UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE CIÊNCIAS ECONÔMICAS
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS

MIKAEL DOMENICI CORREA

PRIVACIDADE NA SEGUNDA ERA DIGITAL: DESAFIO TECNOLÓGICO E POLÍTICO

Porto Alegre
2019

MIKAEL DOMENICI CORREA

PRIVACIDADE NA SEGUNDA ERA DIGITAL: DESAFIO TECNOLÓGICO E POLÍTICO

Trabalho de Conclusão submetido ao Curso de Graduação em Relações Internacionais da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título Bacharel em Relações Internacionais.

Orientador: Prof. Dr. Marco Aurélio Chaves Cepik

Porto Alegre

2019

CIP - Catalogação na Publicação

Correa, Mikael Domenici
PRIVACIDADE NA SEGUNDA ERA DIGITAL: DESAFIO TECNOLÓGICO E POLÍTICO / Mikael Domenici Correa. -- 2019.
77 f.
Orientador: Marco Aurélio Chaves Cepik.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Curso de Relações Internacionais, Porto Alegre, BR-RS, 2019.

1. Governança da Internet. 2. Privacidade. 3. Novas Tecnologias. 4. Vigilância. 5. Segunda Era Digital. I. Cepik, Marco Aurélio Chaves, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

MIKAEL DOMENICI CORREA

PRIVACIDADE NA SEGUNDA ERA DIGITAL: DESAFIO TECNOLÓGICO E POLÍTICO

Trabalho de Conclusão submetido ao Curso de Graduação em Relações Internacionais da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título Bacharel em Relações Internacionais.

Aprovada em: Porto Alegre, _____de _____de 2019.

BANCA EXAMINADORA:

Professor Doutor Marco Aurélio Chaves Cepik – Orientador
UFRGS

Professor Doutor Érico Esteves Duarte
UFRGS

Professor Doutor Eduardo Munhoz Svartman
UFRGS

AGRADECIMENTOS

Gostaria de agradecer aos meus pais, Catarina Domenici e James Correa, pelos anos de amor e educação que me proporcionaram nos últimos 23 anos – sempre me incentivando a atingir grandes objetivos educacionais e me incentivando a conquistar meu lugar na Universidade Federal do Rio Grande Sul, universidade gratuita e de ampla excelência acadêmica. A esta, agradeço pela oportunidade de receber uma educação gratúita e de altíssima qualidade.

Segundamente, gostaria de agradecer à minha companheira, Michelle Perino, por estar presente nas minhas vitórias, derrotas e superações. Obrigado por me apoiar e sempre enxergar a melhor versão de mim – sempre me incentivando a atingir objetivos cada vez mais altos e a explorar todo meu potencial. Agradeço pelos 4 anos de companheirismo e apoio. Sem ti, eu certamente não seria a mesma pessoa que sou hoje.

Ademais, gostaria de agradecer especialmente ao meu orientador, Marco Cepik, por aceitar meu pedido de orientação e comprar junto comigo o desafio que esta monografia presentou, pela confiança em meu trabalho e pelo encorajamento para que eu cumpra uma monografia deste porte e profundidade – muito obrigado pela sua grande convicção e exemplo e por me guiar nos trabalhos deste último ano.

Um obrigado especial a todos os companheiros de curso, funcionários, amigos, colegas e camaradas que, da sua maneira, contribuíram para que chegasse a este momento tão importante da minha jornada como indivíduo e profissional. Obrigado Júlia pela parceria do jardim A até os trancos e barrancos do TCC e formatura. A Pedro, Thiago e Maurício, obrigado pelos momentos de lazer nesse último ano e pela amizade todos os outros anos. Ao grupo de amigos da faculdade, o famoso Amigos 2.0, vivemos muito nestes últimos seis anos de graduação, obrigado pelo companheirismo e pelas boas risadas ao longo deste ciclo. Aos meus amigos não mencionados, isso não faz de vocês menos importantes e sou muito grato por todos vocês.

Por fim, mas longe de ser o menos importante, agradeço mais uma vez a UFRGS e os professores do curso de Relações Internacionais pela educação proporcionada nos últimos anos, apesar de todos os desafios que a universidade pública enfrentou e continua enfrentando desde meu ingresso em 2014. Resistimos.

RESUMO

Esta monografia tem como tema a governança da Internet e privacidade, possuindo como objeto de estudo a privacidade na Segunda Era Digital como desafio tecnológico e político. A problemática geral que se busca responder é como as novas tecnologias da segunda era digital afetam a privacidade dos usuários de internet e como os governos nacionais de países selecionados respondem a este fenômeno. A partir disso, tem-se o objetivo geral de analisar o conjunto de novas tecnologias da Segunda Era Digital, os desafios à privacidade gerados por elas e entender como os governos nacionais estão respondendo a eles. A hipótese do presente trabalho parte da premissa de que as tecnologias da segunda era digital permitem a coleta e análise de uma quantidade cada vez maior de dados pessoais dos usuários de internet. As empresas e Estados adquirem esses dados para fins mercadológicos e/ou de segurança nacional através dessas tecnologias. A infraestrutura que possibilita o desenvolvimento das tecnologias da Segunda Era Digital, combinada com o modelo atual de governança da internet, permite que os dados sejam armazenados fora do território e da jurisdição nacional, limitando ainda mais a capacidade de controle dos usuários sobre seus dados e sobre os governos e corporações. Dado o desconforto que isso gera, os governos nacionais combinam medidas de proteção à privacidade com listas de exceções cada vez mais amplas e vagas. A metodologia empregada consiste de análise de fontes secundárias e análise documental, incluindo documentos vazados da NSA e documentos oficiais dos governos americano e chinês. Esta monografia está organizada em uma introdução, dois capítulos de desenvolvimento e uma conclusão. Este trabalho conclui que na competição entre os estados no sistema internacional, os indivíduos se tornam vítimas da vigilância exercida pelos governos (e empresas) nas empreitadas feitas para avançar suas posições na competição interestatal pelas tecnologias da Segunda Era Digital.

Palavras-chave: governança da internet, privacidade, novas tecnologias, vigilância, Segunda Era Digital

ABSTRACT

This undergraduate thesis investigates Internet governance and privacy focusing on the study of privacy in the Second Digital Age as a technological and political challenge. The main problem this study addresses is how the new technologies of the Second Digital Age affect the privacy of internet users and how national governments of the countries selected for this study respond to this phenomenon. The overall objective of this undergraduate thesis is to analyze the set of new technologies of the Second Digital Age and the privacy challenges generated by them, as well as to understand how national governments are responding to them. The hypothesis of this thesis assumes that the technologies of the Second Digital Age allow the collection and analysis of an increasing amount of personal data from internet users. Companies and states acquire this data for market and/or national security purposes through these technologies. The infrastructure that enables the development of Second Digital Age technologies, combined with the current model of internet governance, allows data to be stored outside the territory and national jurisdiction, further limiting users' ability to control their data and to hold governments and corporations accountable. Given the tensions this creates, national governments combine privacy protection measures with ever-broader and more vague lists of privacy exceptions. The methodology employed in this study comprises secondary source analysis and document analysis, including leaked NSA documents and official US and Chinese government documents. This undergraduate thesis is divided in an introduction chapter, two development chapters, and a conclusion chapter. This study concludes concludes that in the competition between states in the international system, individuals become victims of the vigilance exercised by governments and corporations in the endeavors to advance their positions in the interstate competition for the technologies of the Second Digital Age.

Keywords: internet governance, privacy, new technologies, surveillance, Second Digital Era

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

5G	- Quinta Geração de Redes Móveis
AGI	- *Artificial General Intelligence*
ASD	- *Australian Signals Directorate*
BND	- *Bundesnachrichtendienst*
DSD	- *Defence Signals Directorate*
EPC	- *Electronic Product Code*
EUA	- Estados Unidos da América
GSR	- Global Science Research
IA	- Inteligência Artificial
IaaS	- *Infrastructure as a Service*
SIGINT	- Inteligência de Sinais
IoT	- *Internet of Things*
IP	- *Internet Protocol*
NSA	- *National Security Agency*
NIST	- *National Institute of Standards and Technology*
OTAN	- Organização do Tratado do Atlântico Norte
PaaS	- *Platform as a Service*
SaaS	- *Software as a Service*
TI	- Tecnologia da Informação
RFID	- *Radio Frequency IDentification*
UE	- União Europeia
WSN	- *Wireless Sensor Node*
WWWW	- *World Wide Wireless Web*

SUMÁRIO

1 INTRODUÇÃO

Debates acerca da proteção da privacidade informacional dos indivíduos têm se mostrado cada vez mais presentes na sociedade ao longo dos últimos anos. As legislações de proteção de dados (catalisados pelas revelações de Edward Snowden), as investigações do Facebook após o escândalo da Cambridge Analytica e uma atenção cada vez maior à privacidade e segurança por parte das empresas de tecnologia estão todos conectados a temas como proteção de dados, coleta de dados e direcionamento de propagandas – seja ele de cunho mercadológico ou eleitoral. Para entender o que trouxe esses debates à tona, é preciso entender o que mudou tecnologicamente no mundo digital.

Para iniciar, a Primeira Era Digital viu a democratização do acesso à computação, o surgimento da Internet, o fenômeno da digitalização da informação e o início da dataficação (CANABARRO, 2014). Como um próximo passo, a Segunda Era Digital encontra no seu seio a expansão da dataficação para todos os aspectos da vida *online* e *offline* e um aumento da personalização da mesma. Para isso, cinco paradigmas e tecnologias emergentes se mostram centrais para a Segunda Era Digital: os paradigmas do *big data* e da *Internet of Things*, a inteligência artificial, as tecnologias em nuvem e a quinta geração de redes móveis (5G). O paradigma do *big data* se refere ao novo volume de dados sendo criados, coletados, armazenados e analisados por conta do aprofundamento da dataficação. Com esse novo paradigma de dados, uma cadeia de valor de dados surge, na qual o valor está na extração de informações a partir da análise de dados diversos (LANGWORTHY, 2019). O paradigma da IoT, por sua vez, está relacionado a conexão de sensores e dispositivos diversos à internet, aumentando o alcance da coleta de dados para além dos nossos *smartphones* e computadores pessoais, permitindo não só objetos materiais inteligentes e conectados à internet, mas também a coleta de dados para além da navegação tradicional da internet (VELGHE, 2019; LEHR, 2019; LYON, 2018).

A inteligência artificial, por meio de avanços significativos utilizando técnicas de *deep learning* e arquiteturas de redes neurais inspiradas no cérebro humano, têm revolucionado a análise dos dados, ocupando um papel central na geração de valor a partir da extração de informações dos dados coletados. As tecnologias em nuvem, por sua vez, compõem parte da infraestrutura da Segunda Era Digital. Graças às tecnologias em nuvem, armazenamento e poder computacional tendem a não serem mais problemas para os dispositivos, permitindo a utilização sob demanda destes recursos a um custo baixo. Além do mais, o armazenamento em nuvem busca acompanhar e suportar o volume crescente do *big data*, enquanto a computação em nuvem permite ampliar o acesso às capacidades computacionais necessárias para analisar

os dados. A 5G, por fim, compõe também parte da infraestrutura da Segunda Era Digital. O objetivo da 5G é revolucionar a conectividade através do aumento da velocidade de transmissão de dados, diminuição do tempo de resposta e aumento do número de dispositivos conectados ao mesmo tempo em uma determinada área.

Outro conceito essencial para compreender a Segunda Era Digital é a personalização dos dados que, junto com a dataficação, catalisa a vigilância na Segunda Era Digital. A personalização dos dados cria um paradoxo na Segunda Era Digital: por um lado, ela é vista como necessária para melhorar serviços e produtos, otimizar as atividades e para o progresso sócio-econômico por via dela e da tecnologia (LIU, 2018); por outro lado, a personalização, com tantos dados pessoais disponíveis, possibilita uma vigilância generalizada na qual atores privados e governamentais buscam, através dos dados extremamente personalizados, identificar pessoas que se encaixem em um perfil e influenciá-las ou gerencia-las (LYON, 2014; LYON, 2015; LYON, 2018). Muito da coleta personalizada, entretanto, ocorre sem a ciência ou consentimento explícito dos indivíduos, ferindo, assim, a privacidade dos usuários (LYON, 2014; ETZIONI, 2015).

A personalização está muito ligada à vigilância na Segunda Era Digital. Ela faz uso da vigilância e contribui para o aprofundamento da mesma. A vigilância, por sua vez, se mostra como a maior ameaça à privacidade na Segunda Era Digital. Empresas utilizam a vigilância, catalisada pela personalização, buscando maiores lucros através da utilização das informações para: i) direcionar o seu negócio (como o marketing direcionado, por exemplo); ii) da venda dos dados para outras entidades (públicas e privadas) ou; iii) ofertar serviços que utilizam as informações (como no caso do *political micro-targeting* oferecido pela Cambridge Analytica) (ETZIONI, 2015; LYON, 2014; MANOKHA, 2018; BODÓ; HELBERGER; VREESE, 2017). Atores estatais, por sua vez, utilizam a vigilância para fins de segurança nacional (atividades de inteligência, por exemplo), de segurança pública (policiamento preventivo e CCTV com reconhecimento facial) e, crescentemente, de governança (BAUMAN et al., 2014; LEHR, 2019; MADSEN et al., 2016).

O presente trabalho de conclusão de curso, portanto, tem como tema a privacidade na Segunda Era Digital e a governança da internet, procurando responder às perguntas de como as novas tecnologias da Segunda Era Digital afetam a privacidade dos usuários de internet e de como os governos nacionais de países selecionados respondem a este fenômeno. Assim, a hipótese do presente trabalho parte da premissa de que as tecnologias da segunda era digital permitem a coleta e análise de uma quantidade cada vez maior de dados pessoais dos usuários de internet. As empresas e Estados adquirem esses dados para fins mercadológicos e/ou de

segurança nacional através dessas tecnologias. A infraestrutura que possibilita o desenvolvimento das tecnologias da Segunda Era Digital, combinada com o modelo atual de governança da internet, permitem que os dados sejam armazenados fora do território e da jurisdição nacional, limitando ainda mais a capacidade de controle dos usuários sobre seus dados e sobre os governos e corporações. Dado o desconforto que isso gera, os governos nacionais combinam medidas de proteção à privacidade com listas de exceções cada vez mais amplas e vagas.

Com isso em mente, o objetivo geral desta pesquisa é analisar o conjunto de novas tecnologias da Segunda Era Digital, os desafios à privacidade gerados por elas e entender como os governos nacionais estão respondendo a eles. No que tange os objetivos específicos e complementares da pesquisa, tendo em vista a natureza dinâmica e recente do tema, os objetivos são:

(i) analisar a literatura existente para conceituar e delimitar as novas tecnologias da Segunda Era Digital – *Big Data*, *Internet of Things*, Inteligência Artificial, tecnologias em nuvem e 5G – para, assim entender os desafios que surgem com elas.

(ii) verificar e analisar como os governos nacionais reagem aos desafios impostos à privacidade, tanto ameaçando quanto buscando protegê-la. Busca-se, também, estabelecer como marcos temporais importantes para a discussão da privacidade na Segunda Era Digital as revelações de Edward Snowden, de 2013, e o escândalo da Cambridge Analytica de 2016.

Esta monografia se insere academicamente na pequena produção científica na intersecção dos campos da Tecnologia da Informação e Relações Internacionais. Da mesma forma que o modelo de governança da internet vigente possui um viés e foco técnico, o estudo dos impactos das novas tecnologias e seus desafios ainda está bastante concentrado nos campos técnicos da Informática, Computação e Engenharia. Embora já estejam surgindo produções deste tema a partir de um olhar das Relações Internacionais e da Ciência Política mundo afora[1], ainda verifica-se uma ausência de produções sobre isso no Brasil e na América Latina. Tendo em vista o papel que o Brasil desempenhou nos debates da governança da internet e da privacidade após as revelações de Snowden (vide a CPI da Espionagem, Marco Civil da Internet e o fórum NETMundial) e a centralidade que este tema está tomando nas políticas cibernéticas dos países, é de extrema relevância contribuir para essa discussão e trazê-la para as academias brasileira e latino-americana.

[1] Algumas das obras incluem SÆTNAN; SCHNEIDER; GREEN, 2019; LANGWORTHY, 2019; LEHR, 2019; HANSEN; PORTER, 2017.

A principal metodologia que foi utilizada é a análise qualitativa, com a análise bibliográfica possuindo um papel central na pesquisa. Foi feita uma análise de materiais secundárias como livros, artigos e demais textos científicos que dizem respeito às novas tecnologias, debates de privacidade e das políticas cibernéticas e de dados nacionais, regionais e internacionais. Além do mais, houveram análises documentais de documentos da NSA revelados por Edward Snowden, em específico aqueles que trazem informações sobre programas de vigilância específicos ou das estratégias da NSA para com as mudanças da Segunda Era Digital que estavam em curso na época de elaboração de tais documentos. Os documentos trazem potenciais confirmações de atividades de vigilância que, embora sejam possíveis, eram secretas. A escolha pela análise qualitativa se dá a partir da escassez de dados, métodos e referenciais teóricos quantitativos para o tema da governança da internet e da privacidade e pela necessidade de objetivação e observância.

Inicialmente, foi realizada uma análise de materiais secundários para a elaboração do primeiro capítulo na qual foram analisados artigos, livros, revistas e periódicos que abordam as novas tecnologias para facilitar o entendimento de como funciona o conjunto delas na Segunda Era Digital. Tendo em vista a contemporaneidade e evolução constante do tema, o recorte temporal dos textos foi adequado de acordo com a tecnologia que foi analisada. Textos relacionados a *Big Data* e tecnologias em nuvem foram, preferencialmente, publicados a partir de 2011. No caso dos textos que dizem respeito a *Internet of Things* e 5G, tiveram preferência textos com data de publicação a partir de 2015. Em relação a Inteligência Artificial, foram buscados textos com data de publicação a partir de 2000 até 2019 com o fim de possibilitar uma compreensão maior desse campo interdisciplinar e os termos (e tecnologias) compreendidos por ele. Como se busca elucidar o funcionamento destas tecnologias, boa parte das publicações são dos campos técnicos como a Ciência da Computação, Engenharia e Matemática. Também foram utilizados, como bibliografia secundária de apoio, publicações não-científicas por profissionais qualificados e certificados das áreas técnicas. Para a elaboração do segundo capítulo, foram analisados materiais secundários e alguns primários como os documentos da NSA revelados por Snowden.

Esta monografia, por fim, está dividida em uma introdução, dois capítulos de desenvolvimento e uma conclusão. No primeiro capítulo de desenvolvimento, a Segunda Era Digital será conceitualizada. Delimitado o conceito, as cinco principais tecnologias que caracterizam a Segunda Era Digital – *Big Data*, *Internet of Things*, Inteligência Artificial, tecnologia em nuvem e 5G – e seus funcionamentos serão exploradas e explicadas. Nesta parte do primeiro capítulo, serão elucidadas as relações de cada tecnologia com as outras. No final

do primeiro capítulo, serão apresentados os principais desafios que surgem por causa destas tecnologias – dentre eles, os desafios à privacidade.

Ao longo do segundo capítulo de desenvolvimento, serão apresentados como os dois principais acontecimentos e marcos temporais da Segunda Era Digital – as revelações de Edward Snowden em 2013 e o escândalo da Cambridge Analytica em 2016 – junto com a importância deles para entender algumas das principais ameaças à privacidade e as maneiras como os dados – obtidos ao violar a privacidade – podem ser utilizados. Em seguida, analisa-se algumas atividades de vigilância (*surveillance*) existentes no mundo – como as reveladas por Snowden e o complexo estado-comercial de vigilância – e como eles violam a privacidade. Por fim, analisa-se a questão da proteção de dados olhando, primeiramente, o problema da territorialização de dados e a jurisdição dos mesmos para, então, analisar as medidas governamentais de proteção de dados e, posteriormente, as medidas do setor privado para tal desafio.

2 A SEGUNDA ERA DIGITAL

A Segunda Era Digital é uma evolução da Primeira, causada pela consolidação da Internet como rede das redes e pela convergência de cinco tecnologias e paradigmas principais: o paradigma do *Big Data*; a *Internet of Things*; a Inteligência Artificial; as tecnologias em nuvem e; a quinta geração de redes móveis (5G). Tendo isso em mente, este capítulo irá, em um primeiro momento, apresentar a Primeira Era Digital para então conceitualizar a Segunda Era Digital. Depois, as cinco tecnologias e paradigmas serão apresentadas e explicadas para entender como elas convergem e caracterizam a Segunda Era Digital. Por fim, alguns dos desafios políticos gerados por estas novas tecnologias serão apresentados brevemente.

2.1 DA PRIMEIRA À SEGUNDA ERA DIGITAL

O termo "Era Digital" é utilizado por Canabarro (2014) para se referir a um modelo técnico-econômico caracterizado pela computação e por informações no meio digital que foi desenvolvido e consolidado ao longo da segunda metade do século XX. Em um sentido mais abrangente:

> [...] a Era Digital diz respeito basicamente à manipulação, armazenamento e propagação de informações em formato digital através de dispositivos eletrônicos, o que permitiu o desenvolvimento da computação digital. Como um subproduto decorrente dessa tecnologia, esforços empreendidos para a viabilização da comunicação entre computadores distintos contribuíram para o desenvolvimento de técnicas de organização de redes computacionais variadas. Dentre elas, a Internet consolidou-se como a principal rede de alcance mundial (CANABARRO, 2014 p.49).

Assim, a Era Digital possui no seu centro a digitalização da informação, a computação digital, o desenvolvimento de microcomputadores com cada vez mais poder de processamento (e sistemas de menor tamanho) e a Internet (CANABARRO, 2014).

As duas principais tecnologias responsáveis pela democratização da computação e pela inclusão digital na Era Digital, segundo Canabarro (2014), são os computadores pessoais (PC) e a Internet. Entretanto, com exceção da Internet, verifica-se na literatura que um conjunto de novas tecnologias e paradigmas estão sendo desenvolvidos e consolidados nesta última década e que tais tecnologias estariam gerando mudanças sócio-econômicas e políticas diferentes e mais profundas do que as da Era Digital. Levando em consideração estas mudanças, que serão elaboradas ao longo da monografia, a Era Digital, conforme descrita e conceitualizada por Canabarro (2014), será considerada como a Primeira Era Digital neste trabalho.

Dado o papel central da Internet tanto para a Primeira Era Digital quanto para a Segunda, que será conceitualizada mais para frente neste capítulo, é importante entender como a Internet

funciona e alguns de seus elementos centrais. Na literatura, é possível verificar uma taxonomia para analisar a Internet através de três a quatro camadas verticais: uma primeira camada de infraestrutura física; uma segunda camada lógica englobando protocolos, endereçamento e outros padrões técnicos; uma terceira composta por *softwares*, aplicações, conteúdo e informação, e; uma última camada reservada para relações e atores tanto sociais quanto políticos (CERF; DRAKE; KLEINWACHTER, 2016[2]; DENARDIS, 2016[3]; HILL, 2012[4]; CANABARRO, 2014[5]). A maior variação que existe na literatura em relação a estas taxonomias é a inclusão desta última camada político-social e a divisão dos protocolos, endereçamento, aplicações e conteúdo nas camadas intermediárias, podendo utilizar duas camadas intermediárias – variando em o que está incluso em cada (DENARDIS, 2016; HILL, 2012; CANABARRO, 2014) ou separando em várias camadas intermediárias (CERF; DRAKE; KLEINWACHTER, 2016).

Pode-se dizer que a internet, como a rede de comunicação digital mundial e aberta que conhecemos hoje, nasceu em 1992[6] com a abertura do acesso à rede pelo governo americano, decisão que tornou a infraestrutura física americana a espinha dorsal da internet, conectando

[2] Cerf, Drake e Kleinwachter (2016), em "*Internet Fragmentation: An Overview*", descrevem a internet como tendo cinco camadas verticais – quatro delas vindo da o campo da engenharia computacional e uma camada social criada por eles. A primeira é a de infraestrutura física pela qual os dados são transferidos. A segunda camada é chamada pelos autores de a camada da internet, na qual opera o protocolo IP. A terceira camada é composta pelos protocolos de transporte de dados, e a quarta é a de aplicações e protocolos de utilidade. A quinta e última camada abrange conteúdo e transações, tendo um fim político e social (CERF; CRAKE; KLEINWACHTER, 2016).

[3] Laura DeNardis (2016) em "*One Internet: An evidentiary Basis for Policy Making on Internet Universality and Fragmentation*" combina a segunda e terceira camadas apresentadas por Cerf, Drake e Kleinwachter (2016), apresentando o que ela chama de quatro "categorias conceituais". A primeira, como em Cerf, Drake e Kleinwachter (2016) e a maior parte da literatura, consiste na infraestrutura física que transfere os dados. A segunda camada de DeNardis (2016) combina a segunda e terceira camadas de Cerf, Drake e Kleinwachter (2016) em uma única chamada de "recursos lógicos", englobando aqui endereços de IP e protocolos. Sua terceira camada abrange as aplicações e conteúdo, enquanto sua quarta e última camada é chamada de "camada legal", a qual engloba questões como tratados internacionais e políticas nacionais (DENARDIS, 2016).

[4] Jonah Force Hill (2012) utiliza uma abordagem parecida com a de DeNardis (2016), porém ainda menos técnica. A segunda camada continua sendo chamada de camada lógica, mas passa a englobar não somente protocolos e endereçamento, mas também aplicações. A terceira camada passa a ser chamada de "camada da informação" e contém todo o conteúdo online. A quarta e última camada tem o nome de "*people layer*", que se refere aos atores tanto políticos quanto usuários da internet (HILL, 2012).

[5] Canabarro (2014), por sua vez, apresenta uma abordagem vertical em três camadas: uma primeira de infraestrutura; uma segunda "lógica" englobando os padrões técnicos como protocolos e endereçamento e; por fim, uma de conteúdo e aplicações, composta pelos *softwares* que permitem o compartilhamento e acesso de informações na internet. Todavia, Canabarro (2014) reconhece que pode haver uma camada complementar que capture as "dinâmicas sociais" que ocorrem por conta da e na Internet (CANABARRO, 2014).

[6] Anteriormente a essa decisão, a ARPANET – rede precursora da internet – havia sido desenvolvida sob a tutela do Departamento de Defesa dos Estados Unidos e de pesquisadores de universidades americanas. Em 1982, a ARPANET foi dividida em duas redes: uma militar, chamada a MILNET e de uso exclusivo pelo setor militar americano; e uma civil com finalidade acadêmica, que ficou a cargo da *National Science Foundation* (NSF) e que tomaria o nome de NSFNET em 1987. Por conta da centralidade da academia americana e da importância das redes para a academia como um todo, redes de outras universidades mundo afora buscaram se conectar com a NSFNET. A conexão com a NSFNET e sua infraestrutura, assim era condicionada ao aceite dos Termos de Uso do governo americano (CANABARRO, 2014).

redes espalhadas pelo mundo inteiro (CANABARRO, 2014). Um dos elementos centrais que permitiu o surgimento de uma rede de redes – e posteriormente, da Internet – é o protocolo de TCP/IP. Na computação, os protocolos "servem para abrir o canal de comunicação entre computadores e organizar formal e substancialmente a troca de mensagens entre as duas pontas" (CANABARRO, 2014, p. 64). O TCP (*transfer control protocol*) estabelece as regras para o transporte de pacotes de informação[7]. O IP (*Internetworking protocol*) serve como um "endereço virtual"[8] para os computadores.

Os endereços de IP são representados na forma decimal – representação que já facilita quando comparado ao formato técnico original em *bytes* representados na forma binária. Para facilitar mais ainda, foi desenvolvido o Sistema de Nomes de Domínio (DNS[9]). O DNS, inclusive, é um sistema que permite a tradução de nomes-fantasia para endereços de IP. Assim, é possível utilizar palavras para se conectar a um endereço de IP, diminuindo a complexidade de uso da rede. Para que isso ocorra, o DNS precisa cuidar da distribuição dos nomes de domínio e manter uma lista atualizada dos nomes de domínio e seus endereços de IP correspondentes (CANABARRO, 2014; MUELLER, 2002; WAGNER; CANABARRO, 2014).

A base de dados do DNS e as demais atividades da sua manutenção e operação fazem parte do que se chama de raiz da Internet. "A raiz da Internet é formada por treze servidores espalhados no mundo, controlados por entidades públicas e privadas, com e sem fins lucrativos" (CANABARRO, 2014, p. 86). A gestão da raiz da Internet hoje está sob responsabilidade da *Internet Corporation for Assigned Names and Numbers* (ICANN)[10]. O DNS junto com a infraestrutura física da rede e com o endereçamento IP constituem o que é chamado dos recursos críticos da Internet (CANABARRO, 2014; WAGNER; CANABARRO, 2014). Ao controlar e gerir a raiz, a ICANN acabou se tornando um dos principais focos da governança global da Internet (SEGAL, 2016; CANABARRO, 2014).

---

[7] Para transferir informações digitais, elas são divididas em pequenos pacotes de dados numéricos e enviados até o destino, onde a informação original é remontada a partir dos pacotes de dados (CANABARRO, 2014).

[8] Canabarro e Foruzan utilizam uma analogia com o correio físico, em que uma informação digital é dividida em pacotes, empacotados, endereçados, enviados e recebidos na outra ponta (CANABARRO, 2014; FORUZAN, 2008 apud CANABARRO, 2014, p. 28). Da mesma maneira que endereços físicos, cada dispositivo - ou "complexo"/rede de dispositivos – possui um único endereço de IP exclusivo (que pode ser tanto temporário quanto permanente), assim garantindo uma comunicação estável pela Internet (CANABARRO, 2014).

[9] Sigla vem do nome em inglês, *Domain Name System*.

[10] Antes da criação da ICANN, as funções de administração da raiz eram da *Internet Assigned Numbers Authority* (IANA), que era inicialmente do Instituto de Ciências da Informação da Universidade do Sul da Califórnia (ISI/USC) (CANABARRO, 2014).

Graças a proliferação destes elementos (com destaque para o protocolo TCP/IP), a Internet pôde se tornar a rede das redes (CANABARRO, 2014[11]). Quando se junta, então, os avanços nos microcomputadores e das tecnologias móveis com a Internet, um número cada vez maior de dispositivos passa a estar conectado na Internet, resultando em uma quantia cada vez maior de dados sendo gerados por estes dispositivos (FRENCH; SHIM, 2016). Ao mesmo tempo, surgiram avanços significativos por volta de 2011-2012 na área do *machine learning* dentro da área da Inteligência Artificial (IA) (USA, 2018; MIAILHE; HODES, 2017). French e Shim (2016) chamam essa mudança, que surge a partir da revolução digital, de era da computação ubíqua[12], com um enfoque nas tecnologias da *Internet of Things* (IoT), na quinta geração de redes móveis (5G) e no que os autores chamam de *big data analytics*. Os autores também trazem o conceito de *social IoT* como um passo após a era da computação ubíqua, na qual existiria uma rede de objetos inteligentes e interligados compartilhando informações entre si e entregando serviços ao usuário. Segundo os autores, tal conceito ainda não possui uma definição sólida (FRENCH; SHIM, 2016).

Outros autores englobam estes desenvolvimentos – *big data*, *machine learning*, IoT – dentro do termo da IA (USA, 2018; JOHNSON, 2019; USA, 2016a). Miailhe e Hodes (2017), além de apontarem para a convergência do *Big Data* e do *machine learning*, incluem uma outra tecnologia: a computação em nuvem. Rao e Prasad (2018), ao falarem da "indústria 4.0", ressaltam como tecnologias chaves para esse novo paradigma de produção industrial também a IA, IoT, *machine learning*, tecnologias em nuvem e a 5G. Por outro lado, Li, Xu e Zhao (2018) englobam essas tecnologias dentro de um guarda-chuva da 5G com a IoT, juntando as tecnologias em nuvem e as análises do *Big Data* através da IA dentro da IoT e considerando a 5G como um catalisador para esse novo paradigma. Pant e Tirkey (2018), Chen e Kang (2018) e Lewis (2018) seguem uma linha parecida à de Li, Xu e Zhao (2018), englobando todas essas tecnologias debaixo do guarda chuva da 5G. Langworthy (2019), por sua vez, chama esse novo momento como a era do *big data*, enquanto N'Guyen (2019) aponta para uma sociedade pós-industrial que passou por uma "transmutação digital" por conta da IoT, do *Big Data* e das plataformas envolvidas na cadeia do valor do *Big Data* (como as tecnologias em nuvem). Por fim, Schwarz et al. (2019) adicionam à convergência das novas tecnologias o fenômeno da

[11] Há uma grande revisão da literatura da Ciência Política sobre o poder das redes em Canabarro (2014). Todavia, tal discussão não está no escopo deste trabalho.

[12] "A model for the development of computing in the early 21st century. It envisages a movement away from 'computers' as distinct specialized devices; rather, many objects used in everyday life will contain embedded computing devices that can recognize and interact in useful ways with each other and with their environment" (BUTTERFIELD et al., 2016, p. 1043). O conceito da computação ubíqua está relacionado à IoT.

dataficação, através do qual busca-se transformar aspectos da vida – tais como comportamentos, atitudes e sentimentos – em dados.

Tendo em mente a miríade de nomenclaturas para a convergência das novas tecnologias presentes na literatura, este trabalho utilizará o conceito de Segunda Era Digital. A Segunda Era Digital é uma evolução da primeira, causada pela consolidação da Internet como rede das redes e pela convergência de cinco tecnologias e paradigmas principais: o paradigma do *Big Data*; a *Internet of Things*; a Inteligência Artificial; as tecnologias em nuvem; e a quinta geração de redes móveis (5G). Além do mais, a dataficação e a personalização dos dados ocupam um papel central dentro da Segunda Era Digital, trazendo, junto com as novas tecnologias, novos desafios tecnológicos e políticos.

2.2 AS TECNOLOGIAS DA SEGUNDA ERA DIGITAL

A Segunda Era Digital é fruto da convergência de cinco tecnologias e paradigmas tecnológicos: o *Big Data*, a IoT, a IA, as tecnologias em nuvem e a 5G. Neste subcapítulo, serão explicadas e exploradas cada uma das novas tecnologias, os desafios que cada uma enfrenta – ou soluciona – e as relações entre cada uma delas, com o fim de entender como tal convergência está ocorrendo.

2.2.1 *Big Data*

Big Data se refere a dados em quantidades gigantescas (na casa dos *petabytes* e *exabytes*[13]), bastante complexos e não-estruturados[14], os quais podem ser "minados" para extrair informações, padrões e correlações (ZWITTER, 2015; SKOURLETOPOULOS et al., 2017a). Essa mineração é feita através de técnicas avançadas de análise – geralmente alicerçadas em algoritmos e automatizadas crescentemente (ZWITTER, 2015). Todavia, as capacidades de sistemas de computação tradicionais são inadequadas para capturar, armazenar e analisar essa abundância de dados complexos e não-estruturados (SKOURLETOPOULOS et al., 2017a).

[13] Embora existem algumas especificidades técnicas na computação acerca dos prefixos (por conta da natureza binária dos *bits* e do fato de oito *bits* comporem um *byte*), uma representação aproximada para as medidas de bytes são: 1 *kilobyte* = 1.024 *bytes*; 1 *megabyte* = 1.024 *kilobytes*; 1 *gigabyte* = 1.024 *megabytes*; 1 *terabyte* = 1.024 *gigabytes*; 1 *petabyte* = 1.024 *terabytes*; 1 *exabyte* = 1.024 *petabytes* (IEEE, 2009).

[14] Dados estruturados são fáceis de armazenar, pesquisar e analisar e geralmente são gerenciados via SQL. Geralmente, incluem dados, palavras e datas e são rigidamente organizados. Dados não-estruturados não são organizados em nenhum modelo específico. Exemplos de dados não-estruturados incluem SMS, informação de localização, vídeos e dados de redes sociais. A quantidade de dados não-estruturados têm aumentado com o advento dos *smartphones* e demais dispositivos inteligentes. Por fim, dados semi-estruturados não seguem nenhum sistema de base de dados convencional (como SQL) mas podem estar organizados como dados estruturados (PAPADOKOSTAKI et al., 2017

A grande diferença entre dados (*data*) e *Big Data* é a amplitude em termos de alcance, velocidade e complexidade que o *Big Data* possui, trazendo novas possibilidades e potencialmente revolucionando como processamos e analisamos informações (LANGWORTHY, 2019). Dois elementos centrais, então, quando se fala de *Big Data*, são o volume grande de dados e a importância de extrair valor desses dados (PAPADOKOSTAKI et al., 2017).

A importância do volume de dados como elemento central do *Big Data* advém do fato de que o volume de dados proporcionado pelo *Big Data* é um marco analítico importante, uma vez que os dados coletados não necessitam mais de regras e parâmetros limitados previamente – com o *Big Data*, os dados coletados buscam ser exaustivos (CHANDLER, 2015). Não é mais necessário montar um questionário de preferência de compras, por exemplo, dado que o *Big Data* permite puxar todo o histórico de compras de uma pessoa para então ver as suas preferências. Ou seja, a decisão de o que e como analisar passa a ocorrer depois da obtenção dos dados, e não antes. Assim, *Big Data* é comumente descrito na literatura pelo que os autores chamam dos três "Vs": volume, variedade, velocidade. Outros autores apontam também para o valor e para a veracidade do *Big Data* como outros dois potenciais Vs (SKOURLETOPOULOS et al., 2017a; PAPADOKOSTAKI et al., 2017; CHANDLER, 2015).

i) Volume: o volume se refere ao crescimento constante da quantidade de dados gerados por diversas fontes, os quais as bases de dados tradicionais não são capazes de lidar.

ii) Variedade: a variedade está relacionada aos vários tipos diferentes de dados que são coletados a partir de smartphones, mídias sociais, tráfego na internet e sensores variados. Esses dados variam também no seu formato, podendo ser coletado em áudio, vídeo, ou texto; em formato de email, mensagem ou localização; de forma estruturada, semi-estruturada ou não-estruturada, dentre outros tipos.

iii) Velocidade: se refere à velocidade de criação, aquisição, processamento e análise dos dados (PAPADOKOSTAKI et al., 2017; SKOURLETOPOULOS et al., 2017a; ZWITTER, 2015; ZANOON; AL-HAJ; KHWALDEH, 2017).

Recentemente dois outros Vs estão sendo considerados: veracidade e valor. A veracidade do *Big Data* representa a qualidade e a validade dos dados coletados, sendo ela central para utilizar o *Big Data* com sucesso. Como o valor do *Big Data* – o outro V – provém da análise dos dados e da consequente extração de informação, as formas de coleta e os métodos de análise impactam profundamente o valor do *Big Data*, uma vez que dados enviesados, manipulados ou irrelevantes podem ofuscar os resultados e, consequentemente, prejudicar – ou até destruir – o valor deles (PAPADOKOSTAKI et al., 2017; ZWITTER, 2015;

SKOURLETOPOULOS et al., 2017a; ZANOON; AL-HAJ; KHWALDEH, 2017).

Assim, *Big Data* é o conceito que alimenta e move a Segunda Era Digital e é considerado por alguns como o recurso mais valioso do mundo atualmente (SCHWARZ et al., 2019). Outros traçam uma analogia entre *Big Data* e petróleo, uma vez que ele seria um recurso que requer extração (obtenção dos dados) e processamento para gerar valor (LANGWORTHY, 2019). Busca-se, a partir disso, obter inteligência através destes dados para criar uma vantagem informacional e competitiva – seja ela mercadológica ou securitária, privada ou estatal (SKOURLETOPOULOS et al., 2017a; ZWITTER 2015).

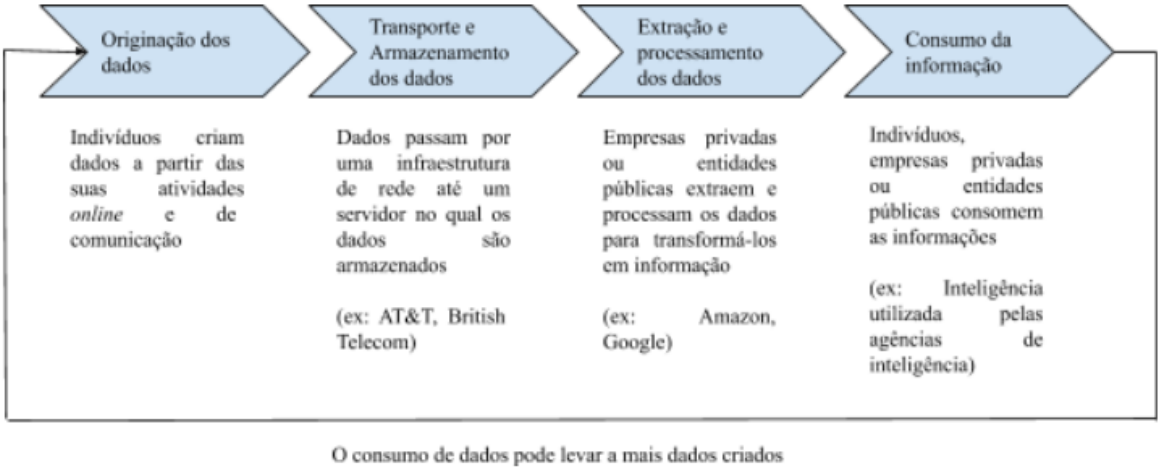
O que torna a inteligência e o valor obtidos do *Big Data* tão diferentes é o fenômeno de *datafication*[15] – ou dataficação – da nossa realidade e das nossas vidas. O aumento no volume dos dados é acompanhado também de uma melhoria qualitativa destes dados – ou seja, ao mesmo tempo em que existem mais dados disponíveis, estes dados estariam, em tese, elucidando interações e relações que antes eram invisíveis e as tornando visíveis, palpáveis e, logo, governáveis (CHANDLER, 2015).

O novo paradigma de dados que o *Big Data* proporciona estaria aproximando os dados cada vez mais da própria realidade (CHANDLER, 2015; SKOURLETOPOULOS et al., 2017a). Isso se dá pelo fato de que os dados não são obtidos tendo alguma pergunta ou motivo que conduziria a coleta, mas sim seriam gerados como um subproduto de diversas atividades com algum ponto de contato tecnológico e digital. Como cada passo e ação que tomamos hoje deixa um rastro digital, a digitalização e consequente dataficação de cada vez mais atividades seria, assim, o que permite a aproximação do *Big Data* à realidade (CHANDLER, 2015).

Consequentemente, as novas dimensões – cada vez mais próximas da realidade – que o *Big Data* está introduzindo para a esfera informativa criaram uma cadeia de valor de dados e uma nova distribuição de poder informativo entre os atores envolvidos (ZWITTER, 2015; LANGWORTHY, 2019). Essa cadeia de valor compreende a criação dos dados; o transporte e armazenamento dos mesmos; a extração, análise e processamento deles e, por fim, o consumo da informação (LANGWORTHY, 2019).

[15] Dataficação é o processo que transforma a vida e a existência em informações fungíveis (SCHWARZ et al 2019).

Figura 1 - Cadeia de Valor de Big Data



Fonte: LANGWORTHY (2019, tradução nossa)

De maneira geral, os atores e *stakeholders* podem ser caracterizados como coletores de *Big Data* e usuários de *Big Data*. Os coletores de *Big Data* – como os provedores de mídias sociais, bancos, navegadores de busca, empresas de marketing e empresas de TI – definem quais dados serão coletados, quais serão armazenados, como eles serão guardados e por quanto tempo (ZWITTER, 2015). Por outro lado, os utilizadores são aqueles agentes que ou analisam os dados, ou consomem dados já processados por outro agente utilizador. São considerados utilizadores agências de inteligência e empresas que utilizam dados para aprimorar os seus serviços. Entretanto, há atores que agem tanto como coletores quanto utilizadores, como a Google, Microsoft e outras empresas de tecnologia (ZWITTER, 2015). Langworthy (2019) também apresenta o indivíduo dataficado (originador dos dados) como um *stakeholder* no processo.

Os agentes coletores, então, são os atores donos dos meios nos quais as atividades de originação dos dados são exercidas, enquanto os agentes utilizadores são aqueles que atuam nas etapas de extração e processamento dos dados e de consumo da informação. Existem ainda mais dois tipos de atores responsáveis pela etapa de transporte e armazenamento dos dados – os detentores da infraestrutura da rede e os detentores dos servidores nos quais os dados ficarão armazenados.

Tradicionalmente, a infraestrutura da rede era considerada um foco de poder central na ecologia digital (CANABARRO, 2014). Um exemplo da importância da infraestrutura é o caso de alguns dos programas revelados por Edward Snowden nos quais os EUA utilizam a sua posição central como espinha dorsal da internet para interceptar e coletar dados que passam

pela infraestrutura conectada aos EUA (CANABARRO, 2014; SEGAL, 2016). No mundo do *Big Data*, todavia, Langworthy (2019) aponta como o novo ator empoderado nessa cadeia de valor não é nem o originador dos dados e nem o coletor dos dados, mas sim aquele que de fato emprega os dados a seu favor. Da mesma forma que o valor dos dados surge quando eles são processados e transformados em informação, o poder também surge nesse processo (SCHWARZ et al., 2019). Mesmo assim, a infraestrutura da rede continua sendo um locus importante de poder na cadeia de valor do *Big Data*, uma vez que a coleta dos dados depende do transporte deles na rede. Todavia, não são as empresas e entidades detentoras da infraestrutura – como as empresas de telecomunicação – que possuem o poder, mas sim os estados territoriais cuja legislação subordina esses atores (LANGWORTHY, 2019).

2.2.2 *Internet of Things* (IoT)

A coleta de dados está sendo transformada por um novo paradigma emergente na tecnologia e na ciência da computação chamado Internet das Coisas (IoT[16]) (PAPADOKOSTAKI et al., 2017). É um novo conceito da rede da internet no qual diversos dispositivos de hardware – como celulares, eletrodomésticos inteligentes, *wearables*[17] e demais eletrônicos com sensores ou interfaces computacionais inteligentes – estão conectados em rede e comunicam entre si (PAPADOKOSTAKI et al., 2017; ZANOON; AL-HAJ; KHWALDEH, 2017; CHANDLER, 2015). Nestas redes da IoT, dados transitam entre todos os dispositivos constantemente, permitindo a coleta de dados e inclusive a análise e utilização de dados através de aplicações em nuvem – graças à computação em nuvem, que será tratado mais para frente – para que decisões possam ser tomadas a partir destes dados o mais rápido possível (ZANOON; AL-HAJ; KHWALDEH, 2017).

Um dispositivo de IoT é composto por três principais elementos e funcionalidades para poder obter dados e transmiti-los. O primeiro é o sensor responsável por obter os dados – e que é geralmente composto ou por um sensor RFID[18]; por um sensor WSN[19]; ou por um dispositivo móvel[20]. O segundo elemento é a conexão à rede, responsável por enviar os dados através ou

[16] Sigla abreviada do nome em inglês, *Internet of Things*.
[17] *Wearables* são dispositivos incorporados em roupas e acessórios que são então utilizados no corpo humano.
[18] Um sensor de *Radio Frequency IDentification* (RFID) possui uma tag de RFID que permite que um sensor leitor possa ler um código único (o *Electronic Product Code*, ou EPC) associado àquela tag. Os dados são, então, enviados pelo sensor leitor para um servidor (PAPADOKOSTAKI et al., 2017).
[19] Um *Wireless Sensor Node* (WSN) possui vários nódulos capazes de utilizar protocolos leves para conectar e interagir com a internet, permitindo uma conexão *peer-to-peer* (P2P) (PAPADOKOSTAKI et al., 2017).
[20] Dispositivos móveis, como celulares, podem possuir diversos sensores como GPS, câmeras e microfones, podendo então captar dados como localização, áudio, vídeo e texto, além dos dados gerados (ou captados) por aplicativos (PAPADOKOSTAKI et al., 2017).

da internet, ou de uma rede interna de dispositivos IoT. Por fim, o terceiro elemento é uma camada de aplicação, na qual os dispositivos, através de softwares, podem desempenhar diversas funções dentro de um ecosistema IoT (PAPADOKOSTAKI et al., 2017). Um *smartwatch*, por exemplo, pode ser utilizado para medir batimentos cardíacos, executar pagamentos por contato (via NFC), controlar mídias em outros dispositivos e receber ligações.

Os dados gerados pela IoT, por sua vez, possuem quatro principais características: i) Volume – por conta tanto do número de sensores, quanto da necessidade de possuir um histórico de dados para os dispositivos inteligentes proverem serviços melhores, são capturados dados em larga escala pela IoT; ii) Diversidade – como os sensores e os dados coletados variam em tipo (texto, imagem, número, etc.), pode-se dizer que os dados obtidos pela IoT são bastante heterogêneos; iii) Importância do tempo e do espaço – tempo e espaço são centrais em muitas das aplicações de IoT, e por isso, os dados devem possuir informações de tempo (hora) e espaço (localização); e iv) Aproveitamento incompleto de dados – de todos os dados coletados pela IoT, uma pequena parcela será utilizado (PAPADOKOSTAKI et al., 2017).

São estes dispositivos inteligentes interconectados que possibilitam o crescimento avassalador da coleta do *Big Data*. Cerca de 64% do tráfego por IP é composto por comunicações entre máquinas, com estimativas de que cerca de 40 bilhões de dispositivos estarão conectados à internet até 2025 (PAPADOKOSTAKI et al., 2017). A *Fifth Generation Public Private Partnership* (5G-PPP) apresenta uma estimativa ainda maior, alegando que a 5G vai conectar sete trilhões de dispositivos (AHMAD et al., 2018). Todavia, junto desse *boom* acompanham desafios para a infraestrutura da internet existente. Alguns – como a demanda de cada um destes dispositivos possuir um endereço de IP, as limitações do protocolo IPv4 e a transição do IPv4 para o IPv6 – são de um caráter mais técnico e não serão abordados neste trabalho. Os dois desafios que estão dentro do escopo deste trabalho – por estarem relacionados a alguns dos desenvolvimentos da Segunda Era Digital – se referem ao armazenamento, análise e captura (o translado, mais especificamente) dos dados (PAPADOKOSTAKI et al., 2017; ZANOON; AL-HAJ; KHWALDEH, 2017). Vale ressaltar que as tecnologias da Segunda Era Digital se retroalimentam no processo de desenvolvimento, de forma que avanços em IoT desenvolvem o ramo do *Big Data*, que pode acelerar o desenvolvimento da IoT e assim por diante, por exemplo (PAPADOKOSTAKI et al., 2017).

A necessidade de se analisar os dados para transformar em informação e gerar valor leva ao desenvolvimento e aprimoramento do campo da inteligência artificial e, até certo ponto, para o desenvolvimento da computação em nuvem, uma vez que boa parte dos dispositivos inteligentes não possuem capacidade computacional para analisar os dados localmente. O

desafio de se armazenar a quantidade de dados gerados, por sua vez, leva ao desenvolvimento do armazenamento em nuvem. Por fim, o transporte dos dados capturados e a conexão dos dispositivos uns com os outros e com a internet demanda uma conexão sem fio de alta velocidade, desenvolvimento que está se concretizando com a conexão 5G.

2.2.3 Inteligência Artificial (IA)

A análise dos dados é a próxima etapa na cadeia de valor do *Big Data*, e o desafio de analisar os dados – para então extrair informação e, consequentemente, gerar valor – recai sobre os algoritmos da inteligência artificial (PAPADOKOSTAKI et al., 2017). O aumento do volume dos dados capturados no *Big Data* aumentaram a importância e ao mesmo tempo catalisaram o desenvolvimento da inteligência artificial, uma vez que *datasets* são necessários para treinar a inteligência artificial (USA, 2018).

É necessário, assim, apresentar brevemente o campo da inteligência artificial, pois diversos termos – como *machine learning*, *deep learning*, *neural networks* e inteligência artificial – se misturam e são utilizados inconsistentemente como sinônimos na literatura fora da Ciência da Computação, especialmente nos campos das Relações Internacionais e da Ciência Política (IRIONDO, 2018; DONGES, 2019).

Inteligência Artificial é um conceito amplo e um campo de conhecimento interdisciplinar no qual, de forma resumida, se busca criar uma entidade artificial que possua a capacidade de ter comportamentos inteligentes que até então são atribuídos exclusivamente à inteligência humana. Na computação, se busca atingir este objetivo é através da atribuição aos computadores da capacidade de exibirem tais comportamentos inteligentes (USA, 2018; NEAPOLITAN; JIANG, 2018; RUSSEL; NORVIG, 2016; IRIONDO, 2018).

Em 2007, surgiu a ideia de uma IA geral – que acompanhou o surgimento do campo da Inteligência Geral Artificial (*Artificial General Intelligence* - AGI) – baseado na busca por um programa ou algoritmo geral para aprender e agir em qualquer situação (NEAPOLITAN; JIANG, 2018; RUSSEL; NORVIG, 2016). Tal ideia se contrasta com o que é chamado de *narrow* IA, ou em outras palavras, uma IA que é capaz de fazer apenas um tipo de tarefa (USA, 2018).

Uma IA pode ser considerada forte ou fraca[21] (USA, 2018; NEAPOLITAN; JIANG, 2018). Para ser caracterizada como IA forte, o computador precisa realmente se equiparar a

[21] Em 1950, Alan Turing criou o teste de Turing para determinar se uma entidade é inteligente ou não. O teste de Turing envolve um humano "interrogador" em uma sala, outro humano numa segunda sala, e uma entidade artificial – no caso, um computador – em uma terceira sala. O humano interrogador deve, então, se comunicar com

uma mente humana no sentido que ele deve ser capaz de compreender e possuir outros estados cognitivos (SEARLE apud. NEAPOLITAN; JIANG, 2018). Por outro lado, uma IA é fraca quando ela consegue agir de maneira inteligente, mas não consegue de fato compreender. Uma IA forte é de fato uma mente e uma IA fraca apenas simula uma mente (NEAPOLITAN; JIANG, 2018).

Mesmo assim, a questão de uma IA ser forte ou fraca se aproxima mais de uma questão filosófica de o que seria inteligência e consciência do que devidamente do campo da ciência da computação. Para a Ciência da Computação, se um programa age como se fosse inteligente, já pode ser considerado uma inteligência artificial[22] (NEAPOLITAN; JIANG, 2018). Para atingir esse objetivo, algoritmos têm sido desenvolvidos baseados nos comportamentos e na racionalidade de seres inteligentes como nós humanos (NEAPOLITAN; JIANG, 2018).

As primeiras abordagens para a inteligência artificial foram baseadas em tentar recriar um modelo dos neurônios do cérebro humano e seu funcionamento (NEAPOLITAN; JIANG, 2018; RUSSEL; NORVIG, 2016). Nestes modelos, um processador chamado de neurônio artificial é tratado como uma variável binária que pode estar ou ligado ou desligado. Surgiu, assim, a abordagem das redes neurais (*neural networks*) dentro do campo da inteligência artificial (NEAPOLITAN; JIANG, 2018; NEGNEVITSKY, 2005). Uma rede neural artificial é a junção de diversos neurônios artificiais – chamados de unidades neurais dentro da rede neural – cujo comportamento é baseado na comunicação dos neurônios do cérebro humano. As unidades neurais são organizadas em camadas, onde um sinal entra na camada de *input*, passa por camadas ocultas intermediárias (*hidden layers*) e termina na camada de *output* (NEAPOLITAN; JIANG, 2018). Entretanto, cada neurônio artificial é capaz de receber diversos sinais de *input* e de produzir um único sinal de *output*, que pode então ser enviado para

---

o humano e a entidade artificial através de um terminal de texto sem saber quem é quem. A partir disso, o interrogador deve tentar distinguir a entidade artificial do humano a partir das respostas de cada um deles às perguntas do interrogador. Caso o interrogador não consiga ou erre, é considerado que a entidade artificial passou do teste de Turing e pode ser considerado uma entidade inteligente. Todavia, Searle, em 1980, vai mais afundo. Partindo da suposição de que um programa de computador para entender e conversar em chinês e tal programa passa no teste de Turing, Searle questiona se o programa realmente compreende chinês, ou se ele está apenas simulando tal habilidade. Ele critica que se ele tivesse uma versão em inglês do programa, um interrogador chinês poderia passar para ele as frases em chinês e Searle conseguiria, seguindo as instruções do programa, processar as frases em chinês e responder frases em chinês para o interrogador, efetivamente fazendo o que o programa de computador faz. Entretanto, Searle não falava chinês e, consequentemente, não compreendia chinês. A partir disso, ele conclui que se ele não pode ser considerado alguém que compreende chinês nessa situação, a máquina também não pode. Se a máquina não está entendendo a conversa, ela não estaria pensando e, como resultado, não poderia ser considerada inteligente. É a partir desse experimento – chamado de experimento da sala chinesa (*Chinese room*) – que surgem as caracterizações de IA forte e IA fraca (NEAPOLITAN; JIANG, 2018).

[22] Ou seja, se o programa passa no teste de Turing.

diversos outros neurônios artificiais da próxima camada até chegar na camada final (NEGNEVITSKY, 2005).

As redes neurais caíram em desuso com os sucessos iniciais das abordagens de lógica no campo da inteligência artificial na década de 1950[23]. Todavia, com os avanços na velocidade e capacidade de processamento dos computadores e o surgimento de novos algoritmos para treinar redes neurais, uma nova subárea dentro das áreas das redes neurais e do *machine learning* foi desenvolvida – o *deep learning*. *Machine learning* consiste, como o nome sugere, em mecanismos adaptativos – algoritmos – que permitem que computadores aprendam a partir de experiência prévia e exemplos[24], dependendo, assim, de dados para aprender – e, consequentemente, servindo para analisar dados (NEGNEVITSKY, 2005; IRIONDO, 2018; DONGES, 2019).

Por sua vez, o *deep learning* é um método específico de *machine learning* que faz uso de camadas múltiplas de processamento para aprender a partir dos dados. Para isso, o *deep learning* utiliza, principalmente, redes neurais artificiais com vários neurônios de *input* e diversas camadas ocultas intermediárias compostas também por uma grande quantia de neurônios artificiais. A ideia é que através de vários níveis de abstração, a máquina consegue aprender funções mais complexas (LECUN; BENGIO; HINTON, 2015; LEE; SHIN; REALFF, 2018; AILISTO et al., 2018; CASTROUNIS, 2019). Embora as primeiras arquiteturas de redes neurais artificiais não possuíam a capacidade de aprender, hoje elas ocupam um papel central no *machine learning* ao possibilitar e contribuir para o desenvolvimento do *deep learning* (SCHMIDHUBER, 2015). O que diferencia tanto as primeiras redes neurais e redes neurais tradicionais das redes neurais com *deep learning* – chamadas de forma geral de *deep neural networks* – é a quantidade de camadas ocultas intermediárias presente nas últimas (NEAPOLITAN; JIANG, 2018).

---

[23] Os primeiros sucessos no campo da inteligência artificial, por sua vez, dependeram da criação de modelos baseados na lógica humana. Entretanto, essas inteligências artificiais baseadas na lógica humana eram efetivos em situações limitadas e conseguiam resolver problemas de baixa complexidade. Assim, a abordagem da lógica logo falhou em se tornar escalável (NEAPOLITAN, JIANG, 2018). Outras abordagens foram desenvolvidas ao longo da segunda metade do século XX e início do século XXI, mas elas não estão no escopo da discussão deste trabalho (ver NEAPOLITAN; JIANG, 2018; NEGNEVITSKY, 2005; RUSSEL; NORVIG, 2016).

[24] *Machine Learning* pode ser caracterizado pelo tipo de aprendizado – supervisionado (*supervised*), não-supervisionado (*unsupervised*) e de reforço (*reinforcement*). O aprendizado supervisionado utiliza exemplos rotulados – ou seja, exemplos onde alguém disse para a máquina que um pato é um pato – e é útil para classificar novos dados a partir do conhecimento prévio ou para regressões. O aprendizado não-supervisionado, por outro lado, utiliza exemplos não-rotulados e serve para identificar padrões, *clustering* e uma série de outras atividades. Existe um híbrido entre o aprendizado supervisionado e o não-supervisionado chamado de semi-supervisionado no qual se mistura alguns poucos dados rotulados com dados não-rotulados (ou rotulados erroneamente) para melhorar a precisão do aprendizado. Por fim, o aprendizado por reforço faz uso de um processo de crítica dos dados – alguma indicação de certo ou errado – para levar a uma relação ótima para algum objetivo (LEE; SHIN; REALFF 2018; RUSSEL; NORVIG, 2016; IRIONDO, 2018).

Se tivéssemos que criar uma taxonomia para esses conceitos recém descritos, poderíamos considerar a Inteligência Artificial como uma grande área interdisciplinar; *machine learning* como uma subárea da Inteligência Artificial e *deep learning* como um método de *machine learning*. Redes neurais, por sua vez, são uma abordagem/arquitetura possível para IAs que, mais recentemente, têm ocupado um papel central dentro da subárea do *machine learning* por conta da sua aplicação no *deep learning* com as *deep neural networks*.

São os avanços recentes no *deep learning* que catalisaram os avanços nos últimos anos da inteligência artificial (USA, 2018). O aumento tanto do poder de processamento dos computadores – e o acesso a computadores poderosos – quanto do crescente volume de dados disponíveis – graças ao *Big Data* – tornou possível o treinamento das máquinas através do *deep learning*, pois possuíam tanto *datasets* grandes para treinar quanto poder computacional para executar (USA, 2018; MIAILHE; RHODES, 2017).

É a inteligência artificial que dá sentido e valor para os dados do *Big Data* e é o *Big Data* que alavanca e possibilita o treinamento das máquinas e os avanços na inteligência artificial através do *machine learning*. Todavia, é necessário armazenar todos os dados do *Big Data* para que possamos treinar as máquinas e depois utilizá-las para extrair valor e informação dos dados. Porém, para treinar e utilizar a inteligência artificial, é preciso também um grande poder computacional. A computação em nuvem surge como uma solução para estes dois desafios – o de armazenamento e, em parte, o de análise dos dados, cujo resto é solucionado pela inteligência artificial..

2.2.4 Tecnologias em Nuvem

Com o volume crescente de dados do *Big Data*, torna-se necessário ter capacidades grandes de armazenamento e de processamento para manejar os dados em larga escala. Perante esta situação, a computação em nuvem surge como uma solução para estas dificuldades, sendo ela uma tecnologia que cria um ambiente acessível e escalável para sistemas de análise de dados funcionarem (PAPADOKOSTAKI et al., 2017; ZANOON; AL-HAJ; KHWALDEH, 2017; SKOURLETOPOULOS et al., 2017a). A computação em nuvem, em específico, têm se mostrado uma tecnologia importante para a evolução da IoT e do *Big Data* (PAPADOKOSTAKI et al., 2017).

A definição de computação em nuvem mais aceita e recorrente na literatura é a do NIST (*National Institute of Standards and Technology*) do Departamento de Comércio americano. O NIST define a computação em nuvem como:

> [...] um modelo que possibilita acesso de forma ubíqua, conveniente e *on-demand* à um conjunto de recursos computacionais configuráveis (como redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente fornecidos e lançados com um esforço mínimo de administração ou de interação do provedor do serviço (MELL; GRANCE, 2011, p. 2, tradução nossa).

Em outras palavras, a computação em nuvem se refere a recursos computacionais e sistemas disponíveis sob demanda via internet (ou alguma outra rede) que permite o acesso a uma série de serviços computacionais integrados – como processamento ou armazenamento – sem a necessidade de recursos locais próprios (ZANOON; AL-HAJ; KHWALDEH, 2017).

Além disso, para o NIST, a computação em nuvem possui cinco características essenciais, três modelos de serviço e quatro modelos de emprego (MELL; GRANCE, 2011). A primeira característica essencial é o *on-demand self-service*, forma pelo qual um consumidor pode unilateralmente requisitar e utilizar recursos computacionais sem necessitar interação humana com os provedores dos serviços. A segunda característica da computação em nuvem é o acesso amplo pela rede – ou seja, os recursos estão disponíveis e são acessados pelos mecanismos que permitem acesso à rede (como celulares, laptops, computadores pessoais, dispositivos inteligentes, etc.) (MELL; GRANCE, 2011).

Outra característica essencial é o chamado *resource pooling*. De maneira resumida, o *resource pooling* é uma técnica que permite que o provedor dos recursos computacionais atenda as demandas de vários consumidores através de recursos físicos e virtuais que são distribuídos e redistribuídos constantemente. Com isso, o consumidor pode determinar quais recursos ele requer, mas geralmente não tem controle ou conhecimento da localização exata dos recursos, embora ele possa ter uma ideia aproximada em alguns casos. A quarta característica está relacionada a o que o *resource pooling* permite, que é a elasticidade rápida da alocação (e realocação) dos recursos de acordo com a demanda – em outras palavras, os recursos e aplicações estão sempre disponíveis e podem ser aumentados ou diminuídos conforme a demanda (MELL; GRANCE, 2011; ZANOON; AL-HAJ; KHWALDEH, 2017). Um exemplo desta elasticidade é a contratação de mais espaço no Google Drive ou Dropbox – assim que uma pessoa requisita mais espaço (e faz a assinatura e pagamento do serviço), o espaço adicional é disponibilizado quase que imediatamente.

Por fim, a última característica essencial elencada pela NIST para a computação em nuvem é o fato dela ser um serviço mensurado. Os sistemas em nuvem conseguem mensurar e monitorar os processos e os recursos sendo utilizados como forma de controle e para fins de transparência para tanto o usuário quanto o provedor (MELL; GRANCE, 2011). Um exemplo

dessa característica na prática é a informação de quantos Gb de armazenamento ainda estão disponíveis no Google Drive ou Dropbox.

Os três modelos de serviço de computação em nuvem apresentados pela NIST, por sua vez, são o *Software as a Service* (Saas), o *Platform as a Service* (PaaS) e o *Infrastructure as a Service* (IaaS). O SaaS é o modelo no qual o que é entregue ao consumidor é uma aplicação que está sendo rodada na infraestrutura da nuvem[25]. Neste modelo, o usuário não precisa instalar a aplicação no computador. Ao usuário, resta apenas ajustar as configurações e customizar os serviços para os níveis adequados às suas necessidades. O provedor do serviço, por sua vez, administra a rede, os servidores, sistemas operacionais, armazenamento e o software da aplicação. No PaaS, o provedor entrega os recursos e ferramentas para desenvolver e executar as próprias aplicações do usuário baseadas em nuvem. Aqui, o usuário possui controle sobre a aplicação, enquanto que o provedor continua administrando a infraestrutura como a rede, servidores, etc (MELL; GRANCE, 2011; ZANOON; AL-HAJ; KHWALDEH, 2017). No IaaS, por fim, como o próprio nome sugere, o provedor entrega o uso dos próprios recursos, como o armazenamento, sistema operacional e aplicações. Assim, o provedor cuida apenas da infraestrutura física, enquanto o usuário administra os demais recursos contratados (MELL; GRANCE, 2011).

A última parte da delimitação conceitual da NIST para a computação em nuvem são os quatro modelos de emprego: a nuvem privada, a nuvem comunitária, a nuvem pública e a nuvem híbrida. Em uma nuvem privada, a infraestrutura é entregue para o uso exclusivo de uma única organização (como uma empresa), podendo existir tanto no local da organização quanto fora e sendo operada por um terceiro ou não. As nuvens comunitárias seguem a mesma lógica que a privada, porém são utilizadas por um conjunto de organizações que possuem um interesse comum específico. Uma nuvem pública, por outro lado, é uma nuvem disponível ao público em geral, podendo ser administrada tanto por uma empresa quanto por uma universidade, organização governamental ou uma combinação de entidades. Tal nuvem em questão existe nas premissas do provedor da nuvem (MELL; GRANCE, 2011; ALALI; YEH, 2012). Por fim, existem as nuvens híbridas, nas quais a infraestrutura da nuvem é composta por um conjunto de infraestruturas de nuvens distintas que são conectadas por alguma tecnologia que permite

[25] A NIST define a infraestrutura da nuvem como "[...] a coleção de hardware e software que possibilita as cinco características essenciais da computação em nuvem. A infraestrutura em nuvem pode ser vista como contendo uma camada física e uma camada abstrata. A camada física consiste nos recursos de hardware que são necessários para apoiar os serviços em nuvem sendo entregues e geralmente inclui servidores, armazenamento e componentes de rede. A camada abstrata consiste no software empregado na camada física, que manifesta as características essenciais da nuvem. Conceitualmente, a camada de abstração fica acima da camada física" (MELL; GRANCE, 2011, p.2, tradução nossa)

portabilidade ou interoperabilidade entre elas, embora cada nuvem continue sendo única (MELL; GRANCE, 2011).

Embora não esteja definido pela NIST, a computação em nuvem pode ser dividida em duas principais funcionalidades: armazenamento em nuvem (*cloud storage*) e estritamente computação em nuvem (*cloud computing*). O armazenamento em nuvem se refere à funcionalidade de armazenamento de dados que se dá em servidores remotos, permitindo que um usuário possa acessar e resgatar estes dados em qualquer dispositivo a qualquer momento que desejar. A computação em nuvem, no seu sentido mais estrito, diz respeito ao processamento remoto de dados. As aplicações de computação em nuvem enviam dados para processadores remotos que então executam uma ação que requer processamento de dados e envia o resultado para o usuário (ZANOON; AL-HAJ; KHWALDEH, 2017). Tendo isso em mente, o presente trabalho utilizará esta delimitação mais específica das duas funcionalidades em nuvem. A computação em nuvem no sentido amplo definido pela NIST será tratado neste trabalho como tecnologias em nuvem.

As tecnologias em nuvem, assim, podem ser vistas como parte da infraestrutura necessária para que a Segunda Era Digital e a computação ubíqua funcionem (SKOURLETOPOULOS et al., 2017b[26]; ZANOON; AL-HAJ; KHWALDEH, 2017). Para o *Big Data* existir e conseguir crescer, torna-se necessário quantidades cada vez maiores de armazenamento disponível a preços acessíveis para os atores (e sem a necessidade de possuir a infraestrutura física). Através das tecnologias em nuvem, têm sido possível acompanhar e suprir tal demanda[27] (SKOURLETOPOULOS et al., 2017a; ZANOON; AL-HAJ; KHWALDEH, 2017). Ao mesmo tempo, é necessário possuir alto poder computacional para conseguir analisar os dados do *Big Data*, e a computação em nuvem permite a obtenção desse poder computacional sem possuir os recursos físicos (ZANOON; AL-HAJ; KHWALDEH, 2017). Quando levamos em consideração a IoT, o papel das tecnologias em nuvem como infraestrutura se torna mais

[26] Skourletopoulos et al. (2017b) fazem esta afirmação quando falam do paradigma de computação em nuvem móvel (*mobile cloud computing*), que é um paradigma emergente que busca fazer com que as operações computacionais ocorram em nuvem e não nos dispositivos móveis. Assim, o problema da falta de recursos computacionais nos dispositivos móveis seria solucionado. Tal afirmação dos autores, todavia, pode ser feita também para as tecnologias em nuvem, uma vez que os autores falam que a computação em nuvem móvel é baseada na arquitetura da computação em nuvem 'não-móvel'. Além do mais, o funcionamento e as motivações por trás dos dois paradigmas são os mesmos: transferir a carga computacional e de armazenamento para recursos poderosos fora do dispositivo, os quais são acessados por via de uma rede, seja ela a internet ou uma rede privada.

[27] Todavia, existe receio de que as capacidades existentes não sejam suficientes, tendo em vista que o volume de dados está crescendo exponencialmente (SKOURLETOPOULOS et al., 2017a). Entretanto, Zanoon, Al-Haj e Khwaldeh (2017) apontam que as tecnologias em nuvem estão expandindo para acomodar o Big Data através do *data splitting*, técnica que envolve armazenar partes de um dado separadamente em mais de um local. Os autores também apontam como as tecnologias em nuvem e o *Big Data* andam juntos – ou seja, avanços em um possibilitam ou levam a avanços no outro.

evidente, uma vez que elas são necessárias para o armazenamento e análise dos dados coletados pelos dispositivos e sensores dentro de um ambiente de IoT (SKOURLETOPOULOS et al., 2017b; ZANOON; AL-HAJ; KHWALDEH, 2017). Pode-se inclusive dizer que, graças às tecnologias em nuvem, a Segunda Era Digital é uma na qual capacidades de armazenamento e de poder computacional estão se tornando disponíveis para todos[28] (SKOURLETOPOULOS et al., 2017a).

Todavia, a tecnologia em nuvem é apenas uma parte da infraestrutura para a Segunda Era Digital. A outra, e da qual a tecnologia em nuvem vai depender, é a quinta geração de redes móveis (5G). As tecnologias em nuvem dependem do acesso à rede para funcionarem, e para que elas possam de fato substituir os recursos físicos pessoais, é necessário ter uma latência (tempo de resposta) mínima no translado de tantos dados e informações.

2.2.5 5G

O último desafio, aquele do translado dos dados, pretende ser solucionado pela quinta geração de redes móveis (5G). Um dos maiores gargalos para as tecnologias em nuvem e para as IoT é a transmissão de volumes grandes de dados, tendo em vista que tanto o volume de dados quanto o número de dispositivos conectados à internet tende a crescer exponencialmente (SKOURLETOPOULOS et al., 2017a; LEE, 2019). A 5G, então, busca revolucionar a velocidade da transmissão de dados e reduzir o tempo de resposta nas transmissões de maior tamanho, consequentemente revolucionando a mobilidade dos dispositivos conectados (LANGWORTHY, 2019; SKOURLETOPOULOS et al., 2017b).

Historicamente, cada década têm trazido uma nova geração de tecnologias para a conexão e transmissão de dados para celulares (RAO; PRASAD, 2018). Com o lançamento dos primeiros celulares em 1980, a primeira geração (1G) surge com um foco em tecnologias de rádio analógicas. Na década de 1990, a segunda geração (2G) passa a utilizar transmissões digitais de rádio em vez de analógicas – reduzindo o consumo de bateria – e introduz as mensagens de texto via SMS. A terceira geração (3G), ao longo dos anos 2000s, introduziu a transmissão de dados em alta velocidade (para a época) ao conectar à rede da internet via IP, o que permitiu comunicações por vídeo, acesso à internet e o *streaming* de diversas mídias para os dispositivos com 3G. A década na qual estamos no final no momento da escrita deste trabalho

[28] É importante ressaltar que a democratização em questão é aquela de poder altíssimo computacional, e não uma democratização do acesso à internet ou ao mundo digital. Isto quer dizer, na prática, que é uma democratização do alto poder computacional para quem já possui acesso ao mundo digital. Essa democratização do poder computacional, assim, não diminui a exclusão digital ou a *digital divide*.

(2010s) viu o advento da quarta geração (4G), caracterizada pelo crescimento da banda larga móvel e um consequente aumento da velocidade de transferência de dados[29].

Agora, estamos no período de transição para a 5G, que já começou a ser disponibilizada em partes de algumas cidades no mundo, como Chicago, Nova Iorque, Londres e Seoul (DOLCOURT, 2019; SWIDER, 2019). A 5G pretende ser de 10 a 100 vezes mais rápida do que a 4G, permitindo a entrega de diversos serviços – desde vídeo em ultra-HD à aplicações de realidade virtual em tempo real – em alta velocidade, com latência negligível e com capacidade para conectar um número massivo de dispositivos ao mesmo tempo (RAO; PRASAD, 2018; KUMAR; GUPTA; SINGH, 2015; LI; XU; ZHAO, 2018). Espera-se também que a 5G traga um consumo menor de energia nas baterias dos dispositivos e uma maior mobilidade e interoperabilidade dos dispositivos (KUMAR; GUPTA; SINGH, 2015).

Atualmente, dois caminhos estão sendo explorados para realizar a 5G: evolução e revolução (CHEN; KANG, 2018). Pelo caminho da evolução, buscaria-se melhorar a infraestrutura já existente do final da 4G (a 4G LTE[30]) para aumentar a eficiência dos sistemas 4G. O caminho da revolução, por outro lado, envolve explorar, inovar e implementar novas tecnologias para dar um salto de eficiência (CHEN; KANG, 2018).

Para isso, alguns novos elementos e arquiteturas são necessários e estão sendo explorados para providenciar a melhor conexão a todo momento para todos os dispositivos. Todavia, como muitas delas ainda estão sendo pesquisadas, testadas e padronizadas, o foco será dado para alguns poucos elementos que já diferenciam a 5G das outras gerações. A principal mudança concreta na 5G (por enquanto) se refere às frequências de rádio utilizadas para transferir dados. A 5G faz uso de tanto bandas de baixa-frequência[31] – utilizadas para uma cobertura maior – quanto de bandas de alta-frequência[32] – utilizadas para alcançar velocidades altas de transmissão de dados em lugares com uma concentração maior de pessoas/dispositivos (*hotspots*), porém à curta distância (CHEN; KANG, 2018). Quanto mais baixa a frequência da banda, maior o alcance e menor a velocidade, enquanto que quanto mais alta a frequência da

[29] Enquanto a 3G possuia uma velocidade de download entre 200kbits/s e alguns Mbits/s, a 4G possui uma velocidade de download de cerca de 100Mbits/s. A 5G, por sua vez, promete até 10Gb/s (KUMAR; GUPTA; SINGH, 2016; KACHHAVAY; THAKARA, 2014; RAO; PRASAD, 2018). Testes de algumas das primeiras redes de 5G nos Estados Unidos e alguns outros lugares do mundo como Londres e Seoul registraram velocidades entre 460Mbits/s e 1.8Gbits/s, que é equivalente a aproximadamente 1.800Mbits/s (DOLCOURT, 2019; SWIDER, 2019).

[30] *Long Term Evolution*

[31] Abaixo de 6GHz (CHEN; KANG, 2018). Entretanto, a Federal Communications Commission (FCC) dos Estados Unidos classifica as bandas de 2.5GHz, 3.5GHz, 3.7-4.2GHz como bandas médias, e bandas baixas como 600MHz, 800MHz, 900MHz (FCC, 2018).

[32] Entre 6 e 100GHz (CHEN; KANG, 2018). As bandas nestas frequências altas também são chamadas de *millimeter-wave spectrum* (FCC, 2018).

banda, menor o alcance e maior a velocidade da transmissão de dados (BEHAR, 2019). Os elementos de virtualização e utilização de *software* como partes centrais da infraestrutura da nova rede merecem destaque também, dado o aumento de possibilidade de ataques diretos à infraestrutura por conta dos elementos virtuais e de *software*. Tais elementos buscam inovar através da abstração e programabilidade da rede, mas é justamente esta programabilidade que potencialmente reduz a segurança da infraestrutura (AHMAD et al., 2018).

O principal desafio e objetivo da 5G é alcançar e implementar uma infraestrutura que permita uma conexão sem fio à rede que seja tão rápida, eficiente e confiável quanto a conexão com fio via fibra ótica. A ideia é que a 5G deixe de ser uma rede para dispositivos móveis (leia-se celulares) e passe a ser, através de uma convergência das tecnologias da telecomunicação com as da informação, uma nova infraestrutura da internet (CHEN; KANG, 2018; PAUL, 2018). Assim, uma *World Wide Wireless Web* (WWWW) se concretizaria, na qual os dispositivos funcionariam remotamente e estariam conectados constantemente à internet sem a necessidade de uma conexão com fio (PAUL, 2018; KUMAR; GUPTA; SINGH, 2015). Nessa realidade descrita, o acesso e transferência de dados seria constante e contínuo (PAUL, 2018).

A 5G, então, constitui um pilar de infraestrutura fundamental para a Segunda Era Digital. A infraestrutura da Segunda Era Digital, então, é composta pela 5G e pelas tecnologias em nuvem. Juntas, elas são encarregadas da transmissão, armazenamento e processamento dos dados. O *Big Data*, por sua vez, é o novo paradigma de dados existente, enquanto a IoT e a IA possuem papéis centrais na cadeia de valor do *Big Data*, sendo responsáveis, respectivamente, pela obtenção de dados e pela análise – e geração de valor – dos dados. Estas tecnologias todas são desenvolvidas para potencializar as outras e são catalisadas pelas mesmas às quais contribuem ao desenvolvimento.

Porém, a Segunda Era Digital ainda tem um caminho a percorrer e gargalos a superar. Como dito anteriormente, a 5G ainda está sendo desenvolvida, testada e padronizada, e muito da Segunda Era Digital depende dela para atingir todo o seu potencial, em especial a IoT (LANGWORTHY, 2019). Sistemas ciber-físicos[33], por exemplo, são um dos avanços da IoT mais esperados tanto para as cidades inteligentes quanto para a chamada "indústria 4.0", ambos alicerçados na automação a partir de dispositivos e sensores da IoT; na realidade aumentada – apenas possível com as velocidades da 5G; na inteligência artificial – que necessita da

[33] Sistemas ciber-físicos, em resumo, combinam a computação com processos físicos e utilização *feedback loops* para melhorar a eficiência. Para isso, são necessários sensores que captam dados constantemente (IoT) e um programa computacional (uma IA, por exemplo) que possa analisar os dados e ajustar a atividade física, que então é também dataficada, analisada e ajustada (LEE, 2008; RAO; PRASAD, 2018).

computação em nuvem; e na robótica (LANGWORTHY, 2019; CHEN; KANG, 2018; RAO; PRASAD, 2018). A 5G, então, além de ser uma infraestrutura essencial para a Segunda Era Digital, atualmente é o seu maior gargalo técnico.

Da mesma maneira que o desenvolvimento destas tecnologias estejam interligados, os desafios técnicos da Segunda Era Digital – armazenamento, transmissão e análise de dados – também se retroalimentam de forma que avanços em uma tecnologia podem retomar desafios em outra, que então se desenvolve e repete este processo com outra. Por mais que, por exemplo, o armazenamento em nuvem se proponha a solucionar o problema de armazenamento dos dados, também é perceptível uma preocupação com o longo prazo dado o crescimento exponencial dos dados (SKOURLETOPOULOS et al., 2017a). A análise dos dados, por sua vez, só foi alavancada recentemente por conta dos avanços na IA com o *deep learning* – e mesmo assim continua um desafio. A 5G, por fim, está ainda sendo desenvolvida, com algumas implementações iniciais ocorrendo a partir da infraestrutura 4G existente – deixando o desafio da transmissão de dados e conexão de dispositivos, na prática, ainda em aberto.

2.3 DO TECNOLÓGICO AO POLÍTICO

Além dos desafios de cunho técnico que a Segunda Era Digital possui, uma série de desafios políticos podem ser identificados envolvendo aspectos sociais, econômicos e securitários nos âmbitos nacionais e internacionais. Os conflitos distributivos explorados por Canabarro (2014) para a Internet e seus recursos críticos na Primeira Era Digital, por exemplo, poderão ser encontrados quando a nova infraestrutura da 5G na Segunda Era Digital for implementada – desafio que poderia explicar o conflito entre China e EUA sobre a implementação da infraestrutura 5G da Huawei. A "corrida" pela 5G entre a China e os EUA está alicerçada em preocupações econômicas e securitárias. Pelo lado econômico, os países estão disputando a fronteira tecnológica. Acredita-se que quem empregar 5G com sucesso primeiro terá enormes vantagens econômicas por conta de possibilidades como as cidades inteligentes, a indústria 4.0 e novas oportunidades para as empresas de tecnologia. Estima-se que a transição para 5G nos EUA teria um custo de cerca de US$ 275 bilhões, porém geraria 3 milhões de empregos e US$ 500 bilhões de crescimento do PIB da economia americana (BRAKE, 2018). Existe também uma vantagem econômica a ser obtida por quem conseguir exportar a infraestrutura 5G primeiro (RÜHLIG; SEAMAN; VOELSEN, 2019).

Pelo viés securitário, a preocupação maior por parte dos EUA e seus aliados é a interceptação de informações e espionagem caso os países implementem infraestrutura de 5G chinesa. As suspeitas e alegações de uma proximidade entre a Huawei e o governo chinês

buscam reforçar essa ameaça percebida pelos EUA e seus aliados (HASKA; BECKVARD; MINÁRIK, 2019; KEWALRAMANI; KANISETTI, 2019; RÜHLIG; SEAMAN; VOELSEN, 2019). A administração Trump explicitamente avisou que se um país utilizar infraestrutura chinesa nos seus sistemas críticos de informação, os EUA não poderiam compartilhar inteligência ou trabalhar junto com aquele país (KEWALRAMANI; KANISETTI, 2019). Na prática, as preocupações do governo americano frente uma vitória da China na corrida pela 5G é que seu papel como espinha dorsal da infraestrutura seja perdido, e com isso todas as vantagens econômicas e securitárias que vêm com essa posição.

É possível traçar também uma conexão entre os desafios distributivos da Primeira Era Digital com a concentração de centros de dados para as tecnologias em nuvem, uma vez que a nuvem possui uma infraestrutura física com localização geográfica – e também dependente, atualmente, da infraestrutura física da Internet, na qual os EUA possuem uma posição vantajosa (LYON, 2015; BAUMAN et al., 2014). Ao mesmo tempo, existem aqueles atores que concentram as tecnologias, *expertise* e dados e aqueles excluídos deste processo, aprofundando o desafio distributivo (HANSEN; PORTER, 2017). Essa questão da distribuição de tecnologias e *expertise* levanta também questionamentos sobre a neutralidade das novas tecnologias, especialmente da inteligência artificial. Por mais que a inteligência artificial possa parecer completamente autônoma e neutra, seus algoritmos e sistemas ainda são criados por humanos, os quais são os únicos que podem calibrar e alterar os algoritmos. Ou seja, é um grupo restrito de pessoas que criam e ditam como uma inteligência artificial vai funcionar e para quais interesses e objetivos ela vai servir (HANSEN; PORTER, 2017; SCHWARZ et al., 2019; ANDREJEVIC, 2015).

Outros desafios que acompanham a Segunda Era Digital e suas tecnologias são a governança da sociedade com base em dados e sua análise (MADSEN et al., 2016) e um desafio mais generalizado à democracia (CRAWFORD; MILTNER; GRAY, 2014; BODÓ; HELBERGER; VREESE, 2017). No âmbito securitário, o crescimento da IoT, como no caso das cidades inteligentes, cria uma série de novos riscos e vulnerabilidades ao conectar à internet dispositivos e objetos que antes não estavam vulneráveis a ataques cibernéticos (carros, por exemplo) (KITCHIN; DODGE, 2017). Johnson (2019), por outro lado, apresenta o desafio que os desenvolvimentos recentes da IA e de outras tecnologias da Segunda Era Digital trazem para a segurança internacional. A corrida pela IA, as incertezas acerca dos usos militares desta tecnologia, a possibilidade de automação e robotização das armas a partir da IA e os usos da IA no meio cibernético geram uma série de desafios securitários, legais e éticos (JOHNSON, 2019; USA, 2016a).

Percebe-se, então, que os desafios proporcionados pela Segunda Era Digital rendem uma agenda de pesquisa extensa. Os desafios apresentados aqui não são os únicos que acompanham a Segunda Era Digital. Todavia, estes desafios não serão o foco deste trabalho por conta da agenda de pesquisa que cada um destes desafios proporciona respectivamente. Existe, entretanto, um desafio que envolve todos os atores da Segunda Era Digital (atores estatais, indivíduos/usuários e entidades privadas) e engloba todos os aspectos anteriormente expostos (social, econômico, securitário) tanto na esfera nacional quanto regional e global: a privacidade, tema central desta monografia.

3 A PRIVACIDADE COMO DESAFIO POLÍTICO

Entre os diversos desafios da Segunda Era Digital, o da privacidade surge como um dos principais, uma vez que perpassa os aspectos políticos, sociais, econômicos e securitários, tanto no âmbito nacional como internacional. Tendo isso em mente, este capítulo irá aprofundar a discussão sobre a privacidade na Segunda Era Digital. Para isso, primeiro será explorado a relação entre a personalização e a vigilância (*surveillance*) na Segunda Era Digital. Depois, serão analisados as revelações de Snowden e o escândalo da Cambridge Analytica como dois marcos importantes para a questão da privacidade na Segunda Era Digital. Por fim, serão explorados as atividades de vigilância dos países dos *Five Eyes* e da China.

3.1 PERSONALIZAÇÃO E VIGILÂNCIA

O principal mecanismo pelo qual a Segunda Era Digital apresenta desafios à privacidade é a personalização dos dados. Personalização é o processo de adaptar um sistema ou o resultado de uma análise ao perfil, contexto ou tipo de usuário. Para isso, se utilizam uma série de informações e características desde a localização geográfica, formação acadêmica, experiência profissional até a participação de grupos, interesses e opiniões (HABEGGER et al., 2017). Paralelamente, a coleta de dados e a análise de indivíduos, grupos e contextos para extrair e criar informações – essencial para a personalização – está no centro das definições de vigilância e é sua característica principal (MARX, 2015; LYON, 2015; LYON, 2018; HAGGERTY; ERICSON, 2006; DUBROFSKY; MAGNET, 2015)[34]. A personalização e a vigilância, assim, avançam juntas na Segunda Era Digital, uma vez que o processo da personalização precisa da análise de indivíduos, grupos e contextos para extrair e criar informações e necessita a coleção de dados para estas análises personalizadas. Em outras palavras, a personalização requer a vigilância. Ao mesmo tempo, como será explorado ao longo deste capítulo, a análise com viés personalizado de dados abre novas possibilidades para a vigilância.

Na Segunda Era Digital, a quantidade de dados coletados e as possibilidades de análise e cruzamento permite que uma série de dados sejam agregados de diversas fontes para montar um perfil robusto de um indivíduo. Além do mais, as diversas fontes ajudam a validar dados recebidos de uma fonte, validando, na prática, se um dado é uma anomalia ao perfil (e deve ser desconsiderado no momento). O objetivo da personalização, no setor privado, é providenciar

[34] O que difere entre uma definição e outra é o escopo analítico para além da análise de indivíduos, grupos e contextos para extrair e criar informações. Marx (2015) encerra a sua definição da nova vigilância nestes termos para trazer uma definição ampla e abrangente de vigilância. Lyon (2015; 2018) e Haggerty e Ericson (2006) incorporam elementos de controle e governabilidade nos seus conceitos de vigilância. Dubrofsky e Magnet (2015) levam em consideração as relações de poder no seu conceito de vigilância para os estudos feministas de vigilância.

serviços melhores e mais adaptados ao consumidor a partir de um perfil montado dos dados dele (HABEGGER et al., 2017). Busca-se, na prática, direcionar informações relevantes ao usuário a partir dos seus dados e do seu histórico digital (HABEGGER et al., 2017; XIE, 2018).

O ato de coletar dados para melhorar o seu negócio a partir da personalização não é, em um primeiro momento, uma infração legal da privacidade – embora seja argumentável que já seja, tendo em vista que muitas vezes os usuários não estão cientes de que estão entregando seus dados para o negócio, ou que tais dados são capazes de identificar o usuário (ETZIONI, 2015; LYON, 2014; XIE, 2018). A coleta dos dados pelas empresas, inclusive, é muitas vezes legalizada. A maior invasão à privacidade, todavia, ocorre quando os dados são ou vendidos ou roubados (e potencialmente vendidos depois) para um terceiro ator, o qual então utiliza estes dados, seja para fins mercadológicos ou outros. Além disso, Etzioni (2015) aponta para a existência de "mercadores da privacidade" – atores (geralmente do setor privado) que, através de *cookies*[35] de rastreamento e de meios de *data mining*[36], acumulam dados e constroem perfis a partir destes dados agregados e analisados. Estes perfis, assim, são capazes de identificar as pessoas e associar a elas uma gama de informações – muitas vezes através de inferências a partir das informações agregadas, mantendo, assim, as ações dentro da legalidade[37] (ETZIONI, 2015).

As maneiras como os dados são coletados, quando falamos de privacidade, podem ser resumidas em três principais categorias: direcionada, automatizada e "voluntária" (LYON, 2014[38]). Na coleção direcionada, um operador humano é quem coleta os dados. Por outro lado, a coleção automatizada é aquela na qual dados são coletados sem um operador humano e é, junto com a voluntária, um dos principais modos de obtenção dos dados na Segunda Era Digital. A coleção voluntária, por fim, é quando os dados coletados são obtidos a partir da entrega "voluntária" dos usuários em mídias sociais e serviços digitais. A razão por trás destas aspas é de que muitas vezes, os usuários não sabem que estão entregando seus dados (LYON, 2014).

Ademais, com o advento da Segunda Era Digital, novos dados estão sendo coletados e novas maneiras de analisar e agregar os dados estão surgindo. Estas mudanças estão ocorrendo em boa parte devido à dataficação da vida e às redes sociais[39]. Outro fator importante é a

[35] É um arquivo pequeno que é deixado em uma máquina por um servidor e que contém informações sobre as atividades do usuário. O arquivo é retornado para o servidor quando o usuário acessa o site de novo (BUTTERFIELD et al., 2016).
[36] É um termo para a extração de informação a partir de dados, nos quais a informação ainda não era sabida antes da extração (BUTTERFIELD et al., 2016).
[37] Vale ressaltar que o âmbito jurídico ao qual o Etzioni (2015) se refere é o dos Estados Unidos.
[38] Lyon (2014) utiliza essa taxonomia dentro do contexto dos estudos de *surveillance*. Porém, como a *surveillance* é uma das principais ameaças à privacidade na Segunda Era Digital, a taxonomia presente em Lyon (2014) é utilizada no contexto da privacidade nesta monografia.
[39] Uma das maneiras pelas quais as redes sociais geram uma quantia enorme de dados referentes às atividades dos seus usuários é pelos botões de "like" e "tweet", por exemplo. Estes botões efetivamente possuem a capacidade de

utilização de metadados, que são os dados dos próprios dados, como o endereço de IP, localização da foto ou da ligação, quem é a pessoa na foto ou quem é o contato, etc. A junção de dados pessoais obtidos das redes sociais, da dataficação e da metadados permite que atores consigam, através do agregado e da análise destes dados, montar não apenas o histórico de um indivíduo, mas também buscar predizer e antecipar ações e processos. A partir disso, torna-se possível que os atores possam intervir antes que os eventos aconteçam com o fim de moldar os comportamentos dos indivíduos e os resultados dos processos (LYON, 2014). Todavia, os impactos da Segunda Era Digital nestas técnicas[40] cabem mais aos estudos comportamentais dentro da economia, sociologia e psicologia.

Kerr e Earle (2013), por sua vez, trazem uma taxonomia de três tipos principais de predição utilizados nas análises do *big data* que são úteis para esta monografia: predições de consequência, de preferência e preventivas. No fundo, toda prevenção é uma predição. É partindo disto que os autores apontam para o primeiro tipo, a de consequência. Tais predições de consequência buscam auxiliar o cliente mostrando o que será benéfico para ele, consequentemente reduzindo, em tese, o risco da decisão (KERR; EARLE, 2013; LYON, 2014). Este tipo de predição baseado no *big data* é pouco utilizado (KERR; EARLE, 2013).

As predições que mais vemos utilizados na Segunda Era Digital por atores do setor privado e por atores estatais, respectivamente, são as de preferência e as preventivas. As predições preferenciais, como o nome indica, buscam prever o que é do interesse do indivíduo e estão por trás dos sistemas de recomendação de produtos e conteúdos na internet. Por fim, as predições preventivas possuem como objetivo restringir a quantidade de decisões futuras que um indivíduo pode ter. Assim, as predições preventivas são a única que não busca beneficiar o indivíduo analisado, mas sim aquele ator fazendo a análise que está buscando prevenir alguma ação, como as *no-fly lists* utilizadas por atores estatais (KERR; EARLE, 2013). Na prática, estas intervenções dos atores com o fim de prever as possibilidades e moldar os comportamentos, processos e resultados se traduz, resumidamente, no marketing direcionado pelo setor privado e em abordagens preventivas de policiamento e de segurança nacional pelo estado, dentre outras aplicações (LYON, 2014; XIE, 2018).

---

rastrear um usuário das redes sociais respectivas (Facebook e Twitter) enquanto o usuário estiver logado (independente se o usuário está com a janela ou aba da rede social aberta) (ETZIONI, 2015).

[40] Verifica-se, por exemplo, a utilização do *nudging* em uma escala maior a partir dos dados agregados (HELBING et al., 2017). *Nudging* é uma abordagem que "guia" as pessoas em direção a alguma decisão, comportamento ou ação desejável pelo *nudger* (SUNSTEIN, 2014; WILKINSON, 2012). Esta abordagem gera uma discussão se ela é, como alguns propõem (SUNSTEIN, 2014), uma abordagem libertária que preserva a liberdade de escolha, ou se ela pode ser enquadrada como manipulação (HELBING et al., 2017; WILKINSON, 2012).

Esse trabalho tem, até o momento, diferenciado os atores privados dos atores estatais e tratado eles com um certo grau de separação. É importante ressaltar, todavia, que o que os diferencia é fim para o qual estes utilizam os dados – os atores estatais utilizam-los para fins de inteligência, vigilância e segurança nacional, enquanto que os atores privados usam-los para aumentar os seus lucros, sua eficiência e a sua conveniência para o consumidor. Os dados utilizados são os mesmos e as técnicas são extremamente similares, se não iguais, entre os atores privados e os estatais (LYON, 2014; LYON, 2015; ETZIONI, 2015).

Existe, assim, um grau considerável de integração entre os dois setores (LYON, 2014; ETZIONI, 2015). Além do diálogo e compartilhamento de técnicas entre os dois setores e a cooperação – às vezes argumentavelmente forçada – do setor privado com programas de vigilância dos Estados (que serão explorados no próximo capítulo), existem empresas privadas – os chamados mercadores da privacidade de Etzioni (2015) – que vendem tanto bases de dados quanto perfis analisados para empresas privadas e governos (ETZIONI, 2015; LYON, 2015). Um único mercador da privacidade nos Estados Unidos, a ChoicePoint, possui no mínimo 35 contratos com entidades estatais americanas. Porém existem grandes chances de que o número seja maior ainda, tendo em vista que muitos dos contratos são classificados. Além da ChoicePoint, existem cerca de quatro mil mercadores da privacidade nos Estados Unidos (ETZIONI, 2015).

Assim, por mais que os atos de vigilância dos atores estatais recebam o holofote na mídia e, em parte, na academia quando falamos de violação da privacidade, é importante lembrar que as ações dos atores privados também violam a privacidade e podem causar efeitos similares (ETZIONI, 2015). Lyon (2015) inclusive argumenta que, na verdade, os fins de tanto os atores privados quanto os estatais podem ser simplificados como utilizar os dados e metadados para identificar "suspeitos", sejam eles suspeitos em relação à segurança nacional, seja em relação à potencial compra de um produto.

Em seu livro *"The Culture of Surveillance*", Lyon (2018), ao argumentar que uma "cultura de vigilância" está emergindo[41], amplia sua definição de vigilância para as "[...] operações e experiências de coletar e analisar dados pessoais para influenciar, para gerenciar e para julgar sua titularidade" (LYON, 2018, p.11, tradução nossa). A partir desta última definição, tanto atores privados quanto estatais podem ser considerados "*surveillers*". O que Lyon (2018) acrescenta ao núcleo duro da definição de vigilância apresentada no início desta seção é a utilização das informações (geradas pela análise) para fins de controle (influência e

[41] Ver LYON (2018).

gerenciamento) e a ênfase Empresas privadas exercem influência ao utilizar o perfil dos indivíduos para indicar os melhores produtos a serem comprados e mídias a serem consumidas; atores privados e estatais podem decidir se um indivíduo qualifica-se ou não para algo (se ele pode ter titularidade ou não), como bancos ou governos quando definem se um indivíduo é elegível a um empréstimo ou a um programa de assistência social e; por fim, todos os atores – incluindo os indivíduos – podem utilizar dados para gerenciar (LYON, 2018).

Utilizando estas definições de vigilância de Lyon (2015; 2018), torna-se possível considerar as ações de atores privados e estatais como vigilância. Embora os motivos pelos quais os atores fazem vigilância possam variar, os fins são os mesmos: identificar pessoas que se encaixem em um perfil (os "suspeitos") e influenciá-las ou gerenciá-las (LYON, 2014; LYON, 2015; LYON, 2018). Tais atividades de vigilância (ainda mais baseadas em dados) não são uma novidade da Segunda Era Digital (LYON, 2014; LYON, 2015; ETZIONI, 2015). O que muda na Segunda Era Digital é a intensidade e a amplitude da vigilância, que pode já ser considerada vigilância em massa (LYON, 2014; 2015; 2018; ETZIONI, 2015; DENCIK; CABLE, 2017). O paradigma do *Big Data* não só envolve um aumento no volume dos dados disponíveis, mas envolve, principalmente, a ideia de que os dados são coletados constantemente antes dos parâmetros de uma análise serem definidos. A IoT está expandindo a coleta de dados e metadados que podem ser utilizados para vigilância; as tecnologias em nuvem são necessárias para armazenar todos estes dados e processá-los; a IA permite analisar todos estes dados em tempo-real e a 5G é a infraestrutura necessária para alavancar o alcance destas tecnologias e integrá-las em tempo-real (e que, como será visto no próximo capítulo, por ser infraestrutura, está vulnerável à intervenção estatal para a coleção de dados).

Ademais, a personalização se mostra como um verdadeiro paradoxo na Segunda Era Digital (SIMOS, 2015; LYON, 2014; LYON, 2015). Por um lado, o valor dos dados analisados e transformados em informação existe por causa da centralidade da personalização – através dos dados – tanto para o desenvolvimento dos negócios através da entrega de produtos e serviços mais adequados (e personalizados) ao consumidor, quanto para o avanço as atividades orientadas a segurança nacional (LYON, 2015), especialmente a vigilância. Por outro lado, a personalização, ao efetivamente permitir uma vigilância em massa, contribui para a grande ameaça à privacidade que são as atividades de vigilância exercidas tanto pelos atores privados quanto os estatais (e, argumentavelmente, os próprios indivíduos).

Manokha (2018) inclusive argumenta que a invasão ou violação da privacidade dos indivíduos é estrutural de uma nova modalidade do capitalismo que surge na Segunda Era Digital, o capitalismo de plataformas (*platform capitalism*) no qual o capital de plataformas

(*platform capital*) ocupa um papel central. Nesta fase do capitalismo, a vigilância possui um papel central na acumulação de capital através da coleta, análise e monetização contínuas de dados, obtidos a partir das atividades de usuários e, por conta da IoT, objetos físicos. Através dos processos apresentados na cadeia de valor do *big data* anteriormente (Figura 1), os dados são gerados, coletados e armazenados. Porém, é apenas através da análise dos dados e da sua futura utilização que o valor é gerado (MANOKHA, 2018; LANGWORTHY, 2018).

Dado, então, o papel central da personalização a partir do *big data* – alimentado, armazenado e analisado graças às tecnologias da Segunda Era Digital – para o desenvolvimento e definição da Segunda Era Digital e da violação à privacidade que ela gera, é possível afirmar que a privacidade é o maior desafio político da Segunda Era Digital. O desafio da privacidade, ademais, é um desafio econômico (dada a importância da personalização para as empresas atualmente), social (por conta das implicações das violações da privacidade para a sociedade) e securitário (por causa, também, do papel da personalização na identificação de ameaças à segurança nacional[42]). Todavia, a privacidade é um desafio por conta das ameaças a ela que existem na Segunda Era Digital. Dois casos ilustram diferentes aspectos da ameaça que a vigilância impõe à privacidade. As revelações de Edward Snowden tratam o lado da coleta dos dados, enquanto o escândalo da Cambridge Analytica abrange o lado da utilização dos dados e informações extraídas para além do marketing direcionado.

3.2 DE SNOWDEN À CAMBRIDGE ANALYTICA

No dia 6 de junho de 2013, o primeiro de muitos documentos da *National Security Agency* (NSA) dos EUA foi vazado por Edward Snowden (que nos primeiros dias era ainda uma fonte anônima) e noticiado exclusivamente por Glenn Greenwald do jornal britânico The Guardian. Este primeiro documento era uma ordem judicial da *Foreign Intelligence Surveillance Court*[43] dos EUA obrigando a empresa de telecomunicações Verizon a entregar a metadados de todas as ligações que passavam pela infraestrutura da Verizon. A entrega da metadata deveria ser feito em formato digital e deveria ocorrer diariamente no período especificado da ordem judicial (GREENWALD, 2013a; VERIZON, 2013). Os metadados

[42] A relação entre as novas tecnologias, a personalização e sua utilização para a identificação de ameaças à segurança é explorado no contexto do contra-terrorismo por LEHR, 2019.

[43] A *Foreign Intelligence Surveillance Court* (FISC) foi criada pelo *Foreign Intelligence Surveillance Act* (FISA) de 1978. Seu objetivo original é avaliar – secretamente – pedidos de utilização dos poderes de vigilância do governo para vigiar "poderes estrangeiros" que possam ser uma ameaça à segurança nacional. Com o *PATRIOT Act* após os atentados de 11 de setembro, o FISA foi alterado e teve seus poderes expandidos, facilitando a obtenção de comunicações desde que o pedido à FISC não seja direcionado exclusivamente à americanos (COHEN; WELLS, 2004).

incluem informações que poderiam ser utilizadas para identificar quem estava ligando quem, por quanto tempo e a localização (LANDAU, 2013; GREENWALD, 2013a).

No dia seguinte, o The Guardian divulgou slides de uma apresentação secreta da NSA que falavam sobre o programa denominado PRISM. O programa permitiria acesso direto aos servidores centrais da Google, Microsoft, Yahoo, Facebook, PalTalk, AOL, Skype, YouTube e Apple para coletar uma série de informações e dados, como e-mails, conversas por vídeo e por voz, dados armazenados, informações publicadas nas redes sociais, entre outros (GREENWALD, 2013b; GELLMAN; POITRAS, 2013; NSA SLIDES, 2013). Com os primeiros documentos do PRISM, surgiram também as primeiras informações do envolvimento e cooperação da GCHQ britânica nas atividades de vigilância dos EUA. Além de permitir que a NSA contornasse os processos judiciais convencionais para obter os dados, o PRISM permitiria que a GCHQ também pulasse os processos legais (e internacionais) para adquirir acesso às informações privadas guardadas por uma empresa de fora do Reino Unido (GELLMAN; POITRAS, 2013).

Ao longo do resto do mês de junho, uma série de outros documentos detalhando atividades de vigilância da NSA e aliados foram divulgados. Alguns dos programas, como o Blarney (ativo desde a década de 1970) e o Rampart-T (ativo desde 1991), seriam direcionados à espionagem de corpos diplomáticos e governos estrangeiros, incluindo aliados como os países europeus e a União Europeia (UE) (POITRAS; ROSENBACH; STARK, 2013a; POITRAS; ROSENBACH; STARK, 2013b) MACASKILL; BORGER, 2013). Outras revelações de Snowden no mês de Junho incluem informações de que a China teria sido alvo de uma série de operações cibernéticas ao longo de quatro anos, dentre elas a invasão de empresas de internet e de telecomunicações (LAM, 2013a; LAM, 2013b; LAM; CHEN, 2013) e a cooperação entre a GCHQ britânica com a NSA e entre a *Bundesnachrichtendienst* (BND), a agência de inteligência externa da Alemanha (MACASKILL et al., 2013; GUDE; POITRAS; ROSENBACH, 2013). Merece destaque aqui o programa Tempora (rodando desde aproximadamente 2008) da GCHQ, no qual a agência britânica teria conseguido acessar a infraestrutura física de fibra ótica (com o aval das empresas) e estaria coletando as informações de tráfego de internet e chamadas telefônicas que passavam por esta infraestrutura, armazenando elas e compartilhando-as com a NSA (MACASKILL et al., 2013). Também vale chamar atenção para a ferramenta *Boundless Informant* revelada na leva de documentos de junho, através da qual seria possível verificar o quanto de metadados foram coletados em cada país pela infraestrutura de Inteligência de Sinais (SIGINT) (GREENWALD; MACASKILL, 2013).

O mês de julho de 2013 começou com revelações de outro programa, o XKeyscore, e com informações de operações de vigilância da NSA no Brasil, através do programa Fairview e de outros previamente vazados (GREENWALD, 2013c; GREENWALD; KAZ; CASADO, 2013;). O programa Fairview envolveria uma parceria com uma grande empresa de telecomunicações dos EUA não identificada, que por sua vez faria parcerias com provedores de internet e telecomunicações no mundo inteiro, tendo acesso, assim, a infraestrutura de comunicações de outros países e aos dados que transitam por aquela infraestrutura (GREENWALD, 2013c; GREENWALD; KAZ; CASADO, 2013). No Brasil, além do mais, a NSA, em conjunto com a CIA, possuiria uma base de inteligência para espionagem através de satélites em Brasília (KAZ; CASADO, 2013).

A ferramenta XKeyscore, por sua vez, permitiria que a NSA pesquisasse em uma base de dados contendo e-mails, conversas e históricos de navegação. Segundo os documentos revelados por Snowden, o XKeyscore seria o programa com alcance mais amplo no que tange atividades na internet (GREENWALD, 2013d; XKEYSCORE, 2013). Através do XKeyscore, seria possível, segundo os documentos, monitorar a atividade de um usuário na internet em tempo-real (PFISTER; POITRAS; ROSENBACH; SCHINDLER; STARK, 2013; XKEYSCORE, 2013). Além do mais, outros documentos apontam para o uso do XKeyscore pelo BND alemão, junto com uma aproximação desta organização com a NSA (PFISTER, 2013; GERMAN, 2013). Julho também foi o mês no qual o envolvimento da Austrália e da Nova Zelândia começou a ser detalhado, incluindo a contribuição desses dois países ao XKeyscore (DORLING, 2013a)

O mês de agosto de 2013 viu revelações do envolvimento de outros membros da parceria de inteligência como os chamados *Five Eyes*, composto pelos EUA, Reino Unido, Canadá, Austrália e Nova Zelândia. No Reino Unido, empresas donas dos cabos de fibra-ótica que passavam pelo país estariam cooperando com a GCHQ, que utilizaria o acesso a esta infraestrutura para interceptar os dados trafegados e alimentar o programa Tempora (BALL; HARDING; GARSIDE, 2013). No outro lado do mundo, agências de inteligência da Austrália e da Singapura estariam trabalhando junto com o Reino Unido para interceptar as comunicações que passavam por um cabo submarino que conectava os três países (além de diversos outros da Ásia, África, Oriente Médio e Europa) e alimentava o Tempora (DORLING, 2013b). Ainda em agosto, alguns outros detalhes das relações entre os EUA e as empresas surgiram, detalhando relações financeiras para aquelas empresas envolvidas com o PRISM e verba direcionada para provedoras de internet e telecomunicações desde o programa Blarney na década de 1970 e

incluindo o Fairview e o Stormbrew, assim obtendo acesso aos cabos da espinha dorsal global de comunicação localizada nos EUA (TIMBER; GELLMAN, 2013; MACASKILL, 2013).

No mês seguinte, setembro de 2013, as revelações que surgiram trouxeram mais alguns métodos utilizados pela NSA, dentre eles a invasão de *smartphones* via OS e via aplicativos específicos (ROSENBACH; POITRAS; STARK, 2013). Veio à tona também o compartilhamento de inteligência da NSA com Israel e a espionagem da Petrobrás e da então presidente da época, Dilma Rousseff (GREENWALD; POITRAS; MACASKILL, 2013; ROMERO; ARCHIBOLD, 2013; PETROBRAS, 2013). Além do mais, foram reveladas informações de um projeto da NSA chamado *Follow the Money*, no qual a agência coletaria informações de transações financeiras (majoritariamente de cartões de crédito) e guardaria elas em um banco de dados chamado Tracfin (NSA SPIES, 2013).

Em outubro de 2013, além de uma série de informações sobre a espionagem de diversos líderes mundiais por parte dos *Five Eyes*, vieram a público um novo programa, o Muscular, e evidências de cooperação entre a NSA e agências de inteligência na França e na Espanha. Entretanto, as revelações do compartilhamento de dados entre a NSA e a França e a Espanha foram rebatidas oficialmente por um general após ser indagado sobre o ocorrido no *House Intelligence Committee*, onde ele alegou que houve uma falta de entendimento (por parte dos jornais franceses e espanhóis) e que os aliados da Organização do Tratado do Atlântico Norte (OTAN) compartilhavam com a NSA informações e dados que os países da aliança coletavam em zonas de guerra (NAKASHIMA; DEYOUNG, 2013). Porém, um dia depois, novos documentos apontaram para a existência da cooperação entre as agências de inteligência dos países em questão (e vários outros)[44] e a NSA (HAMILOS, 2013).

Em relação ao programa Muscular, documentos obtidos pelo Snowden revelaram que a NSA teria conseguido infiltrar as redes internas da Google e Yahoo, obtendo, assim, acesso a todos os dados que transitavam pelas redes fechadas (que possuíam inclusive infraestruturas próprias) destas duas empresas. Na prática, isso permitiria que a NSA tivesse acesso a todos os centros de dados da Google e do Yahoo. No caso específico deste programa, as empresas não estariam cientes da intercepção dos dados. O programa Muscular contava também com a ajuda da GCHQ (GELLMAN; SOLTANI, 2013).

[44] Os documentos vistos pelo jornal El Mundo dividiam os países parceiros por nível de cooperação. A maior cooperação ocorreria entre os países da parceria *Five Eyes* (Reino Unido, Austrália, Canadá e Nova Zelândia). Outro nível seria composto por 19 países, incluindo o Japão, Coreia do Sul e Espanha – 17 dos quais eram europeus. Um terceiro nível, caracterizado como cooperação limitada, consistia da França, Israel, Índia, Paquistão e outros países. Um último nível englobava os países considerados hostis aos EUA e era caracterizado como cooperação em casos de exceção (HAMILOS, 2013)

Em seguida, em novembro de 2013, surgiu um documento detalhando a estratégia geral da NSA para a inteligência de sinais (SIGINT) para o período de 2012 a 2016. Esse documento reconhecia o desafio de desenvolver a SIGINT para acompanhar as mudanças no espaço digital, inclusive chamando atenção para a "era dourada da SIGINT". Ao mesmo tempo, o documento descrevia a necessidade de se adaptar (leia-se potencialmente afrouxar) o aparato legal para a nova era de informações, além de clamar por um aumento da capacidade da NSA de quebrar as práticas de cibersegurança dos adversários para que seja possível adquirir dados de qualquer pessoa, em qualquer lugar e a qualquer hora (RISEN; POITRAS, 2013; A STRATEGY, 2013). A estratégia também detalha a necessidade de revolucionar a capacidade de análise dos dados a partir de automações e de tecnologias baseadas nos processos cognitivos (A STRATEGY, 2013).

Outro documento, revelado ainda em novembro de 2013, trouxe confirmação explícita de que o Reino Unido teria assinado um acordo com a NSA permitindo o acesso a dados pessoais de cidadãos britânicos. Até então, acreditava-se que os cidadãos dos países participantes da parceria *Five Eyes* estariam protegidos perante os outros países da parceria (BALL, 2013a). No final do ano, em Dezembro de 2013, outros documentos revelaram uma situação, agora envolvendo a então *Defence Signals Directorate* (DSD), atual *Australian Signals Directorate* (ASD). Seriam compartilhados metadados no geral, sem nenhuma filtro e sem ter um nacional australiano como alvo. Porém, caso o perfil buscado detectasse um australiano, seria necessário passar por um procedimento judicial. A questão, todavia, é que a DSD entregava a coleção de dados sem retirar os dados dos seus cidadãos, efetivamente entregando dados de australianos na parceria (MACASKILL; BALL; MURPHY, 2013).

Ainda em dezembro de 2013, novos documentos trouxeram à luz relações de compartilhamento de inteligência por parte da Noruega e da Suécia com a NSA (SIMPSON, 2013; HALVORSEN, 2013). Também foram reveladas algumas capacidades da NSA, incluindo a infiltração nos *cookies* de rastreamento (com preferência pelo *cookie* PREF da Google[45]), que as empresas usam para direcionar o marketing, para rastrear as atividades das pessoas que já são consideradas suspeitas (SOLTANI; PETERSON; GELLMAN, 2013); a coleção de aproximadamente 5 bilhões de dados por dia referentes a localização de celulares no mundo que seriam então armazenados numa base de dados chamada FASCIA (GELLMAN;

[45] "Google assigns a unique PREF cookie anytime someone's browser makes a connection to any of the company's Web properties or services. This can occur when consumers directly use Google services such as Search or Maps, or when they visit Web sites that contain embedded "widgets" for the company's social media platform Google Plus. That cookie contains a code that allows Google to uniquely track users to "personalize ads" and measure how they use other Google products." (SOLTANI; PETERSON; GELLMAN, 2013)

SOLTANI, 2013; THE WASHINGTON POST, 2013b) e a decodificação de comunicações feitas via celular, como mensagens SMS (TIMBER; SOLTANI, 2013).

O ano de 2014 começou com a revelação de mais algumas capacidades e programas em Janeiro. Documentos mostraram que a NSA teria coletado quase 200 milhões de mensagens de texto no mundo inteiro e extraiam os metadados destas mensagens, permitindo a determinação da localização, dos contatos na conversa e até detalhes de cartões de crédito e transações financeiras feitas via celular. Estes dados e metadados seriam então armazenados numa base de dados chamada Dishfire. Através da ferramenta de análise automatizada Prefer, seria possível filtrar e procurar dados específicos no Dishfire. A GCHQ britânica, os documentos mostram, possuiria acesso ao Dishfire (BALL, 2014a). Outro programa, o Squeaky Dolphin, coletaria e analisaria dados do YouTube, Facebook e blogs para fazer uma análise de tendências sem o intuito de analisar comportamentos de indivíduos, mas sim questões como vídeos, posts e assuntos que estavam em alta em tempo real (ESPOSITO et al., 2014). Dentre as capacidades reveladas estaria a interceptação (por parte tanto da NSA quanto da GCHQ) de informações de aplicativos em *smartphones* que geralmente são captadas e enviadas para alimentar o marketing direcionado (BALL, 2014b; GLANZ; LARSON; LEHREN, 2014).

Outros programas e capacidades foram sendo revelados ao longo de 2014 (embora bem menos do que em 2013). O programa Turbine, revelado em março daquele ano, teria envolvido o desenvolvimento de um sistema que possuía uma inteligência artificial baseada, pelo o que a linguagem dos documentos indica, em redes neurais. Essa inteligência artificial teria sido desenvolvida para implantar malwares, configurar eles nas máquinas infectadas e coletar dados através destes malwares de forma automatizada. Os *malwares* permitiria, mas não se restringiria, a tomada de controle de computadores infectados; a ativação (e captura usando) de *webcams* e microfones; o roubo de dados de dispositivos externos (como *pendrives*) ao serem conectados a uma máquina infectada; o roubo de credenciais e; interceptação de dados em redes infectadas (GALLAGHER; GREENWALD, 2014).

O sistema Turbine, entretanto, não agiria sozinho: ele dependeria de uma série de sensores denominados Turmoil instalados ao redor do mundo. Enquanto o Turbine extrairia os dados, os sensores do Turmoil direcionaria eles para a NSA para análise. Ao mesmo tempo, os sensores Turmoil poderiam alertar o sistema Turbine quando os sistemas infectados estão comunicando (GALLAGHER; GREENWALD, 2014). Além do mais, os documentos relacionados ao Turbine e Turmoil mostram que a GCHQ teve um papel importante no desenvolvimento e na execução do Turbine (GALLAGHER; GREENWALD, 2014).

O programa Mystic e a ferramenta RETRO, também revelados em março, seriam capazes de coletar todas as conversas telefônicas de uma nação e armazenar elas por 30 dias, tornando possível, até certo ponto, resgatar ligações feitas no passado (GELLMAN; SOLTANI, 2014). Em maio de 2014, detalhes surgiram dos esforços da NSA em obter imagens para montar um banco de dados para reconhecimento facial. Junto a isso, a agência estaria, segundo os documentos, estudando as possibilidades de agregar outros dados biométricos. Dois programas citados nos documentos dessa revelação eram o Pisces, destinado a coletar dados biométricos na entrada e saída de uma série de países, e o Wellspring, que pegava imagens de comunicações e buscava imagens de passaportes. Em relação à inteligência artificial necessária para o reconhecimento facial, a NSA, além de estar desenvolvendo sua própria tecnologia, utilizava também algumas tecnologias disponíveis no mercado para as tarefas de reconhecimento facial (RISEN; POITRAS, 2014).

A Vodafone, no mês seguinte, veio à público e confirmou a existência de conexões diretas (e secretas) à infraestrutura deles e de outros provedores de internet e telecomunicações que permitiam a escuta e o rastreamento de localização dos usuários pelas agências de inteligência (GARSIDE, 2014). Em junho de 2014 também foram revelados novos documentos que apontavam para a cooperação com diversos outros parceiros através do acesso aos cabos de fibra-ótica ou da sediação de equipamentos americanos que permitissem intercepção de comunicações na infraestrutura. O programa sob o qual estas parcerias estariam enquadradas se chamava de Rampart-A. Embora os parceiros não eram explicitamente denominados nos documentos do Rampart-A, outros documentos apontam para uma potencial lista de 33 países[46] (GALLAGHER, 2014a).

Mais uma ferramenta, o ICReach, foi revelado em 2014 no mês de agosto. O ICReach serviria como um portal de pesquisa como o do Google, mas que buscaria em uma série de bases de dados não identificadas nos documentos para "responder" a pesquisa. Teoricamente, segundo os documentos, o ICReach apenas vasculharia e entregaria dados das comunicações de estrangeiros (GALLAGHER, 2014b).

O conjunto de revelações a partir dos documentos vazados por Edward Snowden adquirem importância como um marco para a Segunda Era Digital por conta do impacto na percepção e *awareness* para além da comunidade especializada, especialmente em relação à

[46] Algéria, Áustria, Bélgica, Croácia, República Tcheca, Dinamarca, Etiópia, Finlândia, França, Alemanha, Grécia, Hungria, Índia, Israel, Itália, Japão, Jordânia, Coreia do Sul, Macedônia, Países Baixos, Noruega, Paquistão, Polônia, Romênia, Arábia Saudita, Singapura, Espanha, Suécia, Taiwan, Tailândia, Tunísia, Turquia e Emirados Árabes (GALLAGHER, 2014a).

capacidade estatal de obtenção e utilização dos dados (WILTON, 2017; POHLE; AUDENHOVE, 2017). As revelações também demonstraram como a vigilância estatal depende de uma série de tecnologias da Segunda Era Digital (LYON, 2014). Por mais que o campo acadêmico e os técnicos especializados estivessem discutindo já as possibilidades que o *Big Data* gerava para a vigilância, as revelações de Snowden trouxeram exemplos concretos destas aplicações e levaram o debate para o público em geral (VLADECK, 2014). A exploração das novas tecnologias tanto da Primeira Era Digital quanto da Segunda não era uma novidade. O que mudou foi sair do campo das possibilidades ao ter provas concretas desta exploração (DENCIK; CABLE, 2017).

Antes das revelações, é possível dizer que as principais percepções sobre o uso dos dados eram que: i) a principal ameaça à privacidade vinha das empresas privadas e o marketing direcionado; ii) a utilização dos dados por agências de segurança e de inteligência era restringida, focada e de acordo com a lei; iii) a privacidade da população estaria protegida legalmente (WILTON, 2017). Após, tornou-se claro o alcance estatal e as ameaças à privacidade apresentadas pelos programas de vigilância (WILTON, 2017). A vigilância não está de acordo com a lei, não é restringida e não foca apenas nos malfeitores e terroristas. Ficou claro também a natureza digital que a vigilância estava vindo a possuir, algo que não era claro para o público em geral anteriormente (DENCIK; CABLE, 2017).

Por mais surpreendentes as revelações, a resposta social relativamente muda no longo-prazo reforça uma certa normalização e aceitação da vigilância (tanto estatal quando privada)[47] na Segunda Era Digital por conta da sua relação com as novas tecnologias, a personalização e as vantagens de ambas (BAUMAN et al., 2014; DENCIK; CABLE, 2017). Em parte, isso pode ter ocorrido por conta da falta de visualização de como isso de fato afeta a vida de um indivíduo que "não tem nada a esconder"[48]. Nas palavras de Vladeck (2014), "[...] os dados existirão [...] a questão vai ser como eles serão utilizados – e por quem" (VLADECK, 2014, p. 336, tradução nossa).

A questão da utilização dos dados apontada por Vladeck (2014) nos leva para o próximo marco na Segunda Era Digital, o escândalo da Cambridge Analytica. A história de o que viria a ser o escândalo da Cambridge Analytica começa entre 2013 e 2014, quando um grupo de

[47] Para mais informações sobre as discussões acerca da normalização da *surveillance*, ver Bauman et al., (2014) para informações mais resumidas; Dencik e Cable (2017) para ver a ideia de "*surveillance realism*" e entrevistas sobre as percepções das revelações e *surveillance* no geral e; ver o livro "*The Culture of Surveillance: Watching as a Way of Life*" de Lyon (2018).

[48] Dencik e Cable (2017), através de entrevistas com ativistas políticos diversos, indicam que os ativistas só se preocupam com *surveillance* caso as suas atividades não sejam aceitáveis.

pesquisadores do Centro de Psicometria da Universidade de Cambridge elaboram um teste de perfil psicológico no Facebook que correlacionava o teste com as atividades no Facebook dos entrevistados. Com 350.000 participantes nos EUA, o estudo estabeleceu cientificamente uma relação entre as atividades *online*, como as feitas no Facebook, e o perfil psicológico OCEAN[49] utilizado na pesquisa. A conclusão da pesquisa foi que era possível determinar, com um grau considerável de precisão, o perfil psicológico de um indivíduo a partir dos dados produzidos por um indivíduo na internet (ISAAK; HANNA, 2018).

A psicometria busca medir particularidades psicológicas a partir de cinco características principais: abertura, consciência, extroversão, aceitabilidade e neuroticisimo (OCEAN, a partir das palavras em inglês). Embora a psicometria seja utilizada desde a década de 1980, por muito tempo o principal problema da sua aplicação em larga escala era a limitação na coleta de dados detalhados. Com o advento das redes sociais e do volume de dados disponíveis na Segunda Era Digital, esse problema foi contornado – os *data points* aumentaram exponencialmente e os dados são produzidos e atualizados em tempo real. A análise e agregação destes dados faz com que os perfis montados para as pessoas se tornem precisos. Esta combinação da psicometria com a análise de *big data* é chamada de *psychographic profiling*. Por causa da pesquisa feita em 2013, os pesquisadores, Kosinski e Stillwell, se tornaram donos do maior *dataset* psicométrico do mundo na época (RISSO, 2018).

Em 2014 – inspirado nos estudos de Kosinski e Stillwell – Aleksandr Kogan, através da sua empresa Global Science Research (GSR) e em colaboração com a Cambridge Analytica, montou um teste parecido ao de Kosinski e Stillwell. Utilizando seu vínculo empregatício Universidade de Cambridge, Kogan obteve permissão do Facebook para lançar seu teste como um aplicativo dentro da rede social para coletar dados, embora o desenvolvimento do teste foi feito separado das suas atividades na Universidade (RISSO, 2018; ISAAK; HANNA, 2018; BERGHEL, 2018).

O teste de personalidade desenvolvido por Kogan pedia aos participantes a permissão para acessar o perfil do indivíduo no Facebook (como muitos aplicativos pedem). Todavia, o que não estava sendo exposto era que o aplicativo não só adquiria acesso ao perfil da pessoa fazendo o teste para coletar dados, mas também de todos os amigos na rede social do indivíduo, graças a uma falha na política de privacidade do Facebook que só foi percebida e corrigida em 2015. Com isso, a GSR adquiriou uma base de dados gigantesca de cerca de 87 milhões de pessoas (ISAAK; HANNA, 2018; RISSO, 2018; MANOKHA, 2018). Vale ressaltar, porém,

[49] *Openness, conscientiousness, extraversion, agreeableness,* e *neuroticism* (ISAAK; HANNA, 2018; RISSO, 2018).

que a GSR teve permissão de aproximadamente 270.000 pessoas apenas para coletar dados dos perfis no Facebook, demonstrando a escala que a falha na política de privacidade do Facebook permitiu (MANOKHA, 2018).

Ainda em 2014, um contrato sugere que uma afiliada da Cambridge Analytica teria contratado a GSR para coletar e processar os dados do Facebook (RISSO, 2018). Ao agregar os dados coletados pela GSR no Facebook com dados de outras fontes, a Cambridge Analytica afirmou que possuía mais de 5.000 *data points* em cerca de 230 milhões de adultos nos EUA (ISAAK; HANNA, 2018). Utilizando estes dados e a psicometria, a Cambridge Analytica desenvolveu a capacidade de mirar mensagens específicas em pessoas específicas com o objetivo de influenciar o seu comportamento em campanhas políticas, com os casos mais famosos – e os motivos do escândalo – sendo o referendum do Brexit e as eleições presidenciais americanas, ambos em 2016 (ISAAK; HANNA, 2018; RISSO, 2018). Esta técnica, chamada de *behavioral micro-targeting* ou de *political micro-targeting*, é utilizada estrategicamente para estimular apoio à uma campanha e participação política ou para desincentivar a participação política (por exemplo, mirar nos indecisos e, em vez de trazer eles para o seu candidato, fazer com que os indecisos não participem das eleições) (RISSO, 2018; BODÓ; HELBERGER; VREESE, 2017).

O caso da Cambridge Analytica, então, é importante para a Segunda Era Digital por também trazer a público algo que era apenas teorizado e discutido por grupos especializados. O escândalo representa a primeira vez que, através de uma invasão massiva de privacidade, dados foram coletados e empregados para manipular o comportamento das pessoas fora da esfera do mercado, afetando e alterando o jogo democrático. Embora a utilização de dados em uma campanha *data driven* já estava sendo explorado desde a campanha de reeleição do Barack Obama em 2012 (BENNET, 2016), ela não havia adquirido a escala vista no caso da Cambridge Analytica. Outro diferencial foi a combinação de técnicas de *micro-targeting* com a propaganda computacional, em específico a utilização de *bots* e humanos para manipular os algoritmos nas redes sociais de forma que a sua mensagem, além de ser direcionada, pareça muito maior do que ela realmente é, abrindo margem também para a disseminação em massa de informações falsas (RISSO, 2018). Assim, o caso da Cambridge Analytica representa um novo marco na utilização de dados para além da esfera econômica do marketing direcionado, potencialmente impactando decisivamente os resultados de eleições nos EUA, Reino Unido e outros lugares no mundo. Os dados, além de já existirem e serem coletados, estão também sendo utilizados para além de recomendações melhores e serviços aprimorados e personalizados.

3.3 DO PASSADO AO FUTURO: VIGILÂNCIA NA SEGUNDA ERA DIGITAL

Boa parte dos programas e ferramentas utilizados pela NSA e seus parceiros da aliança *Five Eyes* – EUA, Reino Unido, Canadá, Austrália, Nova Zelândia – podem ser enquadrados em duas dicotomias para agrupar os programas a partir da maneira pela qual os dados são coletados. A primeira dicotomia divide os métodos entre *Upstream* e *Downstream*. Uma coleta *upstream* envolve a obtenção dos dados a partir da intercepção deles diretamente nos cabos de fibra-ótica e demais infraestrutura de comunicações. Programas *upstream* incluem o Fairview, Stormbrew, Blarney, Oakstar e o Tempora . Por outro lado, programas *downstream* coletam os dados por via dos servidores, redes internas ou bases de dados das empresas privadas (BAUMAN et al., 2014; FAA702, 2013; TIMBERG, 2013; SANCHEZ, 2017; EFF, 201-?). É aqui que se encaixam os programas como PRISM e o Muscular.

A outra dicotomia se refere a forma de acesso aos dados ou infraestrutura de uma empresa privada. Este acesso pode ser dar via *front-door*, que envolve a empresa estar ciente do acesso, ou via *back-door*, pela qual a empresa não fica sabendo do acesso. Um acesso *front-door* não implica, necessariamente, no aceite da empresa, pois ele pode ocorrer forçadamente a partir de uma ordem judicial (secreta ou não), como no caso do PRISM. Programas *front-door* incluem o PRISM, Fairview, Stormbrew, Blarney e o Tempora, enquanto os de *back-door* incluem o Muscular, e qualquer outro que inclua a obtenção de dados sem o consentimento ou conhecimento do proprietário do sistema, servidor, infraestrutura, etc.

Bauman et al. (2014) traz outra divisão a partir da forma de coleta dos dados. O primeiro e segundo grupo de atividades apresentado pelos autores são bastante semelhantes à dicotomia *upstream* vs. *downstream*, com um grupo de atividades direcionadas para a coleta ou intercepção de dados na infraestrutura da internet e outro direcionado a obtenção de dados a partir da cooperação forçada das empresas privadas. O terceiro grupo de atividades se refere àqueles programas que coletam dados dos dispositivos, comunicações via satélite e linhas telefônicas tradicionais (BAUMAN et al., 2014). Da mesma maneira que as primeiras duas atividades delineadas pelos autores correspondem aproximadamente a programas *upstream* e *downstream*, este terceiro grupo de atividades de Bauman et al. (2014), que é bastante abrangente, pode ser destrinchado ter os programas enquadrados nas dicotomias apresentadas anteriormente.

Por fim, uma parte das revelações podem ser caracterizados como ferramentas para analisar dados e extrair informações coletadas pelos diversos programas da NSA e dos *Five Eyes* e armazenadas em base de dados. Entre estas ferramentas estão o XKeyscore e o ICReach.

Embora alguns dos programas da NSA e seus parceiros sejam anteriores à Segunda Era Digital, fica claro no documento "*A Strategy for Surveillance Powers*" (A STRATEGY, 2013) que eles estavam cientes das mudanças em trânsito desde 2012 e da necessidade de adaptar as capacidades deles para esta nova realidade. Trechos do documento apontam para: o reconhecimento do aumento das informações e seu potencial de identificação de indivíduos[50]; a necessidade de revolucionar a análise dos dados através da inteligência artificial[51], especificamente as redes neurais[52]; a utilização de um paradigma baseado na IoT[53] e; a adaptação de práticas comerciais de vigilância[54].

Com isso em mente, além dos pontos destacados explicitamente, é necessário olhar para as capacidades reveladas por Snowden pensando em como elas poderiam ser implementadas na Segunda Era Digital. Afinal, a Segunda Era Digital continua sendo uma evolução da Primeira. Em alguns casos, as potencialidades com o advento da Segunda Era Digital já são mais claros, como o Turbine e seu uso de inteligência artificial para escalar em níveis exponenciais a instalação de *malware*. Em outros, é preciso traçar os paralelos possíveis entre as novas tecnologias e os programas revelados. Programas que interceptam dados em trânsito na infraestrutura, por exemplo, podem ser facilitados por conta dos elementos de virtualização e de software presente na infraestrutura planejada para a 5G.

O aumento de dados produzidos e disponíveis na Segunda Era Digital, por via da IoT potencializada pela 5G e computação em nuvem, implica em um aumento de dados armazenados pelas empresas, que podem então ser obtidos por programas como o PRISM. A tendência para uma utilização cada vez maior de tecnologias em nuvem implica em uma maior concentração de dados nos servidores dos provedores de serviços em nuvem. Programas como o Muscular, então, coletariam mais informações ainda. A expansão da IoT, por sua vez, aumenta a quantidade de dispositivos disponíveis para invasão, tomada de controle e extração de dados

[50] "(U) Digital information created since 2006 grew tenfold, reaching 1.8 exabytes in 2011, a trend projected to continue; ubiquitous computing is fundamentally changing how people interact as individuals become untethered from information sources and their communications tools; and the traces individuals leave when they interact with the global network will define the capacity to locate, characterize and understand entities" (A STRATEGY, 2013, p. 2).
[51] "1. (U//FOUO) Revolutionize analysis – fundamentally shift our analytic approach from a production to a discovery bias, enriched by innovative customer/partner engagement, radically increasing operational impact across all mission domains. 1.1. (U//FOUO) Through advanced tradecraft and automation, dramatically increase mastery of the global network." (A STRATEGY, 2013, p. 4).
[52] "1.4. (U//FOUO) Drive an agile technology base mapped to the cognitive processes that underpin large scale analysis, discovery, compliance and collaboration" (A STRATEGY, 2013, p. 4).
[53] "3.2. (TS//SI//REL) Integrate the SIGINT system into a national network of sensors which interactively sense, respond, and alert one another at machine speed" (A STRATEGY, 2013, p. 4).
[54] "3.4. (S//SI/REL) Identify new access, collection, and exploitation methods by leveraging global business trends in data and communication services" (A STRATEGY, 2013, p. 4).

através de programas como o Turbine e outras capacidades reveladas. A Tabela abaixo oferece um quadro resumo dos principais programas dos quais é possível traçar um paralelo para com as tecnologias da Segunda Era Digital.

Tabela 1 - Quadro Resumo dos Programas de Vigilância dos *Five Eyes*

Nome do Programa	Agência responsável	*Upstream* ou *Downstream*?	*Frontdoor* ou *Backdoor*?	Efeito na 1a Era Digital	Potencial na 2a Era Digital
PRISM	NSA	*Downstream*	*Frontdoor*	Coleta de informações dos servidores de 9 grandes empresas de tecnologia	Maior incorporação de dados nos negócios das empresas = mais dados disponíveis através de programas como o PRISM
Tempora	GCHQ	*Upstream*	*Backdoor*	Interceptação de dados em trânsito na infraestrutura física (fibra ótica)	Intercepção potencialmente facilitada na infraestrutura de 5G por conta dos elementos de software e de virtualização
Muscular	NSA (com auxílio da GCHQ)	*Downstream*	*Backdoor*	Obtenção de dados através da infiltração das redes internas fechadas da Google e Yahoo	O aumento da importância e da utilização de nuvens concentra mais dados nos servidores e redes fechadas dos provedores de serviços em nuvem
Fairview, Blarney, Stormbrew	NSA	*Upstream*	*Frontdoor*	Interceptação de dados em trânsito na infraestrutura física de comunicações	Intercepção potencialmente facilitada na infraestrutura de 5G por conta dos elementos de software e de virtualização
Turbine + Turmoil	NSA (com auxílio da GCHQ)	-	*Backdoor*	Instalação automatizada (via IA) de malwares em dispositivos e redes, permitindo controle dos dispositivos e extração de informações	IoT aumenta números de dispositivos que podem ser infectados; infra da 5G com elementos de software pode ser infectada

Fonte: elaboração própria (2019).

Além destes programas, algumas capacidades e intenções de obtenção de dados foram reveladas por Snowden em 2013, dentre elas a busca por elaborar um banco de biometrias e de

imagens para reconhecimento facial (RISEN; POITRAS, 2014), a habilidade de pegar informações de aplicativos em *smartphones* (BALL, 2014b; GLANZ; LARSON; LEHREN, 2014) e a capacidade de invadir *smartphones* tanto via o sistema operacional, quanto via aplicativos específicos (ROSENBACH; POITRAS; STARK, 2013c). Quando levamos em consideração a personalização por parte das empresas e a incorporação de mecanismos de segurança em dispositivos como *smartphones* utilizando biometrias e reconhecimento facial, surge uma margem para construir uma relação de dados de biometria com diversos outros dados de um indivíduo. Embora isso possa parecer uma possibilidade remota, alguns desenvolvimentos na China nos trazem exemplos concretos da relação entre a Segunda Era Digital e a busca incessante por dados da vigilância.

A China têm investido fortemente numa política voltada para a Segunda Era Digital. Parte dessa estratégia envolve a cooperação entre o governo chinês e empresas privadas nacionais, as quais possuem um grande aparato de vigilância, e um foco na dataficação. A dataficação têm sido uma prioridade para a China desde o 18º Congresso do Partido Comunista Chinês e a administração de Xi Xinping, com o objetivo de fortalecer a nação e a economia e transformar a China em um poderoso ator na internet. Para isso, a China buscou incorporar as novas tecnologias da Segunda Era Digital, buscando aumentar o potencial de inovação da economia e a capacidade de governança do governo (VELGHE, 2019). A IoT, internet móvel (5G), *big data*, inteligência artificial e tecnologias em nuvem são explicitamente apontadas por atores governamentais e privados chineses como motores para o desenvolvimento digital chinês (VELGHE, 2019; LIU, 2019). Para entender o alcance e a escala que este processo já obteve, é preciso olhar para uma das maiores empresas de tecnologia da China e do mundo, a Tencent.

A Tencent é uma mega-corporação chinesa avaliada em 540 milhões de dólares em 2018 e possui: duas maiores redes sociais da China (WeChat e QQ), totalizando quase 2 bilhões de usuários; o maior grupo editorial de literatura online com mais de 50% do mercado; o maior aplicativo de notícias da China; o segundo maior motor de buscas (Sougou); os quatro maiores aplicativos de música na China; parte da DiDi, empresa que comprou as operações da Uber na China (e dona da 99 no Brasil); o maior aplicativo de tele-entrega de comida da China; participação no segundo maior e-commerce da China; a maior plataforma de propaganda digital do país e; uma das maiores financeiras virtuais da China, oferecendo serviços bancários, financeiros e de pagamento (LIU, 2019). Isto tudo é apenas na China, não leva em consideração as operações da Tencent no exterior.

Liu (2019) argumenta que este ecosistema gigantesco da Tencent – interconectado por um login único – consiste em uma infraestrutura comercial de vigilância. Ao oferecer

plataformas de geração e consumo de conteúdo, redes sociais e sistemas de pagamento, inúmeras conexões são possíveis a partir dos dados gerados dentro dos serviços da Tencent. Assim, os produtos e serviços da Tencent abordam todos os aspectos da vida de um indivíduo. Um indivíduo conversa no WeChat, vai trabalhar com um DiDi, ouve música em um dos quatro aplicativos de música da Tencent ao longo do trajeto, lê o jornal no Tencent News, encomenda o almoço e paga ele utilizando serviços todos da Tencent e com um único login (LIU, 2019). A quantidade de dados gerados – e coletados por uma única empresa – é gigantesca.

Um ponto importante dentro do ecosistema da Tencent é o sistema de pagamentos deles, que abrange todo tipo de operação financeira imaginável, desde compras pela internet até empréstimos e compras no mercado. A partir disso, torna-se possível rastrear cada gasto que um indivíduo faz com uma precisão jamais vista. Junta isso com o rastreamento de todas as outras atividades sob o argumento da personalização e os perfis dos indivíduos deixam de ter uma margem de erro. A combinação da gama de serviços e produtos, geração e consumo de conteúdo, redes sociais e sistema de pagamentos criam um ecosistema que permite acompanhar as atividades de um indivíduo tanto *online* quanto *offline* (LIU, 2019).

O alcance do ecosistema da Tencent e do WeChat, porém, não se restringe apenas para atividades no mercado. O login do WeChat pode ser utilizado para acessar, utilizar e pagar serviços municipais e, desde 2018, o governo chinês passou a emitir um "documento de identidade" do WeChat, o WeChat ID. O WeChat ID funciona como se fosse um documento de identidade físico emitido pelo governo chinês, o que implica na conexão do WeChat ID com os sistemas de segurança pública e de segurança nacional do governo. Na prática, o governo efetivamente possui acesso a todos os dados que fazem parte do ecosistema Tencent (LIU, 2019).

Outra frente pela qual o governo chinês, em parceria com algumas empresas privadas nacionais, têm atuado na vigilância na Segunda Era Digital é no desenvolvimento de sistemas de reconhecimento facial baseados em inteligência artificial e integrados a uma rede inteligente de câmeras CCTV espalhadas pelas ruas dos países (VELGHE, 2019; LIU, 2019). Ademais, a intenção é expandir a capacidade deste sistema de câmeras inteligentes para reconhecer não só rostos, mas também placas, modelos e cores de carros, além de cor de roupa e gênero de pessoas (LIU, 2019). Como o governo tem acesso *dossiers* detalhados dos indivíduos graças à cooperação com a Tencent, a integração entre esse sistema de câmeras inteligentes e os dados das pessoas se torna possível.

O que os países ocidentais do *Five Eyes* estão tentando fazer através de uma gama de programas secretos – coletar dados capazes de identificar, construir *dossiers* personalizados dos

indivíduos e acompanhá-los – a China faz através de uma cooperação aberta entre o Estado e grandes empresas do setor privado. Além disso, enquanto a *big tech* americana ainda está tentando extrair dados das atividades offline (como compras no supermercado), a *big tech* chinesa já está lá (LIU, 2019). O que é ainda muitas vezes futurista para as empresas de tecnologia ocidentais já é uma realidade na China. A cooperação aberta e explícita entre as empresas e o governo chinês – no que Liu (2019) chama de complexo estado-comercial de vigilância (*commercial-state surveillance complex*) – facilita a vigilância na escala desejada pelas agências de inteligência do *Five Eyes*.

É importante ressaltar, todavia, que embora esta monografia apresentou o complexo de vigilância da Tencent, existem empresas ocidentais que possuem ou estão buscando operacionalizar seus próprios complexos de vigilância. A Google, por exemplo, está investindo maciçamente em IoT e já possui grandes formas de coletar dados em massa através do seu próprio ecosistema que já possui grande parcela do mercado digital via Google Maps, Google Earth, Google Street View, Google AdWords, Google Assistant, Google Pay, G-Suite, Google Drive, Google Photos, Android, etc. (ZUBOFF, 2015). O que diferencia a Tencent da Google é o quão mais explícita a Tencent é nos seus objetivos na Segunda Era Digital e nas suas relações com o governo nacional (LIU, 2019; ZUBOFF, 2015). Embora seja argumentável que a Tencent está mais avançada no seu complexo de vigilância, a Google e as gigantes da tecnologia ocidentais (leia-se americanas do Vale do Silício) não estão muito atrás. Nas palavras de Lehr (2019), “[...] ainda não estamos lá [no nível de vigilância na China] no Ocidente, e ainda nos resta decidir se vamos chegar lá – ou, sendo mais realista, quando e sob quais condições e circunstâncias” (LEHR, 2019, p. 172).

4 CONCLUSÃO

A Primeira Era Digital viu a democratização do acesso à computação, o surgimento da Internet, o fenômeno da digitalização da informação e o início da dataficação (CANABARRO, 2014). Como um próximo passo, a Segunda Era Digital encontra no seu seio a expansão da dataficação para todos os aspectos da vida *online* e *offline* e um aumento da personalização da mesma. Para isso, cinco paradigmas e tecnologias emergentes se mostram centrais para a Segunda Era Digital: os paradigmas do *big data* e da *Internet of Things*, a inteligência artificial, as tecnologias em nuvem e a quinta geração de redes móveis (5G). O paradigma do *big data* se refere ao novo volume de dados sendo criados, coletados, armazenados e analisados por conta do aprofundamento da dataficação. Com esse novo paradigma de dados, uma cadeia valor de dados surge, na qual o valor está na extração de informações a partir da análise de dados diversos (LANGWORTHY, 2019). O paradigma da IoT, por sua vez, está relacionado a conexão de sensores e dispositivos diversos à internet, aumentando o alcance da coleta de dados para além dos nossos *smartphones* e computadores pessoais, permitindo não só objetos materiais inteligentes e conectados à internet, mas também a coleta de dados para além da navegação tradicional da internet (VELGHE, 2019; LEHR, 2019; LYON, 2018).

A inteligência artificial, por meio de avanços significativos utilizando técnicas de *deep learning* e arquiteturas de redes neurais inspiradas no cérebro humano, têm revolucionado a análise dos dados, ocupando um papel central na geração de valor a partir da extração de informações a partir dos dados coletados. As tecnologias em nuvem, por sua vez, compoem parte da infraestrutura da Segunda Era Digital. Graças às tecnologias em nuvem, armazenamento e poder computacional tendem a não serem mais problemas para os dispositivos, permitindo a utilização sob demanda destes recursos a um custo baixo. Além do mais, o armazenamento em nuvem busca acompanhar e suportar o volume crescente do *big data*, enquanto a computação em nuvem permite ampliar o acesso às capacidades computacionais necessárias para analisar os dados. Da mesma maneira que o *big data* estimula avanços nas tecnologias em nuvem, as tecnologias em nuvem podem acabar por limitar o aumento do *big data* caso o armazenamento em nuvem não acompanhe o volume crescente de dados.

A 5G, por fim, compõe também parte da infraestrutura da Segunda Era Digital. O objetivo da 5G é revolucionar a conectividade através do aumento da velocidade de transmissão de dados, diminuição do tempo de resposta e aumento do número de dispositivos conectados ao mesmo tempo em uma determinada área. Para atingir este objetivo, dois caminhos estão sendo seguidos: a evolução das redes 4G e a revolução das redes móveis através da pesquisa e

futura utilização de novas tecnologias como a virtualização de redes, entre outras. A 5G, atualmente, é um dos maiores desafios tecnológicos para a Segunda Era Digital, tendo em vista que ela não foi implementada ainda, os custos altos de implementação e as potenciais brechas na segurança por conta da virtualização (AHMAD et al., 2018; BRAKE, 2018).

Olhando para a cadeia de valor dos dados (Figura 1), conseguimos conectar as tecnologias e os atores às atividades contidas dentro dela. Na originação dos dados, temos os indivíduos interagindo com dispositivos conectados à internet – como *smartphones*, computadores pessoais e IoT – e gerando dados, que são coletados pelos mesmos dispositivos. O transporte e armazenamento dos dados, então, é feita pela infraestrutura vigente. Atualmente, além da infraestrutura física da internet composta por cabos de fibra ótica, a infraestrutura de redes móveis na escrita deste trabalho é a 4G. Esta infraestrutura, todavia, não é satisfatória para muitas das aplicações da Segunda Era Digital (LANGWORTHY, 2019; SKOURLETOPOULOS et al., 2017b), e por isso a 5G está sendo desenvolvida e implementada. O armazenamento, por sua vez, ocorre na nuvem.

A geração de valor ocorre na próxima etapa, a de extração e processamento dos dados. É aqui que a inteligência artificial e a computação em nuvem entram e possuem um papel essencial. Sem a capacidade de análise da inteligência artificial, seria impossível analisar um volume tão grande de dados e extrair informações deles. A última etapa, por fim, é a de consumo das informações extraídas na etapa de análise. Ela consiste no emprego pelos atores governamentais e privados das informações extraídas, seja para marketing direcionado, policiamento preventivo, identificação de ameaças à segurança nacional ou identificação de alvos para engenharia eleitoral. Todavia, é importante ressaltar que o envolvimento dos atores já começa na própria etapa de análise, uma vez que são eles que moldam a análise dos dados para as suas necessidades (LANGWORTHY, 2019; HANSEN; PORTER, 2017; SCHWARZ et al., 2019; ANDREJEVIC, 2015).

A última característica central da Segunda Era Digital, e que catalisa a maior ameaça à privacidade, é a personalização dos dados. A personalização dos dados cria um paradoxo na Segunda Era Digital: por um lado, ela é vista como necessária para melhorar serviços e produtos, otimizar as atividades e para o progresso sócio-econômico por via dela e da tecnologia (LIU, 2018); por outro lado, a personalização com tantos dados pessoais disponíveis possibilita uma vigilância generalizada na qual atores privados e governamentais buscam, através dos dados extremamente personalizados, identificar pessoas que se encaixem em um perfil e influenciá-las ou gerencia-las (LYON, 2014; LYON, 2015; LYON, 2018). Muito da coleta personalizada, entretanto, ocorre sem a ciência ou consentimento explícito dos indivíduos,

ferindo, assim, a privacidade dos usuários (LYON, 2014; ETZIONI, 2015). A personalização requer atividades de vigilância, e a vigilância cresce com a personalização.

Neste contexto, dois acontecimentos se destacam na Segunda Era Digital – as revelações de Edward Snowden em 2013 e o escândalo da Cambridge Analytica em 2016. As revelações de Snowden incluem uma série de atividades de vigilância exercidas pela NSA em conjunto com o Reino Unido, Canadá, Austrália e Nova Zelândia (os *Five Eyes*), dentre elas a interceptação, coleta, armazenamento e análise de dados e metadados de pessoas do mundo inteiro através da cooperação ou cooptação de empresas privadas, infiltração de redes privadas e adulteração da infraestrutura física de comunicações. A importância das revelações de Snowden para a Segunda Era Digital reside na afirmação de suspeitas e discussões antes restritas à especialistas e acadêmicos acerca da capacidade estatal de vigilância utilizando tecnologias. O que antes eram suposições e avisos se tornaram uma realidade pública, fato que também trouxe o debate para o público em geral. Embora possa ser argumentado que houve uma normalização da vigilância após o choque inicial das revelações (BAUMAN et al., 2014; DENCIK; CABLE, 2017), é possível afirmar que houve uma conscientização maior para além da comunidade especializada.

O caso da Cambridge Analytica, por sua vez, é importante por demonstrar como os dados podem ser utilizados para além do marketing direcionado. Até então, estavam relativamente claros a utilização dos dados para o marketing direcionado e para identificação de ameaças à segurança. O caso da Cambridge Analytica serviu não só para mostrar como é possível identificar as preferências e alinhamentos dos usuários a partir de dados, mas também como se pode utilizar os dados para manipular as pessoas e, consequentemente, alterar o jogo democrático. O principal ponto no escândalo da Cambridge Analytica, todavia, foi a revelação da quebra total de privacidade que pode ocorrer. O acesso consentido de milhares de pessoas abriu as portas para o acesso aos dados de milhões de pessoas, com a transferência de dados confiados à uma empresa (Facebook) para outras que os usuários nem sequer estavam cientes.

Verifica-se, então, que as novas tecnologias da Segunda Era Digital orbitam em torno do objetivo de coletar dados em massa, analisá-los para extrair informações extremamente personalizadas e utilizá-los para influenciar on manejar os indivíduos, visando lucros maiores, vitórias eleitorais ou a segurança nacional. É em busca da personalização maior e sem o conhecimento (e consentimento explícito) do usuário que as tecnologias da Segunda Era Digital afetam a privacidade dos usuários e a ameaça. Os atores não só adquirem uma quantia cada vez maior de dados, mas também empregam as informações extraídas destes dados. A vigilância na

Segunda Era Digital é ao mesmo tempo em massa na coleta e personalizada na utilização das informações extraídas.

Em relação às respostas dos governos nacionais ao fenômeno da Segunda Era Digital, verifica-se que eles jogam a favor da ameaça à privacidade e da utilização de práticas de vigilância, muitas vezes em cooperação com o setor privado. Por mais que esforços e legislações de proteção de dados tenham avançado – vide as legislações da União Europeia (*General Data Protection Regulation* - GDPR), do Brasil (Lei Geral de Proteção de Dados - LGPD) e do estado da California (*California Consumer Privacy Act* - CCPA) –, as revelações de Snowden foram acompanhadas também por um processo de legalização e normalização das práticas de vigilância estatal. No caso dos países ocidentais dos *Five Eyes* (e demais parceiros revelados por Snowden), algumas das práticas de vigilância foram normalizadas e legalizadas no âmbito nacional após as revelações de Snowden (TRÉGUER, 2017; POHLE; AUDENHOVE, 2017).

Por um lado, então, temos uma competição interestatal securitária e econômica em volta do desenvolvimento das novas tecnologias e suas aplicações. O viés securitário está relacionado à proteção das informações, redes de comunicações, dados dos países e, futuramente, sistemas ciber-físicos nessa transição para uma nova infraestrutura física – a 5G – e na proliferação da IoT (HASKA; BECKVARD; MINÁRIK, 2019; KEWALRAMANI; KANISETTI, 2019; RÜHLIG; SEAMAN; VOELSEN, 2019). Novas possibilidades surgem também na cibersegurança por conta dos avanços na inteligência artificial, trazendo mais uma tecnologia a ser contestada pelos países no âmbito securitário (JOHNSON, 2019; USA, 2016b; CHINA, 2017). Pelo viés econômico, a competição gira em torno da implementação das novas tecnologias da Segunda Era Digital para obter uma vantagem econômica, seja por ser o primeiro a romper a fronteira tecnológica atual e implementar modelos como a indústria 4.0 e cidades inteligentes; seja por possuir um monopólio temporário sobre as novas tecnologias (em especial a infraestrutura da 5G), sendo, assim, o único fornecedor enquanto os outros países não alcançarem o vanguardista (HASKA; BECKVARD; MINÁRIK, 2019; KEWALRAMANI; KANISETTI, 2019; RÜHLIG; SEAMAN; VOELSEN, 2019; CHINA, 2017).

No outro lado da moeda dos desafios políticos enfrentados na Segunda Era Digital, temos os desafios enfrentados pelos indivíduos da sociedade. Na competição entre os estados no sistema internacional, os indivíduos se tornam vítimas da vigilância exercida pelos governos (e empresas) nas empreitadas feitas para avançar suas posições na competição interestatal pelas tecnologias da Segunda Era Digital. São os dados das pessoas comuns que são interceptados, coletados, negociados e utilizados pelas agências de inteligência e pelas empresas para fins

securitários e econômicos. Embora os governos estejam interessados em proteger, até certo ponto, as informações e dados nacionais, a vigilância é mantida e expandida na Segunda Era Digital. É necessário observar se as medidas de proteção de dados sendo discutidas e implementadas nos níveis estaduais, nacionais e regionais serão suficientes para proteger a privacidade informacional dos indivíduos, e caso não sejam, como podemos proceder para efetivamente proteger a privacidade na Segunda Era Digital.

Para acompanhar os desenvolvimentos da Segunda Era Digital e seus impactos na privacidade e em demais temas que se relacionem com as Relações Internacionais para além do que foi analisado nesta monografia, torna-se importante, além das medidas de proteção de dados, analisar também as políticas e planos governamentais referentes à inteligência artificial. Outras agendas de pesquisa de interesse para a Segunda Era Digital incluem a corrida pela 5G, a implementação de cidades inteligentes, a utilização da personalização e das tecnologias da Segunda Era Digital para uma guerra de (des)informação e os impactos das novas tecnologias no âmbito securitário e na guerra em geral, abordando temas na intersecção da inteligência artificial com capacidades cibernéticas e com a robotização da guerra.

REFERÊNCIAS

AHMAD, Ijaz et al. Overview of 5G Security Challenges and Solutions. **Ieee Communications Standards Magazine**, [s.l.], v. 2, n. 1, p.36-43, mar. 2018. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/mcomstd.2018.1700063.

ALALI, Fatima A.; YEH, Chia-lun. Cloud Computing: Overview and Risk Analysis. **Journal Of Information Systems**, [s.l.], v. 26, n. 2, p.13-33, nov. 2012. American Accounting Association. http://dx.doi.org/10.2308/isys-50229.

ANDREJEVIC, Mark. Foreword. In: DUBROFSKY, Rachel E.; MAGNET, Shoshana Amielle. **FEMINIST SURVEILLANCE STUDIES.** Londres: Duke University Press, 2015. p. ix - xviii

BALL, James; HARDING, Luke; GARSIDE, Juliette. BT and Vodafone among telecoms companies passing details to GCHQ. **The Guardian**, Londres, 2 de ago. de 2013. Disponível em: < https://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq >. Acesso em: 30 de out. de 2019.

BALL, James. US and UK struck secret deal to allow NSA to ‘unmask’ Britons’ personal data. **The Guardian**, Londres, 20 de nov. 2013. Disponível em: <https://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data>. Acesso em : Acesso em: 30 de out. de 2019.

BALL, James. NSA collects millions of text messages daily in 'untargeted' global sweep. **The Guardian**, Londres, 16 de jan. 2014a. Disponível em: <https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep>. Acesso em: 30 de out. de 2019.

BALL, James. Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data. The Guardian, Londres, 28 de jan. 2014b. Disponível em: <https://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data>. Acesso em: 30 de out. de 2019.

BAUMAN, Zygmunt et al. After Snowden: Rethinking the Impact of Surveillance. **International Political Sociology**, [s.l.], v. 8, n. 2, p.121-144, 29 maio 2014. Oxford University Press (OUP). http://dx.doi.org/10.1111/ips.12048.

BELLMAN, Barton; SOLTANI, Ashkan. NSA tracking cellphone locations worldwide, Snowden documents show. **The Washington Post**, Washington, 04 de dez. de 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: 30 de out. de 2019.

BEHAR, Rose. Millimeter wave to low-band: The different types of 5G and how they work. **Digital Trends**, [s.l.], 6 de janeiro de 2019. Disponível em: <https://www.digitaltrends.com/mobile/5g-spectrum-variants/>. Acesso em: 21 out. 2019.

BENNETT, Colin J.. Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?. **International Data Privacy Law**,

[s.l.], v. 6, n. 4, p.261-275, nov. 2016. Oxford University Press (OUP). http://dx.doi.org/10.1093/idpl/ipw021.

BERGHEL, Hal. Malice Domestic: The Cambridge Analytica Dystopia. **Computer**, [s.l.], v. 51, n. 5, p.84-89, maio 2018. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/mc.2018.2381135.

BODÓ, Balázs; HELBERGER, Natali; VREESE, Claes H. de. Political micro-targeting: a Manchurian candidate or just a dark horse?. **Internet Policy Review**: Journal on internet regulation, [s. L.], v. 6, n. 4, p.1-13, dez. 2017. Disponível em: <http://policyreview.info/articles/analysis/political-micro-targeting-manchurian-candidate-or-just-darkhorse>. Acesso em: 22 out. 2019.

BRAKE, Doug. Economic Competitiveness and National Security Dynamics in the Race for 5G between the United States and China. **Ssrn Electronic Journal**, [s.l.], p.1-30, 2018. Elsevier BV. http://dx.doi.org/10.2139/ssrn.3142229.

BUTTERFIELD, Andrew et al. **Oxford Dictionary of Computer Science.** 7. ed. Nova Iorque: Oxford University Press, 2016.

CANABARRO, Diego Rafael. **Governança Global da Internet:** Tecnologia, Poder e Desenvolvimento. 2014. 2 v. Tese (Doutorado) - Curso de Ciência Política, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014.

CASTROUNIS, Alex. **AI for People and Business:** A Framework for Better Human Experiences and Business Success. Sebastopol: O'reilly, 2019. 316 p.

CERF, Vinton G.; DRAKE, William J.; KLEINWÄCHTE, Wolfgang. Internet Fragmentation: An Overview. Genebra: World Economic Forum, 2016. 80 p. Disponível em: <http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf >. Acesso em: 15 de out. de 2019.

CHANDLER, David. A World without Causation: Big Data and the Coming of Age of Posthumanism. **Millennium**: Journal of International Studies, [s.l.], v. 43, n. 3, p.833-851, 27 maio 2015. SAGE Publications. http://dx.doi.org/10.1177/0305829815576817.

CHEN, Shan-zhi; KANG, Shao-li. A tutorial on 5G and the progress in China. **Frontiers Of Information Technology & Electronic Engineering**, [s.l.], v. 19, n. 3, p.309-321, mar. 2018. Zhejiang University Press. http://dx.doi.org/10.1631/fitee.1800070.

CHINA. **A Next Generation Artificial Intelligence Development Plan**. Tradução de Rogier Creemers, Graham Webster, Paul Triolo, Elsa Kania. New America. 2017.

COHEN, David B.; WELLS, John W.. **American National Security And Civil Liberties In An Era Of Terrorism.** Nova Iorque: Palgrave Macmillan, 2004.

CRAWFORD, Kate; MILTNER, Kate; GRAY, Mary L.. Critiquing Big Data: Politics, Ethics, Epistemology. **International Journal Of Communication.** [s. L.], p. 1663-1672. 2014.

DENARDIS, Laura. One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation. Global Commission On Internet Governance Paper Series. Londres, p. 1-12. jul. 2016. Disponível em:

<https://www.cigionline.org/sites/default/files/gcig_no.38_web.pdf>. Acesso em: 02 abr. 2019.

DENCIK, Lina; CABLE, Jonathan. The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks. **International Journal Of Communication.** Los Angeles, p. 763-781. 2017.

DOLCOURT, Jessica. **We ran 5G speed tests on Verizon, AT&T, EE and more: Here's what we found.** 2019. Disponível em: <https://www.cnet.com/features/we-ran-5g-speed-tests-on-verizon-at-t-ee-and-more-heres-what-we-found/>. Acesso em: 21 out. 2019.

DONGES, Niklas. **The Non-Technical AI Guide**. Disponível em: https://towardsdatascience.com/the-non-technical-guide-to-artificial-intelligence-e9e5da1a15c5. Acesso em: 14 de outubro de 2019

DORLING, Philip. Snowden reveals Australia's links to US spy web. **The Sydney Morning Herald**, Sydney, 8 de jul. de 2013a. Disponível em:< https://www.smh.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html>. Acesso em: 30 de outubro de 2019.

DORLING, Philip. Australian spies in global deal to tap undersea cables. **The Sydney Morning Herald**, Sydney, 29 de ago. de 2013b. Disponível em:< https://www.smh.com.au/technology/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58.html>. Acesso em: 30 de outubro de 2019.

DUBROFSKY, Rachel E.; MAGNET, Shoshana Amielle. Feminist Surveillance Studies: Critical Interventions. In: DUBROFSKY, Rachel E.; MAGNET, Shoshana Amielle. **FEMINIST SURVEILLANCE STUDIES.** Londres: Duke University Press, 2015. p. 1-27

ELECTRONIC FRONTIER FOUNDATION (EFF). **Upstream vs. PRISM.** 201-?. Disponível em: <https://www.eff.org/pages/upstream-prism>. Acesso em: 1 nov. 2019.

ETZIONI, Amitai. **Privacy in a Cyber Age:** Policy and Practice. Nova Iorque: Palgrave Macmillan, 2015.

ESPOSITO, R.; COLE, M.; SHONE, M.; GREENWALD, G. Snowden docs reveal British spies snooped on YouTube and Facebook. **NBC News**, Nova Iorque, 27 de jan. de 2014.Disponível em: <http://investigations.nbcnews.com/_news/2014/01/27/22469304-snowden-docs-reveal-british-spies-snooped-on-youtube-and-facebook?lite>. Acesso em: 30 de out. de 2019.

FAA702 Operations: Two Types of Collection. **The Guardian**, Londres, 9 de jun. de 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google>. Acesso em: 30 de outubro de 2019.

Federal Communications Commission (FCC). **The FCC's 5G FAST Plan.** FCC, 2018. Disponível em:<https://docs.fcc.gov/public/attachments/DOC-354326A1.pdf>. Acesso em 10 de out. de 2019.

FRENCH, Aaron M.; SHIM, J. P.. The Digital Revolution: Internet of Things, 5G and Beyond. **Communications Of The Association For Information Systems**, [s.l.], v. 38, n. 40, p.840-850, 2016. Association for Information Systems. http://dx.doi.org/10.17705/1cais.03840.

GALLAGHER, Ryan; GREENWALD, Glenn. How the NSA Plans to Infect 'Millions' of Computers with Malware. **The Intercept**, Estados Unidos, 12 de mar. de 2014. Disponível em: <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/>. Acesso em: 30 de out. de 2019.

GALLAGHER, Ryan. How Secret Partners Expand NSA's Surveillance Dragnet. **The Intercept**, Estados Unidos, 18 de jun. de 2014a. Disponível em: <https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/>. Acesso em: 30 de out. de 2019.

GALLAGHER, Ryan. How the NSA Built Its Own Secret Google. **The Intercept**, Estados Unidos, 25 de ago. de 2014b. Disponível em: <https://theintercept.com/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/>. Acesso em: 30 de out. de 2019

GARSIDE, Juliette. Vodafone reveals existence of secret wires that allow state surveillance. **The Guardian**, Londres, 6 de jun. de 2014. Disponível em: <https://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance>. Acesso em: 30 de out. de 2019.

GELLMAN, Barton; POITRAS, Laura. U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. **The Washington Post**, Washington, 7 de jun. de 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: 30 de outubro de 2019.

GELLMAN, Barton; SOLTANI, Ashkan. NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. **The Washington Post**, Washington, 30 de out. de 2013. Disponível em: < https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html>. Acesso em: 30 de outubro de 2019.

GELLMAN, Barton; SOLTANI, Ashkan. NSA surveillance program reaches 'into the past' to retrieve, replay phone calls. **The Washington Post**, Washington, 18 de mar. de 2014. Disponível em: <https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html>. Acesso em: 30 de out. de 2019.

GERMAN Intelligence Used NSA Spy Program. **Spiegel Online**, Nova Iorque, 20 de jul. de 2013. Disponível em: < https://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html>. Acesso em: 30 de outubro de 2019.

GLANZ, James; LARSON, Jeff; LEHREN, Andrew. Spy Agencies Tap Data Streaming From Phone Apps. **The New York Times**, Nova Iorque, 27 de jan. de 2014. Disponível em: <https://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html>. Acesso em: 30 de out. de 2019.

GREENWALD, Glenn. NSA collecting phone records of millions of Verizon customers daily. **The Guardian**, Londres, 6 de jun. de 2013a. Disponível em: <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>. Acesso em: 30 de out. de 2019.

GREENWALD, Glenn. NSA Prism program taps in to user data of Apple, Google and others. **The Guardian**, Londres, 7 de jun. de 2013b. Disponível em: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em: 30 de out. de 2019.

GREENWALD, Glenn. The NSA's mass and indiscriminate spying on Brazilians. **The Guardian**, Londres, 7 de jul. de 2013c. Disponível em: < https://www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying>. Acesso em: 30 de out. de 2019.

GREENWALD, Glenn. XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. **The Guardian**, Londres, 31 de jul. de 2013d. Disponível em: < https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>. Acesso em: 30 de out. de 2019.

GREENWALD, Glenn; MACASKILL, Ewin. Boundless Informant: the NSA's secret tool to track global surveillance data. **The Guardian**, Londres, 11 de jun. de 2013. Disponível em: < https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining >. Acesso em: 30 de out. de 2019.

GREENWALD, Glenn; KAZ, Roberto; CASADO, José. EUA espionaram milhões de e-mails e ligações de brasileiros. **O Globo**, Rio de Janeiro, 7 de jul. de 2013. Disponível em: < https://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934 >. Acesso em 30 de out. de 2013.

GUDE, Hubert; POITRAS, Laura; ROSENBACH, Marcel. Transfers from Germany Aid US Surveillance. **Spiegel Online**, Nova Iorque, 5 de ago. de 2013. Disponível em: < https://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html>. Acesso em: 30 de out. de 2019.

GREENWALD, Glenn; POITRAS, Laura; MACASKILL, Ewen. NSA shares raw intelligence including Americans' data with Israel. **The Guardian**, Londres, 11 de set. de 2013. Disponível em: < https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents>. Acesso em: 30 de out. de 2019.

HABEGGER, Benjamin et al. Personalization vs. Privacy in Big Data Analysis. **International Journal Of Big Data.** [s. L.], p. 25-35. 2014.

HAGGERTY, Kevin D.; ERICSON, Richard V.. **The New Politics of Surveillance and Visibility.** Toronto: University Of Toronto Press, 2006.

HALVORSEN, A.; BLINDHEIM, A.; KLUNGTVEIT, H.; et al. Norway´s secret surveillance of Russian politics for the NSA. **Dabladet**, Noruega, 17 de dez. de 2013. Disponível em: <https://www.dagbladet.no/nyheter/norways-secret-surveillance-of-russian-politics-for-the-nsa/61923431>. Acesso em: 30 de out. de 2019.

HAMILOS, Paul. Spain colluded in NSA spying on its citizens, Spanish newspaper reports. **The Guardian**, Madrid, 30 de out. de 2013. Disponível em: < https://www.theguardian.com/world/2013/oct/30/spain-colluded-nsa-spying-citizens-spanish-el-mundo-us>. Acesso em: 30 de out. de 2019

HANSEN, Hans Krause; PORTER, Tony. What Do Big Data Do in Global Governance? **Global Governance**: A Review of Multilateralism and International Organizations, [s.l.], v. 23, n. 1, p.31-42, 19 ago. 2017. Brill. http://dx.doi.org/10.1163/19426720-02301004.

KASKA, Kadri; BECKVARD, Henrik; MINÁRIK, Tomáš. **Huawei, 5G and China as a Security Threat.** Tallin: Ccdcoe, 2019.

HELBING, Dirk et al. **Will Democracy Survive Big Data and Artificial Intelligence?** 2017. Disponível em: <https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/>. Acesso em: 22 out. 2019.

HILL, Jonah Force. **Internet Fragmentation**: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers. Cambridge, Ma: Harvard University, 2012.

IEEE. **IEEE Standard for Prefixes for Binary Multiples.** Nova Iorque, NY: Ieee, 2009.

IRIONDO, Roberto. **Machine Learning vs. AI, Important Differences Between Them**. Disponível em: https://medium.com/datadriveninvestor/differences-between-ai-and-machine-learning-and-why-it-matters-1255b182fc6. Acesso em: 14 de out. de 2018

ISAAK, Jim; HANNA, Mina J.. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. **Computer**, [s.l.], v. 51, n. 8, p.56-59, ago. 2018. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/mc.2018.3191268.

JOHNSON, James. Artificial intelligence & future warfare: implications for international security. **Defense & Security Analysis**, [s.l.], v. 35, n. 2, p.147-169, 3 abr. 2019. Informa UK Limited. http://dx.doi.org/10.1080/14751798.2019.1600800.

KAZ, Roberto; CASADO, José. NSA e CIA mantiveram em Brasília equipe para coleta de dados filtrados de satélite. **O Globo**, Rio de Janeiro, 8 de jul. de 2013. Disponível em: <https://oglobo.globo.com/mundo/nsa-cia-mantiveram-em-brasilia-equipe-para-coleta-de-dados-filtrados-de-satelite-8949723&sa=D&ust=1572907587761000&usg=AFQjCNGMCxHOb1YsJv_CLTFyvWaXwqfoNA >. Acesso em 30 de out. de 2013.

KERR, Ian; EARLE, Jessica. Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy. **Stanford Law Review Online**, [s. L.], v. 66, n. 65, p.65-72, set. 2013.

KEWALRAMANI, Manoj; KANISETTI, Anirudh. 5G, Huawei & Geopolitics: An Indian Roadmap. **Ssrn Electronic Journal**, [s.l.], p.1-32, jun. 2019. Elsevier BV. http://dx.doi.org/10.2139/ssrn.3414860.

KITCHIN, Rob; DODGE, Martin. The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. **Journal Of Urban Technology**, [s.l.], v. 26, n. 2, p.47-65, 12 dez. 2017. Informa UK Limited. http://dx.doi.org/10.1080/10630732.2017.1408002.

KUMAR, Sanjay; GUPTA, Gagan; SINGH, Kunwar Rajat. 5G: Revolution of future communication technology. **2015 International Conference On Green Computing And Internet Of Things (icgciot)**, [s.l.], p.143-147, out. 2015. IEEE. http://dx.doi.org/10.1109/icgciot.2015.7380446.

LAM, Lana. US hacked Pacnet, Asia Pacific fibre-optic network operator, in 2009. **South China Morning Post**, Hong, Kong, 22 de jun. de 2013a. Disponível em: <

https://www.scmp.com/news/hong-kong/article/1266875/exclusive-us-hacked-pacnet-asia-pacific-fibre-optic-network-operator>. Acesso em: 30 de out. de 2019.

LAM, Lana. NSA targeted China's Tsinghua University in extensive hacking attacks, says Snowden. **South China Morning Post**, Hong, Kong, 22 de jun. de 2013b. Disponível em: < https://www.scmp.com/news/china/article/1266892/exclusive-nsa-targeted-chinas-tsinghua-university-extensive-hacking>. Acesso em: 30 de out. de 2019.

LAM, Lana; CHEN, Stephen. US spies on Chinese mobile phone companies, steals SMS data: Edward Snowden. **South China Morning Post**, Hong, Kong, 22 de jun. de 2013. Disponível em: < https://www.scmp.com/news/china/article/1266821/us-hacks-chinese-mobile-phone-companies-steals-sms-data-edward-snowden>. Acesso em: 30 de out. de 2019.

LANGWORTHY, Stacy. **Power Dynamics in an Era of Big Data.** [s. l.]: Lse Ideas, 2019. 17 p.

LECUN, Yann; BENGIO, Yoshua; HINTON, Geoffrey. Deep learning. **Nature**, [s.l.], v. 521, n. 7553, p.436-444, maio 2015. Springer Science and Business Media LLC. http://dx.doi.org/10.1038/nature14539.

LEE, Edward A.. **Cyber Physical Systems:** Cyber Physical Systems: Design Challenges. Berkeley: Eecs Department, University Of California, 2008.

LEE, Nicol Turner. **Enabling opportunities:** 5G, the internet of things, and communities of color. 2019. Disponível em: <https://www.brookings.edu/research/enabling-opportunities-5g-the-internet-of-things-and-communities-of-color/>. Acesso em: 10 ago. 2019.

LEE, Jay H.; SHIN, Joohyun; REALFF, Matthew J.. Machine learning: Overview of the recent progresses and implications for the process systems engineering field. **Computers & Chemical Engineering**, [s.l.], v. 114, p.111-121, jun. 2018. Elsevier BV. http://dx.doi.org/10.1016/j.compchemeng.2017.10.008

LEHR, Peter. **Counter-Terrorism Technologies:** A Critical Assessment. [s.l.]: Springer, 2019.

LEWIS, James A.. **How Will 5G Shape Innovation and Security:** A Primer. Washington, D.c: Csis, 2018.

LI, Shancang; XU, Li da; ZHAO, Shanshan. 5G Internet of Things: A survey. **Journal Of Industrial Information Integration**, [s.l.], v. 10, p.1-9, jun. 2018. Elsevier BV. http://dx.doi.org/10.1016/j.jii.2018.01.005.

LIU, Kevin Ziyu. Commercial-State Empire: A Political Economy Perspective on Social Surveillance in Contemporary China. **The Political Economy Of Communication.** [s.l.], p. 3-29. 2019.

LYON, David. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. **Big Data & Society**, [s.l.], v. 1, n. 2, p.1-13, 9 jul. 2014. SAGE Publications. http://dx.doi.org/10.1177/2053951714541861.

LYON, David. The Snowden Stakes: Challenges for Understanding Surveillance Today. **Surveillance & Society.** [s. L.], p. 139-152. jul. 2015.

LYON, David. **The Culture of Surveillance:** Watching as a Way of Life. Cambridge: Polity, 2018.

MACASKILL, Ewen. NSA paid millions to cover Prism compliance costs for tech companies. **The Guardian**, Londres, 23 de ago. de 2013. Disponível em: < https://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid>. Acesso em: 30 de out. de 2019.

MACASKILL, Ewen; BORGER, Julian. New NSA leaks show how US is bugging its European allies. **The Guardian**, Londres, 30 de jun. de 2013b. Disponível em: < https://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies>. Acesso em: 30 de out. de 2019.

MACASKILL, Ewen; BORGER, Julian; HOPKINS, Nick; DAVIES, Nick; BALL, James. GCHQ taps fibre-optic cables for secret access to world's communications. **The Guardian**, Londres, 21 de jun. de 2013. Disponível em: < https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>. Acesso em: 30 de out. de 2019.

MACASKILL, Ewen; BALL, James; MURPHY, Katharine. Revealed: Australian spy agency offered to share data about ordinary citizens. **The Guardian**, Londres, 02 de dez. de 2013. Disponível em: <https://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens>. Acesso em: 30 de out. de 2019.

MANOKHA, Ivan. Surveillance: The DNA of Platform Capital—The Case of Cambridge Analytica Put into Perspective. **Theory & Event**, [s.l.], v. 21, n. 4, p.891-913, out. 2018.

MARX, Gary T.. Surveillance Studies. **International Encyclopedia Of The Social & Behavioral Sciences**, [s.l.], p.733-741, 2015. Elsevier. http://dx.doi.org/10.1016/b978-0-08-097086-8.64025-4.

MELL, Peter; GRANCE, Timothy. **The NIST Definition of Cloud Computing:** Recommendations of the National Institute of Standards and Technology. Gaithersburg: Nist - National Institute Of Standards And Technology, 2011.

MIAILHE, Nicolas; HODES, Cyrus. The Third Age of Artificial Intelligence. **Field Actions Science Reports: The journal of field actions.** [s. L.], p. 6-11. dez. 2017.

MUELLER, Milton. **Ruling the Root**: Internet Governance and the Taming of Cyberspace. Cambridge, MA: MIT Press, 2002.

N'GUYEN, Godefroy Dang. Companies: The Great Transformation. In: CHAMOUX, Jean-pierre. **The Digital Era 2:** Political Economy Revisited. Londres: Iste e John Wiley & Sons, 2019. p. 7-22

NAKASHIMA, Ellen; DEYOUNG, Karen. NSA chief said NATO allies shared phone records with U.S. spy agency. **The Washington Post**, Washington, 30 de out. de 2013. Disponível em: <https://www.washingtonpost.com/world/national-security/top-intelligence-officials-called-to-testify-on-nsa-surveillance-programs/2013/10/29/e9e9c250-40b7-11e3-a751-f032898f2dbc_story.html>. Acesso em: 30 de outubro de 2019.

NEAPOLITAN, Richard E.; JIANG, Xia. **Artificial Intelligence:** With an Introduction to Machine Learning. 2. ed. Boca Raton: Taylor & Francis Group, 2018. 457 p.

NEGNEVITSKY, Michael. **Artificial Intelligence:** A Guide to Intelligent Systems. 2. ed. Harlow: Pearson Education, 2005.

NSA SLIDES explain the PRISM data-collection program. **The Washington Post**, Washington, 6 de jun. de 2013. Disponível em: < https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>. Acesso em: 30 de outubro de 2019.

NSA SPIES on International Payments. **Spiegel Online**, Nova Iorque, 15 de set. de 2013. Disponível em: < https://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html>. Acesso em: 30 de outubro de 2019.

PAPADOKOSTAKI, Koralia et al.. Handling Big Data in the Era of Internet of Things (IoT). In: MAVROMOUSTAKIS, Constandinos X.; MASTORAKIS, George; DOBRE, Ciprian. **Advances in Mobile Cloud Computing and Big Data in the 5G Era.** [s.l.]: Springer, 2017

PANT, Harsh V.; TIRKEY, Aarshi. **Emerging technologies and geopolitical contestation.** 2019. Disponível em: <https://www.orfonline.org/expert-speak/emerging-technologies-and-geopolitical-contestation-50562/>. Acesso em: 10 ago. 2019.

PAUL, Dipam. An analysis of the evolution of 5G communication system with regards to development of World Wide Wireless Web (WWWW), Dynamic Ad hoc Wireless Networks (DAWN) and Real Wireless World. **American Journal Of Engineering Research (ajer).** [s. L.], p. 247-252. jul. 2018.

PETROBRAS foi espionada pelos EUA, apontam documentos da NSA. **O Globo**, Rio de Janeiro, 8 de set. de 2013. Disponível em: < http://g1.globo.com/fantastico/noticia/2013/09/petrobras-foi-espionada-pelos-eua-apontam-documentos-da-nsa.html >. Acesso em 30 de out. de 2013.

PFISTER Reneé; POITRAS, Laura; ROSENBACH, Marcel; SCHINDLER, Jorg; STARK, Holger. Secret Links Between Germany and the NSA. **Spiegel Online**, Nova Iorque, 22 de jul. de 2013. Disponível em: < https://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355-2.html>. Acesso em: 30 de out. de 2019.

POHLE, Julia; VAN AUDENHOVE, Leo. Post-Snowden Internet Policy: Between Public Outrage, Resistance and Policy Change. **Media And Communication**, [s.l.], v. 5, n. 1, p.1-6, 22 mar. 2017. Cogitatio. http://dx.doi.org/10.17645/mac.v5i1.932.

POITRAS, Laura; ROSENBACH, Marcel; STARK, Holger. How America Spies on Europe and the UN. **Spiegel Online**, Nova Iorque, 26 de ago. de 2013a. Disponível em: < https://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html>. Acesso em: 30 de out. de 2019.

POITRAS, Laura; ROSENBACH, Marcel; STARK, Holger. NSA Snoops on 500 Million German Data Connections. **Spiegel Online**, Nova Iorque, 30 de jun. de 2013b. Disponível em: < https://www.spiegel.de/international/germany/nsa-spies-on-500-million-german-data-connections-a-908648.html>. Acesso em: 30 de out. de 2019.

RAO, Sriganesh K.; PRASAD, Ramjee. Impact of 5G Technologies on Industry 4.0. **Wireless Personal Communications**, [s.l.], v. 100, n. 1, p.145-159, 13 mar. 2018. Springer Nature. http://dx.doi.org/10.1007/s11277-018-5615-7.

RISEN, James; POITRAS, Laura. N.S.A. Report Outlined Goals for More Power. **The New York Times**, Washington, 22 de nov. de 2013. Disponível em: < https://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html>. Acesso em: 30 de out. de 2019.

RISEN, James; POITRAS, Laura. N.S.A. Collecting Millions of Faces From Web Images. The New York Times, Nova Iorque, 32 de mai. de 2014. Disponível em: <https://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html>. Acesso em: 30 de out. de 2019.

RISSO, Linda. Harvesting Your Soul? Cambridge Analytica and Brexit. In: BREXIT MEANS BREXIT?, 1., 2017, Mainz. **The Selected Proceedings of the Symposium.** Mainz: Akademie Der Wissenschaften Und Der Literatur, 2018. p. 75 - 87.

ROMERO, Simon; ARCHIBOLD, Randal. Brazil Angered Over Report N.S.A. Spied on President. **The New York Times**, Rio de Janeiro, 2 de set. de 2013. Disponível em: < https://www.nytimes.com/2013/09/03/world/americas/brazil-angered-over-report-nsa-spied-on-president.html?_r=0>. Acesso em: 30 de out. de 2019.

ROSENBACH, Marcel; POITRAS, Laura; STARK, Holger. How the NSA Accesses Smartphone Data. **Spiegel Online**, Nova Iorque, 9 de set. de 2013. Disponível em: < https://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html >. Acesso em: 30 de out. de 2019.

SÆTNAN, Ann Rudinow; SCHNEIDER, Ingrid; GREEN, Nicola. **The Politics and Policies of Big Data:** Big Data, Big Brother?. [s. L.]: Routledge, 2019.

RÜHLIG, Tim; SEAMAN, John; VOELSEN, Daniel. 5G and the US-China tech rivalry - a test for Europe's future in the digital age: how can Europe shift back from back foot to front foot?. **Swp Comment**, Berlin, v. 29, n. 1, p.1-9, jun. 2019.

RUSSEL, Stuart J.; NORVIG, Peter. **Artificial Intelligence:** A Modern Approach. 3. ed. Harlow: Pearson Education, 2016.

SANCHEZ, Julian. All About "About" Collection. **Just Security**. 29 de abr. de 2017. Disponível em: <https://www.justsecurity.org/40384/ado-about/>. Acesso em: 1 de novembro de 2019.

SEGAL, Adam. **The Hacked World Order:** How Nations Fight, Trade, Maneuver, And Manipulate in the Digital Age. Nova Iorque: Publicaffairs, 2016.

SCHWARZ, Elke et al. **Datafying the Globe: Critical Insights into the Global Politics of Big Data Governance**. Disponível em: http://bigdatasoc.blogspot.com/p/essays-and-provocations.html. Acesso em: 10 de agosto de 2019.

SCHMIDHUBER, Jürgen. Deep learning in neural networks: An overview. **Neural Networks**, [s.l.], v. 61, p.85-117, jan. 2015. Elsevier BV. http://dx.doi.org/10.1016/j.neunet.2014.09.003.

SIMO, Hervais. Big Data: Opportunities and Privacy Challenges. **Privatheit, Öffentlichkeit Und Demokratische Willensbildung In Zeiten von Big Data**, [s.l.], p.13-44, 2015. Nomos. http://dx.doi.org/10.5771/9783845264165-13.

SIMPSON, Peter Vinthagen. Cold War treaty confirms Sweden was not neutral. **The Local SE**, Suíça, 09 de dez. de 2013. Disponível em: <https://www.thelocal.se/20131209/secret-cold-war-treaty-confirms-sweden-was-never-neutral>. Acesso em: 30 de out. de 2019.

SKOURLETOPOULOS, Georgios et al.. Big Data and Cloud Computing: A Survey of the State-of-the-Art and Research Challenges. In: MAVROMOUSTAKIS, Constandinos X.; MASTORAKIS, George; DOBRE, Ciprian. **Advances in Mobile Cloud Computing and Big Data in the 5G Era.** [s.l.]: Springer, 2017a.

SKOURLETOPOULOS, Georgios et al.. Towards Mobile Cloud Computing in 5G Mobile Networks: Applications, Big Data Services and Future Opportunities. In: MAVROMOUSTAKIS, Constandinos X.; MASTORAKIS, George; DOBRE, Ciprian. **Advances in Mobile Cloud Computing and Big Data in the 5G Era.** [s.l.]: Springer, 2017b.

SOLTANI, A.; PETERSON, A.; BELLMAN, B. NSA uses Google cookies to pinpoint targets for hacking. **The Washington Post**, Washington, 10 de dez. de 2013. Disponível em: <https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/?arc404=true>. Acesso em: 30 de out. de 2019.

SOLTANI, Ashkan; DELONG, Matt. FASCIA: The NSA's huge trove of location records. **The Washington Post**, Washington, 04 de dez. de 2013. Dispnível em: <http://apps.washingtonpost.com/g/page/world/what-is-fascia/637/>. Acesso em: 30 de out. de 2019.

A STRATEGY for Surveillance Powers. **The New York Times**, Washington, 23 de nov. de 2013. Disponível em: < https://archive.nytimes.com/www.nytimes.com/interactive/2013/11/23/us/politics/23nsa-sigint-strategy-document.html>. Acesso em: 30 de out. de 2019.

SUNSTEIN, Cass R.. Nudging: A Very Short Guide. **Journal Of Consumer Policy**, [s.l.], v. 37, n. 4, p.583-588, 16 out. 2014. Springer Science and Business Media LLC. http://dx.doi.org/10.1007/s10603-014-9273-1.

SWIDER, Matt. **5G speed test:** 1.4Gbps in Chicago, but only if you do the '5G shuffle'. 2019. Disponível em: <https://www.techradar.com/news/5g-speed-test>. Acesso em: 21 out. 2019.

TIMBERG, Craig; GELLMAN, Barton. U.S., NSA paying U.S. companies for access to communications networks. **The Washington Post**, Washington, 29 de ago. de 2013. Disponível em: < https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html >. Acesso em: 30 de outubro de 2019.

TIMBERG, Craig. NSA slide shows surveillance of undersea cables. **The Washington Post**, Washington, 10 de jun. de 2013. Disponível em: <https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html>. Acesso em: 30 de out. de 2019.

TIMBERG, Craig; SOLTANI, Askan. By cracking cellphone code, NSA has ability to decode private conversations. **The Washington Post**, Washington, 04 de dez. de 2013. Disponível em: <https://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-

has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html>. Acesso em: 30 de out. de 2019.

TRÉGUER, Félix. Intelligence Reform and the Snowden Paradox: The Case of France. **Media And Communication**, [s.l.], v. 5, n. 1, p.17-28, 22 mar. 2017. Cogitatio. http://dx.doi.org/10.17645/mac.v5i1.821.

UNITED STATES OF AMERICA (USA). **Preparing for the Future of Artificial Intelligence**. 2016a

USA. **The National Artificial Intelligence Research and Development Strategic Plan.** 2016b

USA. **AI, China, Russia, and the Global Order:** Technological, Political, Global and Creative Perspectives. 2018

VELGHE, Pieter. "Reading China". **China Perspectives**, [s.l.], v. 2019, n. 1, p.85-89, 20 mar. 2019. OpenEdition. http://dx.doi.org/10.4000/chinaperspectives.8874.

VERIZON forced to hand over telephone data – full court rulling. **The Guardian**, Londres, 6 de jun. de 2013. Disponível em: <https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order>. Acesso em: 30 de out. de 2019.

VLADECK, Stephen I.. Big Data Before and After Snowden. **Journal Of National Security Law & Policy**, [s.l.], v. 7, n. 2, p.333-339, maio 2014.

WAGNER, Flávio Rech; CANABARRO, Diego Rafael. A Governança da Internet: Definição, Desafios e Perspectivas. In: PIMENTA, Marcelo Soares; CANABARRO, Diego Rafael. **Governança Digital.** Porto Alegre: Editora da Ufrgs, 2014. p. 191 - 209

WILKINSON, T. M.. Nudging and Manipulation. **Political Studies**, [s.l.], v. 61, n. 2, p.341-355, 7 set. 2012. SAGE Publications. http://dx.doi.org/10.1111/j.1467-9248.2012.00974.x.

WILTON, Robin. After Snowden – the evolving landscape of privacy and technology. **Journal Of Information, Communication And Ethics In Society**, [s.l.], v. 15, n. 3, p.328-335, 14 ago. 2017. Emerald. http://dx.doi.org/10.1108/jices-02-2017-0010.

XIE, Lingjun. Who Moved My data? Information Privacy Concerns In the Big Data Era. **Proceedings Of The 4th International Symposium On Social Science (isss 2018)**, [s.l.], p.306-310, 2018. Atlantis Press. http://dx.doi.org/10.2991/isss-18.2018.61.

XKEYSCORE presentation from 2008 – read in full**. The Guardian**, Londres, 31 de jul. de 2013. Disponível em: < https://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation>. Acesso em: 30 de out. de 2019.

ZANOON, Nabeel; AL-HAJ, Abdulah; KHWALDEH, Sufian M. Cloud Computing and Big Data is there a Relation between the Two:: A Study. **International Journal Of Applied Engineering Research.** [s. L.], p. 6970-6982. set. 2017.

ZUBOFF, Shoshana. Big other: Surveillance Capitalism and the Prospects of an Information Civilization. **Journal Of Information Technology**, [s.l.], v. 30, n. 1, p.75-89, mar. 2015. SAGE Publications. http://dx.doi.org/10.1057/jit.2015.5.