setor privado.

Já o programa PRISM, que ficou internacionalmente conhecido, envolve a aquisição de informações pessoais por meio de pressões exercidas sobre empresas privadas que regularmente coletam grandes quantidades de dados pessoais para fins comerciais, incluindo, dentre esses dados pessoais: históricos de pesquisas, conteúdo de e-mails, transferências de arquivos, vídeos, fotos, registros de chamadas de voz e vídeo, logins e quaisquer outros dados em poder destas "empresas de Internet" (GREENWALD; MACASKILL, 2013).

Segundo os documentos divulgados por Snowden, incluso um conjunto de slides aparentemente voltado ao treinamento de funcionários dos serviços de inteligência das agências do governo norte-americano, o programa PRISM é executado mediante colaboração com uma série de prestadores privados norte-americanos de serviços de internet como *Microsoft*, *Google*, *Yahoo*, *Facebook*, *Paltalk*, *YouTube*, *Skype*, AOL, *Apple* e empresas de telecomunicações, como *BT*, *Vodafone Cable*, *Verizon Business*, *Global Crossing*, *Viatel* e *Interroute* (GREENWALD; MACASKILL, 2013). A imagem a seguir, bem como a tabela apresentada, listam as empresas, e a data, que essas haviam aderido ao programa PRISM.

Imagem 1 - Slide listando as empresas e as datas nas quais se junta ao PRISM



Fonte: Greenwald e MacAskill (2013)

Tabela 1 – Tabela contendo a lista de companhias envolvidas no programa PRISM e descrição de data

Companhia	**Início da Cooperação**
Microsoft	11 de setembro de 2007
Yahoo.Inc	12 de março de 2008
Google.Inc	14 de janeiro de 2009
Facebook.Inc	3 de junho de 2009
PalTalk	07 de dezembro de 2009
Youtube	24 de setembro de 2010
Skype	6 de fevereiro de 2011
AOL	31 de março de 2011
Apple	Outubro de 2012

Fonte: Powers e Jablonski (2015)

O programa PRISM era, portanto, responsável por coletar dados que posteriormente seriam analisados e armazenados através de outros programas de vigilância voltados a prática de *data mining*. Graças ao setor privado o governo não precisava se ocupar da atividade de captação de informações, delegando às grandes empresas de internet essa função, visto que a concessão de informações pessoais de usuários para a utilização de um serviço online e a retenção dessas informações pelas entidades privadas era naturalmente percebida como uma moeda de troca.

Outros programas de espionagem também foram tornados públicos. O programa *"Fairview",* um programa de vigilância em massa da NSA estabelecido após o 11 de setembro, foi descrito como capaz de ampliar a capacidade do governo de coletar dados de telefone, internet e e-mail acessando os dados diretamente de computadores e telefones celulares dos cidadãos de países estrangeiros. Documentos iniciais destacavam a forte colaboração de uma empresa de internet junto a esse programa sem, contudo, nomear qual seria tal empresa. Mais tarde identificada como a AT&T em um relatório produzido pelo ProPublica[14] em parceria com o New York Times (GELLMAN; POITRAS, 2013).

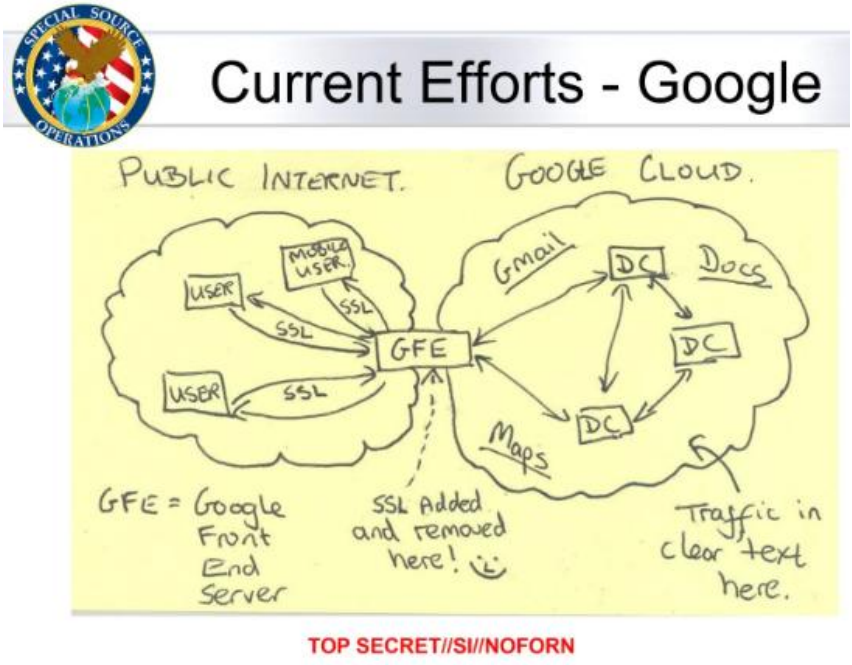
O também descrito programa MUSCULAR ganhou proeminência e gerou forte desconforto principalmente com a empresa Google.Inc. Este programa de vigilância global

[14] É uma corporação sem fins lucrativos com sede em Nova York. Descreve-se como uma redação independente que produz jornalismo investigativo de interesse público. Em 2010 tornou-se o primeiro portal de notícias da internet a vender um Prêmio Pulitzer.

operado de maneira associada com o serviço de informações britânico – GCHQ (como já tradicionalmente ocorria dentro dos outros programas) – invadia secretamente os principais enlaces de comunicações dos centros de processamento de dados da empresa *Yahoo! e Google.Inc,* tendo acesso aos dados da nuvem de ambos.

Imagens de uma apresentação de slide preparada pela divisão de Operações Especiais da NSA sobre "acesso de parceiros corporativos" foram publicadas, deixando claro que a agência dependia de "parcerias corporativas-chaves" para lograr sucesso diante dessas práticas. De acordo com uma nota estilo post-it inserida na apresentação de slide, a captação de informações pelo serviço de inteligência norte-americano só era possível graças ao fato de que as informações que circulavam de um datacenter para o outro, de empresas como a *Google.Inc*, não eram criptografados (imagem 2) (GELLMAN; POITRAS, 2013; GREENWALD et. al, 2013).

Imagem 2 - Slide da apresentação da NSA sobre a exploração do Nuvem do Google.



Fonte: Gellman e Soltani (2013)

A partir dessas revelações, tornava-se visível a instrumentalização dessas grandes corporações pelo governo norte-americano para fins de inteligência. Nas palavras de Bruce Schneier (2015, p. 60, tradução nossa) "A NSA não construiu um sistema massivo de intercepção da Internet a partir do zero, mas percebeu que o mundo corporativo já estava construindo e dele se aproveitou". Os documentos da NSA revelados por Snowden mostram,

deste modo, como a NSA transformou grandes corporações de internet de abrangência global em um aparato de coleta de inteligência, tudo com a ajuda dessa própria indústria (LEVINE,2018).

Ainda, nesta linha argumentativa, destacamos a reflexão de Edward Snowden:

> O governo dos EUA coopta o poder corporativo dos EUA para seus próprios fins. Empresas como Google, Facebook, Apple e Microsoft se reúnem com a NSA. [Eles] fornecem à NSA acesso direto aos *back-ends* de todos os sistemas que você usa para se comunicar, armazenar dados, colocar coisas na nuvem e até enviar felicitações de aniversário, mantendo um registro de sua vida. Eles dão acesso direto à NSA, para que não precisem supervisionar, para que não sejam responsabilizados por isso (HARDING, 2014, p. 143)

Diante das alegações de Edward Snowden as agências de inteligência argumentavam que seus programas eram constitucionais e sujeitos a rigorosa supervisão do congresso e do judiciário, pontuando que o segredo é essencial para atingir seu objetivo primordial de proteger o público contra ataques terroristas. Apesar das respostas internacionais ao abuso norte-americano contra o direito de privacidade em ambiente online, tendo como expressão máxima a resolução lançada pelo Brasil e Alemanha na Organização das Nações Unidas (ONU) condenando a vigilância ilegal e arbitrária, o congresso norte-americano relutou em aprovar qualquer legislação abrangente que buscasse regulamentar a proteção de dados no país, situação que persiste até o momento.

Berço dos principais players da internet, o país não possui até o presente momento uma legislação federal que regulamente a proteção de dados em seu território. Segundo Eichensehr (2017), essa negligência se justifica no interesse do governo em manter acesso especial a dados privados visando a segurança nacional e a aplicação da lei, bem como uma tentativa de não se indispor com o setor privado. O mais recente avanço obtido no país no tocante à essa temática foi a recente aprovação da *California Consumer Privacy Act* (CCPA), em 2018, contudo, sua aplicabilidade se restringe ao âmbito estadual. Essa legislação exige que as empresas dos Estados Unidos contemplem os residentes do Estado da Califórnia com uma série de iniciativas que resguardem seu direito à privacidade de dados.

Em vigor desde primeiro de janeiro de 2020, a lei se aplica a todos os negócios que coletam e vendem informações pessoais do consumidor ou divulgam dados pessoais para fins comerciais no Estado da Califórnia, mesmo que a empresa não esteja localizada fisicamente neste Estado. Dentre os direitos garantidos pela legislação consta (i) o direito à transparência sobre a coleta de dados pessoais, (ii) o direito a ser esquecido, (iii) o direito de optar pela não venda de seus dados. Direitos que podem incorrer em obstáculos significativos para as *Big Techs* e sua economia de dados baseada no capitalismo de vigilância. Contudo, apesar de seus efeitos

positivos essa legislação não impede realmente as empresas de coletarem informações pessoais ou de armazenarem essas informações, de modo que caso um usuário demande que a empresa exclua seus dados, não há nenhum impeditivo de que ela comece a coletá-los novamente na próxima vez que este se utilizar de seus serviços. Para além de tal fato, a proteção fica a cargo do exercício requerente do consumidor (STATE OF CALIFORNIA, 2018).

Essa é, portanto, uma legislação com impacto positivo à proteção da privacidade de dados, que sem dúvida apresenta limitações. Apesar de seu efeito positivo, foi homologada apenas em 2020 e não em 2013 momento de convulsão à discussão da privacidade e da prática de vigilância irrestrita pelo governo norte-americano com o setor privado.

A despeito da resistência em instituir legislações verdadeiramente restritivas à prática de vigilância, o governo Federal não pode à época ignorar totalmente tais acontecimentos. Buscando diminuir o déficit de confiança gerado com as declarações de Edward Snowden, o presidente Obama lançou em 17 de janeiro de 2014 uma *Presidential Policy Directive* nº28 reconhecendo expressamente o direito global à privacidade (U.S. GOVERNMENT, 2014b). Ainda dentro deste escopo, o governo Obama criou o *Privacy Shield Agreement*, em cooperação com o governo da União Europeia[15]. Acordo responsável por reger as transferências de dados comerciais entre os Estados Unidos e a União Europeia (UE). Esse acordo criava dentro do Departamento de Estado um cargo intitulado *ombudperso*n responsável por tratar de reclamações da UE sobre a vigilância dos Estados Unidos. Contudo, esse acordo carecia de normas e mecanismos de aplicação mais efetivos, a ausência de especificações sobre os poderes do *ombudsperson*, acabava por impactar na capacidade desta pessoa verificar as práticas da comunidade de inteligência, o que resolvia apenas parcialmente o problema (PRIVACY SHIELD FRAMEWORK, 2020).

A necessidade de atenção a essas políticas se deu, dentre outros fatores, pela pressão do setor privado. De acordo com Poitras (2013), em suas manifestações públicas esse setor empresarial expressava forte indignação perante a capacidade das agências de inteligência norte-americanas em acessar seus sistemas e colher suas informações, mesmo que membros da própria NSA afirmassem que a ação da agência através do programa PRISM tenha sido realizada com consciência e consentimento desse setor (GELLMAN; POITRAS, 2013). O posicionamento público das grandes empresas de comunicação era racionalmente compreensível, pois as revelações geravam amplo risco de prejuízos econômicos.

[15] Cf. Privacy Shield Framework (2020)

Apesar de estarmos vivendo dentro do chamado “capitalismo de vigilância” ou em claro período de comoditização da informação, parte da cultura empresarial dessas *Big Techs* está pautada na confiança que o usuário tem em se utilizar de seus serviços. Sendo necessário manter a ideia ilusória de que suas informações estão protegidas, pelo menos da vigilância estatal.

A resposta das grandes empresas de Internet foi, portanto, imediata. Em 1º de junho de 2013 o diretor jurídico do Google, David Drummond, encaminhou uma carta ao procurador geral dos EUA e ao Diretor do FBI pedindo permissão para publicar “números agregados de solicitações para obtenção de informações sob seu domínio para fins de segurança nacional, incluindo divulgações sob a lei FISA. O Google foi a primeira empresa a se expressar de maneira tão incisiva publicamente sob o episódio. (ASKING…, 2013). Drummond comunicou que a empresa tem feito esforços significativos para proteger as informações de seus usuários, mas se vê constantemente impelida pelo governo a retroceder nessas práticas.

Na carta enviada pontua que:

> O Google trabalhou tremendamente nos últimos quinze anos para ganhar a confiança de nossos usuários. Por exemplo, oferecemos criptografia em todos os nossos serviços; contratamos alguns dos melhores engenheiros de segurança do mundo; e temos sido constantemente empurrados para trás com solicitações do governo excessivamente amplas para a obtenção de dados de nossos usuários (ASKING…, 2013, tradução nossa).

Ainda em suas considerações David Drummond afirma que a empresa de fato atende às solicitações do governo que sejam legalmente válidas para obtenção informações de seus usuários, contudo, são falsas as alegações da imprensa sobre a benevolência da empresa com solicitações do governo para obter acesso irrestrito aos dados de seus usuários. As especulações seriam justificadas por um mal entendido gerado pelas obrigações de confidencialidade impostas à empresa, em especial, a respeito de solicitações realizadas sob a lei FISA, sendo, portanto, de fundamental importância para implementação de políticas que permitam incluir também divulgações demandadas pela FISA. Drummond assevera que os números mostrariam claramente que a empresa Google. Inc tem agido em conformidade com essas solicitações e que as acusações estão muito aquém das reivindicações feitas, de maneira que a empresa não tem nada a esconder (ASKING…, 2013).

Medidas eram necessárias para retomar a confiança pública e preservar sua fatia de mercado. Em 2010 o Google instituiu uma iniciativa intitulada *Google Transparency Report*, cujo objetivo é divulgar relatórios sobre o número de compartilhamento de dados de seus usuários com entidades governamentais em comparação ao número de pedidos de

compartilhamento de dados feitos pelas entidades governamentais à empresa, sob a justificativa de otimizar a segurança nacional (GOOGLE TRANSPARENCY REPORT, 2020).

O apelo realizado pela empresa *Google. Inc* seria reiterado por outras companhias como as empresas Facebook e Microsoft. Em *post* realizado no *twitter,* o conselheiro geral do Facebook, Ted Ullyot, concordou com as declarações realizadas pelo diretor jurídico do Google, afirmando que o Facebook adoraria fornecer um relatório de transparência, a exemplo daquele realizado pelo Google, contudo, não atingiria os resultados esperados, pois se trataria de um relatório enganoso em decorrência das restrições impostas pelo governo em publicizar os pedidos de concessão de informação feitos através da legislação FISA (BOHN, 2013).

Outro caminho estabelecido pelos atores privado para recuperar sua credibilidade foi instituir uma resistência técnica especialmente através da criptografia responsável por gerar um efeito inibidor na capacidade de vigilância das agências de inteligência e aplicação da lei norte-americanas em captar informações em trânsito nas redes do setor privado. Esse tipo de empreendimento impossibilitava que programas de vigilância como o UPSTREAM, baseados na lógica de intercepção de dados através dos cabos de fibra-óptica, obtivesse êxito. Para Tréguer (2019), esse tipo de iniciativa por parte das empresas poderia ser interpretado como uma maneira de garantir que a vigilância da comunicação de seus usuários só ocorresse com o seu conhecimento e consentimento, o que impreterivelmente alavancaria seu papel no campo da segurança e seu poder político. Perante essa lógica, o relacionamento entre as *Big Techs* e o governo precisava começar a ser repensado. Não era vantajoso ao governo norte-americano, e às suas pretensões de inteligência, que as empresas norte-americanas perdessem legitimidade.

Ainda na visão de Tréguer (2019) o episódio em questão foi responsável por gerar um efeito paradoxal na sociedade, pois ao mesmo tempo em que as declarações de Edward Snowden foram responsáveis por promover um debate crítico sobre a capacidade de vigilância ilegal estabelecida pelos serviços de inteligência, o episódio foi concomitantemente responsável por direcionar os formuladores de políticas rumo à legalização dessa prática buscando findar com o sentimento anti-vigilância sem, contudo, abrir mão definitivamente dessa prática através de regulamentações rígidas de proteção à privacidade.

Muitos membros do congresso acreditavam que após as divulgações de Snowden surgia a necessidade de uma restauração da confiança do público, exigindo, portanto, mudanças legislativas voltadas à restrição da autoridade do governo federal em praticar vigilância. Nesse contexto, mais de 20 projetos de lei foram escritos desde o início das divulgações com o objetivo de esclarecer os poderes de vigilância do governo, ao mesmo tempo em que buscava conferir legalidade e legitimidade a esta prática e não extingui-la.

Para Tréguer (2019), a legislação mais significativa deste novo contexto foi a *USA Freedom Act*, aprovada no senado em uma votação de 67 a 32 e promulgada apenas em junho de 2015, um dia após a *USA Patrioct Act* expirar. Essa legislação apesar de suas provisões a favor de um maior respeito à privacidade, não findava com vigilância. Dentre as medidas adotadas a favor da privacidade podemos mencionar a proibição da coleta em massa de dados de clientes por agências governamentais de inteligência, aumentando a transparência do governo em relação a *Foreign Intelligence Surveillance Court* (FISC) e a autorização para que as grandes empresas de tecnologia como Google, Facebook, Yahoo informassem ao público em geral informações sobre quais, e quantos, dados de seus usuários haviam sido repassados para as agência de inteligência. Contudo, a *USA Freedom Act* é percebida como contendo várias concessões pró vigilância, permitindo que a NSA continuasse sua coleção massiva uma vez que não extingue a seção 702 da Lei de emendas da Fisa. Na visão dos grupos opositores, se a lei não proíbe a vigilância em massa, ela torna-se responsável por corroborar com essa prática (KAYYALI; TIEN, 2014).

O projeto foi originalmente apresentado em ambas às casas do congresso dos Estados Unidos em 29 de outubro de 2013 em resposta às declarações de Edward Snowden. Inserido tanto na Câmara dos Representantes quanto no Senado como uma proposta para ampliar a privacidade nos Estados Unidos esse projeto de lei apresenta em seu histórico de tramitação inúmeras tentativas em converter essa legislação em um mecanismo para a legalização da captação de informações de maneira indiscriminada. Nesse momento o setor privado era favorável à instituição de políticas de privacidade mais rígidas, pois seu apoio público ao debate contribuiria para a retomada de confiança dos usuários em seus produtos.

Grandes empresas de tecnologia dos Estados Unidos como *Google*, *Apple*, *Microsoft*, *Facebook* e *Twitter* construíram a coalizão *Reform Government Surveillance* e divulgaram uma declaração em 2013 afirmando que a legislação *USA Freedom Act*, em seu rascunho mais recente, abria uma brecha inaceitável que poderia permitir a coleta em massa de dados dos usuários de Internet, enfatizando que embora a legislação trouxesse progressos relevantes, não seria possível apoiar esse projeto de lei em sua conformação original. Apesar da pressão realizada, os grupos de inteligência dispunham de forte poder de influência, e a aprovação do projeto de lei se manteve paralisado até 2015 (GIBBS, 2014).

Observa-se, deste modo que a busca pela reforma da vigilância em regimes liberais com poderosas agências de inteligência conduz a uma lógica intitulada de “paradoxo Snowden”, termo cunhado por Tréguer (2019). O “paradoxo de Snowden” promove as reformas dos programas de inteligência do governo através do abandono da prática de vigilância em larga

escala operada de maneira sigilosa, como eram os exemplos do programa PRISM, para a constituição de uma base jurídica detalhada capaz de conferir à prática de vigilância legitimidade, ao trazer novas salvaguardas e diminuir o nível de sigilo sobre essas atividades.

Diante do acima exposto, compreendemos que o estabelecimento de políticas de compartilhamento de informações entre setor público e privado em segurança cibernética, a exemplo das legislações CISPA e CISA, manifestam-se também como uma alternativa para contornar possíveis indisposições legais que venham a prejudicar o estabelecimento da prática de inteligência, seguindo a lógica do paradoxo de Snowden descrito por Tréguer.

Os indícios que nos levam a crer que essas legislações busquem atender a este propósito estão na instituição de um (i) texto pouco claro sobre quais categorias de informações se enquadram de fato em fundamentos para prevenir ataques cibernéticos, (ii) estabelecimento da superioridade dessas legislações sobre quadros legais anteriormente estabelecidos, construindo uma brecha para violações de privacidade realizadas e (iii) patrocinadores das leis *(sponsors)* pertencentes à Agência de Segurança Nacional, ou seja, relacionados ao Comitê Especial de Inteligência do Comitê do Senado ou da Câmara, diretamente vinculados aos interesses de inteligência.

Como apresentado no início deste capítulo, a definição do equilíbrio entre privacidade e segurança para políticas voltadas ao espaço cibernético envolve também outras variáveis como por exemplo, a disputa interburocrática para a coordenação da política de segurança cibernética nos Estados Unidos e a complacência do setor privado. Um estudo exploratório do processo de inserção da legislação CISPA até a aprovação de uma legislação de conteúdo semelhante em 2015 nos permite compreender, sem esgotar o tema, como legislações descritas como cibersegurança tem se convertido em legislações de cibervigilância.

4.2 Legislações CISPA e CISA: Leis de Segurança Cibernética ou Cibervigilância?

4.2.1 *Cyber Intelligence Sharing and Protection Act* (CISPA)

A *Cyber Intelligence Sharing and Protection Act*- popularmente conhecida pelo acrônimo CISPA - é um projeto de lei inicialmente inserido no 112º congresso norte-americano pelo deputado republicano Mike Rogers e o pelo deputado democrata Dutch Ruppersberger. O projeto de lei contou com a colaboração de outros 112 co-patrocinadores, dentre os quais 86 eram pertencentes ao partido republicano e 26 ao partido democrata. Rogers à época ocupava a cadeira de presidente do Comitê Permanente de Inteligência da Câmara dos Deputados e

historicamente carregava um perfil de apoio às legislações que flexibilizavam e ampliavam a capacidade do governo de obter informações, buscando, deste modo, facilitar a atuação das agências de segurança nacionais. A título ilustrativo em anos anteriores Rogers havia votado sim na controversa legislação *FISA Amendments Act de 2008* ,emblemática dentro de um propósito do governo norte-americano em manter os poderes adquiridos no período dos pós 11 de setembro, buscando senão ampliar ao menos manter sua capacidade de captação de informações sem impeditivos legais rígidos como detalhamos em seção anterior.

Seguindo sua tradicional postura, Rogers posicionou-se favoravelmente à Agência de Segurança Nacional diante das declarações de Edward Snowden em 2013, afirmando a necessidade de que atividades desta natureza fossem instituição na intenção de preservar a segurança nacional norte-americana. Já Ruppersberger representava o distrito de Maryland, onde está situada a sede da NSA, o que pode explicar ou informar sua opinião pró-CISPA (SIDHU, 2015).

Em linhas gerais, o projeto de lei CISPA permitia o compartilhamento de informações de tráfego da Internet entre o governo dos EUA e o setor privado – empresas de tecnologia e manufatura - sob a justificativa de ampliar a capacidade do governo norte-americano em investigar e responder à ameaças cibernéticas, ampliando a segurança de suas redes e infraestruturas críticas contra-ataques cibernéticos (MITCHELL, 2016). O projeto de lei removia obstáculos legais que desencorajassem as empresas a compartilhar dados de ameaças cibernéticas com o governo, uma vez que na visão de seus patrocinadores as empresas mostravam-se hesitantes em partilhar informações valiosas à promoção da segurança cibernética em decorrência do medo de serem alvos de processos legais. A CISPA introduzia uma emenda à Lei de Segurança Nacional de 1947, que em decorrência de uma questão temporal, não continha disposições sobre crime cibernético.

Já em sua primeira inserção no congresso, em 2011, o projeto de lei suscitou discussões sobre privacidade, sendo criticadas de forma unânime por organizações defensoras da privacidade e das liberdades civis na internet, como *Electronic Frontier Foundation* (EFF) e a *American Civil Liberties Union* (ACLU). Na visão dos grupos opositores, o projeto de lei possuía uma linguagem fortemente abrangente que poderia ser usada de maneira inadequada para a prática de vigilância estatal. A CISPA permitia, como anteriormente mencionado, que plataformas de mídia social e outras empresas de tecnologia enviassem informações para Agência de Segurança Nacional, o que gerava preocupações sobre a proteção à privacidade (TIEN, 2013).

Outras disposições problemáticas contidas no corpo de texto da lei como, por exemplo, a permissão para que as informações compartilhadas sob o resguardo desta lei fossem utilizadas para outros fins além da promoção da segurança cibernética e a concessão de imunidade às empresas privadas em relação à aplicação das leis de privacidade já existentes no ordenamento jurídico norte-americano corroborava com a percepção de que a legislação CISPA comportava-se mais como uma lei de vigilância do que de segurança cibernética.

Como resposta às preocupações com a privacidade, o projeto de lei foi revisado e emendas foram instituídas ao seu texto original. Dentre as alterações realizadas, o deputado McCaul (Republicano do Texas) à época Presidente do Comitê de Segurança Interna da Câmara, e, portanto, representante dos interesses do DHS, apresentou uma emenda responsável por garantir que apenas agências civis recebessem dados da CISPA, impedindo, assim que agências de inteligência, como a NSA recebessem esses dados diretamente (MINDOCK, 2015; TIEN, 2013). Contudo, na opinião de grupos pró liberdade, como a EFF essas alterações eram meramente cosméticas. No que se refere, por exemplo, o já mencionado recebimento de dados pela NSA e o estabelecimento de uma emenda restritiva apresentada pelo deputado McCaul para o compartilhamento de informações apenas com agências civis, a EFF destacava que esta emenda na prática não obtinha o efeito desejado. A alteração proposta por McCaul (D-MD) tinha um caráter sugestivo, recomendando que as empresas enviassem informações relacionadas à ameaça a segurança cibernética ao Departamento de Segurança Interna, e, informações relacionadas a "crimes cibernéticos" ao Departamento de Justiça (*Department of Justice* - DOJ). A emenda não exigia que as informações compartilhadas fossem realizadas de maneira restrita a esses dois departamentos civis, ou mesmo que as informações compartilhadas com os mesmos permaneçam restritas à essas agências (TIEN, 2013). Segundo Tien (2013), esta nuance é de extrema relevância, pois, não altera de fato as principais disposições do projeto de lei que permite que uma empresa compartilhe dados com quem escolher, seja com o setor público ou privado; civil ou militar. Portanto, legislações como a CISPA pouco fazem para tentar resolver a questão da sobreposição de autoridades legais no que diz respeito ao compartilhamento de informações cibernéticas (NOLAN, 2015).

A oposição ao projeto de lei não se restringia apenas aos grupos pró liberdade norte-americanos, mas pelo próprio governo Federal que diante da pressão negativa ameaçava inclusive vetar o projeto de lei caso ele chegasse à mesa de assinatura do presidente. Apesar da oposição destes grupos o projeto de lei recebeu significativo apoio das grandes corporações de Internet. A lista de apoiadores privados à CISPA em 2012 incluía mais de 800 empresas de tecnologia dentre elas a empresa Facebook. Em carta datada de 06 de fevereiro de 2012, assinada

por Joel Kaplan, Vice-presidente de *Public Policy* do Facebook, a empresa elogiava o projeto de lei, enfatizando que suas diretrizes eliminavam regras que podiam inibir a proteção do ecossistema da Internet (ROBERTSON, 2012). Vale mencionar que Joel Kaplan havia ocupado entre 2006 e 2009 o cargo de Vice-Chefe de Política do Gabinete de George W. Bush.

Em 10 de abril de 2013, a TechNet, rede nacional e bipartidária de CEOs e executivos sênior de tecnologia, em atitude semelhante endereçou uma carta à Mike Rogers e Dutch Ruppersberger parabenizando a iniciativa de inserção deste projeto lei e declarando apoio a iniciativa. Ficava estabelecido que:

> "este projeto de lei reconhece a necessidade de uma legislação eficaz de segurança cibernética que incentive o compartilhamento voluntário, bidirecional e em tempo real de informações acionáveis sobre ameaças cibernéticas para proteger as redes". Além disso, a mensagem elogiava "o comitê por fornecer proteções de responsabilidade a empresas que participam de compartilhamento voluntário de informações e aplaudimos os esforços do comitê em trabalhar com uma ampla gama de partes interessadas para tratar de questões como o fortalecimento das proteções de privacidade". (TECHNET, 2013, tradução nossa)

Os membros da *TechNet* vão desde pequenas *startups* norte-americanas até as mais emblemáticas empresas de tecnologia. Dentre os membros de seu conselho executivo, incluía-se à época Eric Schmidt, diretor executivo do Google. Outros importantes representantes desse setor como *Yahoo* e *Microsoft* também faziam parte da *TechNet*. O apoio do setor privado se apresenta como uma das principais justificativas para a reinserção de um projeto de lei tão controverso quanto a CISPA mesmo diante de suas sucessivas derrotas, o projeto de lei foi reintroduzido em 2013 e 2015 na Câmara norte-americana.

A comunidade empresarial em sua diversidade como, por exemplo, bancos, empresas de energia, empresas de defesa, produtores de Provedores de Internet, e Big Techs apoiaram essa legislação. Dentre os grandes apoiadores da legislação CISPA, podemos mencionar *General Dynamics*, *Lockheed Martin*, *General Electric*, *Northrop Grumman*, *SAIC*, *Google*, *Yahoo*, a Câmara de Comércio norte-americana, *IBM*, dentre outros. Havendo também importantes representantes do setor financeiro e das grandes corporações de Internet (CHOMA, 2012a).

Segundo levantamento realizado por Choma (2012a,2012b) utilizando dados levantados através do *Center for Responsive Politics,* 206 organizações registraram lobby nesse projeto de lei (CHOMA, 2012a, 2012b). Dentre as empresas que praticaram lobby na legislação CISPA, doze haviam financiado Mike Rogers, autor desse projeto de lei, ou a sua liderança PAC durante o ciclo eleitoral de 2012, havendo uma alta expressividade do lobby praticado pelas empresas provedoras de serviço de internet, como AT&T*; National Cable & Telecommunications Assn*. Esse financiamento totalizou um montante de US$103.000 dólares (Ver Tabela 2).

Tabela 2 - Lista de empresas que fizeram *lobby* e contribuíram com o Congressista Mike Rogers (Rep.) ou com seu *Political Action Commitee* (PAC)[16]

Organization	Individual	PAC	Totals
SAIC Inc	–	$20,000	$20,000
Lockheed Martin	–	$15,000	$15,000
AT&T Inc	$1,000	$11,000	$12,000
CMS Energy	–	$12,000	$12,000
Northrop Grumman	–	$11,000	$11,000
General Dynamics	–	$8,000	$8,000
National Rural Electric Cooperative Assn	–	$6,000	$6,000
National Cable & Telecommunications Assn	–	$5,000	$5,000
Time Warner Cable	–	$5,000	$5,000
US Telecom Assn	–	$3,000	$3,000
Cellular Telecom & Internet Assn	–	$3,000	$3,000
Exxon Mobil	–	$3,000	$3,000
		TOTAL	$103,000

Fonte: Choma (2012a)

Dentre as empresas que praticaram lobby na legislação CISPA, e que financiaram Mike Rogers ou sua PAC, está a conhecida empreiteira militar SAIC, especializada em fornecer serviços governamentais e suporte à tecnologia da informação. A SAIC havia lucrado bastante no passado vendendo tecnologias de processamento e armazenamento de dados ao governo norte-americano (CHOMA, 2012a)[17].

Segundo McChesney (2013), um dos motivos do apoio dado pelas grandes corporações de Internet a esse projeto de lei estava no fato de que este conferia cobertura legal para atividades que já estavam sendo praticadas por esse setor, contudo, de maneira clandestina como as declarações de Edward Snowden viriam expor. Para as intituladas empreiteiras militares, como a SAIC, que lucravam com a venda de tecnologias de mineração de dados, a flexibilização dessa categoria de legislação apenas ampliava os negócios.

[16] O *Political Action Commitee* (PAC) é um termo popular para um comitê político organizado com o objetivo de arrecadar e gastar dinheiro para eleger e derrotar candidatos. A maioria dos PACs representa interesses comerciais, trabalhistas ou ideológicos.

[17] A *Science Applications International Corporation* (SAIC) é considera uma das mais importantes empreiteiras militares norte-americanas. Como destaca Eliot Cohen (2010) o SAIC foi um dos arquitetos principais do programa TIA descrito nessa dissertação como uma das tecnologias precursoras da coleta de informações em massa.

Para a autora Beatrice Edwards (2014, p.46), a tentativa de consolidar uma lei como CISPA era um indicativo do processo gradual de consolidação de um complexo de vigilância governamental-corporativo nos Estados Unidos. Nas palavras da autora o que até então havia se manifestado de forma confidencial e informal, passava a ser institucionalizado mediante a construção de leis públicas que carregavam um texto amplo e impreciso abrindo espaço para que a coleta indevida de informações pela NSA continuasse. A percepção de Edward (2014) vai de encontro com a lógica do paradoxo Pós-Snowden descrito por Tréguer (2019) onde a vigilância não é extinta, apenas é submetida a um processo de institucionalização.

Aproveitando o cenário de alerta ocasionado pelo ataque cibernético direcionado a Sony Pictures, o Comitê de Inteligência da Câmara dos Representantes fez sua última tentativa de introduzir a legislação CISPA no congresso (H.R 234). Em um movimento divergente da posição adotada em momentos anteriores, a Casa Branca sinalizou apoio ao projeto caso se adequasse aos parâmetros necessários a preservação da privacidade em ambiente online. Contudo, diante dos sucedidos fracassos da legislação CISPA em avançar na Câmara dos Representantes, essa legislação passaria a ser tramitada agora no Senado, sob o codinome de *Cybersecurity Information Sharing Act,* conhecida como CISA.

4.2.2 *Cybersecurity Information Sharing Act* (CISA)

Até julho de 2014 o Senado não havia apresentado uma alternativa à controversa legislação de compartilhamento de informações aprovada na Câmara. A primeira tentativa de inclusão de um projeto de lei sobre essa temática foi feita pela Presidente do Comitê de Inteligência do Senado, Dianne Feinstein, contudo, o projeto não chegou a uma votação completa no Senado. Esse projeto de lei reapareceu novamente no 114º congresso, em março de 2015, sendo patrocinada pelo Senador Richard Burr (R-NC). Quando se avalia o histórico de iniciativas de Burr podemos observar uma preocupação em manter a capacidade do governo norte-americano em ter acesso à quantidade necessária de dados (informações) para produzir Inteligência. Em retrospectiva histórica Burr havia proposto, quando Presidente do Comitê de Inteligência do Senado, instituir uma emenda para estender em dois anos algumas disposições contidas no *Patriot Act* previstas para expirar em maio de 2015. Dentre essas disposições constava a permissão para a coleta massiva de metadados de registros telefônicos privados pela NSA.

A reinserção do projeto de lei foi proposta em um momento de agitação entre os legisladores do Congresso, em decorrência do ataque cibernético realizado por norte-coreanos à

empresa Sony Picture. Os ataques geraram na Casa Branca um sentimento de urgência em relação à necessidade de ampliar o escopo de suas políticas para o ciberespaço e a capacidade de ação diante de ataques cibernéticos. O episódio envolvendo a Sony Pictures apontava uma deficiência do governo em identificar e auxiliar o setor privado no combate a potenciais ataques cibernéticos, o que poderia ser resolvido com o compartilhamento de indicadores de ameaça cibernética entre esses dois atores. Nas palavras de Mitchell:

> Sony Pictures era apenas um estúdio de cinema, e mesmo assim o ataque cibernético rapidamente se tornou uma sensação pública e preocupou a discussão política em Washington. Havia uma sensação de ultraje diante de um ataque estrangeiro descarado, era relativamente fácil de entender, pelo menos em suas consequências, e era assustador (MITCHELL, 2016, p. 5, tradução nossa)

A resposta do poder Executivo foi imediata. O governo federal quase que imediatamente começou a trabalhar em uma nova ordem executiva sobre segurança cibernética voltada à área temática de compartilhamento de informações. O lançamento da *Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing* de 20 de fevereiro de 2015 é um exemplo dessa iniciativa. (SULLIVAN & CROMWELL, 2015; U.S. GOVERNMENT, 2015a). Essa ordem executiva consolidava mais uma vez a relevância atribuída ao compartilhamento de dados como fator de garantia à segurança nacional norte-americana, afirmando a necessidade de atuação conjunta entre empresas privadas, organizações sem fins lucrativos, departamentos executivos e agências, bem como quaisquer outras entidades capazes de colaborar para deter e responder a ataques cibernéticos com a maior velocidade. Buscando atingir esse objetivo a ordem executiva propunha a criação dos intitulados ISAOs (*Information Sharing and Analysis Organizations*), a serem coordenados pelo Departamento de Segurança Interna.

A reinserção da legislação CISA acompanhava essa tendência. Embora a nova versão inclua melhorias em relação ao rascunho do projeto de lei anterior, ela apresenta disposições muito semelhantes. Seu texto ainda é muito pouco preciso permitindo o compartilhamento quase ilimitado de dados para uma lista vaga e abrangente de objetivos. A definição de segurança cibernética presente no corpo da lei é muito ampla, abrindo precedente para que quase toda informação seja compartilhada. Assim como o projeto de lei anterior, a versão inserida no senado também não resolve a disputa interburocrática (NOLAN, 2015). Embora exista uma ampla autoridade legal para o DHS servir como repositório e distribuidor central de inteligência para o governo federal, o texto do projeto de lei abre precedente para que o setor privado compartilhe grandes quantidades de dados com várias agências governamentais dos Estados Unidos, incluindo a NSA.

4.2.3 *Cybersecurity Act* 2015

Em 18 de dezembro de 2015, o presidente Barack Obama sancionou o *Cybersecurity Act*, que incluiu dentre suas disposições, a regulamentação de políticas direcionadas à promoção da segurança cibernética. Contido num *Omnibus Appropriations Act*, ou melhor, *Consolidated Appropriations Act 2016*, o *Cybersecurity Act 2015* contém seções sobre o monitoramento da Internet, as quais modificaram questões relacionadas à Internet nos Estados Unidos, ampliando os poderes dos operadores de rede para conduzir a vigilância para fins de segurança cibernética (KERR, 2015). Especificamente, o texto fornece o arcabouço legal que, por exemplo, retira responsabilidade de empresas privadas que compartilham informações relacionadas à cibersegurança - em modalidades correspondentes a certos procedimentos - e ainda autoriza várias entidades, inclusive fora do governo federal norte-americano, a monitorar determinados sistemas de informações, além de operar medidas defensivas de propósitos de cibersegurança (SULLIVAN & CROMWELL, 2015).

Pode-se argumentar que o *Cybersecurity Act 2015* é o dispositivo legal mais importante sobre a matéria (JAFFER, 2015). Não apenas porque a lei estabelece um mecanismo de compartilhamento de informações relacionadas à cibersegurança entre o setor privado e entidades do governo federal, a subseção 1ª *Cybersecurity Information Sharing Act* (CISA), mas também porque a aprovação e sanção do *Cybersecurity Act* é um momento divisor de águas, uma vez que representa o resultado de um esforço legislativo de mais de quatro anos (das maiorias bi-partidárias nas duas casas do Congresso norte-americano).Em grande medida, pode-se dizer que o *Cybersecurity Act* 2015 é decorrência de uma iniciativa do Poder Executivo dos Estados Unidos. A Ordem Executiva nº 13691 de 13 de fevereiro de 2015, assinada pelo Presidente Barack Obama, tinha como propósito desenvolver, principalmente, as chamadas ISAOs (*Information Sharing and Analysis Organizations*). Essas organizações estariam envolvidas no compartilhamento de informações relacionadas a riscos e incidentes de segurança cibernética (SULLIVAN & CROMWELL, 2015), através de mecanismos capazes de permitir que empresas privadas, organizações sem fins lucrativos, departamentos executivos e agências e outras entidades mantivessem voluntariamente parcerias com o Governo Federal norte-americano.

A disputa ao redor do conteúdo do *Cybersecurity Act* 2015 perpassou inúmeros debates, projetos de lei e discussões sobre a privacidade e os riscos de responsabilidade legal relacionados ao compartilhamento de informações. Segundo Sullivan & Cromwell (2015), dois grupos políticos tinham maior interesse na matéria. De um lado, grupos defensores de liberdades civis (e.g. *Fight for the Future)* expressavam preocupação com a não restrição ao compartilhamento

direto de informações entre entidades governamentais, como a NSA e o Pentágono (NOJEIM; LAPERRUQUE, 2015). De outro lado, grupos empresariais, como a *U.S. Chamber of Commerce* e a *Financial Services Roundtable*, elogiaram a lei como um passo crucial na proteção dos dados e da propriedade intelectual dos cidadãos norte-americanos contra ataques cibernéticos (U.S.CHAMBER..., 2015; SPENDING..., 2015). No cômputo geral, as implicações legais do *Cybersecurity Act 2015* trouxeram benefícios óbvios para o setor privado, sobretudo no que diz respeito a garantia de autonomia às empresas em termos de monitoramento de ameaças cibernéticas, o uso de medidas defensivas contra estas e o compartilhamento de informações dentro setor e junto ao governo (JAFFER, 2015).

O grande fator de diferenciação entre estes, as duas leis CISPA e CISA e o Cybersecurity Act de 2015 , está expresso na maneira através da qual esse compartilhamento seria realizado. Como mencionado anteriormente, a *Cybersecurity Act*, derivada de discussões que moldaram a legislação CISA em 2015, estabelece que o compartilhamento de informações via setor privado para o governo ocorra através de um site criado pelo DHS. No caso da CISPA esse compartilhamento ocorreria de maneira menos regulada, permitindo que as entidades privadas divulgassem sem a necessidade de qualquer mandato advindo das entidades governamentais as informações dos usuários de maneira direta para a Agência Nacional de Segurança Norte-Americana (NSA). Em termos de conjuntura política é curioso observar o movimento que se realiza em direção a aprovação de uma lei que regulamenta a apropriação de informações pelo governo norte-americano via grandes corporações privadas, em especial, empresas de telecomunicação de alcance global. Isso porque entre a reprovação do primeiro projeto de lei CISPA (entre os anos de 2011 a 2014) e a aprovação da CISA, em 2015, temos um importante acontecimento na política nacional norte-americana repercutindo no debate internacional, qual seja as denúncias realizadas em 2013 pelo ex-funcionário da NSA, Edward Snowden, sobre um esquema interno e internacional de vigilância em massa estabelecido pelo governo dos Estados Unidos, mais especificamente pela NSA, o que em partes pode justificar a transferência de autoridade ao DHS.

5 ALGUMAS CONCLUSÕES

O ritmo acelerado das mudanças tecnológicas, promovido pela quase total digitalização do cotidiano, transformou profundamente a vida das pessoas. As tecnologias digitais tornaram-se cruciais para as relações sociais, moldando não apenas a interação entre indivíduos, mas também a maneira como os atores estatais e não estatais interagem entre si, incorrendo em transformações, inclusive nas relações internacionais.

A produção massiva de dados sobre o comportamento humano tem transformado o dado em um artefato central à geopolítica contemporânea, responsável por fornecer poder a quem é capaz de controlá-lo. Nesse contexto, os Estados reescrevem seus termos de compromisso com os mercados e com seus cidadãos redefinindo seus interesses nacionais e suas prioridades estratégicas.

Como enfatiza Rosenbach e Mansted (2019), a competição estratégica no século XXI é caracterizada por uma disputa de soma zero pelo controle de dados, bem como pelo domínio sobre a tecnologia e o talento necessário para converter estes dados em informações úteis. Dentre as estratégias utilizadas para prosperar nesse novo cenário os Estados devem se posicionar perante a guerra comercial em torno do mercado digital. Os Estados Unidos, em decorrência de seu papel central na criação da Internet, adquiriram vantagens nessa disputa, no entanto, o país tem no presente encontrado adversários robustos como a China. Na contemporaneidade, as empresas chinesas tem dominado o mercado do 5G, tanto no que se refere ao número de patentes produzidas quanto à permeabilidade de empresas de capital chinês no mercado estrangeiro, isso permitiria que o país se tornasse o principal detentor da estrutura de circulação de dados hoje em curso, conferindo vantagem estratégica ao país[18].

As transformações na lógica de poder, e, portanto, na concepção estratégica dos Estados, é acompanhada pela própria alteração da lógica de mercado ocasionada por essas transformações tecnológicas fazendo ascender uma nova categoria de atores privados com interesses econômicos específicos. Essa nova lógica econômica é descrita como capitalismo de vigilância e está centrado na monetização de dados pessoais e também na rentabilização de tecnologias capazes de aprimorar a coleta, o armazenamento e o processamento de tais informações. O segundo capítulo dessa dissertação abordou tais questões destacando que os efeitos tecnológicos hoje presenciados não são inevitáveis, mas derivam do social, sendo produto de duas racionalidades: a

[18] Como anteriormente enfatizado, os Estados Unidos foram capazes de dominar praticamente toda a infraestrutura crítica global necessária ao funcionamento da Internet, em decorrência de seu papel na criação desta rede. A questão é que a tecnologia 5G tem a potencialidade de tornar obsoleto esse domínio, pois, redefine a estrutura de circulação de dados. Cf. EUA...(2018).

governamental e a dos negócios que se valem de uma mesma lógica, qual seja, promover vigilância para atender seus objetivos.

Os estudos realizados por nós identificaram que as estruturas de poder norte-americanas, tanto governamentais quanto privadas foram fundamentais para construir o que hoje entendemos como sociedade do Big Data. Traçando uma linha que vai desde a criação da Internet até a administração Bush (2001-2008), debatemos no capítulo *"Histórias Cruzadas: como Estado e empresas norte-americanas construíram a sociedade do Big Data"* como o domínio do setor privado norte-americano sobre a infraestrutura da internet e dos dados que nela circulam ocorreu com apoio governamental, seguindo, por sua vez, as modificações da visão de poder pelos formuladores de política norte-americanos.

A própria conversão da Internet de um empreendimento acadêmico/militar - que até então havia gerado pouco interesse fora das comunidades militares e de pesquisa-, para uma rede privatizada e aberta ao tráfego comercial liderada por empresas norte-americanas foi fruto das políticas de incentivo instituídas pelo governo dos Estados Unidos. Os esforços empreendidos para criar uma Internet universal baseada nas preferências legais, políticas e sociais ocidentais foram movidas por motivações econômicas e geopolíticas norte-americanas, os tomadores de decisão à época no poder acreditavam que a Internet, uma vez comercializada e privatizada, tinha o potencial de gerar crescimento econômico capaz de sustentar o poder estadunidense.

Nos anos 2000, com o boom das ponto.com, as agências de inteligência passaram a atuar como grandes investidoras de capital de risco em pesquisas privadas voltada a aprimorar a coleta, armazenamento e processamento de dados. No cômputo geral, priorizou-se a segurança nacional, instrumentalizada pela vigilância, em detrimento de direitos e garantias civis, como a privacidade, fazendo-se uso, especialmente no pós 11 de setembro, de flexibilizações em legislações e do incentivo à participação privada no desenvolvimento de novas tecnologias e aportes para uma vigilância mais contemplativa aos interesses norte-americanos.

A relação público-privada na construção de um espaço legítimo de vigilância digital poderia ser facilmente observada. O estudo exploratório de documentos, manifestações de agentes importantes dos dois setores foram utilizados para mapear momentos chave nos quais ganhou corpo certa institucionalidade na política de segurança cibernética norte-americana, cujo aspecto em destaque era o escamoteando das práticas de vigilância sob o manto da "segurança nacional". Deste modo, legislações e regulamentações relacionadas à promoção da segurança e privacidade no ciberespaço são um importante termômetro para avaliar não apenas o posicionamento de atores públicos, mas também, de atores privados sobre a promoção da vigilância.

Identificamos que as legislações CISPA (*Cyber Intelligence Sharing and Protect Act*[19]*)* e CISA (*Cybersecurity Information Sharing Act*[20]*),* tramitadas no congresso norte-americano durante a administração Obama, são importantes exemplos para melhor compreender a relação que se estabelece entre as grandes empresas de internet nos Estados Unidos, o governo federal e as estruturas de inteligência norte-americanas quando debate-se vigilância na era do Big Data, e portanto, a relação equacional entre privacidade e segurança ao avaliarmos as políticas para o ambiente digital. Inseridas no congresso norte-americano como legislações de segurança cibernética, tais legislações passaram a ser enquadradas por grupos opositores como projetos de lei de cibervigilância, uma vez que ambos buscavam ampliar o compartilhamento de informações entre setor público e privado para fins de segurança, ao mesmo tempo em que conferiam ao setor privado proteção de responsabilidade contra possíveis processos relacionados à invasão de privacidade. Essas disposições, associadas a um texto pouco claro, justificavam sua fama violadora. Apesar da forte oposição a esses projetos de lei, em parte exacerbada pelo momento político delicado vivido após as declarações de Edward Snowden em 2013, a CISPA e a CISA receberam apoio de importantes atores do setor privado.

No estudo exploratório feito no capítulo quatro dessa dissertação pudemos verificar que as agências de inteligência norte-americanas apoiando-se no discurso securitizador em torno da menção da ampla vulnerabilidade do ciberespaço e da necessidade de intensificar medidas de defesa nesse domínio, dedicaram-se a instituir legislações que tendiam a deixar janelas abertas para práticas de vigilância, principalmente através de previsões legais, que conferiam também vantagens ao setor privado, estimulando que esse corroborasse com essas práticas. As legislações CISPA e CISA, por exemplo, retiraram responsabilidade de empresas no compartilhamento de dados de usuários.

Decisões políticas tomadas durante a administração Trump, ainda em curso, reforçam a a percepção de que a interação entre atores público e privados durante o processo de decisão entre segurança e privacidade no domínio digital incorpora dois propósitos distintos. Primeiro, a manutenção de uma lógica de mercado baseada na vigilância e dominada pelo monopólio norte-americano no setor das tecnologias da informação e comunicação. E, segundo, o interesse do governo norte-americano em se utilizar do setor privado - e da legitimidade que este possui em captar dados pessoais para reordenar suas políticas de inteligência e torná-las mais eficientes. O exemplo mais concreto de uma política nessa direção durante a administração Trump é a

[19] Cf. U.S.Government (2011)
[20] Cf. U.S.Government (2015b, 2015c)

legislação *The Clarifying Lawful Overseas Use of Data Act* ou conhecido mais popularmente como *USA Cloud Act* promulgada em 2018. Essa lei permite que autoridades federais norte-americanas obriguem as empresas de tecnologia baseadas nos Estados Unidos, por meio de mandato ou intimação, a fornecer dados armazenados em seus servidores, independente, se esses dados se encontram armazenados nos Estados Unidos ou no exterior, ou seja, a lei permite que uma companhia sujeita à jurisdição de determinado país possa ser requerida a produzir a apresentar dados sob seu controle a qualquer momento, independentemente de onde estes dados estejam armazenados. Essa legislação manifesta-se como uma clara intenção do governo norte-americano em contornar as questões de territorialidade que podem se apresentam como um impeditivo ao governo norte-americano obter acessos aos dados, elevando inclusive a possibilidade de barganha com demais entidades estatais visto que a lei autoriza os Estados Unidos a entrar em acordos executivos com outros países para facilitar a obtenção a tais dados. Esse novo capítulo da política norte-americana corrobora com o debate instituído nessa dissertação, de modo que destacamos que as considerações aqui feitas comportam-se como uma importante base para estudos futuros.

REFERÊNCIAS

ABBATE, Janet. **Inventing the internet**. Cambridge: MIT press, 2000.

ARQUILLA, John; RONFELDT, David. Cyberwar is coming! In: ARQUILLA, John; RONFELDT, David. **In Athena's camp:** Preparing for conflict in the information age. Pittsburgh: Rand corporation, 1997, p. 23-60.

ARQUILLA, John; RONFELDT, David. **Networks and netwars:** The future of terror, crime, and militancy. Pittsburgh: Rand Corporation, 2001.

ARTHUR, Charles. Tech giants may be huge, but nothing matches big data. **The Guardian,** 23 ago. 2013. Disponível em: https://www.theguardian.com/technology/2013/aug/23/tech-giants-data. Acesso em: 30 jan. 2020.

ASKING the U.S.Government to allow Google to publish more national security request data.**Google Blog.** 11 jun.2013. Disponível em:https://googleblog.blogspot.com/2013/06/asking-us-government-to-allow-google-to.html Acesso em:14 jan. 2020.

BALL, Kirstie; WEBSTER, Frankie (Eds). The intensification of surveillance. In: BALL, Kristie; WEBSTER, Frankie (Eds).**The Intensification of Surveillance**: Crime, Terrorism and Warfare in the Information Era. London: Pluto Press, pp. 1–15.

BALL, Kirstie; SNIDER, Laureen (Eds.). **The surveillance-industrial complex:** A political economy of surveillance. New York: Routledge, 2013.

BERNAL, Paul. Data gathering, surveillance and human rights: recasting the debate. **Journal of Cyber Policy**, v. 1, n. 2, p. 243-264, 2016.

BLOCK, Fred. Swimming against the current: the rise of a hidden developmental state in the United States. **Politics & society**, v. 36, n. 2, p. 169-206, 2008.

BOHN, Dieter. Facebook, Microsoft rolling FISA national security request numbers into transparency reports. **The Verge.** June 14, 2013. Disponível em: https://www.theverge.com/2013/6/14/4432060/facebook-to-include-national-security-requests-in-transparency-report Acesso em: 4 jan. 2020.

BOUSSIOS, Emanuel G. The "Right" to Privacy?-The Debate over the United States Government's Control over its Cyberspace**. Athens Journal of Law**. v.2, Issue 4. p. 211-224.

BORRUS, Michael; ZYSMAN, John. Globalization with Borders: The Rise of Wintelism as the Future of Global Competition. **Industry and Innovation**, v. 4, n. 2, p. 141-166, 1997.

BROSE, Christian. The New Revolution in Military Affairs: War's Sci-Fi Future. **Foreign Affairs**, v. 98, may-jun, 2019. Disponível em: https://www.foreignaffairs.com/articles/2019-04-16/new-revolution-military-affairs Acesso em: 14 jan. 2020.

CARR, Madeline. **US power and the internet in international relations:** The irony of the information age. London: Springer, 2016.

CASTILLO, Andrea. Snowden leaks confirm: CISA is a surveillance bill.**Plain text.** 09 jun. 2015. Disponível em: https://readplaintext.com/snowden-leaks-confirm-cisa-is-a-surveillance-bill-1e21a76abbab Acesso em: 15 jan. 2020.

CAVELTY, Myriam Dunn. **Cyber-security and threat politics:** US efforts to secure the information age. London: Routledge, 2007.

CAVELTY, Myriam Dunn. The militarisation of cyber security as a source of global tension. In: CAVELTY, Myriam Dunn et. al. **Strategic Trends 2012:** Key Developments in Global Affairs. Zurich: ETH Zurich, Center for Security Studies (CSS), 2012. p. 103- 124. Disponível em: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Strategic-Trends-2012.pdf Acesso em: 04 fev.2019.

CAVELTY, Myriam Dunn; BRUNNER, Elgin M. Introduction: Information, Power, and Security – An Outline of Debates and Implications. In: CAVELTY, Myriam Dunn; MAUER, Victor; KRISHNA-HENSEL, Sai Felicia (Eds). **Power and security in the information age:** Investigating the role of the state in cyberspace. New York: Routledge, 2016. p. 1-18.

CAVELTY, Myriam Dunn; EGLOFF, Florian J. The politics of cybersecurity: Balancing different roles of the state. **St Antony's International Review**, v. 15, n. 1, p. 37-57, 2019. Disponível em: https://www.ingentaconnect.com/content/stair/stair/2019/00000015/00000001/art00004 Acesso em: 10 jan. 2020

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e terra, 2005.

CHOMA, Russ. Facts on #CISPA. **Open Secrets News,** 20 abril 2012a. Disponível em: https://www.opensecrets.org/news/2012/04/cispa-facts/ Acesso em: 10 jan. 2020

CHOMA, Russ. #CISPA, #SOPA, #PIPA and #BigLobbying. **Open Secrets News,** 27 abril 2012b. Disponível em: https://www.opensecrets.org/news/2012/04/cispa-sopa-pipa-and-biglobbying/ Acesso em: 03 jan. 2020.

CISA: The Internet Surveillance Act No One is Discussing. **Project Censored.** 4 out. 2016. Disponível em: https://www.projectcensored.org/10-cisa-internet-surveillance-act-no-one-discussing/?doing_wp_cron=1580781796.1551148891448974609375 Acesso em: 21 mai. 2019.

CLINTON, William J.; GORE JR, Albert. Technology for America's economic growth, a new direction to build economic strength. **Executive Office of the President**. Washington DC, 1993. Disponível em: http://www.channelingreality.com/Reinvention/Documents/1993_Technology_for_Americas_Economic_Growth.pdf Acesso em: 10 jan. 2020.

COHEN, Elliot.The Military-Industrial Information Network. In: COHEN, Elliot. **Mass surveillance and state control**: the total information awareness project. New York: Palgrave Macmillan, 2010. p.47-56.

COLDEBELLA, Gus P.; WHITE, Brian M. Foundational questions regarding the federal role in cybersecurity. **J. Nat'l Sec. L. & Pol'y**, v. 4, p. 233, 2010.

COOPERATION or Resistance?: the Role of Tech Companies in Government Surveillance.**Harvard Law Review.** Developments in the Law — More Data, More Problems, v.131, 2018, p. 1715-22. Disponível em: https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/ Acesso em: 10 jan. 2020.

DEVRIES, Will Thomas. Protecting privacy in the digital age. **Berkeley Technology Law Journal**, v. 18, 2003. p. 283-311. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/berktech18&div=25&id=&page = Acesso em: 4 mai. 2019.

DICKINSON, Elizabeth. Internet Freedom. Document. **Foreing Policy,** 21 jan. 2010. Disponível em: https://foreignpolicy.com/2010/01/21/internet-freedom/ Acesso em: 10 jan. 2020.

EDWARDS, Beatrice. **The Rise of the American Corporate Security State:** Six Reasons to Be Afraid. San Francisco: Berrett-Koehler Publishers, 2014.

EICHENSEHR, Kristin E. Would the United States Be Responsible for Private Hacking?. **Just Security**, 17 Oct. 2017. Disponível em: https://www.justsecurity.org/46013/united-states-responsible-private-hacking/ Acesso em: 10 jan. 2020.

EUA pedem a aliados que evitem produtos de Telecom da chinesa Huawei. **Valor Econômico.** São Paulo, 22 de novembro de 2018.

FERREIRA NETO, Walfredo Bento. Territorializando o "novo" e (re)territorializando os tradicionais: a cibernética como espaço e recurso de poder. In: MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo Bento; GONZALES, Selma Lúcia de Moura (Orgs). Segurança e Defesa Cibernética: da fronteira física aos muros virtuais. Recife: Editora UFPE, 2014. p. 69-99.

FLYVERBOM, Mikkel; DEIBERT, Ronald; MATTEN, Dirk. The governance of digital technology, big data, and the internet: new roles and responsibilities for business. **Business & Society**, v. 58, n. 1, p. 3-19, 2019. Disponível em: https://journals.sagepub.com/doi/abs/10.1177/0007650317727540 Acesso em: 3 set. 2019

FOSTER, John Bellamy; MCCHESNEY, Robert W. Surveillance capitalism: Monopoly-finance capital, the military-industrial complex, and the digital age. **Monthly Review**, v. 66, n. 3, p. 1, 2014. Disponível em: https://monthlyreview.org/2014/07/01/surveillance-capitalism/?v=19d3326f3137 Acesso em: 22 jul. 2018.

GANDY, Oscar H. Data mining and surveillance in the post 9/11 environment. In: HIER, Sena P.; GREENBERG, Joshua (Eds.). **The surveillance studies reader**. Berkshire: McGraw-Hill Education (UK), 2007.p. 147-157.

GANDY, Oscar H. Statistical Surveillance: remote sensing in the digital age. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (Ed.). **Routledge handbook of surveillance studies**. New York: Routledge, 2012.p. 125-132.

GELLMAN, Barton; POITRAS, Laura. U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. **The Washington Post**, 07 jun. 2013. Disponível em: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-

internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html Acesso em: 12 nov. 2019.

GELLMAN, Barton; SOLTANI, Ashkan. NSA tracking cellphone locations worldwide, Snowden documents show. **The Washington Post,** 04 dez. 2013. Disponível em: https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html Acesso em: 10 jan. 2020

GERMANO, Judith. Cybersecurity Partnerships: A New Era of Public-Private Collaboration. **The Center on Law and Security**. New York: NYU School of Law.Oct. 2014. 20p. Disponível em: https://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf Acesso em 04 fev. 2019

GIBBS, Samuel. Facebook, Google and Apple lobby for curb to NSA surveillance. **The Guardian**. Nov 17, 2014. Disponível em: https://www.theguardian.com/technology/2014/nov/17/facebook-google-apple-lobby-senate-nsa-surveillance Acesso em: 4 dez. 2019.

GOLDENBERG, Suzanne. Big Brother will be watching America.**The Guardian,** 23 nov. 2002. Disponível em: https://www.theguardian.com/world/2002/nov/23/usa.suzannegoldenberg Acesso em: 11 set. 2019.

GOOGLE TRANSPARENCY PROJECT. Google Transparency Project. 2020. Disponível em: https://www.googletransparencyproject.org/ Acesso em: 12 jan. 2020.

GOLDSMITH, Jack. **The Failure of Internet Freedom**. New York, NY: Knight First Amendment Institute.2018.

GRANT, John. Will there be cybersecurity legislation. **J. Nat'l Sec. L. & Pol'y**, v. 4, p. 103-117, 2010. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/jnatselp4&div=11&id=&page= Acesso em: 6 mai.2018.

GREENWALD, Glen; MACASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others. **The Guardian,** 07 jun.2013. Disponível em: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data Acesso em: 10 jan. 2018.

GREENWALD, Glen; MACASKILL, Ewen; POITRAS, Laura; ACKERMAN, Spencer; RUSHE, Dominic. Microsoft handed the NSA access to encrypted messages.**The Guardian,** 12 jul. 2013. Disponível em: https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data Acesso em: 10 jan. 2020.

GUNDALINI, Bruno;TOMIZAWA, Guilherme. Mecanismo Dsiciplinar de Foucault e o Panóptico de Nentham na Era da Informação. **ANIMA**: Revista Eletrônica do Curso de Direito das Faculdades OPET. Curitiba PR - Brasil. Ano IV, nº 9, jan/jun 2013.

HANSEN, Lene; NISSENBAUM, Helen. Digital disaster, cyber security, and the Copenhagen School. **International studies quarterly**, v. 53, n. 4, p. 1155-1175, 2009. Disponível em: https://academic.oup.com/isq/article/53/4/1155/1815351 Acesso em: 10 fev. 2019
HARDING, Luke. **The Snowden files**: The inside story of the world's most wanted man. New York: Guardian Faber Publishing, 2014.

HARKNETT, Richard J.; STEVER, James A. The new policy world of cybersecurity. **Public Administration Review**, v. 71, n. 3, p. 455-460, 2011. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1540-6210.2011.02366.x
Acesso em: 19 mar.2019

HARRIS, Shane. Giving In To The Surveillance State.**The New York Times,** 22 ago. 2012. Disponível em: https://www.nytimes.com/2012/08/23/opinion/whos-watching-the-nsa-watchers.html Acesso em: 27 jan.2020.

IGNATIUS, David. The U.S.-China trade war is cooling off. But the tech war is heating up. **The Washington Post,** 7 nov.2019. Disponível em: https://www.washingtonpost.com/opinions/global-opinions/the-us-china-trade-war-is-cooling-off-but-the-tech-war-is-heating-up/2019/11/07/0c13a126-01ae-11ea-9518-1e76abc088b6_story.html Acesso em: 14 dez. 2019.

JAFFER, Jamil N. Carrots and Sticks In Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015. **SCL Rev.**, v. 67, p. 585, 2015. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/sclr67&div=35&id=&page= Acesso em: 4 jan. 2018

JOHNSON, Ericka. The CLOUD Act, Bridging the Gap between Technology and the Law. **The National Law Review** March 19, 2018. Disponível em: https://www.natlawreview.com/article/cloud-act-bridging-gap-between-technology-and-law Acesso em: 15 mar. 2019.

KAYYALI, Dia; TIEN, Lee. EFF Dismayed by House's Gutted USA FREEDOM Act. **Electronic Frontier Foundation.** May 20, 2014. Disponível em: https://www.eff.org/deeplinks/2014/05/eff-dismayed-houses-gutted-usa-freedom-act Acesso em: 15 nov. 2019.

KERR, Orin S. Internet surveillance law after the USA Patriot Act: The big brother that isn't. **Northwestern University Law Review 607.**, v. 97, 2003. p.607-676. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=317501 Acesso em: 17 jun. 2019

KERR, Orin S. How does the Cybersecurity Act of 2015 change the Internet surveillance laws? **The Washington Post,** 24 dez. 2015. Disponível em: https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/24/how-does-the-cybersecurity-act-of-2015-change-the-internet-surveillance-laws/ Acesso em: 03 jan. 2019

KITCHIN, Rob. **The data revolution:** Big data, open data, data infrastructures and their consequences. London: Sage, 2014LIBICKI, Martin C. **Conquest in cyberspace:** national security and information warfare. New York: Cambridge University Press, 2007.

KOMINSKY, Mitchell. The current landscape of cybersecurity policy: Legislative issues in the 113th congress. **Harvard Law School National Security Journal**, 2014. Disponível em: https://harvardnsj.org/2014/02/the-current-landscape-of-cybersecurity-policy-legislative-issues-in-the-113th-congress/ Acesso em: 14 jan. 2020.
LEE, Newton. **Facebook nation.** Total information awareness. New York: Springer, 2014.

LEVINE, Yasha. **Surveillance valley:** The secret military history of the Internet. New York: PublicAffairs, 2018.

LYON, David. **Surveillance studies**: An overview. Cambridge: Polity Press, 2007.

LYON, David. **Surveillance after snowden**. Cambridge: Polity Press, 2015.

MARGULIES, Peter. Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy. **Indiana Journal of Global Legal Studies**, v. 24, n. 2, 2017. p. 459-496. Disponível em: https://www.jstor.org/stable/10.2979/indjglolegstu.24.2.0459?seq=1 Acesso em: 31 jul.2019.

MINDOCK, Clark. Sounds like CISPA? Get ready for Lobbying Overdrive. **Opensecrets News.** 15 jan. 2015. Disponível em: https://www.opensecrets.org/news/2015/01/obama-cybersecurity-push-sounds-like-cispa/ Acesso em: 06 jan. 2020.

MITCHELL, Charlie. **Hacked:** The inside story of America's struggle to secure cyberspace. Lanham: Rowman & Littlefield, 2016.

MCADAMS, A. James. Internet surveillance after September 11: Is the United States becoming Great Britain?. 2005. **Comparative Politics**, v.37, issue(4), p. 479-498.

MCBRIDE, Sarah. **Pentagon turns to Silicon Valley for leads.** Reuters, 14 out. 2011. Disponível em: https://www.reuters.com/article/venture-pentagon/pentagon-turns-to-silicon-valley-for-leads-idUSN1E79C21O20111014 Acesso em 10 dez. 2019.

MCCHESNEY, Robert W. **Digital disconnect:** How capitalism is turning the Internet against democracy. New York: The New Press, 2013.

MCLAUGHIN, Jenna. Last-Minute Budget Bill Allows New Privacy-Invading Surveillance in the Name of Cybersecurity. **The Intercept.** 18 dez. 2015. Disponível em: https://theintercept.com/2015/12/18/last-minute-budget-bill-allows-new-privacy-invading-surveillance-in-the-name-of-cybersecurity/ Acesso em: 5 jan. 2019.

MOROZOV, Evgeny. **Big Tech**: a ascensão dos dados e a morte da política. São Paulo:Ubu Editora, 2018.

MOSCO, Vincent. **To the cloud:** Big data in a turbulent world. New York: Routledge, 2015.

MOTTA, Bárbara Vasconcellos de Carvalho. Securitização e política de exceção: o excepcionalismo internacionalista norte-americano na segunda Guerra do Iraque. 2014. 125 f. Dissertação (mestrado) - UNESP/UNICAMP/PUC-SP, Programa San Tiago Dantas, 2014.

MOWERY, David C. The US National Innovation System: Origins and Prospects for Change. In: MOWERY, David C (Ed.) **Science and technology policy in interdependent economies.** Springer, Dordrecht, 1994. p. 79-106.

NAUGHTON, John. The evolution of the Internet: from military experiment to General Purpose Technology. **Journal of Cyber Policy**, v. 1, n. 1, p. 5-28, 2016.

NOJEIM, Greg.; LAPERRUQUE, Jake. Cyber-Surveillance Bill to Move Forward, Secretly. **Center for Democracy & Technology.** 04 mar. 2015. Disponível em: https://cdt.org/insights/cyber-surveillance-bill-to-move-forward-secretly/ Acesso em: 31 jan. 2020.

NOLAN, Andrew. Cybersecurity and Information Sharing: Legal Challenges and Solutions. **Congressional Research Service**, Washington, DC. March 16, 2015. Disponível em: https://fas.org/sgp/crs/intel/R43941.pdf Acesso em: 10 set. 2019

NUSBAUM, Rachel. CISA Isn't About Cybersecurity, It's About Surveillance. **ACLU Washington Legislative Office.** 13 mar. 2015. Disponível em: https://www.aclu.org/blog/national-security/cisa-isnt-about-cybersecurity-its-about-surveillance Acesso em: 15 abr. 2019

NYE JR, Joseph S.; OWENS, William A. America's information edge. **Foreign Affairs**, v. 75, 1996.
PETERSON, Andrea. The Sony Pictures hack, explained. The Switch. **The Washington Post**. Dec.18, 2014. Disponível em: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/ Acesso em: 14 dez. 2019

PETRELLA, Simone. Google This Internet Surveillance: A Case Study of the Complex Relationship Between Telecommunications Companies and the US Government. **Journal of Law, Technology and Public Policy®**, v. 1, n. 1, p. 429, 2014. Disponível em: https://journal-law-tech-public-policy.scholasticahq.com/article/429.pdf Acesso em: 13 abr. 2019.

PHILLIPS, Macon. Introducing the New Cybersecurity Coordinator. **The White House Blog**. 22 dez. 2009. Disponível em: https://obamawhitehouse.archives.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator Acesso em: 10 jan. 2020.

POPP, Robert et al. Countering terrorism through information technology. **Communications of the ACM**, v. 47, n. 3, p. 36-43, 2004. Disponível em: https://dl.acm.org/doi/fullHtml/10.1145/971617.971642#sec-terms Acesso em: 14 fev.2019

POWERS, Shawn M.; JABLONSKI, Michael. **The real cyber war:** The political economy of internet freedom. University of Illinois Press, 2015.

PRESIDENT Bush Signs Anti-Terrorism Bill. **PBS New Hour,** 26 Oct. 2001. Disponível em: https://www.pbs.org/newshour/world/terrorism-july-dec01-bush_terrorismbill Acesso em: 31 mar. 2019.

PRIVACY SHIELD FRAMEWORK. Privacy Shield Framework Overview. 2020. Disponível em: https://www.privacyshield.gov/EU-US-Framework Acesso em: 10 jan. 2020.

REARDON, Marguerite. How 5G got tied up in a trade war between Trump and China. **Cnet,** 15 jul.2019. Disponível em: https://www.cnet.com/news/how-5g-got-tied-up-in-a-trade-war-between-trump-and-china/ Acesso em: 10 jan. 2020

REIDENBERG, Joel R. The data surveillance state in the United States and Europe. **Wake Forest L. Rev.**, v. 49, p. 583, 2014.Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/wflr49&div=21&id=&page= Acesso em: 04 mar. 2017

REITMAN, Rainey. NSA Internet Surveillance Under Section 702 Violates the First Amendment. **Electronic Frontier Foundation.** 22 nov.2017. Disponível em: https://www.eff.org/pt-br/deeplinks/2017/11/nsa-internet-surveillance-under-section-702-violates-first-amendment Acesso em: 30 nov.2019

RISEN, James; LICHTBLAU, Eric. Bush Lets U.S. Spy on Callers Without Cards. **The New York Times,** New York, Dec.16 2005. Disponível em: https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html Acesso em: 14 dez. 2019.

ROBERTSON, Adi. Who supports and opposes CISPA, and why? **The Verge.** May 2, 2012. Disponível em: https://www.theverge.com/2012/5/2/2993495/cispa-hr-3523-business-support-opposition Acesso em: 13 nov. 2019

ROSENBACH, Eric; MANSTED, Katherine. **The Geopolitics of Information**. Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School. May 28, 2019. Disponível em: https://www.belfercenter.org/publication/geopolitics-information Acesso em: 01 fev.2020.

ROSENZWEIG, Paul. **Cyber warfare:** how conflicts in cyberspace are challenging America and changing the world. Santa Barbara: ABC-CLIO, 2013.

ROZENSHTEIN, Alan Z. Surveillance intermediaries. **Stanford Law Review**, v. 70, jan.2018. p. 99-189. Disponível em: https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/01/70-Stan.-L.-Rev.-99.pdf Acesso em: 4 dez.2019.

RUPPERT, Evelyn; ISIN, Engin; BIGO, Didier. Data politics. **Big Data & Society**, v. 4, n. 2, jul.-dec. 2017, p. 1-7.

SCHNEIER, Bruce. The battle for power on the internet. **The Atlantic**, 24 out. 2013. Disponível em: http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824 Acesso em: 05 fev. 2019.

SCHNEIER, Bruce. **Data and Goliath**: The hidden battles to collect your data and control your world. New York: WW Norton & Company, 2015.

SIDHU, Kiran. A Call for Minority Involvement in Cybersecurity Legislation Reform and Civil Rights Protests: Lessons from the Anti-SOPA/ PIPA Demonstrations. **Hastings Communications & Entertainment Law Journal.** v.38, n.1, 2015, p. 117-144. Disponível em: https://repository.uchastings.edu/hastings_comm_ent_law_journal/vol38/iss1/5 Acesso em: 02 fev.2020.

SIMCOX, Robin. **Surveillance After Snowden**. Effective Espionage in an Age of Transparency London: Henry Jackson Society, 2015.

SINGER, Peter W.; FRIEDMAN, Allan. **Cybersecurity**: What everyone needs to know. New York: Oxford University Press, 2014.

SIVAN-SEVILLA, Ido. Trading privacy for security in cyberspace: A study across the dynamics of US federal laws and regulations between 1967 and 2016. In: **2017 9th International Conference on Cyber Conflict (CyCon)**. IEEE, 2017. p. 1-19. Disponível: https://ccdcoe.org/uploads/2018/10/Art-05-Trading-Privacy-for-Security-in-Cyberspace-A-Study-Across-the-Dynamics-of-US-Federal-Laws-and-Regulations.pdf Acesso em: 08 mar. 2018.

SPENDING Bill Inclusion of Cybersecurity Information Sharing Legislation is Victory for Strengthening Defenses Against Cyber Attacks. **Financial Service Roundtable**. 15 dez. 2015. Disponível em: http://fsroundtable.org/spending-bill-inclusion-of-cybersecurity-information-sharing-legislation-is-victory-for-strengthening-defenses-against-cyber-attacks Acesso em: 10 set.2019

STATE OF CALIFORNIA. Department of Justice. **California Consumer Privacy Act (CCPA)**. 2018. Disponível em: https://oag.ca.gov/privacy/ccpa Acesso em: 05 out. 2019.

SULLIVAN & CROMWELL LLP. **The Cybersecurity Act of 2015**. Dez. 2015.13 p. Disponível em: https://www.sullcrom.com/siteFiles/Publications/SC_Publication_The_Cybersecurity_Act_of_2015.pdf Acesso em: 10 mar.2019

TECH TRANSPARENCY PROJECT. Google's Revolving Door Explorer (US). April 26, 2016. Disponível em: https://www.techtransparencyproject.org/articles/googles-revolving-door-us Acesso em: 10 jan. 2020.

TECHNET. Letter to U.S. House Rep. Mike Rogers and Dutch Ruppersberger. 10 abril. 2013 Disponível em: https://pt.scribd.com/doc/135417743/TechNet-CISPA-support-letter Acesso em: 10 jan. 2020.

TEHAN, Rita. **Cybersecurity**: Legislation, Hearings, and Executive Branch Documents. Washington, DC: Congressional Research Service, 2018. 8 nov. 2018.

TEXT- Obama Remarks on Cybersecurity. **The New York Times,** 29 mai.2019. Disponível em: https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html Acesso em: 15 jan. 2020.

TIEN, Lee. CISPA Passes Out of the House Without Any Fixes to Core Concerns. **Electronic Frontier Foundation.** 1 mai. 2013. Disponível em: https://www.eff.org/pt-br/deeplinks/2013/04/cispa-passes-out-house-without-any-fixes-core-concerns Acesso em: 14 jan. 2020.

TRÉGUER, Félix. Seeing Like Big Tech: Security Assemblages, Technology, and the Future of State Bureaucracy. In: BIGO, Didier; ISIN, Engin; RUPPERT, Evelyn (Eds.). **Data Politics**: Worlds, Subjects, Rights. London: Routledge, 2019. p. 145-164.

UNIÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados**.2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN Acesso em: 10 jul.2019

UPSTREAM vs. PRISM. **Electronic Frontier Foundation.** [s.d.]. Disponível em: https://www.eff.org/pt-br/pages/upstream-prism Acesso em: 12 fev. 2019.
U.S. GOVERNMENT. **High-Performance Computing Act of 1991.** 102th Congress, 1991. Disponível em: https://web.archive.org/web/20070929115744/http://www.eff.org/Net_culture/Net_info/Misc/gore.bill Acesso em: 10 jan. 2020.

U.S. GOVERNMENT. Department of Defense Appropriations for 1996. **Hearings before a Subcommitee on Appropriations.** House of Representatives. Subcommitee on National Security. 1996.

U.S. GOVERNMENT. Department of State. **Global Internet Freedom Task Force (GIFT) Strategy**: A Blueprint for Action. 2006. Disponível em: https://2001-2009.state.gov/g/drl/rls/78340.htm Acesso em: 3 jan.2020.

U.S. GOVERNMENT. **Foreign Intelligence Surveillance Act of 1978 Amendments Act Of 2008**. 2008. Disponível em: https://www.congress.gov/110/plaws/publ261/PLAW-110publ261.htm Acesso em: 05 fev. 2020.

U.S. GOVERNMENT. The White House. **Remarks by the President on Securing Our Nation's Cyber Infrastructure.** 29 maio 2009. Disponível em: https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure Acesso em: 3 nov. 2019

U.S. GOVERNMENT. H.R.3523.– **Cyber Intelligence Sharing and Protection Act,** 112th Congress, 2011. Disponível em: https://www.congress.gov/bill/112th-congress/house-bill/3523 Acesso em: 26 jan. 2019

U.S. GOVERNMENT. United States Executive Office of the President. **Cyberspace Policy Review**: Assuring a Trusted and Resilient Information and Communication Infrastructure. 2014a. Disponível em: https://www.nationalcyberwatch.org/ncw-content/uploads/2016/03/Cyberspace_Policy_Review_final-1-1.pdf

U.S. GOVERNMENT. The White House. **Presidential Policy Directive nº28.** 17 jan. 2014b. Disponível em: https://www.dni.gov/index.php/ic-legal-reference-book/presidential-policy-directive-28 Acesso em: 14 jan. 2020.

U.S. GOVERNMENT. **Executive Order n 13691**.“Promoting Private Sector Cybersecurity Information Sharing,” 13 de fevereiro de 2015a. Disponível em: https://www.govinfo.gov/content/pkg/CFR-2016-title3-vol1/pdf/CFR-2016-title3-vol1-eo13691.pdf Acesso em: 10 mai. 2019.

U.S. GOVERNMENT. H.R.234 – **Cybersecurity Intelligence Sharing and Protect Act,** 114th Congress, 2015b, https://www.congress.gov/114/bills/s754/BILLS-114s754es.pdf

U.S. GOVERNMENT. **Consolidated Appropriations Act of 2016**. 16 dez. 2015c. Disponível em: https://docs.house.gov/billsthisweek/20151214/CPRT-114-HPRT-RU00-SAHR2029-AMNT1final.pdf Acesso em: 10 out. 2019.

U.S. GOVERNMENT. Department of Homeland Security. **Privacy Impact Assessments.** 2015 d. Disponível em: https://www.dhs.gov/privacy-documents-cisa Acesso em: 10 jan.2020.

U.S. CHAMBER President Comments on Omnibus Spending Bill. **U.S. Chamber of Commerce.** 16 dez. 2015. Disponível em: https://www.uschamber.com/press-release/us-chamber-president-comments-omnibus-spending-bill, Acesso em: 07 set.2019

VENDITUOLI, Monica. Cybersecurity, Privacy Issues Spurred Lobbying Even Before NSA Programs Revealed. **OpenSecrets News.** June 11, 2013. Disponível em: https://www.opensecrets.org/news/2013/06/privacy-issues-2013/ Acesso em: 18 set. 2019

WEISS, N. Eric. **Legislation to facilitate cybersecurity information sharing:** Economic analysis. Washington, DC: Congressional Research Service, 2015. 23 fev. 2015.

WELLS, Maren. The USA Patriot Act and Internet Surveillance. **Brigham Young University Prelaw Review**, v. 17, n. 1, p. 7, 2003. p. 53-60. Disponível em: https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=1058&context=byuplr Acesso em: 31 jan. 2020.

WEST, Sarah Myers. Data capitalism: Redefining the logics of surveillance and privacy. **Business & Society**, v. 58, n. 1, p. 20-41, 2019. Disponível em: https://journals.sagepub.com/doi/10.1177/0007650317718185 Acesso em: 12 jun. 2019

WILLS, Jocelyn. **Tug of War:** Surveillance Capitalism, Military Contracting, and the Rise of the Security State. McGill-Queen's Press-MQUP, 2017.

WOLOSYN, André Luís. **Vigilância & espionagem digital**: a legislação internacional e o contexto brasileiro. Curitiba: Juruá Editora, 2016.

YOUNG, Mark D. Electronic Surveillance in an Era of Modern Technology and Evolving Threats To National Security. **Stan. L. & Pol'y Rev.**, v. 22, p. 11, 2011. Disponível: https://www-cdn.law.stanford.edu/wp-content/uploads/2018/03/young-1.pdf Acesso em: 10 mar. 2019

ZUBOFF, Shoshana. Big other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda et al. (Orgs.). **Tecnopolíticas da vigilância:** perspectivas da margem. São Paulo: Boitempo Editorial, 2018. pp. 17-68.

ZUBOFF, Shoshana. **The age of surveillance capitalism:** The fight for a human future at the new frontier of power. New York: Profile Books, 2019.